Parere 32/2021 relativo al progetto di decisione di esecuzione della Commissione europea a norma del regolamento (UE) 2016/679 sull'adeguata protezione dei dati personali nella Repubblica di Corea

Versione 1.0

Adottato il 24 settembre 2021

Translations proofread by EDPB Members.
This language version has not yet been proofread.

INDICE

Il comitato europeo per la protezione dei dati

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

visto l'accordo sullo Spazio economico europeo («**SEE**»), in particolare l'allegato XI e il protocollo 37 dello stesso, modificato dalla decisione del Comitato misto SEE n. 154/2018, del 6 luglio 2018 ([1]),

visti gli articoli 12 e 22 del proprio regolamento interno,

HA ADOTTATO IL SEGUENTE PARERE:

1. SINTESI

1. Il 16 giugno 2021 la Commissione europea ha avviato la procedura formale per l'adozione del proprio progetto di decisione di esecuzione («**progetto di decisione**») sull'adeguata protezione dei dati personali nella Repubblica di Corea a norma della legge sulla protezione dei dati personali (Personal Information Protection Act, PIPA) ai sensi del RGPD ([2]).

2. Lo stesso giorno la Commissione europea ha chiesto il parere del comitato europeo per la protezione dei dati («**EDPB**») ([3]). La valutazione dell'EDPB sull'adeguatezza del livello di protezione riconosciuto nella Repubblica di Corea è stata effettuata sulla base dell'esame del progetto di decisione stesso nonché dell'analisi della documentazione messa a disposizione ([4])dalla Commissione europea.

3. L'EDPB si è concentrato sulla valutazione sia degli aspetti generali legati al RGPD del progetto di decisione, sia dell'accesso da parte delle autorità pubbliche ai dati personali trasferiti dal SEE a fini di applicazione della legge e di sicurezza nazionale, compresi i mezzi di ricorso a disposizione delle persone nel SEE. L'EDPB ha inoltre valutato se le garanzie previste dal quadro giuridico coreano siano in atto ed efficaci.

4. Per tale lavoro l'EDPB si è basato principalmente sui i criteri di riferimento per l'adeguatezza ai sensi del RGPD ([5]) («**criteri di riferimento per l'adeguatezza ai sensi del RGPD**») adottati nel febbraio 2018 e sulle raccomandazioni 2/2020 dell'EDPB relative alle garanzie essenziali europee per le misure di sorveglianza ([6]).

1.1. Aree di convergenza

5. L'obiettivo principale dell'EDPB è fornire un parere alla Commissione europea circa l'adeguatezza del livello di protezione riconosciuto alle persone i cui dati personali siano trasferiti alla Repubblica di

([1]) Nel presente parere, con il termine «**Stati membri**» si intendono gli «Stati membri del SEE».
([2]) Cfr. il comunicato stampa https://ec.europa.eu/commission/presscorner/detail/en/ip_21_2964.
([3]) Ibidem.
([4]) L'EDPB ha basato la propria analisi su traduzioni ufficiali preparate dal governo coreano.
([5]) WP 254, criteri di riferimento per l'adeguatezza ai sensi del RGPD, 6 febbraio 2018 (approvato dall'EDPB, cfr. https://edpb.europa.eu/our-work-tools/general-guidance/endorsed-wp29-guidelines).
([6]) Cfr. raccomandazioni 2/2020 dell'EDPB relative alle garanzie essenziali europee per le misure di sorveglianza, adottate il 10 novembre 2020, https://edpb.europa.eu/our-work-tools/our-documents/preporki/recommendations-022020-european-essential-guarantees_en.

Corea. È importante rilevare che l'EDPB non si aspetta che il quadro giuridico coreano in materia di protezione dei dati riproduca la normativa europea sulla protezione dei dati.

6. Tuttavia, l'EDPB ricorda che, affinché il livello di protezione di un paese terzo sia considerato adeguato, l'articolo 45 del RGPD e la giurisprudenza della Corte di giustizia dell'Unione europea («**CGUE**») richiedono che la legislazione di tale paese terzo sia in linea con la sostanza dei principi fondamentali sanciti nel RGPD. In tale contesto, il quadro coreano sulla protezione dei dati presenta numerose somiglianze con il quadro europeo sulla protezione dei dati, essendo costituito da un atto legislativo principale, riguardante sia il settore pubblico sia quello privato, integrato da atti legislativi settoriali specifici.

7. Per quanto concerne il contenuto, l'EDPB rileva l'allineamento di aree chiave del quadro del RGPD e del quadro coreano sulla protezione dei dati circa alcune disposizioni fondamentali quali, ad esempio, le nozioni (ad esempio «dati personali», «trattamento», «interessato»); i criteri di liceità e correttezza del trattamento per finalità legittime; la limitazione della finalità; la qualità e la proporzionalità dei dati; la conservazione dei dati, la sicurezza e la riservatezza; la trasparenza; e le categorie particolari di dati.

8. In aggiunta a quanto precede, l'EDPB accoglie con favore gli sforzi compiuti dalla Commissione europea e dalle autorità coreane per assicurare che la Repubblica di Corea fornisca un livello di protezione adeguato a quello del RGPD attraverso l'adozione di notifiche da parte dell'autorità di controllo coreana (applicabili non solo ai dati personali trasferiti dal SEE alla Corea) allo scopo di colmare le lacune tra il RGPD e il quadro coreano sulla protezione dei dati. In questo contesto, l'EDPB desidera sottolineare la rilevanza di tali notifiche ai fini della valutazione dell'adeguatezza della Repubblica di Corea osservando, ad esempio, che le notifiche forniscono chiarimenti pertinenti su alcune importanti garanzie, tra l'altro in relazione all'ambito di applicazione delle esenzioni dal PIPA per quanto riguarda il trattamento dei dati personali pseudonimizzati a fini scientifici, statistici e di ricerca, i trasferimenti successivi e le norme applicabili nel contesto dell'accesso ai dati da parte delle autorità pubbliche.

1.2. Sfide

9. Se da un lato l'EDPB ha identificato molti aspetti del quadro coreano sulla protezione dei dati come sostanzialmente equivalenti al quadro europeo sulla protezione dei dati, dall'altro ha anche concluso che per alcune questioni potrebbero essere necessari chiarimenti e un'analisi più approfondita. In particolare, l'EDPB ritiene che, al fine di assicurare un livello di protezione sostanzialmente equivalente, dovrebbero essere ulteriormente valutati i seguenti aspetti, che la Commissione europea dovrebbe sottoporre a un attento monitoraggio.

1.2.1. Aspetti generali

10. L'EDPB prende atto che la notifica n. 2021-1 *ha lo status di una norma amministrativa con valore giuridicamente vincolante per il titolare del trattamento dei dati personali, nel senso che qualsiasi violazione della notifica può essere considerata come una violazione delle disposizioni pertinenti del PIPA* ([7]). Tuttavia, considerando che la notifica non include norme aggiuntive di per sé, ma piuttosto chiarimenti su come il testo normativo del PIPA dovrebbe intendersi come applicabile e alla luce della sua importanza complessiva, in particolare per quanto riguarda le disposizioni di pseudonimizzazione ai sensi del PIPA, che l'EDPB comprende siano oggetto di procedimenti giudiziari in corso, l'EDPB invita la Commissione europea a fornire ulteriori informazioni sulla natura vincolante, l'applicabilità e la validità della notifica n. 2021-1 e raccomanda un attento monitoraggio del suo rispetto nella pratica, in particolare per ciò che concerne la sua applicazione non solo da parte dell'autorità di controllo

([7]) Cfr. il punto I dell'allegato I del progetto di decisione.

coreana, ma anche da parte dei tribunali, soprattutto quando il livello equivalente di protezione offerto dal quadro giuridico coreano si basa sui chiarimenti ivi previsti.

1.2.2. Aspetti generali relativi alla protezione dei dati

11. In relazione all'ambito di applicazione della decisione di adeguatezza, l'EDPB nota che riguarderà i trasferimenti dal quadro giuridico del SEE ai «titolari del trattamento dei dati personali» pubblici e privati che rientrano nell'ambito di applicazione del PIPA. L'EDPB comprende che i soggetti che agiscono come responsabili del trattamento ai sensi del RGPD sono inclusi in questo termine; tuttavia, al fine di evitare malintesi, invita la Commissione europea a chiarire ulteriormente che la decisione di adeguatezza riguarderà anche i trasferimenti a «responsabili del trattamento» in Corea.

12. Un aspetto importante su cui l'EDPB vorrebbe richiamare l'attenzione riguarda la nozione di informazioni pseudonimizzate nel quadro coreano sulla protezione dei dati. Il diritto coreano prevede che le esenzioni da una serie di disposizioni pertinenti, comprese quelle sui diritti individuali degli interessati e sulla conservazione dei dati, si applichino al trattamento dei dati personali pseudonimizzati. Secondo la Commissione europea, ciò avviene soltanto quando i dati personali pseudonimizzati sono trattati a fini statistici, di ricerca scientifica o di archiviazione nell'interesse pubblico. Tuttavia, questa affermazione è principalmente supportata dalla notifica n. 2021-1 che rende particolarmente pertinente, in questo contesto, la già menzionata necessità di informazioni aggiuntive circa la natura vincolante, l'applicabilità e la validità della notifica, nonché del monitoraggio di questi aspetti. Inoltre, l'EDPB invita la Commissione europea a valutare ulteriormente l'impatto della pseudonimizzazione nell'ambito del diritto coreano e, soprattutto, il modo in cui essa possa influire sui diritti e sulle libertà fondamentali degli interessati i cui dati personali sono trasferiti alla Repubblica di Corea ai sensi della decisione di adeguatezza. In particolare, l'EDPB sollecita la Commissione europea a valutare ulteriormente le deroghe contenute nell'articolo 28, paragrafo 7, PIPA e nell'articolo 40, paragrafo 3, CIA e a monitorare attentamente la loro applicazione e la giurisprudenza pertinente allo scopo di assicurare che i diritti degli interessati non siano indebitamente limitati quando i dati personali trasferiti ai sensi della decisione di adeguatezza sono trattati per queste finalità.

13. L'EDPB rileva inoltre che l'ordinamento coreano prevede il diritto di revocare il consenso solo in circostanze specifiche ed invita pertanto la Commissione europea a valutare ulteriormente l'impatto dell'assenza di un diritto generale di revocare il consenso e a fornire ulteriori garanzie in modo da assicurare che un livello essenziale di protezione dei dati sia garantito in ogni momento anche, se del caso, chiarendo il ruolo del diritto alla sospensione ai sensi del PIPA in assenza di un diritto generale di revocare il consenso.

14. Per quanto riguarda i trasferimenti successivi, l'EDPB riconosce che il consenso informato dell'interessato sarà generalmente utilizzato come base per i trasferimenti di dati da un titolare del trattamento dei dati personali con sede in Corea a un destinatario con sede in un paese terzo e che la notifica n. 2021-1 prevede che le persone debbano essere informate sul paese terzo al quale saranno forniti i loro dati. Tuttavia, l'EDPB invita la Commissione europea a garantire che le informazioni da fornire all'interessato comprendano anche informazioni sui possibili rischi associati ai trasferimenti dovuti all'assenza di protezione nonché di garanzie adeguate nel paese terzo. Inoltre, l'EDPB accoglierebbe con favore l'inclusione, nella decisione di adeguatezza, di rassicurazioni che i dati personali non saranno trasferiti dai titolari del trattamento dei dati personali coreani a un paese terzo in qualsiasi situazione in cui ai sensi del RGPD non possa essere fornito un consenso valido, ad esempio a causa di uno squilibrio di potere.

15. Per quanto riguarda la nomina dei membri dell'autorità di controllo coreana, anche se la procedura formale sarebbe in linea con il RGPD e supererebbe pertanto il test di equivalenza con il quadro giuridico del SEE, l'EDPB accoglierebbe con favore un monitoraggio, da parte della Commissione

europea, di qualsiasi sviluppo suscettibile di influenzare l'indipendenza dei membri dell'autorità di controllo sudcoreana.

16. Per quanto concerne il bilancio, sempre sulla base delle informazioni fornite dalla Commissione europea, non viene fatto alcun riferimento alle specificità del personale assegnato alla Commissione per la protezione dei dati personali (Personal Information Protection Commission, PIPC) né alle risorse finanziarie messe a sua disposizione. L'EDPB accoglierebbe quindi con favore informazioni aggiuntive su questi due argomenti pertinenti nel progetto di decisione.

1.2.3. Sull'accesso da parte delle autorità pubbliche a dati trasferiti alla Repubblica di Corea

17. L'EDPB ha inoltre analizzato il quadro giuridico coreano per quanto riguarda l'accesso del governo ai dati personali trasferiti dal SEE alla Corea a fini di applicazione della legge e di sicurezza nazionale. Pur riconoscendo le dichiarazioni e le assicurazioni fornite dal governo coreano, come indicato nell'allegato II del progetto di decisione, l'EDPB ha individuato una serie di aspetti che richiedono chiarimenti o suscitano preoccupazioni.

18. L'EDPB nota che le disposizioni del PIPA si applicano senza limitazioni nell'ambito dell'applicazione della legge. L'EDPB osserva inoltre che il trattamento dei dati nell'ambito della sicurezza nazionale è soggetto a un insieme più limitato di disposizioni contenute nel PIPA.

19. Per quanto riguarda la comunicazione volontaria di dati personali da parte dei fornitori di telecomunicazioni alle autorità di sicurezza nazionale, l'EDPB teme che la relazione tra il punto 3 dell'allegato I del progetto di decisione, che specifica che i fornitori in linea di principio devono notificare la persona interessata quando soddisfano volontariamente una richiesta, e l'articolo 58, paragrafo 1, punto 2, PIPA, ossia l'esenzione parziale a fini di sicurezza nazionale, non sia chiara. Ciò potrebbe rendere inefficaci i requisiti in materia di informazione, rendendo notevolmente più difficile per gli interessati far valere i loro diritti in materia di protezione dei dati, soprattutto per quanto riguarda il ricorso giurisdizionale.

20. Anche se ciò non è affermato esplicitamente nel progetto di decisione, l'EDPB comprende dalle spiegazioni fornite dalla Commissione europea che il quadro giuridico coreano non consente l'intercettazione massiva di dati di telecomunicazione. Pertanto, la recente giurisprudenza della Corte europea dei diritti dell'uomo («**CEDU**») sui regimi di intercettazione massiva non sarebbe direttamente pertinente ai fini della valutazione del livello di protezione dei dati in Corea.

21. Il progetto di decisione non contiene alcuna informazione sul quadro giuridico per i trasferimenti successivi nell'ambito della sicurezza nazionale. Pur comprendendo che, secondo la Commissione europea, i trasferimenti successivi a fini di sicurezza nazionale sono sufficientemente disciplinati dalle garanzie generali e dai principi derivanti dal quadro costituzionale e dal PIPA, l'EDPB si chiede se ciò possa essere considerato conforme ai requisiti di precisione e chiarezza del diritto e se contenga garanzie efficaci e applicabili. Le garanzie cui la Commissione europea fa riferimento sono di natura molto generale e non affrontano, in una base giuridica, le circostanze e le condizioni specifiche in cui i trasferimenti successivi a fini di sicurezza nazionale possono avere luogo. In tale contesto, l'EDPB osserva inoltre che la Commissione europea non ha preso in considerazione l'esistenza di accordi internazionali conclusi tra la Repubblica di Corea e paesi terzi od organizzazioni internazionali che possono prevedere disposizioni specifiche per il trasferimento internazionale di dati personali da parte dei servizi preposti all'applicazione della legge e/o di intelligence a paesi terzi. L'EDPB ritiene che la conclusione di accordi bilaterali o multilaterali con paesi terzi ai fini dell'applicazione della legge o della cooperazione in materia di intelligence possa incidere sul quadro giuridico coreano sulla protezione dei dati, come valutato.

22. L'EDPB nota che il controllo dell'applicazione del diritto penale nonché delle autorità di sicurezza nazionale è garantito da un insieme di organismi diversi interni ed esterni, in particolare la PIPC, che è dotata di sufficienti poteri esecutivi.

23. Affinché i mezzi di ricorso siano effettivi, gli interessati devono potersi rivolgere a un organismo competente che soddisfi i requisiti dell'articolo 47 della Carta dei diritti fondamentali dell'Unione europea («**la Carta**»), che sia cioè competente nel determinare se un trattamento di dati ha luogo e nel verificare la liceità del trattamento, e che, in caso di trattamento illecito, sia in grado di esercitare poteri correttivi. In questo contesto, l'EDPB chiede alla Commissione europea di chiarire se un reclamo alla PIPC o qualsiasi azione dinanzi a un tribunale sia soggetta a requisiti sostanziali e/o procedurali, come l'onere della prova, e se le persone nel SEE siano in grado di soddisfare tale condizione preliminare.

1.3. Conclusione

24. L'EDPB ritiene che la presente decisione di adeguatezza sia di fondamentale importanza anche in considerazione del fatto che – con le eccezioni evidenziate nel parere – riguarderà i trasferimenti sia nel settore pubblico sia in quello privato.

25. L'EDPB accoglie con favore gli sforzi compiuti dalla Commissione europea e dalle autorità coreane per allineare il quadro giuridico coreano a quello europeo. I miglioramenti che si intendono apportare con la notifica n. 2021-1 per colmare alcune delle divergenze tra i due quadri sono molto importanti e sono stati accolti favorevolmente. Tuttavia, l'EDPB osserva che permangono alcune preoccupazioni, anche riguardo alla notifica n. 2021-1, che si aggiungono alla necessità di ulteriori chiarimenti in merito ad altre questioni, e raccomanda alla Commissione europea di rispondere alle preoccupazioni e alle richieste di chiarimento espresse dall'EDPB e di fornire ulteriori informazioni e spiegazioni circa le questioni sollevate nel presente parere.

2. INTRODUZIONE

2.1. Quadro coreano in materia di protezione dei dati

26. Il principale atto legislativo che disciplina la protezione dei dati nella Repubblica di Corea è l'atto sulla protezione dei dati personali (atto legislativo n. 10465, del 29 marzo 2011, modificato da ultimo dall'atto legislativo n. 16930, del 4 febbraio 2020, Personal Information Protection Act, «**PIPA**»). Esso è integrato da un decreto di applicazione (decreto presidenziale n. 23169, del 29 settembre 2011, modificato da ultimo dal decreto presidenziale n. 30892, del 4 agosto 2020, «decreto di applicazione del PIPA»), che è giuridicamente vincolante e applicabile.

27. Oltre al PIPA, il quadro coreano sulla protezione dei dati comprende «notifiche» normative emesse dall'autorità di controllo coreana, la Commissione per la protezione dei dati personali (Personal Information Protection Commission, «**PIPC**»), che forniscono ulteriori norme sull'interpretazione e l'applicazione del PIPA. Recentemente, la PIPC ha adottato la notifica n. 2021-1 del 21 gennaio 2021 (che ha modificato la precedente notifica n. 2020-10 del 1º settembre 2020, di seguito «**notifica n. 2021-1**») sull'interpretazione, l'applicazione e l'attuazione di alcune disposizioni del PIPA. Più specificamente, questa notifica è il risultato delle discussioni sull'adeguatezza tenute dalle autorità coreane e dalla Commissione europea. Essa contiene chiarimenti sull'applicazione di specifiche disposizioni del PIPA, anche per quanto riguarda il trattamento dei dati personali trasferiti alla Corea sulla base della decisione di adeguatezza prevista ([8]) e *ha lo status di una norma amministrativa*

([8]) Cfr. il punto I dell'allegato I del progetto di decisione.

giuridicamente vincolante per il titolare del trattamento dei dati personali, nel senso che qualsiasi violazione della notifica può essere considerata una violazione delle pertinenti disposizioni del PIPA ([9]). In questo contesto, l'EDPB desidera rilevare che, pur essendo indicata tra le «norme integrative» nel progetto di decisione, la notifica non contiene norme aggiuntive di per sé, ma piuttosto spiegazioni volte a chiarire come il testo normativo del PIPA dovrebbe intendersi come applicabile, in particolare per quanto riguarda i dati trasferiti dal SEE. Alla luce di quanto detto, l'EDPB raccomanda un attento monitoraggio del rispetto della notifica n. 2021-1 nella pratica, in particolare per quanto riguarda la sua applicazione non solo da parte della PIPC ma anche dei tribunali, soprattutto quando il livello di protezione equivalente offerto dal quadro giuridico coreano si basa sui chiarimenti contenuti nella notifica n. 2021-1.

28. Nel quadro legislativo coreano vi sono altre leggi pertinenti in materia di protezione dei dati che stabiliscono norme per il trattamento dei dati personali in specifici settori industriali, quali:

- l'atto legislativo sull'utilizzo e la protezione delle informazioni relative al credito (Act on the Use and Protection of Credit Information, «**CIA**») e il relativo decreto di applicazione («**decreto di applicazione del CIA**»), che stabiliscono norme specifiche applicabili agli operatori commerciali e alle entità specializzate (come agenzie di rating del credito ed istituti finanziari) che trattano informazioni personali relative al credito necessarie per determinare l'affidabilità creditizia delle parti in operazioni finanziarie o commerciali;
- L'atto legislativo sulla promozione dell'utilizzo delle reti di informazione e comunicazione e sulla protezione dei dati (Act on the Promotion of Information and Communications Network Utilisation and Data Protection, «**atto legislativo sulle reti**»); e
- l'atto legislativo sulla protezione della privacy nelle comunicazioni (Communications Privacy Protection Act, «**CPPA**»).

29. Nell'ambito dell'accesso da parte del governo, oltre alle disposizioni pertinenti contenute nel PIPA e nel CPPA, l'EDPB ha considerato altri atti legislativi, ossia il codice di procedura penale (Criminal Procedure Act, «**CPA**»), l'atto sulle attività di telecomunicazione (Telecommunications Business Act, «**TBA**»), l'atto sulla segnalazione e l'utilizzo di informazioni specifiche sulle operazioni finanziarie (Act on Reporting and Using Specified Financial Transaction Information, «**ARUSFTI**») e l'atto sui servizi di intelligence nazionali (National Intelligence Service Act, «**NISA**»).

2.2. Ambito di applicazione della valutazione dell'EDPB

30. Il progetto di decisione della Commissione europea è il risultato di una valutazione del quadro coreano sulla protezione dei dati, seguita da discussioni con il governo coreano. Ai sensi dell'articolo 70, paragrafo 1, lettera s), RGPD, l'EDPB dovrebbe fornire un parere indipendente sui risultati della Commissione europea, individuare eventuali carenze nel quadro giuridico in materia di adeguatezza e adoperarsi per presentare proposte che affrontano tali carenze.

31. Per evitare ripetizioni e allo scopo di contribuire alla valutazione del quadro giuridico coreano, l'EDPB ha deciso di concentrarsi su alcuni punti specifici presentati nel progetto di decisione e di fornire la propria analisi e il proprio parere al riguardo, astenendosi dal riprodurre la maggior parte delle constatazioni e valutazioni fattuali laddove l'EDPB non ha alcuna indicazione per presumere che il diritto della Repubblica di Corea non sia sostanzialmente equivalente al diritto del SEE. Inoltre, in linea con la giurisprudenza della CGUE, una parte molto importante dell'analisi riguarda il regime giuridico dell'accesso per finalità di sicurezza nazionale ai dati personali trasferiti alla Repubblica di Corea e della pratica del suo apparato di sicurezza nazionale.

([9]) Ibidem.

32. Nella sua valutazione, l'EDPB ha tenuto conto del quadro europeo applicabile in materia di protezione dei dati, compresi gli articoli 7, 8 e 47 della Carta, che tutelano rispettivamente il diritto alla vita privata e familiare, il diritto alla protezione dei dati di carattere personale e il diritto a un ricorso effettivo e a un giudice imparziale, nonché l'articolo 8 della Convenzione europea dei diritti dell'uomo che tutela il diritto alla vita privata e familiare. Oltre a quanto sopra, l'EDPB ha preso in considerazione i requisiti del RGPD nonché la giurisprudenza pertinente.

33. L'obiettivo di questo esercizio è fornire alla Commissione europea un parere sulla valutazione dell'adeguatezza del livello di protezione nella Repubblica di Corea. La nozione di «livello di protezione adeguato», che era già presente nella direttiva 95/46, è stato ulteriormente sviluppato dalla CGUE. È importante ricordare il principio stabilito dalla CGUE nella sentenza Schrems I, secondo cui il «livello di protezione» nel paese terzo deve essere «sostanzialmente equivalente» a quello garantito nell'UE, ma «*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'Unione*» ([10]). Pertanto, l'obiettivo non è riprodurre punto per punto la legislazione europea, bensì stabilire i requisiti sostanziali – di base – della normativa in esame. L'adeguatezza può essere conseguita attraverso una combinazione di diritti degli interessati e obblighi in capo a chi effettua il trattamento dei dati personali o esercita il controllo sul trattamento, e controllo da parte di organismi indipendenti. Le norme in materia di protezione dei dati, tuttavia, sono efficaci solo se hanno forza esecutiva e sono rispettate nella pratica. È pertanto necessario considerare non soltanto 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. La presenza di meccanismi di applicazione efficienti è di fondamentale importanza per garantire l'efficacia delle norme sulla protezione dei dati ([11]).

2.3. Osservazioni di carattere generale e preoccupazioni

2.3.1. Impegni internazionali assunti dalla Repubblica di Corea

34. A norma dell'articolo 45, paragrafo 2, lettera c), RGPD e dei criteri di riferimento per l'adeguatezza ai sensi del RGPD ([12]), nel valutare l'adeguatezza del livello di protezione di un paese terzo, la Commissione europea prende in considerazione, fra l'altro, gli impegni internazionali assunti dal paese terzo o altri obblighi derivanti dalla partecipazione del paese terzo a sistemi multilaterali o regionali, in particolare in relazione alla protezione dei dati personali nonché l'attuazione di tali obblighi.

35. La Corea è parte di diversi accordi internazionali che garantiscono il diritto alla privacy, come il Patto internazionale relativo ai diritti civili e politici (articolo 17), la Convenzione sui diritti delle persone con disabilità (articolo 22) e la Convenzione sui diritti dell'infanzia e dell'adolescenza (articolo 16). Inoltre, la Corea, come membro dell'OCSE, aderisce al quadro per la sfera privata (Privacy Framework) dell'OCSE, in particolare alle linee guida che disciplinano la protezione della sfera privata e i flussi transfrontalieri di dati personali.

36. L'EDPB prende nota inoltre della partecipazione della Corea come Stato osservatore ai lavori del comitato consultivo della Convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati di carattere personale del Consiglio d'Europa, sebbene non abbia ancora deciso se aderirvi.

([10]) C-362/14, *Maximilian Schrems contro Data Protection Commissioner*, 6 ottobre 2015, ECLI:EU:C:2015:650, punti 73-74.
([11]) WP 254, pag. 2.
([12]) WP 254, pag. 2.

2.3.2. Ambito di applicazione della decisione di adeguatezza

37. Secondo il considerando 5 del progetto di decisione, la Commissione europea è giunta alla conclusione che la Repubblica di Corea garantisce un livello di protezione adeguato per i dati personali trasferiti da un titolare o da un responsabile del trattamento nell'Unione ai titolari del trattamento dei dati personali (ad esempio, persone fisiche o giuridiche, organizzazioni, istituzioni pubbliche) che rientrano nell'ambito di applicazione del PIPA, fatta eccezione per il trattamento dei dati personali per attività missionarie da parte di organizzazioni religiose e per la nomina di candidati da parte di partiti politici ([13]) o per il trattamento di informazioni personali relative al credito ai sensi del CIA da parte di titolari del trattamento che sono soggetti al controllo della Commissione per i servizi finanziari.

38. L'EDPB nota che la decisione sull'adeguatezza riguarderà i trasferimenti dal quadro giuridico del SEE ai «titolari del trattamento dei dati personali» sia pubblici sia privati che rientrano nell'ambito di applicazione del PIPA. L'EDPB comprende che le entità che agiscono come responsabili del trattamento ai sensi del RGPD rientrano anche nella definizione di «titolare del trattamento dei dati personali», considerando che il PIPA si applicherà analogamente ad essi e che sono previsti obblighi specifici quando un titolare del trattamento dei dati personali (il «committente») coinvolge un terzo per il trattamento dei dati personali (il «fornitore»); tuttavia, al fine di evitare malintesi, l'EDPB invita la Commissione europea a chiarire meglio che la decisione di adeguatezza riguarderà anche i trasferimenti a «responsabili del trattamento» in Corea e che il livello di protezione dei dati personali trasferiti dal SEE non sarà compromesso anche in questi casi.

39. Inoltre, tenendo conto del fatto che la decisione di adeguatezza riguarda anche i trasferimenti di dati personali tra organismi pubblici, l'EDPB comprende che ciò riguarderà anche i trasferimenti tra autorità di controllo della protezione dei dati e, a fini di chiarezza, invita la Commissione europea ad affrontare specificamente tale questione.

40. Oltre a ciò, per quanto riguarda le entità escluse dall'ambito di applicazione della decisione di adeguatezza, l'EDPB desidera sottolineare che tale decisione potrebbe trarre vantaggio da una più chiara identificazione delle «organizzazioni commerciali» che sono soggette al controllo della PIPC (articolo 45, paragrafo 3, CIA) cosicché i titolari e i responsabili del trattamento con sede nel SEE possano facilmente valutare se l'importatore rientra anche nell'ambito di applicazione della decisione di adeguatezza prima di trasferire i dati a entità che rientrano nell'ambito di applicazione del CIA o, almeno, essere consapevoli della necessità di valutare questo aspetto.

41. Per quanto riguarda l'ambito di applicazione della decisione di adeguatezza, l'EDPB ha compreso dalle spiegazioni aggiuntive della Commissione europea che anche l'Unità di informazione finanziaria della Corea (Korea Financial Intelligence Unit, «**KOFIU**»), che è istituita nell'ambito della Commissione per i servizi finanziari e supervisiona la prevenzione del riciclaggio di denaro e del finanziamento del terrorismo ai sensi dell'ARUSFTI ([14]), non rientra nell'ambito di applicazione, in quanto la sua giurisdizione è limitata agli istituti finanziari che non rientrano a loro volta nel progetto di decisione. Tuttavia, l'articolo 1, paragrafo 2, lettera c), del progetto di decisione esclude dal proprio ambito di applicazione solo i titolari del trattamento dei dati personali che sono soggetti al controllo della Commissione per i servizi finanziari e che trattano informazioni personali relative al credito ai sensi del CIA. In questo contesto, l'EDPB chiede alla Commissione europea di chiarire se la KOFIU e le sue attività di trattamento dei dati rientrano nel progetto di decisione.

([13]) Per maggiore contesto si veda più avanti la sezione 3.1.2 del presente parere.
([14]) Cfr. l'allegato II, punto 2.2.3.1.

3. ASPETTI GENERALI RELATIVI ALLA PROTEZIONE DEI DATI

3.1. Principi di contenuto

42. Il capitolo 3 dei criteri di riferimento per l'adeguatezza ai sensi del RGPD è dedicato ai «principi di contenuto». Il sistema di un paese terzo deve comprendere tali principi affinché il livello di protezione fornito sia considerato sostanzialmente equivalente a quello garantito dalla legislazione dell'UE.

43. Pur non essendo espressamente sancito dalla Costituzione coreana di per sé, il diritto alla protezione dei dati personali è riconosciuto come fondamentale, derivato dai diritti costituzionali alla dignità umana e alla ricerca della felicità (articolo 10), alla vita privata (articolo 17) e alla riservatezza delle comunicazioni (articolo 18). Ciò è stato confermato sia dalla Corte suprema sia dalla Corte costituzionale, come indicato nel progetto di decisione della Commissione europea ([15]). L'EDPB prende nota di questo riconoscimento poiché ne deriva che la protezione dei dati come diritto fondamentale, a norma dell'articolo 37 della Costituzione coreana, «*può essere limitata soltanto dalla legge e qualora sia necessario per motivi di sicurezza nazionale o per il mantenimento dell'ordine pubblico o per il benessere pubblico*» e che «*anche quando tali limitazioni sono imposte, non possono intaccare l'essenza della libertà o del diritto*».

44. Secondo la Commissione europea ([16]), la Corte costituzionale ha stabilito che anche i cittadini stranieri sono titolari dei diritti fondamentali. In base alle dichiarazioni ufficiali del governo coreano ([17]), anche se la giurisprudenza finora non ha trattato specificamente il diritto alla privacy dei cittadini non coreani, è ampiamente accettato tra gli studiosi che gli articoli da 12 a 22 della Costituzione definiscono «diritti degli esseri umani». Inoltre, la Repubblica di Corea ha emanato una serie di leggi nell'ambito della protezione dei dati che forniscono garanzie per tutte le persone, indipendentemente dalla loro nazionalità, come il PIPA. A questo proposito, l'EDPB osserva che l'articolo 6, paragrafo 2, della Costituzione prevede che lo status dei cittadini stranieri sia garantito come prescritto dal diritto e dai trattati internazionali e prende atto della giurisprudenza citata nel progetto di decisione secondo cui uno «straniero» può essere titolare di «diritti fondamentali». Data la pertinenza del riconoscimento del diritto alla protezione dei dati riconosciuto ai «cittadini stranieri», l'EDPB richiama l'attenzione della Commissione europea sulla necessità di continuare a monitorare la giurisprudenza relativa alla protezione dei dati come un diritto fondamentale riconosciuto non soltanto ai cittadini coreani ma a tutti gli interessati, in modo da assicurare che il livello di protezione delle persone fisiche garantito dal RGPD non sia compromesso quando i dati personali sono trasferiti alla Corea a norma della decisione di adeguatezza.

3.1.1. Nozioni

45. Ai sensi dei criteri di riferimento per l'adeguatezza ai sensi del RGPD, nel quadro giuridico del paese terzo dovrebbero essere presenti nozioni e/o principi basilari in materia di protezione dei dati. Pur non dovendo necessariamente riprendere la terminologia del RGPD, tali nozioni e principi dovrebbero rispecchiare le nozioni racchiuse nel diritto europeo in materia di protezione dei dati ed essere coerenti con esse. A titolo esemplificativo, il RGPD contiene le seguenti nozioni fondamentali: «dati personali», «trattamento di dati personali», «titolare del trattamento», «responsabile del trattamento», «destinatario» e «dati sensibili» ([18]).

([15]) Cfr. il considerando 8 del progetto di decisione e la giurisprudenza pertinente (le cui sintesi sono disponibili soltanto in lingua inglese) citata nella nota a piè pagina 10 del progetto di decisione.
([16]) Cfr. il considerando 9 del progetto di decisione.
([17]) Cfr. il punto 1.1 dell'allegato II del progetto di decisione.
([18]) WP 254, pag. 4.

46. Il PIPA contiene una serie di definizioni, tra cui quelle di «dati personali», «trattamento» e «interessato», molto simili ai termini corrispondenti del RGPD.

3.1.1.1. *Nozione di dati pseudonimizzati*

47. Tra le definizioni contenute nel PIPA, l'articolo 2, paragrafo 1, PIPA definisce, in particolare, i dati personali come una qualsiasi delle seguenti informazioni relative a una persona vivente: a) informazioni che identificano una persona specifica attraverso il nome completo, il numero di registrazione residente, l'immagine ecc. e b) informazioni che, pur non identificando di per sé una persona specifica, possono essere facilmente combinate con altre informazioni per identificarla. Per la seconda tipologia di informazioni, la facilità di combinazione è determinata considerando ragionevolmente il tempo, il costo, la tecnologia ecc. impiegati per identificare la persona, come ad esempio la probabilità che si possano ottenere le altre informazioni.

48. Inoltre, a norma dell'articolo 2, paragrafo 1, lettera c), PIPA, anche le «informazioni pseudonimizzate» sono considerate dati personali. Per informazioni pseudonimizzate si intendono le informazioni di cui ai punti a) o b) sopra che sono pseudonimizzate in conformità del comma 1-2 e non consentono quindi di identificare una persona specifica senza l'utilizzo o la combinazione di informazioni per il ripristino dello stato originale. Le informazioni che sono completamente rese anonime sono escluse dall'ambito di applicazione del PIPA. A norma dell'articolo 58, paragrafo 2, PIPA, l'atto non si applica alle informazioni che non identificano più una determinata persona se combinate con altre informazioni, considerando ragionevolmente il tempo, i costi, la tecnologia ecc.

49. La Commissione europea afferma nel considerando 17 del suo progetto di decisione che ciò corrisponde all'ambito di applicazione materiale del RGPD e alle sue nozioni di «dati personali», «pseudonimizzazione» e «informazioni rese anonime».

50. Tuttavia, a norma dell'articolo 28, paragrafo 7, PIPA gli articoli 20, 21, 27, l'articolo 34, paragrafo 1, gli articoli da 35 a 37, l'articolo 39, paragrafi 3 e 4, e l'articolo 39, paragrafi da 6 a 8, non si applicano ai dati personali pseudonimizzati.

51. Nel suo progetto di decisione, la Commissione europea afferma che l'articolo 28, paragrafo 7, PIPA è applicabile ai dati personali pseudonimizzati solo quando sono trattati a fini statistici, di ricerca scientifica o di archiviazione nell'interesse pubblico ([19]). Tuttavia, ciò non deriva direttamente dalla lettera della legge, ma dalle spiegazioni fornite nella notifica n. 2021-1 ([20]). Pur riconoscendo che, sulla base della struttura e della logica del PIPA, si possa sostenere che l'articolo 28, paragrafo 2, PIPA debba essere inteso e logicamente interpretato come applicabile anche all'articolo 28, paragrafo 7, PIPA, alla luce dell'importanza della notifica n. 2021-1 nella valutazione della Commissione europea dell'adeguatezza del livello di protezione dei dati personali nella Repubblica di Corea e per evitare qualsiasi dubbio, l'EDPB invita la Commissione europea a fornire ulteriori informazioni sulla natura vincolante, l'applicabilità e la validità della notifica n. 2021-1 e a monitorarne l'applicazione in questo contesto specifico.

52. In questo contesto, l'EDPB desidera ricordare che ai sensi del RGPD la pseudonimizzazione è intesa come una misura di sicurezza raccomandata. In altre parole, a norma del RGPD i dati pseudonimizzati rimangono dati personali ai quali si applica pienamente il RGPD. Sulla base di quanto precede, l'EDPB teme che il livello di protezione dei dati personali pseudonimizzati a norma del RGPD possa essere compromesso quando i dati personali sono trasferiti alla Corea. L'EDPB invita quindi la Commissione europea a valutare ulteriormente l'impatto della pseudonimizzazione ai sensi del PIPA e, soprattutto, il modo in cui essa possa influire sui diritti e le libertà fondamentali degli interessati i cui dati personali

([19]) Cfr., tra l'altro, il considerando 82 del progetto di decisione.
([20]) Punto 4 dell'allegato I del progetto di decisione.

sarebbero trasferiti alla Repubblica di Corea sulla base della decisione di adeguatezza. Pertanto, l'EDPB invita la Commissione europea a fornire garanzie che il livello di protezione dei dati personali ottenuti dagli interessati nel SEE non diminuirà in seguito al trasferimento verso la Repubblica di Corea anche quando i dati personali trasferiti sono pseudonimizzati.

3.1.1.2. *Nozione di titolare del trattamento dei dati personali*

53. L'articolo 2, paragrafo 5, PIPA contiene una definizione di «titolare del trattamento dei dati personali» che indica un'istituzione pubblica, una persona giuridica, un'organizzazione o una persona fisica ecc. che tratta dati personali direttamente o indirettamente per gestire archivi di dati personali «*come parte delle proprie attività*». Tuttavia, nelle garanzie aggiuntive di cui alla notifica n. 2021-1, il termine titolare del trattamento dei dati personali è definito come un'istituzione pubblica, una persona giuridica, un'organizzazione, una persona fisica ecc. che tratta dati personali direttamente o indirettamente per gestire archivi di dati personali «*a fini commerciali*». D'altra parte, la nota a piè pagina 272 del progetto di decisione afferma quanto segue circa la nozione di titolare del trattamento dei dati personali: «*Come definito nell'articolo 2, PIPA, ossia un'istituzione pubblica, una persona giuridica, un'organizzazione, una persona fisica ecc. che tratta dati personali direttamente o indirettamente per gestire archivi di dati personali "a fini ufficiali o commerciali"*».

54. L'EDPB riconosce che queste incongruenze possono essere dovute alle traduzioni del testo originale fornite dalle autorità coreane e invita la Commissione europea a verificare regolarmente la qualità e la sicurezza delle traduzioni. Tuttavia, l'EDPB sottolinea il fatto che, per poter valutare la sostanziale equivalenza del livello di protezione dei dati del quadro giuridico coreano, è necessaria una chiara comprensione delle finalità del trattamento che rientrano nell'ambito di applicazione materiale del PIPA. Inoltre, in questo contesto, l'EDPB osserva che il PIPA non usa la stessa terminologia del RGPD in relazione alla nozione di «titolare del trattamento» e «responsabile del trattamento» e invita la Commissione europea a chiarire la corretta definizione e l'ambito di applicazione della nozione di «titolare del trattamento dei dati personali» e a verificare specificamente se questo termine riguardi anche i responsabili del trattamento ai sensi del RGPD, poiché ciò influisce direttamente sull'ambito di applicazione della decisione di adeguatezza ([21]).

3.1.2. Esenzioni parziali previste dal PIPA

55. L'articolo 58, paragrafo 1, PIPA esclude l'applicazione di parti del PIPA (ossia gli articoli da 15 a 57) con riguardo a quattro categorie di trattamento dei dati personali, come descritto di seguito. In particolare, le esenzioni riguardano le disposizioni del PIPA concernenti i motivi specifici del trattamento, alcuni obblighi in materia di protezione dei dati, le norme dettagliate per l'esercizio dei diritti individuali nonché le norme che disciplinano la risoluzione delle controversie. Tuttavia, l'EDPB prende atto che alcune disposizioni generali del PIPA rimangono ancora applicabili, ad esempio quelle relative ai principi di protezione dei dati (articolo 3 del PIPA) e ai diritti individuali (articolo 4 del PIPA). Inoltre, l'articolo 58, paragrafo 4, PIPA stabilisce obblighi specifici per queste quattro categorie di trattamento dei dati.

56. In primo luogo, l'esenzione parziale riguarda i dati personali raccolti ai sensi della legge sulle statistiche per il trattamento da parte delle istituzioni pubbliche. La Commissione europea afferma nel considerando 27 del suo progetto di decisione che, in base ai chiarimenti ricevuti dal governo coreano, i dati personali trattati in questo contesto riguardano normalmente i cittadini coreani e potrebbero solo eccezionalmente includere informazioni sugli stranieri, in particolare nel caso di statistiche sull'entrata e uscita dal territorio o relative agli investimenti stranieri. Secondo il progetto di decisione, tuttavia, anche in queste situazioni tali dati non sono generalmente trasferiti da titolari/responsabili

([21]) Cfr. anche il precedente punto 38.

del trattamento nel SEE, ma sarebbero piuttosto raccolti direttamente dalle autorità pubbliche in Corea.

57. L'EDPB prende atto del ragionamento della Commissione europea sull'eccezionalità dell'applicazione della legge sulle statistiche al trattamento dei dati personali trasferiti ai sensi della decisione di adeguatezza; tuttavia, accoglierebbe con favore ulteriori informazioni e rassicurazioni sulle garanzie specifiche che sarebbero applicate nel caso in cui i dati personali trasferiti dal SEE siano ulteriormente raccolti ai sensi della legge sulle statistiche per il trattamento da parte delle istituzioni pubbliche, in particolare per quanto riguarda l'esercizio dei diritti individuali degli interessati in linea con l'articolo 89, paragrafo 2, RGPD nella misura in cui tali diritti non rischino di rendere impossibile o di pregiudicare gravemente il conseguimento delle finalità specifiche e tali deroghe non siano necessarie al conseguimento di dette finalità.

58. In questa prospettiva, l'applicazione dell'articolo 4, PIPA anche a questo tipo di trattamento sembra fornire rassicurazioni; nondimeno, l'EDPB gradirebbe ulteriori informazioni e chiarimenti nella decisione di adeguatezza sugli obblighi specifici imposti, in conformità dell'articolo 58, paragrafo 4, PIPA, a tali attività di trattamento, in particolare per quanto riguarda la minimizzazione dei dati, la conservazione limitata dei dati, le misure di sicurezza e il trattamento dei reclami.

59. In secondo luogo, l'esenzione parziale riguarda i dati personali raccolti o richiesti per l'analisi di informazioni relative alla sicurezza nazionale. L'EDPB è consapevole del fatto che nelle questioni di sicurezza nazionale gli Stati hanno un ampio margine di apprezzamento riconosciuto dalla CEDU. L'EDPB nota anche che, a norma dell'articolo 37, paragrafo 2, della Costituzione coreana, qualsiasi limitazione alle libertà e ai diritti, ad esempio qualora sia necessaria per la protezione della sicurezza nazionale, non può violare l'aspetto sostanziale della libertà o del diritto in questione. Inoltre, l'EDPB prende atto delle garanzie nella sezione 6 della notifica n. 2021-1 per quanto riguarda il trattamento dei dati personali a fini di sicurezza nazionale, comprese le indagini sulle violazioni e l'applicazione della legge. Tuttavia, nel presente contesto, l'EDPB invita la Commissione europea a chiarire ulteriormente l'ambito di applicazione delle esenzioni e si chiede se tutte le esenzioni previste dall'articolo 58, paragrafo 1, punto 2, PIPA (capitoli da III a VII) siano pertinenti per il lavoro dei servizi di intelligence e se garantiscano l'equivalenza con i principi di necessità e proporzionalità. In particolare, l'EDPB invita la Commissione europea a fornire maggiori chiarimenti riguardo alle circostanze in cui un servizio di intelligence potrebbe invocare le esenzioni. L'EDPB ritiene necessario monitorare da vicino l'impatto di queste limitazioni nella pratica, in particolare durante l'esercizio effettivo e l'applicazione dei diritti degli interessati.

60. In terzo luogo, l'esenzione parziale si applica ai «*dati personali trattati temporaneamente quando ciò è urgentemente necessario per la sicurezza pubblica, la sanità pubblica, ecc.*». In base al considerando 29 del progetto di decisione della Commissione europea, questa categoria è interpretata rigorosamente dalla PIPC e si applica solo in casi di emergenza che richiedono un'azione urgente, ad esempio per rintracciare agenti infettivi o per salvare e aiutare le vittime di disastri naturali.

61. L'EDPB sottolinea inoltre che qualsiasi deroga al livello di protezione dei dati personali dovrebbe essere interpretata rigorosamente. Allo stesso tempo, l'EDPB nota che la disposizione non è definita rigorosamente e non fornisce un elenco esaustivo di esempi di situazioni in cui il trattamento dei dati personali potrebbe essere considerato «*urgentemente necessario*». A titolo esemplificativo, l'EDPB si chiede se anche i trasferimenti internazionali di dati sanitari durante la pandemia di COVID-19 in corso rientrerebbero nell'ambito di applicazione di questa esenzione. Alla luce di quanto detto, l'EDPB invita la Commissione europea a fornire ulteriori chiarimenti sull'ambito di applicazione di questa esenzione e a monitorarne pienamente l'applicazione e l'ambito di applicazione per garantire che non porti a un abbassamento del livello di protezione dei dati personali provenienti dal SEE dopo il trasferimento in Corea sulla base della decisione di adeguatezza.

62. Infine, l'esenzione parziale si applica ai dati personali raccolti o utilizzati a fini di informazione da parte della stampa, per attività missionarie da parte di organizzazioni religiose e per la nomina di candidati da parte di partiti politici ([22]). Per quanto riguarda il trattamento dei dati personali da parte della stampa per attività giornalistiche, la Commissione europea afferma nel considerando 31 del proprio progetto di decisione che l'equilibrio tra la libertà di espressione e altri diritti, compreso il diritto alla privacy, è definito dalla legge sull'arbitrato e i ricorsi ecc. per danni causati da notizie di stampa (di seguito «**legge sulla stampa**»), e presenta garanzie specifiche che derivano dalla legge citata. L'EDPB vorrebbe, tuttavia, invitare la Commissione europea a monitorare accuratamente questa esenzione e la giurisprudenza pertinente al fine di garantire che nel quadro giuridico coreano sia assicurato un livello equivalente di protezione dei dati anche nella pratica.

3.1.3. Criteri di liceità e correttezza del trattamento per fini legittimi

63. In linea con i criteri di riferimento per l'adeguatezza ai sensi del RGPD, e conformemente a quest'ultimo, i dati devono essere trattati in modo lecito, corretto e legittimo. 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, ad 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 sugli interessi della persona.

64. Seguendo una struttura simile a quella del RGPD, il PIPA introduce innanzitutto il principio di liceità, correttezza e trasparenza all'inizio (articolo 3, paragrafi 1 e 2, PIPA), stabilendo successivamente le norme specifiche per la sua applicazione (articoli da 15 a 19 del PIPA). In particolare, l'articolo 15 del PIPA riporta un catalogo di fondamenti giuridici sui quali i titolari del trattamento dei dati personali possono basare la raccolta di dati personali e utilizzarli nell'ambito di applicazione della finalità per cui è stata effettuata la raccolta. Detti fondamenti giuridici consistono in: 1) consenso informato dell'interessato; 2) autorizzazione per legge o necessità per l'adempimento di un obbligo giuridico; 3) necessità per l'esecuzione delle funzioni di un'istituzione pubblica; 4) necessità per l'esecuzione di un contratto concluso con un interessato; 5) necessità per la protezione degli interessi legati alla vita, al corpo o alla proprietà dell'interessato o di un terzo da un pericolo imminente (qualora non sia possibile ottenere il consenso preventivo); 6) necessità di perseguire un interesse giustificabile di un titolare del trattamento dei dati personali che ha la priorità su quello dell'interessato.

65. Inoltre, l'articolo 17 del PIPA elenca i fondamenti giuridici applicabili per la condivisione di dati personali con un terzo che comprendono: 1) il consenso informato dell'interessato; 2) l'autorizzazione per legge o la necessità per l'adempimento di un obbligo giuridico; 3) la necessità per l'esecuzione delle funzioni di un'istituzione pubblica; e 4) la necessità per la protezione degli interessi legati alla vita, al corpo o alla proprietà dell'interessato o di un terzo da un pericolo imminente (qualora non sia possibile ottenere il consenso preventivo). Anche in assenza del consenso dell'interessato, la condivisione dei dati personali è consentita se rientra nell'ambito di applicazione ragionevolmente connesso alle finalità per cui i dati personali sono stati inizialmente raccolti (articolo 17, paragrafo 4, PIPA).

66. L'articolo 18 del PIPA stabilisce norme specifiche per l'utilizzo e la condivisione di dati personali al di fuori dell'ambito di applicazione della finalità iniziale della raccolta o della comunicazione di detti dati. Tra l'altro, anche in questo caso il consenso fa parte di tali norme che forniscono l'autorizzazione.

([22]) Di conseguenza, il trattamento dei dati personali da parte di organizzazioni religiose per le loro attività missionarie e il trattamento dei dati personali da parte dei partiti politici nel contesto della nomina dei candidati sono anch'essi esclusi dall'ambito di applicazione della decisione di adeguatezza. Si veda anche il punto 37 sopra, nella sezione 2.3.2.

67. Pur riconoscendo la sostanziale somiglianza del diritto coreano con il RGPD per quanto riguarda il principio di liceità e l'esistenza di un diritto generale alla sospensione (articolo 37 del PIPA), che può essere invocato anche quando i dati personali sono trattati sulla base del consenso, l'EDPB desidera rilevare l'assenza di un diritto generale di revocare il consenso ai sensi del PIPA ([23]). Data l'importanza del consenso come fondamento giuridico in tutti gli scenari descritti precedentemente, e tenendo conto del ruolo dei diritti individuali in un ordinamento giuridico di protezione dei dati ai fini della salvaguardia dei diritti e delle libertà fondamentali degli interessati, l'EDPB invita la Commissione europea a valutare ulteriormente l'impatto dell'assenza di un diritto generale di revocare il consenso ai sensi dell'ordinamento coreano e a fornire ulteriori rassicurazioni per far sì che un livello sostanziale di protezione dei dati come quello previsto dal RGPD sia garantito in ogni momento anche, se del caso, chiarendo il ruolo del diritto alla sospensione in questo contesto specifico.

3.1.4. Principio della finalità limitata

68. I criteri di riferimento per l'adeguatezza ai sensi del RGPD, conformemente a quest'ultimo, stabiliscono che i dati personali siano trattati per una finalità specifica e successivamente utilizzati soltanto nella misura in cui non vi sia incompatibilità con la finalità del trattamento.

69. Ai sensi dell'articolo 3, paragrafi 1 e 2, PIPA i titolari del trattamento dei dati personali specificano ed esplicitano le finalità del trattamento e garantiscono che il trattamento sia compatibile con tali finalità. Se questo principio è confermato in altre disposizioni (ossia l'articolo 15, paragrafo 1, l'articolo 18, paragrafo 1, e l'articolo 19, paragrafo 1, PIPA), il trattamento per finalità «ragionevolmente connesse» è consentito in determinate circostanze (cfr. l'articolo 17, paragrafo 4, PIPA) ([24]) così come l'utilizzo e la fornitura di dati personali al di fuori della finalità (cfr. gli articoli 18 e 19, PIPA) ([25]).

70. L'EDPB comprende che in caso di trasferimenti di dati personali dal SEE alla Repubblica di Corea sulla base della decisione di adeguatezza, la finalità della raccolta da parte dei titolari del trattamento con sede nel SEE costituisce la finalità per cui i dati sono trasferiti, applicabile al trattamento da parte del titolare del trattamento dei dati personali con sede in Corea che lo riceve. Un cambiamento di finalità da parte del titolare con sede in Corea sarebbe consentito solo come previsto dall'articolo 18, paragrafo 2, punti 1-3, PIPA, «*salvo che ciò non possa verosimilmente violare ingiustamente l'interesse di un interessato o di un terzo*» ([26]). Nel presente contesto, l'EDPB riconosce la dichiarazione della Commissione europea nel considerando 55 del progetto di decisione secondo la quale, quando i cambiamenti di finalità sono autorizzati dalla legge, tale legge deve rispettare il diritto fondamentale alla privacy e alla protezione dei dati. Tuttavia, l'EDPB osserva che non sono state fornite informazioni specifiche a sostegno di questa specifica affermazione, ad esempio non è stato fatto alcun riferimento all'articolo 37 della Costituzione (coreana). Pertanto, l'EDPB invita la Commissione europea a fornire ulteriori assicurazioni e garanzie nel progetto di decisione per far sì che qualsiasi normativa che

([23]) Anche se gli interessati possono rifiutare il consenso in determinate circostanze, cfr. ad esempio l'articolo 18, paragrafo 3, punto 5, PIPA. Al contrario, il diritto di revocare il consenso sembra esistere solo in casi specifici; ai sensi dell'articolo 27, paragrafo 1, punto 2, PIPA gli interessati hanno il diritto di revocare il consenso se non desiderano che i loro dati personali siano trasferiti a un terzo a causa del trasferimento parziale o totale delle attività del titolare del trattamento dei dati personali, di una fusione ecc.; ai sensi dell'articolo 39, paragrafo 7, PIPA gli utenti possono revocare il consenso alla raccolta, all'utilizzo e alla comunicazione di dati personali in qualsiasi momento da parte del fornitore di servizi di informazione e comunicazione ecc.; inoltre, ai sensi dell'articolo 37 del CIA un interessato può revocare il consenso alla comunicazione delle proprie informazioni personali relative al credito che era stato precedentemente concesso a un fornitore/utente di informazioni di credito.

([24]) Per cui la compatibilità della finalità deve essere accertata in anticipo sulla base dei criteri di cui all'articolo 14-2 del decreto di applicazione del PIPA.

([25]) Cfr. anche il precedente punto 66.

([26]) Articolo 18, paragrafo 2, PIPA.

autorizzi un cambiamento di finalità del trattamento sia tenuta a rispettare i diritti e le libertà fondamentali degli interessati in materia di privacy e protezione dei dati.

3.1.5. Principio della qualità e della proporzionalità

71. Nei criteri di riferimento per l'adeguatezza ai sensi del RGPD si afferma che i dati dovrebbero essere precisi e aggiornati laddove necessario, nonché adeguati, pertinenti e non eccedenti rispetto alle finalità per le quali sono trattati.

72. Ai sensi del PIPA, i titolari del trattamento dei dati personali devono garantire che i dati personali siano accurati, completi e aggiornati nella misura necessaria rispetto alle finalità per le quali sono trattati (articolo 3, paragrafo 3, PIPA). I titolari del trattamento dei dati personali sono tenuti a raccogliere il minor numero di dati personali necessario al conseguimento di un determinato scopo e sono soggetti all'onere della prova nel merito (articolo 16, paragrafo 1, PIPA).

73. In questo contesto, l'EDPB condivide la valutazione della Commissione europea relativamente all'equivalenza sostanziale del livello di protezione ai sensi del PIPA rispetto al RGPD a tale riguardo.

3.1.6. Principio della conservazione dei dati

74. Secondo i criteri di riferimento per l'adeguatezza ai sensi del RGPD, di norma i dati dovrebbero essere conservati per un arco di tempo non superiore a quello necessario per il conseguimento delle finalità per le quali sono trattati. Come da articolo 21, paragrafo 1, PIPA, questo principio esiste anche nel diritto coreano. A norma del PIPA, i titolari del trattamento dei dati personali sono tenuti a distruggere i dati personali senza indugio qualora tali dati personali non siano più necessari alla scadenza del periodo di conservazione o al conseguimento della finalità prevista dal trattamento, salvo che non si applichino periodi di conservazione imposti dalla legge.

75. L'EDPB tuttavia nutre alcune preoccupazioni per il fatto che l'articolo 21, paragrafo 1, PIPA non è applicabile ai dati personali pseudonimizzati. L'EDPB prende atto del fatto che, in conformità della sezione 4, punto iii), della notifica n. 2021-1, «*laddove un titolare del trattamento dei dati personali sia incaricato del trattamento di dati pseudonimizzati a fini di elaborazioni di statistiche, ricerca scientifica, conservazione di registri pubblici ecc. e qualora i dati pseudonimizzati non siano stati distrutti una volta conseguita la finalità specifica del trattamento, in conformità dell'articolo 37 della Costituzione e dell'articolo 3 (Principi per la protezione dei dati personali) dell'atto, il titolare rende anonimi i dati al fine di garantire che questi, da soli o in combinazione con altri dati, non identifichino più una persona specifica, tenendo ragionevolmente conto del tempo, dei costi, della tecnologia ecc., conformemente all'articolo 58, paragrafo 2, PIPA*». Data, anche in questo caso, l'importanza della notifica n. 2021-1 e al fine di avere la certezza del diritto sull'equivalenza del livello di protezione dei dati personali trasferiti alla Repubblica di Corea ai sensi della decisione di adeguatezza, l'EDPB rinnova l'invito alla Commissione europea a fornire ulteriori informazioni volte a chiarire specificamente in che modo la notifica n. 2021-1 è resa vincolante e in che modo sono garantite l'applicabilità e la validità di detta notifica ([27]).

3.1.7. Principio della sicurezza e della riservatezza

76. Come descritto nei criteri di riferimento per l'adeguatezza ai sensi del RGPD, il principio di sicurezza e riservatezza richiede che le entità incaricate del trattamento dei dati si assicurino che tali dati siano trattati in maniera da garantirne un'adeguata sicurezza, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla

([27]) Cfr. anche il precedente punto 51 nella sezione 3.1.1.1 del presente parere nonché il punto 52 per le preoccupazioni generali dell'EDPB circa l'impatto della pseudonimizzazione ai sensi del diritto coreano.

distruzione o dal danno accidentali. Il livello di sicurezza dovrebbe tenere in considerazione lo stato dell'arte e i relativi costi.

77. La Commissione europea ha individuato un principio simile relativo alla sicurezza dei dati nell'articolo 3, paragrafo 4, PIPA, che è ulteriormente specificato nell'articolo 29 del PIPA. Inoltre, le disposizioni sulla sicurezza dei dati si applicano quando il titolare del trattamento dei dati personali assume un «fornitore». La sicurezza del trattamento dei dati personali deve essere garantita attraverso garanzie tecniche e gestionali, che devono inoltre essere incluse nell'accordo vincolante sul trattamento dei dati (articolo 26 del PIPA e articolo 28 del decreto di applicazione del PIPA). Inoltre, il PIPA prevede obblighi specifici in caso di violazione dei dati, tra cui l'obbligo di notificare gli interessati dalla violazione e l'autorità di controllo se il numero di interessati supera la soglia applicabile (articolo 34 del PIPA in combinato disposto con l'articolo 39 del decreto presidenziale del PIPA), tranne quando i dati in questione sono dati personali pseudonimizzati trattati a fini statistici, di ricerca scientifica o di archiviazione nell'interesse pubblico (articolo 28, paragrafo 7, PIPA). Anche in questo caso ([28]), l'EDPB nutre preoccupazioni riguardo all'ampia portata delle esenzioni per le informazioni pseudonimizzate e rinnova alla Commissione europea l'invito a valutare ulteriormente questo aspetto al fine di accertare che un livello di protezione sostanzialmente equivalente sia previsto dal diritto coreano ([29]).

78. Ciononostante, in sintesi, l'EDPB è soddisfatto della valutazione e della conclusione della Commissione europea riguardo l'equivalenza sostanziale del diritto coreano rispetto al principio di sicurezza e riservatezza.

3.1.8. Principio di trasparenza

79. Ai sensi dell'articolo 5, paragrafo 1, lettera a), RGPD, la trasparenza è uno dei principi fondamentali del sistema di protezione di dati dell'UE. Il considerando 39 del RGPD definisce la funzione essenziale di tale principio affermando che «[d]*ovrebbero essere trasparenti per le persone fisiche le modalità con cui sono raccolti, utilizzati, consultati o altrimenti trattati dati personali che li riguardano nonché la misura in cui i dati personali sono o saranno trattati. (...) È opportuno che le persone fisiche siano sensibilizzate ai rischi, alle norme, alle garanzie e ai diritti relativi al trattamento dei dati personali, nonché alle modalità di esercizio dei loro diritti relativi a tale trattamento.*»

80. I criteri di riferimento per l'adeguatezza ai sensi del RGPD 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. Più nello specifico, si afferma che «[o]*gni persona dovrebbe essere informata in merito a tutti i principali elementi del trattamento dei dati personali che la riguardano in forma chiara, facilmente accessibile, concisa, trasparente e di facile comprensione. Tali informazioni dovrebbero includere la finalità del trattamento, l'identità del titolare del trattamento, i diritti di cui gode e altre informazioni, purché ciò sia necessario a garantire la correttezza. A determinate condizioni, sono ammesse alcune eccezioni a tale diritto di informazione, ad esempio per salvaguardare le indagini penali, la sicurezza nazionale, l'indipendenza della magistratura e dei procedimenti giudiziari o altri importanti obiettivi di interesse pubblico generale, come nel caso dell'articolo 23 del RGPD.*»

81. Analogamente al RGPD, il PIPA prevede un principio generale di trasparenza che impone ai titolari del trattamento dei dati personali di rendere pubblica la loro politica sulla privacy e altre questioni relative al trattamento dei dati personali (articolo 3, paragrafo 5, PIPA). Obblighi specifici di informazione si applicano quando i titolari del trattamento dei dati personali cercano di ottenere il consenso degli interessati per la raccolta e il trattamento dei dati personali (articolo 15, paragrafo 2, PIPA), per la condivisione delle informazioni personali con terzi (articolo 17, paragrafo 2, PIPA) e per il trattamento

([28]) Come già stabilito nei punti 51 e 52 precedenti e nella sezione 3.1.1.1 del presente parere.
([29]) Cfr. anche le sezioni 3.1.6 e 3.1.10 del presente parere.

al di fuori della finalità (articolo 18, paragrafo 3, PIPA). Va notato che questi obblighi di informazione si applicano anche, *mutatis mutandis*, al fornitore (articolo 26, paragrafo 7, PIPA).

82. L'EDPB riconosce e accoglie con favore le garanzie aggiuntive di cui alla sezione 3, punti i) e ii), della notifica n. 2021-1 ([30]) relative alle informazioni da fornire agli interessati quando i loro dati sono trasferiti da un'entità nel SEE, tenendo conto del fatto che, a norma dell'articolo 20, paragrafo 1, PIPA, quando i dati non sono stati ottenuti dall'interessato, gli interessati sono informati solo su richiesta, mentre un diritto generale di essere informati è riconosciuto solo ai sensi dell'articolo 20, paragrafo 2, PIPA quando determinati trattamenti superano le soglie stabilite dal decreto di applicazione del PIPA (articolo 15, paragrafo 2).

83. Nel complesso, l'EDPB constata che il livello di protezione ai sensi del diritto coreano per quanto riguarda il principio di trasparenza è sostanzialmente equivalente a quello previsto dal RGPD.

3.1.9. Categorie particolari di dati personali

84. Affinché il sistema di protezione dei dati di un paese terzo sia riconosciuto come idoneo a fornire un livello di protezione dei dati personali sostanzialmente equivalente a quello del RGPD, dovrebbero esistere garanzie specifiche quando sono coinvolte categorie speciali di dati personali ai sensi degli articoli 9 e 10 del RGPD.

85. A norma del PIPA, si applicano disposizioni specifiche al trattamento dei cosiddetti dati sensibili, che comprendono i dati personali che rivelano l'ideologia, le convinzioni, l'ammissione o il ritiro da un sindacato o da un partito politico, le opinioni politiche, la salute, la vita sessuale e altri dati personali che possono minacciare notevolmente la privacy di qualsiasi interessato nonché, con riferimento al decreto di applicazione del PIPA, le informazioni sul DNA acquisite da test genetici, i dati che costituiscono un precedente penale; i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona allo scopo di identificare in modo univoco tale persona; nonché i dati personali che rivelano l'origine razziale o etnica.

86. Analogamente al RGPD, la normativa coreana sulla protezione dei dati vieta il trattamento dei dati sensibili salvo che non si applichino specifiche esenzioni che consistono in 1) informare l'interessato e ottenere un consenso specifico e 2) disposizioni giuridiche che autorizzano il trattamento (articolo 23, paragrafo 2, PIPA).

87. Su questa base, l'EDPB in linea di principio concorda con la conclusione della Commissione europea circa l'equivalenza sostanziale del diritto coreano per quanto riguarda il trattamento di categorie speciali di dati personali. Tuttavia, l'EDPB desidera rilevare che non ha ricevuto il manuale del PIPA né i chiarimenti della PIPC per quanto riguarda l'interpretazione del termine «vita sessuale» come comprendente anche l'orientamento o le preferenze sessuali della persona, sono inclusi nella notifica n. 2021-1. L'EDPB chiede quindi alla Commissione europea di fornire queste informazioni per poterle valutare in modo indipendente. Inoltre, l'EDPB invita la Commissione europea a citare specificamente i documenti in cui si possono trovare le informazioni cui fa riferimento su questo argomento.

3.1.10. Diritti di accesso, rettifica, cancellazione e opposizione

88. Nel quadro giuridico coreano i diritti degli interessati sono riconosciuti nell'articolo 3, paragrafo 5, PIPA, a norma del quale il titolare del trattamento dei dati personali garantisce i diritti degli interessati elencati nell'articolo 4 del PIPA e ulteriormente specificati negli articoli da 35 a 37, nell'articolo 39 e nell'articolo 39, paragrafo 2, PIPA e, per quanto riguarda le «informazioni personali relative al credito» (ossia «informazioni sul credito, cioè informazioni necessarie per determinare l'affidabilità creditizia

([30]) Allegato I del progetto di decisione.

delle parti in operazioni finanziarie o commerciali» - cfr. il considerando 13 del progetto di decisione), negli articoli 37, 38, e nell'articolo 38, paragrafo 3, CIA.

89. L'EDPB nota che il diritto di accesso (e di rettifica e cancellazione che può essere esercitato da un «*interessato che ha avuto accesso ai propri dati personali ai sensi dell'articolo 35*» del PIPA) può essere limitato o negato «*quando l'accesso è vietato o limitato dalle leggi*», «*qualora l'accesso possa causare danni alla vita o all'organismo di un terzo, o una violazione ingiustificata della proprietà e di altri interessi di qualsiasi altra persona*» e inoltre, per le istituzioni pubbliche, qualora la concessione dell'accesso «*possa causare gravi difficoltà*» nello svolgimento di determinate funzioni, ulteriormente specificate nell'articolo 35, paragrafo 4, PIPA ([31]). Disposizioni simili sono contenute anche nell'articolo 37 del PIPA relativo al diritto di sospensione del trattamento dei dati personali.

90. L'articolo 23 del RGPD consente al diritto dell'Unione o degli Stati membri di limitare i diritti individuali qualora tale limitazione rispetti l'essenza dei diritti e delle libertà fondamentali e sia una misura necessaria e proporzionata in una società democratica e prevede tali limitazioni per salvaguardare, tra l'altro, la tutela dell'interessato o dei diritti e delle libertà altrui e «*una funzione di controllo, d'ispezione o di regolamentazione connessa, anche occasionalmente, all'esercizio di pubblici poteri nei casi di cui alle lettere da a), a e) e g)*» del medesimo articolo.

91. In questo contesto, l'EDPB accoglierebbe con favore rassicurazioni generali nel progetto di decisione circa la necessità che qualsiasi normativa o statuto che limiti i diritti degli interessati soddisfi i requisiti della Costituzione coreana secondo cui un diritto fondamentale può essere limitato solo se necessario per la sicurezza nazionale o il mantenimento dell'ordine pubblico per il benessere pubblico e che tale limitazione non possa incidere sull'essenza della libertà o del diritto in questione (articolo 37, paragrafo 2, della Costituzione coreana).

92. Inoltre, per quanto riguarda l'eccezione relativa a «*una violazione ingiustificata della proprietà o di altri interessi di qualsiasi altra persona*», l'EDPB riconosce che ciò «*implica che sarebbe necessario trovare un equilibrio tra i diritti e le libertà della persona sanciti dalla Costituzione, da un lato, e quelli di altre persone, dall'altro*» ([32]); tuttavia, inviterebbe la Commissione europea a monitorare pienamente l'applicazione di questa eccezione e la giurisprudenza pertinente al fine di assicurare che un livello equivalente di protezione dei diritti degli interessati sia garantito anche in pratica nel quadro giuridico coreano.

93. Allo stesso modo, l'EDPB accoglierebbe con favore un attento monitoraggio dell'applicazione dell'eccezione per gli organismi pubblici, in particolare per quanto riguarda i casi in cui la concessione dell'accesso sarebbe considerata causa di «*gravi difficoltà*» nell'esercizio delle loro funzioni, considerando che questa espressione sembra essere più ampia di quella utilizzata in altre disposizioni del PIPA, ad esempio nell'articolo 18, paragrafo 2, punto 5 ([33]), e dovrebbe essere interpretata in modo restrittivo al fine di evitare indebite limitazioni dei diritti degli interessati.

94. Inoltre, l'EDPB si chiede se le eccezioni in base alle quali le disposizioni relative alla trasparenza su richiesta (articolo 20 del PIPA) e ai diritti individuali (articoli da 35 a 37, PIPA) – così come le disposizioni simili relative ai requisiti per i fornitori di servizi di informazione e comunicazione (articolo 39, paragrafo 2, articolo 39, paragrafi da 6 a 8, PIPA) e quelle contenute nel CIA (cfr. le eccezioni previste dall'articolo 40, paragrafo 3, CIA) – non si applica alle informazioni pseudonimizzate quando queste

([31]) Le stesse condizioni ed eccezioni ai diritti di accesso e correzione previsti dal PIPA si applicano anche al diritto di accesso e correzione previsto dal CIA per le informazioni personali relative al credito (nota a piè pagina 135 del progetto di decisione).

([32]) Considerando 76 del progetto di decisione.

([33]) In relazione alle eccezioni relative alla limitazione all'utilizzo e alla fornitura di dati personali al di fuori della finalità, l'articolo 18, paragrafo 2, punto 5, PIPA si riferisce a situazioni in cui, per le istituzioni pubbliche, «*è impossibile*» eseguire i propri doveri.

sono trattate a fini statistici, di ricerca scientifica o di archiviazione nell'interesse pubblico (articolo 28, paragrafo 7, PIPA) siano in linea con le garanzie previste dal quadro giuridico europeo.

95. Queste disposizioni sembrano introdurre una deroga generale per questo tipo di trattamento, mentre il RGPD dispone che, quando i dati personali (compresi i dati personali pseudonimizzati) sono trattati a fini di ricerca scientifica o storica o a fini statistici, il diritto dell'Unione o degli Stati membri può prevedere deroghe ai diritti degli interessati ma solo «*nella misura in cui tali diritti rischiano di rendere impossibile o di pregiudicare gravemente il conseguimento delle finalità specifiche e tali deroghe sono necessarie al conseguimento di dette finalità*», essendo la pseudonimizzazione solo una delle misure tecniche e organizzative da adottare per garantire il rispetto del principio della minimizzazione dei dati (articolo 89, paragrafo 1, RGPD).

96. La Commissione europea ritiene che la deroga prevista dall'articolo 28, paragrafo 7, PIPA sia giustificata anche alla luce dell'articolo 28, paragrafo 5, PIPA che vieta espressamente al titolare del trattamento dei dati personali di trattare le informazioni pseudonimizzate allo scopo di identificare una persona specifica e fa riferimento all'approccio previsto dall'articolo 11, paragrafo 2, RGPD (in combinato disposto con il considerando 57, RGPD) per il trattamento che non richiede l'identificazione ([34]).

97. Di fatto, ai sensi dell'articolo 11 del RGPD, il titolare del trattamento non è obbligato a «*conservare, acquisire o trattare ulteriori informazioni per identificare l'interessato*» al solo fine di rispettare il RGPD se, per le finalità previste, può trattare dati personali che non richiedono o non richiedono più l'identificazione di un interessato; in tali casi, quando il titolare del trattamento può dimostrare che non è in grado di identificare l'interessato, i diritti degli interessati non si applicano. Come riconosciuto dalla Commissione europea ([35]), il RGPD richiede quindi, in tali casi, un'impossibilità «pratica» per il titolare del trattamento e, in conformità del principio di minimizzazione dei dati, riconosce che nessun dato aggiuntivo deve essere trattato «a causa» del RGPD.

98. Tuttavia, l'EDPB ritiene che questa situazione sia diversa da quella in cui un titolare del trattamento è in grado, in termini pratici, di identificare l'interessato ma non è autorizzato a farlo da una disposizione di legge come quella contenuta nell'articolo 28, paragrafo 5, PIPA. A questo proposito, l'EDPB accoglie con favore i chiarimenti forniti dalla PIPC nella notifica n. 2021-1 ([36]) che confermano che la sezione 3 del PIPA (compreso l'articolo 28, paragrafo 7) e l'eccezione contenuta nell'articolo 40, paragrafo 3, CIA si applicano solo in caso di trattamento di informazioni pseudonimizzate a fini di ricerca scientifica, a fini statistici o per l'archiviazione nell'interesse pubblico. Tuttavia, e in aggiunta alle preoccupazioni già espresse circa l'effettiva natura vincolante della notifica n. 2021-1 ([37]), l'EDPB continua a chiedersi se le deroghe previste dagli articoli 28, paragrafo 7, PIPA e 40, paragrafo 3, CIA possano essere considerate necessarie e proporzionate in una società democratica nella misura in cui limitano i diritti degli interessati in tutti i casi in cui le informazioni pseudonimizzate sono trattate per tali scopi, vale a dire anche quando il titolare del trattamento dei dati personali è in grado in termini pratici di identificare l'interessato e i diritti non rischiano di rendere impossibile o di pregiudicare gravemente il conseguimento delle finalità specifiche.

([34]) Occorre notare che lo stesso ragionamento non sarebbe applicabile in quanto tale all'eccezione prevista dall'articolo 40, paragrafo 3, CIA per il trattamento delle informazioni pseudonimizzate relative al credito, poiché l'articolo 40, paragrafi 2 e 6, prevede che «*una società di informazioni creditizie ecc. non tratta le informazioni pseudonimizzate in modo tale che una persona specifica possa essere identificata per fini di lucro o sleali*» e potrebbe quindi consentire la nuova identificazione per uno scopo leale come ad esempio soddisfare una richiesta dell'interessato.

([35]) Cfr. il considerando 82 del progetto di decisione.

([36]) Punto 4 dell'allegato I del progetto di decisione.

([37]) Cfr. la precedente sezione 3.1.1.1.

99. In particolare, l'EDPB teme che queste deroghe non siano giustificate e debbano essere ulteriormente esaminate soprattutto se applicate dal titolare del trattamento dei dati personali che pseudonimizza i dati «*a fini statistici, di ricerca scientifica e di archiviazione nel pubblico interesse ecc.*», conformemente all'articolo 28, paragrafo 2, PIPA «*senza il consenso degli interessati*» (e senza fornire le informazioni previste dall'articolo 20 del PIPA) ([38]), nella misura in cui detto titolare del trattamento conservi le informazioni che consentono la nuova identificazione. Ai sensi del RGPD le persone dovrebbero essere in grado di esercitare i propri diritti per quanto riguarda qualsiasi informazione che sia in grado di identificarle o individuarle, anche se le informazioni sono considerate «pseudonimizzate», salvo che non si applichi il già citato articolo 11 del RGPD. A questo proposito, l'EDPB osserva che solo quando questi dati vengono forniti a terzi per gli stessi fini statistici, di ricerca scientifica e di archiviazione, le informazioni che possono essere utilizzate per identificare una persona specifica non dovrebbero essere incluse e pertanto solo il titolare del trattamento dei dati personali cui vengono forniti dati pseudonimizzati a norma dell'articolo 28-2, paragrafo 2, PIPA probabilmente non sarebbe in grado «in termini pratici» di identificare l'interessato in mancanza di informazioni aggiuntive.

100. In sintesi, considerando che, come riconosciuto dalla Commissione europea, «*anziché fare affidamento sulla pseudonimizzazione come eventuale garanzia, il PIPA la impone come precondizione per svolgere determinate attività di trattamento a fini statistici, di ricerca scientifica e di archiviazione nel pubblico interesse (come ad esempio poter trattare i dati senza consenso o combinare diverse serie di dati)*» ([39]), ma prevede per tali casi importanti limitazioni ai diritti degli interessati, l'EDPB invita la Commissione europea a valutare ulteriormente le deroghe contenute nell'articolo 28, paragrafo 7, PIPA e nell'articolo 40, paragrafo 3, CIA e a monitorare attentamente la loro applicazione e la giurisprudenza pertinente ([40]) al fine di garantire che i diritti degli interessati non siano indebitamente limitati quando i dati personali trasferiti ai sensi della decisione di adeguatezza sono trattati per queste finalità, tenendo conto del fatto che, in molti casi, tali diritti aiutano anche il titolare del trattamento ad assicurare la qualità dei dati trattati.

3.1.11. Restrizioni ai trasferimenti successivi

101. I criteri di riferimento per l'adeguatezza ai sensi del RGPD chiariscono che il livello di tutela delle persone fisiche i cui dati sono trasferiti a norma di una decisione di adeguatezza non deve essere compromesso dal trasferimento successivo e pertanto ulteriori trasferimenti «*dovrebbero essere consentiti soltanto quando anche il secondo destinatario (ossia il destinatario del trasferimento successivo) è soggetto a norme (comprese le norme contrattuali) che assicurano un livello di protezione adeguato e prevedono il rispetto delle istruzioni pertinenti durante il trattamento dei dati per conto del titolare del trattamento*».

102. Per quanto riguarda i trasferimenti successivi ai fornitori (ossia i «responsabili del trattamento») stabiliti in altri paesi terzi, l'EDPB prende atto che il quadro giuridico coreano non dispone di norme specifiche per i casi di questo tipo e che, come considerato dalla Commissione europea ([41]), un titolare del trattamento dei dati personali coreano deve garantire il rispetto delle disposizioni del PIPA in

([38]) Cfr. l'articolo 28, paragrafo 7, PIPA, come spiegato nella notifica n. 2021-1, che afferma che determinate garanzie contenute nel PIPA, ossia «*gli articoli 20, 21, 27, l'articolo 34, paragrafo 1, gli articoli da 35 a 37, l'articolo 39, paragrafi 3 e 4, e l'articolo 39, paragrafi da 6 a 8*», non si applicano ai dati personali pseudonimizzati trattati a fini di elaborazioni di statistiche, ricerca scientifica, conservazione di registri pubblici ecc.
([39]) Considerando 42 del progetto di decisione.
([40]) Cfr., ad esempio, le sfide costituzionali di Open Net (informazioni disponibili all'indirizzo https://opennet.or.kr/19909, soltanto in lingua coreana).
([41]) Considerando 87 del progetto di decisione.

materia di esternalizzazione (articolo 26 del PIPA) mediante uno strumento giuridicamente vincolante e sarà responsabile dei dati personali che sono stati trasmessi al fornitore (articolo 26 del PIPA).

103. Per quanto riguarda i trasferimenti successivi a terzi (ossia altri titolari del trattamento dei dati personali), a norma dell'articolo 17, paragrafo 3, PIPA, un titolare del trattamento dei dati personali coreano deve informare gli interessati di eventuali trasferimenti all'estero, e ottenere il loro consenso a riguardo, e «*non stipula un contratto per il trasferimento transfrontaliero di dati personali in violazione del PIPA*». L'EDPB nota che quest'ultima disposizione garantirà, come osservato dalla Commissione europea ([42]), che nessun contratto per i trasferimenti transfrontalieri possa contenere obblighi che contraddicono i requisiti imposti dal PIPA al titolare del trattamento dei dati personali e potrebbe quindi essere considerata come una garanzia, se non fosse che non impone alcun obbligo di mettere in atto garanzie per assicurare che lo stesso livello di protezione offerto dal PIPA sarà fornito dal destinatario. Pertanto, l'EDPB riconosce che il consenso informato dell'interessato sarà generalmente utilizzato come base per i trasferimenti di dati da un titolare del trattamento di dati personali con sede in Corea a un destinatario con sede in un paese terzo.

104. A questo proposito, gli ulteriori chiarimenti forniti dalla PIPC nella notifica n. 2021-1 in merito all'obbligo di informare le persone sul paese terzo al quale saranno forniti i loro dati ([43]) sono accolti con favore in quanto ciò – come evidenziato dalla Commissione europea ([44]) – aiuterebbe gli interessati nel SEE a decidere con cognizione di causa se fornire o meno il consenso alla trasmissione in un paese terzo.

105. Tuttavia, come osservato anche nel parere 28/2018 relativo al progetto di decisione di esecuzione della Commissione europea sull'adeguata protezione dei dati personali in Giappone, è opportuno sottolineare che, ai sensi del RGPD, gli interessati devono essere esplicitamente informati, prima di prestare il consenso, circa i possibili rischi di tali trasferimenti derivanti dall'assenza di protezione e di garanzie adeguate nel paese terzo. Tale informazione dovrebbe indicare ad esempio che nel paese terzo potrebbero non esserci un'autorità di controllo e/o principi per il trattamento dei dati e/o diritti dell'interessato ([45]). Secondo l'EDPB, 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]). L'EDPB, pertanto, ha riserve riguardo alle conclusioni della Commissione europea nel progetto di decisione di adeguatezza rispetto a questa tipologia specifica di trasferimenti. Gli interessati solitamente non sono a conoscenza del quadro sulla protezione dei dati nei paesi terzi. Non si può quindi concludere che un interessato possa valutare il rischio di un trasferimento conoscendo soltanto il paese specifico di destinazione. Occorre piuttosto garantire un'informazione chiara sui rischi specifici di un tale trasferimento di dati personali verso un paese al di fuori del territorio della Repubblica di Corea prima del consenso dell'interessato.

106. L'EDPB invita pertanto la Commissione europea a verificare che le informazioni da fornire all'interessato circa «*le circostanze relative al trasferimento*» comprendano informazioni sui possibili rischi associati al trasferimento dovuti all'assenza di protezione adeguata nonché di garanzie adeguate nel paese terzo. Ciò è importante per l'EDPB al fine di valutare se i requisiti relativi al consenso siano sostanzialmente equivalenti a quelli del RGPD.

107. Inoltre, considerando che il consenso deve essere informato, specifico e inequivocabile, nonché espresso liberamente, l'EDPB accoglierebbe con favore rassicurazioni nella decisione di adeguatezza

([42]) Considerando 88 del progetto di decisione.
([43]) Ibidem.
([44]) Ibidem.
([45]) EDPB, Linee guida 2/2018 sulle deroghe di cui all'articolo 49 del regolamento 2016/679, 25 maggio 2018, pag. 8.
([46]) EDPB, Linee guida 2/2018 sulle deroghe di cui all'articolo 49 del regolamento 2016/679, 25 maggio 2018, pag. 7.

volte a specificare che i dati personali non saranno trasferiti dai titolari del trattamento dei dati personali coreani a un terzo, in un paese terzo, in qualsiasi situazione in cui ai sensi del RGPD non potrebbe essere fornito un consenso valido, ad esempio a causa di uno squilibrio di potere.

108. In relazione ai casi in cui il titolare del trattamento dei dati personali può fornire dati personali a un terzo in un paese terzo senza il consenso dell'interessato – ossia nel caso in cui 1) le informazioni personali siano fornite nell'ambito di applicazione ragionevolmente connesso alla finalità iniziale della raccolta, a norma dell'articolo 17, paragrafo 4, PIPA; e 2) le informazioni personali possano essere fornite a terzi nei casi eccezionali di cui all'articolo 18, paragrafo 2, PIPA – l'EDPB prende atto dei chiarimenti forniti dalla PIPC nella sezione 2 della notifica n. 2021-1 (e accoglie con favore il previsto obbligo imposto al titolare del trattamento con sede in Corea e al destinatario all'estero di garantire, attraverso uno strumento giuridicamente vincolante, come un contratto, un livello di protezione equivalente a quello del PIPA, anche per quanto riguarda i diritti degli interessati).

3.1.12. Marketing diretto

109. A norma dell'articolo 21, paragrafi 2 e 3, RGPD e dei criteri di riferimento per l'adeguatezza ai sensi del RGPD, l'interessato dovrebbe essere in grado, in qualsiasi momento e gratuitamente, di opporsi al trattamento dei dati personali per finalità di profilazione e marketing diretto.

110. Per quanto riguarda il diritto alla sospensione previsto dall'articolo 37 del PIPA, l'EDPB riconosce che la Commissione europea ritiene che questo diritto si applichi anche quando i dati sono utilizzati per finalità di marketing diretto ([47]). Tuttavia, l'EDPB gradirebbe ulteriori informazioni e chiarimenti nel progetto di decisione in relazione a questa valutazione e, in particolare, per quanto concerne l'applicazione pratica del diritto di sospensione nel contesto del marketing diretto (ad esempio, riferimenti alla giurisprudenza pertinente ecc.). A questo proposito, l'EDPB tiene inoltre a sottolineare che il diritto di un interessato di chiedere a un fornitore/utente di informazioni relative al credito di smettere di contattarlo allo scopo di proporre o sollecitare l'acquisto di beni o servizi è esplicitamente previsto dal CIA (articolo 37, paragrafo 2).

111. Inoltre, come riconosciuto dalla Commissione europea ([48]), nel quadro giuridico coreano tale trattamento richiede generalmente il consenso specifico (aggiuntivo) dell'interessato (cfr. l'articolo 15, paragrafo 1, punto 1, e l'articolo 17, paragrafo 2, punto 1, PIPA).

112. Dal momento che non si può escludere che i dati personali trasferiti dal SEE possano essere trattati in Corea per tali finalità, l'EDPB accoglierebbe con favore chiarimenti nella decisione di adeguatezza anche sull'esistenza del diritto di un interessato di revocare il consenso ([49]) e del diritto di ottenere che i suoi dati personali siano cancellati e non più trattati qualora il trattamento sia basato sul consenso (come nel caso di un trattamento effettuato per finalità di marketing) e l'interessato lo abbia revocato.

3.1.13. Processo decisionale automatizzato e profilazione

113. Come riconosciuto dalla Commissione europea nel suo progetto di decisione ([50]), il PIPA e il suo decreto di applicazione non contengono disposizioni generali che affrontino la questione delle decisioni riguardanti l'interessato e basate esclusivamente sul trattamento automatizzato dei dati

([47]) Considerando 79 del progetto di decisione.
([48]) Ibidem.
([49]) Cfr. anche il precedente punto 67: mentre la possibilità di revocare il consenso è chiaramente prevista dall'articolo 37, paragrafo 1, CIA, tale diritto è citato soltanto due volte nel PIPA in relazione a circostanze specifiche di cui all'articolo 27, paragrafo 1, punto 2 e all'articolo 39, paragrafo 7.
([50]) Cfr. il considerando 81 del progetto di decisione.

personali. Tuttavia, l'ordinamento giuridico coreano prevede tale diritto nel CIA, che contiene norme sulle decisioni automatizzate (articolo 36, paragrafo 2) anche se la loro applicazione sembra essere al di fuori dell'ambito di applicazione del controllo della PIPC (e, in quanto tale, al di fuori dell'ambito di applicazione del presente progetto di decisione – cfr. la precedente sezione 2.3.2 sull'ambito di applicazione del progetto di decisione).

114. Come già osservato dal Gruppo dell'articolo 29 per la tutela dei dati ([51]) nel suo parere 1/2016 sullo scudo per la privacy e dall'EDPB nel suo precedente parere sulla decisione di adeguatezza relativa al Giappone ([52]), la crescente importanza del processo decisionale automatizzato, della profilazione e dell'IA suggerirebbe di adottare un approccio più protettivo al riguardo. Contrariamente alle argomentazioni della Commissione europea ([53]) secondo cui è improbabile che l'assenza di norme specifiche sul processo decisionale automatizzato nel PIPA influisca sul livello di protezione per quanto riguarda i dati personali che sono stati raccolti nell'Unione (poiché qualsiasi decisione basata sul trattamento automatizzato è generalmente presa dal titolare del trattamento nell'Unione che ha una relazione diretta con l'interessato), l'EDPB ritiene che non sia possibile escludere che il processo decisionale automatizzato possa essere utilizzato da un titolare del trattamento dei dati personali con sede in Corea nel caso di dati trasferiti a norma della decisione di adeguatezza (ad esempio, nell'ambito dei rapporti di lavoro, per valutare il rendimento professionale, l'affidabilità, la condotta, ecc.).

115. Lo sviluppo di nuove tecnologie permette alle aziende di implementare più facilmente o considerare l'implementazione di sistemi decisionali automatizzati che potrebbero indebolire la posizione delle persone. Quando le decisioni prese esclusivamente da questi sistemi automatizzati producono effetti sulla situazione giuridica delle persone o incidono significativamente su di esse (ad esempio mediante l'inserimento in una lista nera che le priva dei loro diritti), è fondamentale prevedere le necessarie garanzie, compreso il diritto a essere informati sui motivi particolari sottesi alla decisione e sulla sua logica, a rettificare informazioni inaccurate o incomplete e a contestare la decisione qualora questa sia stata adottata sulla base di un fondamento di fatto errato ([54]).

116. In questo contesto, l'EDPB nutre perplessità circa l'assenza di disposizioni giuridiche sul processo decisionale automatizzato nel PIPA e invita quindi la Commissione europea ad affrontare questa questione e a continuare a monitorare lo sviluppo del quadro legislativo coreano a tale riguardo.

3.1.14. Responsabilizzazione

117. Il quadro giuridico coreano contiene diverse norme volte a garantire che i titolari del trattamento dei dati personali del trattamento mettano in atto misure tecniche e organizzative adeguate per soddisfare efficacemente i loro obblighi in materia di protezione dei dati e che siano in grado di dimostrare tale conformità, tra le altre cose, all'autorità di controllo competente. In particolare, l'EDPB apprezza l'esistenza di norme che prevedono l'adozione di un piano di gestione interno (articolo 29 del PIPA), dell'obbligo di effettuare una cosiddetta valutazione d'impatto sulla privacy (privacy impact assessment, «**PIA**») per i casi in cui il trattamento presenta un rischio più elevato di possibili violazioni della privacy (articolo 33, paragrafo 1, PIPA e articolo 35 del decreto di applicazione del PIPA), di norme sulla formazione e la supervisione del personale (articolo 28 del PIPA) nonché dell'obbligo di designare

([51]) Il Gruppo è stato istituito in virtù dell'articolo 29 della direttiva 95/46/CE, come un organo 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 l'EDPB.
([52]) 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.
([53]) Considerando 81 del progetto di decisione.
([54]) WP 254, pag. 7.

un responsabile della privacy (articolo 31 del PIPA in combinato disposto con l'articolo 32 del decreto di applicazione del PIPA).

118. L'EDPB condivide il punto di vista della Commissione europea per quanto riguarda la protezione sostanzialmente equivalente che tali norme assicurano – anche nei casi in cui le norme sembrano relativamente divergere da quelle previste dal RGPD, ad esempio non vi è alcuna disposizione che affermi la necessità che il responsabile della privacy sia indipendente, tuttavia è chiaramente stabilito che deve riferire alla direzione del titolare del trattamento dei dati personali (articolo 31, paragrafo 4, PIPA) e che non deve subire svantaggi ingiustificati come conseguenza dell'esercizio di tali funzioni (articolo 31, paragrafo 5, PIPA) – e suggerirebbe alla Commissione europea di monitorare, in sede di riesame della decisione di adeguatezza, l'applicazione pratica di tali disposizioni al fine di valutarne l'effettiva attuazione.

3.2. Meccanismi di procedura e applicazione

119. Sulla base dei criteri definiti nel documento sui criteri di riferimento per l'adeguatezza ai sensi del RGPD, l'EDPB ha analizzato i seguenti aspetti del quadro sulla protezione dei dati coreano, per come risultano dal progetto di decisione: 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 di un sistema di accesso a idonei meccanismi di ricorso che forniscano alle persone del SEE i mezzi per esercitare i propri diritti e per proporre ricorsi senza dover affrontare ostacoli di difficile superamento nella presentazione di ricorsi giurisdizionali e amministrativi.

120. Ai sensi del capo VI del RGPD e del capitolo 3 dei criteri di riferimento per l'adeguatezza ai sensi del RGPD devono esistere una o più autorità di controllo indipendenti, incaricate di monitorare, garantire e controllare il rispetto delle disposizioni in materia di protezione dei dati e di privacy in un paese terzo per assicurare un livello di protezione equivalente al SEE.

121. In questo contesto, l'autorità di controllo del paese terzo deve agire in piena indipendenza e imparzialità nell'adempimento dei suoi compiti e nell'esercizio dei suoi poteri senza richiedere né accettare istruzioni. Inoltre, l'autorità di controllo dovrebbe disporre di tutti i necessari poteri e incarichi disponibili per garantire la conformità ai diritti in materia di protezione dei dati e per sensibilizzare l'opinione pubblica al riguardo. Dovrebbero altresì essere presi in considerazione il personale e il bilancio dell'autorità di controllo. L'autorità di controllo dovrebbe essere in grado di avviare procedimenti di propria iniziativa.

3.2.1. Autorità di controllo competente indipendente

122. Nella Repubblica di Corea l'autorità indipendente incaricata di monitorare e far rispettare il PIPA è la PIPC, che è composta da un presidente, da un vicepresidente e da sette commissari. Il presidente e il vicepresidente della PIPC sono nominati dal Presidente della Repubblica di Corea su raccomandazione del Primo Ministro. Due dei commissari sono nominati su raccomandazione del presidente della PIPC, due su raccomandazione dei rappresentanti del partito politico cui appartiene il Presidente della Repubblica di Corea e i tre rimanenti su raccomandazione dei rappresentanti di altri partiti politici (articolo 7-2, paragrafo 2, PIPA). La PIPC è assistita da un segretariato (articolo 7, paragrafo 13) e può istituire sottocommissioni (composte da tre commissari) per gestire le violazioni minori e le questioni ricorrenti (articolo 7, paragrafo 12, PIPA).
123. In questo senso, l'EDPB riconosce che, malgrado la recente riorganizzazione che ne ha profondamente modificato lo status e i poteri, la PIPC ha compiuto notevoli sforzi per creare l'infrastruttura necessaria per l'attuazione del PIPA e delle sue modifiche più recenti. Tra questi sforzi si possono citare l'istituzione delle norme della PIPC, l'elaborazione di orientamenti volti a fornire indicazioni sull'interpretazione del PIPA e la creazione di una linea di assistenza per offrire consulenza agli operatori economici e alle persone sulle disposizioni in materia di protezione dei dati nonché un servizio di mediazione per gestire i reclami. In particolare, i compiti della PIPC includono la consulenza

in materia di normative e regolamenti relativi alla protezione dei dati, lo sviluppo di politiche e orientamenti sulla protezione dei dati, le indagini sulle violazioni dei diritti individuali, la gestione dei reclami e la mediazione delle controversie, il controllo della conformità alle norme del PIPA, la formazione e la promozione nell'ambito della protezione dei dati, lo scambio e la cooperazione con le autorità di paesi terzi incaricate della protezione dei dati ([55]).

124. La nomina e la composizione della PIPC sono stabilite dall'articolo 7, paragrafo 2, PIPA. Sebbene la PIPC rientri nella giurisdizione del Primo Ministro (e il presidente e il vicepresidente della PIPC siano nominati dal Presidente della Repubblica di Corea su raccomandazione del Primo Ministro), il quadro giuridico impone che i commissari svolgano le loro funzioni in modo indipendente, nel rispetto della legge e secondo la propria coscienza. L'EDPB riconosce le garanzie istituzionali e procedurali contenute nel PIPA e in particolare nell'articolo 7, paragrafi da 4 a 7. Tuttavia, l'EDPB gradirebbe che la Commissione europea monitorasse qualsiasi sviluppo suscettibile di influenzare l'indipendenza dei membri dell'autorità di controllo sudcoreana.

125. Inoltre, il progetto di decisione non comprende ancora un'analisi del bilancio della PIPC, comprese le fonti di finanziamento e la trasparenza del bilancio. L'EDPB ritiene che questo elemento, che è citato sia nell'articolo 56, paragrafo 1, RGPD sia nei principi e meccanismi di procedura e applicazione della protezione dei dati da considerare nell'ambito dei criteri di riferimento per l'adeguatezza ai sensi del RGPD quando si valuta il sistema di un paese o di un'organizzazione internazionale, debba essere preso in considerazione in modo approfondito, in quanto è un indicatore delle risorse economiche e umane a disposizione dell'autorità di controllo per lo svolgimento indipendente dei propri obblighi e compiti previsti per legge in materia di protezione dei dati, e consiglia pertanto alla Commissione europea di illustrarlo in modo più dettagliato nel progetto di decisione.

3.2.2. Esistenza di un sistema di protezione dei dati che garantisce un buon livello di conformità

126. In materia di applicazione, l'EDPB riconosce la gamma di poteri di esecuzione e sanzioni della PIPC come previsto dal PIPA e dal CIA e prende atto dei chiarimenti contenuti nella notifica n. 2021-1 secondo cui le condizioni di cui all'articolo 64, paragrafo 1, PIPA e all'articolo 45, paragrafo 4, CIA ([56]) saranno applicabili ogni volta che è violato uno qualsiasi dei principi, diritti e doveri inclusi nella normativa per la protezione dei dati personali. Tuttavia, raccomanda alla Commissione europea di monitorare attentamente l'applicazione pratica dei poteri della PIPC che prevedono di imporre al trasgressore di adottare la misura che ritiene appropriata tra quelle elencate nell'articolo 64, paragrafo 1, o nell'articolo 45, paragrafo 4, CIA.

127. Inoltre, per quanto riguarda le misure correttive previste dall'articolo 64, paragrafo 1, PIPA, in caso di mancato rispetto di una misura correttiva, la PIPC ha il potere di imporre una multa per un importo massimo di 50 milioni di KRW (articolo 75, paragrafo 2, lettera 13, PIPA), equivalenti a 36 564 EUR. L'EDPB ritiene e teme che tale gamma limitata di sanzioni pecuniarie potrebbe non avere un effetto deterrente particolarmente forte sui trasgressori, come previsto dalla legge al fine di garantire l'applicazione delle norme sulla protezione dei dati, in quanto non sembra avere un potere dissuasivo sufficiente, soprattutto nel caso di grandi organizzazioni o imprese con risorse finanziarie significative.

128. Per quanto riguarda la possibilità che la PIPC possa ordinare che il capo di un'agenzia amministrativa centrale indaghi sul titolare del trattamento dei dati personali o sia coinvolto congiuntamente in un'indagine sulle violazioni del PIPA e addirittura ordini misure correttive nei confronti dei titolari del trattamento dei dati personali sotto la loro giurisdizione (articolo 63, paragrafi 4 e 5, PIPA), l'EDPB

([55]) I compiti e i poteri della PIPC sono definiti principalmente all'articolo 7, paragrafi 8 e 9, e agli articoli da 61 a 66, PIPA.

([56]) Ossia «*si ritiene che una violazione della legge sia suscettibile di ledere i diritti e la libertà delle persone per quanto riguarda i dati personali e che la mancata azione possa causare un danno difficile da rimediare».*

rileva che, sebbene alcune informazioni siano state fornite nel considerando 122 del progetto di decisione, nel complesso la natura di queste altre agenzie e le loro relazioni giuridiche con la PIPC rimangono alquanto vaghe. Inoltre, l'articolo 68, paragrafo 1, PIPA fa riferimento a molte entità a cui sarebbe possibile delegare l'autorità della PIPC. Benché sembri che questa disposizione sia stata applicata solo in relazione alla Korea Internet and Security Agency ([57]), l'EDPB accoglierebbe con favore chiarimenti riguardo alla natura delle possibili interazioni tra queste entità e un attento monitoraggio dell'applicazione di questa disposizione in futuro al fine di garantire l'indipendenza delle entità incaricate di applicare le norme sulla protezione dei dati.

129. Per quanto riguarda le sanzioni, il sistema coreano sembra combinarne diversi tipi, da misure correttive e sanzioni amministrative a sanzioni penali, che possono avere un forte effetto deterrente, e le autorità coreane hanno presentato diversi esempi di multe applicate recentemente dalla PIPC, tra cui una di 6,7 miliardi di KRW, inflitta nel dicembre 2020 a una società per la violazione di una serie di disposizioni del PIPA, e una di 103,3 milioni di KRW, inflitta il 28 aprile 2021 a una società di tecnologie di IA per la violazione delle norme di liceità del trattamento, in particolare il consenso, e il trattamento delle informazioni pseudonimizzate.

130. Sebbene gli importi summenzionati possano avere un effetto dissuasivo, l'EDPB gradirebbe ricevere ulteriori informazioni sul metodo utilizzato dalla PIPC per calcolare il livello delle sanzioni amministrative, ad esempio per quanto riguarda le sanzioni imposte per il mancato rispetto di una misura correttiva emessa ai sensi dell'articolo 64, paragrafo 1, PIPA (cfr. l'articolo 75, paragrafo 2, punto 13, PIPA). Ciò è particolarmente pertinente per ciò che concerne le sanzioni penali e l'applicazione del codice penale (coreano).

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

131. Per quanto riguarda i ricorsi, il sistema coreano sembra offrire varie vie per garantire una protezione adeguata e, in particolare, l'applicazione dei diritti individuali con un mezzo di ricorso effettivo in sede amministrativa e giurisdizionale, anche ai fini del risarcimento per i danni.

132. Il sistema coreano mette inoltre a disposizione meccanismi alternativi, oltre alle vie amministrative e giudiziarie, cui le persone possono ricorrere per ottenere riparazione, come spiegato nei considerando 132 e 133 del progetto di decisione, relativi rispettivamente al call centre per la privacy («Privacy Call Centre») e al comitato per la mediazione delle controversie («Dispute Mediation Committee»). Poiché si tratta di vie di ricorso supplementari, l'EDPB gradirebbe ricevere spiegazioni più dettagliate sul modo in cui integrano le possibilità di ricorso dinanzi alla PIPC e ai tribunali per gli interessati i cui dati personali sono trasferiti verso la Corea ai sensi della decisione di adeguatezza.

4. ACCESSO E UTILIZZO DEI DATI PERSONALI TRASFERITI DA AUTORITÀ PUBBLICHE DALL'UNIONE EUROPEA ALLA COREA DEL SUD

133. Per quanto riguarda la valutazione del livello di protezione dei dati nell'ambito dell'applicazione della legge e della sicurezza nazionale, la Commissione europea ha fornito informazioni esaustive nel suo progetto di decisione e negli allegati messi a disposizione. Pertanto, l'EDPB si astiene dal riprodurre nel presente parere la maggior parte delle constatazioni e valutazioni fattuali.

([57]) Cfr. il considerando 117 del progetto di decisione e l'articolo 62 del decreto di applicazione.

134. La Commissione europea giunge alla conclusione che nei settori summenzionati esiste un livello di protezione dei dati che corrisponde ai requisiti stabiliti dalla giurisprudenza della CGUE e può pertanto essere considerato sostanzialmente equivalente a quello dell'Unione europea.

135. Come osservazione generale, l'EDPB desidera sottolineare che anche nei casi in cui sembra o è affermato dalla Commissione europea che è improbabile che i dati trasferiti dall'UE alla Corea del Sud siano interessati dal diritto coreano pertinente, è comunque opportuno valutare l'adeguatezza del livello coreano di protezione dei dati con riferimento a tali casi. La loro pertinenza è dimostrata anche dal fatto che la stessa Commissione europea li ha esaminati nel progetto di decisione.

4.1. Quadro generale di protezione dei dati nel contesto dell'accesso da parte del governo

136. Per quanto riguarda l'accesso ai dati personali da parte delle autorità pubbliche, per valutare il livello di protezione del diritto alla privacy e alla protezione dei dati occorre esaminare una serie di leggi coreane. Innanzitutto, l'EDPB osserva che il PIPA, come legge centrale in materia di protezione dei dati, rivendica un'ampia applicabilità. Tuttavia, se il PIPA è pienamente applicabile al settore dell'applicazione della legge, la sua applicazione al trattamento dei dati a fini di sicurezza nazionale è limitata. Ai sensi dell'articolo 58, paragrafo 1, punto 2, PIPA, i capitoli da III a VII non si applicano al trattamento dei dati personali a fini di sicurezza nazionale. Tuttavia, i capitoli I, II, IX e X rimangono applicabili al settore della sicurezza nazionale. Pertanto, i principi centrali del PIPA, così come le garanzie fondamentali per i diritti degli interessati e le disposizioni in materia di controllo, applicazione e mezzi di ricorso si applicano di fatto all'accesso e all'utilizzo dei dati personali da parte delle autorità di sicurezza nazionale.

137. Anche la Costituzione sudcoreana sancisce principi fondamentali in materia di protezione dei dati, ossia i principi di legalità, necessità e proporzionalità. Tali principi sono applicabili anche all'accesso ai dati personali da parte delle autorità pubbliche sudcoreane nei settori dell'applicazione della legge e della sicurezza nazionale ([58]).

138. Nell'ambito dell'applicazione della legge, la polizia, i pubblici ministeri, i tribunali e altri organismi pubblici possono raccogliere dati personali sulla base di una legislazione specifica, ossia il codice di procedura penale (Criminal Procedure Act, «**CPA**»), l'atto legislativo sulla protezione della privacy nelle comunicazioni (Communications Privacy Protection Act, «**CPPA**»), l'atto legislativo sulle attività di telecomunicazione (Telecommunications Business Act, «**TBA**») e l'atto legislativo sulla segnalazione e l'utilizzo di informazioni specifiche sulle operazioni finanziarie (Act on Reporting and Using Specified Financial Transaction Information, «**ARUSFTI**»), che si applica al perseguimento e alla prevenzione del riciclaggio di denaro e del finanziamento del terrorismo. Queste normative specifiche stabiliscono ulteriori limitazioni, garanzie ed esenzioni.

139. Nell'ambito della sicurezza nazionale, a norma dell'atto legislativo sui servizi di intelligence nazionali (National Intelligence Service Act, «**NISA**») e di altre «normative in materia di sicurezza nazionale» ([59]), il servizio di intelligence nazionale (National Intelligence Service, «**NIS**») può raccogliere dati personali e intercettare comunicazioni. Nell'esercizio dei suoi poteri, l'EDPB comprende che il NIS deve rispettare le suddette disposizioni giuridiche nonché il PIPA.

140. L'EDPB invita la Commissione a chiarire se, oltre al NIS, vi siano altre autorità in Corea responsabili nell'ambito della sicurezza nazionale, poiché dall'allegato I, punto 6, del documento della

([58]) Cfr. il considerando 145 del progetto di decisione.
([59]) Tra le normative in materia di sicurezza nazionale figurano, ad esempio, l'atto legislativo sulla protezione della privacy nelle comunicazioni, l'atto legislativo antiterrorismo per la protezione dei cittadini e della pubblica sicurezza e l'atto legislativo sulle attività di telecomunicazione.

Commissione europea sembra emergere che il NIS sia soltanto una delle agenzie di sicurezza nazionale, citato a titolo di esempio.

4.2. Protezione e garanzie per i dati di conferma delle comunicazioni nel contesto dell'accesso del governo a fini di applicazione della legge

141. Sulla base della normativa pertinente, la CPPA, le autorità incaricate dell'applicazione della legge possono adottare due tipi di misure di accesso alle informazioni sulle comunicazioni. La CPPA distingue tra misure di limitazione delle comunicazioni, che comprendono sia la raccolta del contenuto della posta ordinaria sia l'intercettazione diretta del contenuto delle telecomunicazioni ([60]), e la raccolta dei cosiddetti dati di conferma delle comunicazioni. Questi ultimi includono la data delle telecomunicazioni, la loro ora di inizio e fine, il numero di chiamate in uscita e in entrata e il numero dell'altro abbonato, la frequenza di utilizzo, i file di log sull'utilizzo dei servizi di telecomunicazione e le informazioni relative all'ubicazione ([61]).

142. L'EDPB nota che i dati di conferma delle comunicazioni non sembrano beneficiare delle stesse garanzie dei dati raccolti tramite misure di limitazione delle comunicazioni, cioè i dati sui contenuti. Di fatto, l'EDPB rileva che la raccolta dei contenuti beneficia di maggiori garanzie rispetto alla raccolta dei dati di conferma delle comunicazioni a fini di applicazione della legge. In primo luogo, a differenza della raccolta dei dati sui contenuti, la raccolta dei dati di conferma delle comunicazioni non è limitata alle indagini su alcuni reati gravi, ma può essere eseguita ogni qualvolta la si ritenga necessaria per condurre «qualsiasi indagine o eseguire qualsiasi pena» (articolo 13, paragrafo 1, CPPA). In secondo luogo, in linea di principio la raccolta dei dati di conferma delle comunicazioni non è strutturata come misura di ultima istanza da utilizzare solamente qualora sia altrimenti difficile impedire la commissione di un reato, arrestare il criminale o raccogliere prove ([62]). I dati di conferma delle comunicazioni possono essere raccolti ogni volta che un pubblico ministero o un ufficiale di polizia giudiziaria «lo ritiene necessario» a fini di indagini su un crimine o esecuzione di una pena. Tuttavia, esiste un'eccezione a questo proposito per i dati di tracciamento in tempo reale e i dati di conferma delle comunicazioni riguardanti una specifica stazione di base a norma dell'articolo 13, paragrafo 2, CPPA. In terzo luogo, le agenzie incaricate dell'applicazione della legge che raccolgono i contenuti delle comunicazioni devono cessare immediatamente di farlo quando l'accesso continuo non è più ritenuto necessario ([63]). Per quanto riguarda i dati di conferma delle comunicazioni, ciò non è quantomeno esplicitamente previsto dalla CPPA o dal suo decreto d'applicazione.

143. L'EDPB prende atto del fatto che la raccolta dei dati di conferma delle comunicazioni può avvenire solo sulla base di un mandato emesso da un tribunale. Inoltre, la CPPA richiede che siano fornite informazioni dettagliate sia nella domanda di mandato che nel mandato stesso ([64]). Tale autorizzazione giudiziaria preliminare serve a limitare la discrezionalità delle autorità incaricate dell'applicazione della legge nell'esercizio delle relative funzioni e a verificare se esistono ragioni sufficienti per raccogliere dati di conferma delle comunicazioni in ciascun caso. L'EDPB riconosce inoltre che il diritto della Repubblica di Corea non sembra prevedere la conservazione generale e indiscriminata dei dati di conferma delle comunicazioni. Pertanto, l'accesso del governo a tali dati riguarda sempre i dati che sono ancora conservati ai fini della fatturazione e della fornitura dei servizi di comunicazione stessi.

([60]) Articolo 3, paragrafo 2, articolo 2, paragrafi 6 e 7, CPPA.
([61]) Articolo 2, paragrafo 11, CPPA.
([62]) È il caso dei dati sui contenuti di cui all'articolo 3, paragrafo 2, e all'articolo 5, paragrafo 1, CPPA.
([63]) Articolo 2, decreto di applicazione della CPPA.
([64]) Cfr. il considerando 156 del progetto di decisione.

144. Tuttavia, l'EDPB sottolinea che la CGUE ha messo in discussione il fatto che i dati sul traffico siano meno sensibili rispetto ad altri dati, in particolare i dati sui contenuti ([65]). Tenendo conto del fatto che i dati di conferma delle comunicazioni godono, sotto diversi aspetti, di un livello di protezione inferiore rispetto ai dati sui contenuti, l'EDPB invita la Commissione europea a monitorare attentamente se le garanzie previste dal diritto coreano per tale categoria di dati personali assicurino un livello di protezione sostanzialmente equivalente a quello garantito nell'UE, in particolare per quanto riguarda la proporzionalità e la prevedibilità della legge.

4.3. Accesso alle informazioni sulle comunicazioni da parte delle autorità pubbliche coreane a fini di sicurezza nazionale

145. Per quanto riguarda il quadro giuridico in materia di accesso delle autorità di sicurezza nazionali alle informazioni sulle comunicazioni trasferite dal SEE alla Corea, l'EDPB ha individuato due punti che danno origine a timori, entrambi relativi al regime di accesso alle comunicazioni tra cittadini non coreani che rientrano in una serie specifica di casi d'uso (cfr. il punto 29). In questi casi, per quanto riguarda sia i dati di conferma delle comunicazioni sia i dati sui contenuti, alcune garanzie altrimenti previste non sono applicabili. In altre parole, in tali casi specifici questi dati non beneficiano delle stesse garanzie dei dati comunicati quando almeno un cittadino coreano è coinvolto nella comunicazione.

4.3.1. Nessun obbligo di notificare alle persone l'accesso del governo alle comunicazioni tra cittadini stranieri

146. In uno scenario come quello delineato in precedenza, ossia quando nessuna delle parti coinvolte in una comunicazione ha la cittadinanza coreana, le autorità di sicurezza nazionale non sono obbligate a notificare alle persone la raccolta e il trattamento dei loro dati. L'EDPB riconosce che tale questione riguarda solo alcuni casi. In primo luogo, come già sottolineato, ogni volta che almeno un cittadino coreano è coinvolto in una comunicazione, i requisiti di notifica a norma della CPPA si applicano a tutte le parti della comunicazione, indipendentemente dalla loro nazionalità ([66]). In secondo luogo, la raccolta di dati personali derivanti da comunicazioni esclusivamente tra cittadini stranieri è sottoposta a una serie specifica di casi d'uso. In particolare, il diritto di accesso in tali casi si estende alle comunicazioni di a) paesi ostili alla Repubblica di Corea, b) agenzie, gruppi o cittadini stranieri sospettati di essere impegnati in attività anti-coreane ([67]) o c) membri di gruppi che operano all'interno della penisola coreana ma sono di fatto al di fuori della sovranità della Repubblica di Corea e dei loro gruppi ombrello con sede in paesi stranieri. Le comunicazioni tra persone dell'UE trasferite dal SEE alla Corea possono quindi essere raccolte a fini di sicurezza nazionale solo se rientrano in una delle tre categorie sopra menzionate ([68]). Come ulteriore fattore limitante, l'EDPB ha compreso dalle

([65]) Cfr. CGUE, C-623/17, *Privacy International*, 6 ottobre 2020, ECLI:EU:C:2020:790, punto 71: «*L'ingerenza nel diritto fondamentale sancito dall'articolo 7 della Carta che la trasmissione dei dati relativi al traffico e dei dati relativi all'ubicazione ai servizi di sicurezza e di intelligence comporta dev'essere considerata particolarmente grave, alla luce in particolare del carattere sensibile delle informazioni che possono fornire tali dati e, in particolare, della possibilità di stabilire, sulla base di questi ultimi, il profilo delle persone interessate, informazione, questa, tanto sensibile quanto il contenuto stesso delle comunicazioni. Inoltre, essa può ingenerare nelle persone interessate la sensazione che la loro vita privata costituisca l'oggetto di una sorveglianza continua (v., per analogia, sentenze dell'8 aprile 2014, Digital Rights Ireland e a., C-293/12 e C-594/12, EU:C:2014:238, punti 27 e 37, nonché del 21 dicembre 2016, Tele2, C-203/15 e C-698/15, EU:C:2016:970, punti 99 e 100)*.»

([66]) Cfr. il considerando 192 del progetto di decisione.

([67]) Cfr. l'allegato II, nota a piè pagina 244, in base alla quale con «attività anti-coreane» si intendono attività che minacciano l'esistenza, la sicurezza e l'ordine democratico della nazione o la sopravvivenza e la libertà del suo popolo.

([68]) Cfr. il considerando 187 del progetto di decisione.

spiegazioni aggiuntive della Commissione europea che il quadro giuridico applicabile non prevede l'intercettazione di dati in transito al di fuori della Corea.

147. Quindi, la criticità legata alla mancanza di un requisito in materia di notifica potrebbe, in termini di impatto pratico, essere considerata limitata. Tuttavia, l'EDPB sottolinea l'importanza della (successiva) notifica di accesso da parte del governo, in particolare per quanto riguarda la garanzia di mezzi di ricorso effettivi. Secondo la CGUE, tale informazione è «*necessaria per consentire a dette persone di esercitare i loro diritti, derivanti dagli articoli 7 e 8 della Carta, di chiedere l'accesso ai propri dati personali costituenti l'oggetto di tali misure e, se del caso, la rettifica o la cancellazione degli stessi, nonché di proporre, conformemente all'articolo 47, primo comma, della Carta, un ricorso effettivo dinanzi a un giudice*» ([69]). L'accesso del governo a fini di sicurezza nazionale prevede spesso misure di sorveglianza segreta, il che significa che gli oggetti della sorveglianza, ossia gli interessati, non sono a conoscenza del trattamento dei loro dati. Pertanto, «*in linea di principio vi sono scarse possibilità di ricorso al giudice da parte della persona interessata, salvo che quest'ultima non sia informata delle misure adottate a sua insaputa e possa quindi contestarne la legalità a posteriori o, in alternativa, salvo che chiunque sospetti che le sue comunicazioni siano o siano state intercettate possa rivolgersi al giudice, in modo che la competenza del giudice non dipenda dalla comunicazione al soggetto intercettato dell'avvenuta intercettazione delle sue comunicazioni*» ([70]). In questo contesto e coerentemente con ciò, l'EDPB ha espresso molte volte la sua preoccupazione riguardo ai mezzi di ricorso effettivi nei casi di sorveglianza. L'EDPB sottolinea che la segretezza delle misure governative non deve avere come risultato che tali misure siano effettivamente incontestabili. In base a quanto detto, per stabilire se la mancanza di un requisito di notifica per le comunicazioni tra cittadini stranieri incida o meno sul livello di protezione dei dati quale valutato nel progetto di decisione, la valutazione deve fare parte di una valutazione globale con particolare riguardo ai meccanismi di controllo e ricorso previsti dal diritto coreano (cfr. le sezioni 4.7 e 4.8).

148. Inoltre, a tale proposito l'EDPB nota che la normativa si riferisce a termini piuttosto ampi come attività anti-coreane o anti-nazionali ([71]) e che è difficile prevedere come queste nozioni siano da intendersi ai sensi del diritto coreano. L'EDPB invita la Commissione europea a monitorare il modo in cui questi termini sono definiti nel diritto coreano e se la loro applicazione pratica soddisfa i requisiti di proporzionalità derivanti dal diritto dell'UE.

4.3.2. Nessuna autorizzazione preventiva indipendente per la raccolta di informazioni sulle comunicazioni tra cittadini stranieri

149. Nei casi in cui i dati personali nel SEE ricavati da comunicazioni tra cittadini non coreani (e che rientrano in uno dei casi d'uso summenzionati) debbano essere trattati in Corea a fini di sicurezza nazionale, la raccolta di tali dati non è soggetta all'approvazione preventiva di un organismo indipendente (come nel caso delle comunicazioni in cui almeno una delle persone interessate è di nazionalità coreana). ([72])

([69]) CGUE, cause riunite C-511/18, C-512/18 e C-520/18, *La Quadrature du Net e a.*, 6 ottobre 2020, ECLI:EU:C:2020:791, punto 190.
([70]) CEDU, *Big Brother Watch e altri contro Regno Unito*, 25 maggio 2021, ECLI:CE:ECHR:2021:0525JUD005817013, punto 337 e CEDU, *Roman Zakharov c. Russia*, 4 dicembre 2015, ECLI:CE:ECHR:2015:1204JUD004714306, punto 234.
([71]) La Commissione europea ha chiarito che, in base alle spiegazioni del governo coreano, il termine si riferisce ad «attività che minacciano l'esistenza, la sicurezza e l'ordine democratico della nazione o la sopravvivenza e la libertà del suo popolo», come indicato anche nella nota a piè pagina 319 del progetto di decisione di adeguatezza.
([72]) Cfr. il considerando 190 del progetto di decisione.

150. Soprattutto alla luce delle recenti decisioni della Corte europea dei diritti dell'uomo («**CEDU**») «Big Brother Watch e altri contro Regno Unito» e «Centrum för Rättvisa c. Svezia», l'EDPB ritiene necessario indagare se ciò costituisca una carenza critica del quadro coreano sulla protezione dei dati. A questo proposito, l'EDPB ricorda che, come sottolineato nelle sue raccomandazioni aggiornate relative alle garanzie essenziali europee per le misure di sorveglianza ([73]), l'articolo 6, paragrafo 3, del trattato sull'Unione europea stabilisce che i diritti fondamentali garantiti dalla Convenzione europea dei diritti dell'uomo fanno parte del diritto dell'Unione in quanto principi generali mentre, come ricorda la CGUE nella sua giurisprudenza, la suddetta Convenzione non costituisce, finché l'Unione non vi abbia aderito, un atto giuridico formalmente integrato nell'ordinamento giuridico dell'Unione ([74]). Pertanto, il livello di protezione dei diritti fondamentali richiesto dall'articolo 45 del RGPD deve essere determinato sulla base delle disposizioni di tale regolamento, lette alla luce dei diritti fondamentali sanciti dalla Carta. Ciò premesso, ai sensi dell'articolo 52, paragrafo 3, della Carta, i diritti in essa contenuti corrispondenti ai diritti garantiti dalla Convenzione europea dei diritti dell'uomo devono avere lo stesso significato e lo stesso ambito di applicazione di quelli previsti dalla suddetta convenzione. Occorre dunque tenere conto della giurisprudenza della CEDU relativa ai diritti previsti anche nella Carta ai fini dell'interpretazione dei diritti corrispondenti contenuti nella Carta, in quanto livello minimo di protezione, ossia nella misura in cui la Carta, come interpretata dalla CGUE, non preveda un livello di protezione superiore ([75]).

151. L'EDPB nota che, se l'approvazione preventiva (indipendente) delle misure di sorveglianza è considerata una garanzia importante contro l'arbitrarietà, tale approvazione non può essere ricavata dalla giurisprudenza della CGUE come requisito assoluto per la proporzionalità delle misure di sorveglianza. Tuttavia, la CEDU ha ora stabilito espressamente il requisito relativo all'autorizzazione indipendente ex ante per le intercettazioni massive ([76]). Anche se il progetto di decisione non lo menzione esplicitamente, l'EDPB comprende che il quadro giuridico della Repubblica di Corea non prevede l'intercettazione massiva ma solo l'intercettazione mirata delle telecomunicazioni ([77]). La Commissione europea ha confermato questa interpretazione.

152. Ciò detto, le suddette decisioni della CEDU, in linea con la giurisprudenza della CGUE ([78]) e con la precedente giurisprudenza della CEDU ([79]), mostrano ancora una volta l'importanza di una supervisione globale da parte di autorità di controllo indipendenti. L'EDPB sottolinea che il controllo indipendente in tutte le fasi del processo di accesso da parte del governo a fini di applicazione della legge e di sicurezza nazionale è una garanzia importante contro misure di sorveglianza arbitrarie e quindi per la valutazione di un adeguato livello di protezione dei dati. La garanzia di indipendenza delle autorità di controllo ai sensi dell'articolo 8, paragrafo 3, della Carta è intesa a garantire un

([73]) Cfr. EDPB, Raccomandazioni 2/2020 relative alle garanzie essenziali europee per le misure di sorveglianza, punti 10 e 11.

([74]) Cfr. CGUE, C-311/18, *Data Protection Commissioner contro Facebook Ireland Ltd. e Maximilian Schrems*, 16 luglio 2020, ECLI:EU:C:2020:559 (in appresso «*Schrems II*»), punto 98.

([75]) Cfr. CGUE, cause riunite C-511/18, C-512/18 e C-520/18, *La Quadrature du Net e a.*, 6 ottobre 2020, punto 124.

([76]) Cfr. CEDU, *Big Brother Watch e altri contro Regno Unito*, 25 maggio 2021, ECLI:CE:ECHR:2021:0525JUD005817013, punto 351: «L'intercettazione massiva dovrebbe essere soggetta ad un'autorizzazione iniziale indipendente», «l'intercettazione massiva dovrebbe essere autorizzata da un organismo indipendente; cioè, un organismo che è indipendente dall'esecutivo».

([77]) Solo l'allegato II, punto 3.2, contiene una dichiarazione esplicita in merito alle finalità legate alla sicurezza nazionale, quando specifica che le limitazioni e le garanzie «*assicurano che la raccolta e il trattamento delle informazioni sono limitati a quanto strettamente necessario per il conseguimento di una finalità legittima. Ciò esclude qualsiasi raccolta massiccia e indiscriminata di dati personali a fini di sicurezza nazionale*».

([78]) Cfr., ad esempio, CGUE, cause riunite C-203/15 e C-698/15, *Tele2 Sverige AB e altri*, ECLI:EU:C:2016:970.

([79]) Cfr., ad esempio, CEDU, *Roman Zakharov c. Russia*, 4 dicembre 2015, ECLI:CE:ECHR:2015:1204JUD004714306.

monitoraggio efficace e affidabile del rispetto delle norme sulla protezione delle persone in relazione al trattamento dei dati personali. Ciò vale in particolare nelle circostanze in cui, a causa della natura della sorveglianza segreta, la persona non può proporre un riesame o partecipare direttamente a un procedimento di riesame prima o durante l'esecuzione della misura di sorveglianza.

153. L'assenza di un'approvazione preventiva indipendente non può essere considerata di per sé una carenza sostanziale del diritto coreano in relazione alla valutazione di un livello di protezione dei dati sostanzialmente equivalente. La valutazione dell'adeguatezza dipende, ancora una volta, da tutte le circostanze del caso, in particolare dall'efficacia del controllo ex post e dei mezzi di ricorso previsti dal quadro giuridico coreano (cfr. le sezioni 4.7 e 4.8 successive).

4.4. Comunicazioni volontarie

154. A norma dell'articolo 83, paragrafo 3, TBA, i fornitori di servizi di telecomunicazioni possono trasmettere volontariamente i cosiddetti «dati degli abbonati» ([80]) alle autorità incaricate dell'applicazione della legge e della sicurezza nazionale. Pur osservando che i casi riguardanti dati personali trasferiti dal SEE alla Corea sono generalmente poco frequenti, l'EDPB rileva che essi devono comunque essere analizzati per valutare il livello di protezione dei dati, come già menzionato precedentemente.

155. L'EDPB comprende che in questi casi si applicano le garanzie di protezione dei dati di cui al PIPA e che tanto le autorità pubbliche quanto i fornitori di telecomunicazioni devono conformarsi a tali requisiti ([81]); inoltre entrambi possono essere ritenuti responsabili per qualsiasi violazione dei diritti e delle libertà degli interessati ([82]). L'EDPB comprende altresì che i fornitori di telecomunicazioni non sono tenuti a soddisfare tali richieste.

156. Tuttavia, per quanto concerne la nozione di accesso ai dati degli abbonati da parte delle autorità nazionali per l'applicazione della legge, nonché, in particolare, per la sicurezza nazionale attraverso la «comunicazione volontaria» degli operatori di telecomunicazioni, si teme un aumento del rischio per i diritti e le libertà degli interessati, specie per quanto riguarda il loro diritto all'informazione.

157. Ai sensi dell'articolo 58, paragrafo 1, punto 2, PIPA, le disposizioni dei capitoli da III a VII non si applicano ai dati personali di cui si richiede la comunicazione in relazione alla sicurezza nazionale. A tale riguardo, ad esempio, le disposizioni dell'articolo 18 (Limitazione all'utilizzo e alla fornitura di dati personali al di fuori della finalità) e dell'articolo 20 (Notifica delle fonti ecc. dei dati personali raccolti da terzi) del PIPA non sono applicabili a tali richieste. Nei casi in cui la richiesta è presentata da un'autorità di sicurezza nazionale, da un lato ciò solleva la questione se l'articolo 58, paragrafo 1, punto 2, precluda l'applicazione del PIPA anche ai fornitori di telecomunicazioni. Dall'altro, si pone la questione se l'esclusione dell'applicazione dell'articolo 20 del PIPA in tali casi si applichi anche alla disposizione corrispondente del punto 3 dell'allegato I (Notifica dei dati quando i dati personali non sono stati ottenuti dall'interessato, articolo 20 della legge). Se questo fosse il caso e se l'articolo 58, paragrafo 1, punto 2, riguardasse anche i fornitori di telecomunicazioni, potrebbe sussistere il rischio, in base alle informazioni disponibili, che non vi sia alcun obbligo legale di informare gli interessati circa la comunicazione volontaria.

158. L'EDPB teme quindi che l'efficacia dei requisiti di informazione possa essere compromessa, rendendo notevolmente più difficile per gli interessati far valere i loro diritti in materia di protezione dei dati,

([80]) Le serie di dati interessate sarebbero: il nome, il numero di registrazione residente, l'indirizzo e il numero di telefono degli utenti, le date in cui gli utenti si abbonano o terminano il loro abbonamento e i codici di identificazione degli utenti (utilizzati per identificare l'utente legittimo di sistemi informatici o reti di comunicazione).
([81]) Cfr. i considerando 164 e 194 del progetto di decisione.
([82]) Cfr. il considerando 166 del progetto di decisione.

soprattutto per quanto riguarda il ricorso giurisdizionale. A questo proposito, l'EDPB invita la Commissione europea a chiarire l'ambito di applicazione delle disposizioni pertinenti.

1.5. Ulteriore utilizzo delle informazioni

159. Il principio della limitazione della finalità è un requisito giuridico fondamentale della protezione dei dati. Esso prevede che i dati personali siano raccolti solo per finalità determinate, esplicite e legittime e successivamente trattati in modo che non sia incompatibile con tali finalità. Inoltre le autorità pubbliche sono autorizzate dal diritto dell'UE a trattare i dati personali a fini di prevenzione, indagine o perseguimento di reati, anche se tali dati sono stati inizialmente ottenuti per finalità diverse, se dette autorità hanno una base giuridica per trattare i dati in questione ai sensi della normativa pertinente e se l'ulteriore trattamento non è sproporzionato ([83]).

160. In base a ciò l'EDPB rileva che il quadro coreano sulla protezione dei dati prevede garanzie e limitazioni simili a quelle previste dal diritto dell'UE in relazione all'ulteriore utilizzo delle informazioni raccolte a fini di applicazione della legge e di sicurezza nazionale, ad esempio il principio della limitazione della finalità di cui all'articolo 3, paragrafi 1 e 2, PIPA.

1.6. Trasferimenti successivi e condivisione dell'intelligence

161. L'articolo 44 del RGPD prevede che i trasferimenti e i trasferimenti successivi di dati personali abbiano luogo soltanto se il livello di protezione garantito dal RGPD non è pregiudicato. Pertanto, il livello di protezione garantito ai dati personali trasferiti dal SEE alla Corea non deve essere pregiudicato dall'ulteriore trasferimento a destinatari in un paese terzo; in altre parole, i trasferimenti successivi dovrebbero essere consentiti solo quando è garantito un livello costante di protezione sostanzialmente equivalente a quello garantito dal diritto dell'UE. Di conseguenza, nel valutare se un paese terzo garantisce un livello adeguato di protezione dei dati, occorre tenere conto del quadro giuridico del paese in questione in relazione ai trasferimenti successivi. Ciò è indiscutibile e in linea con il parere sia della Commissione europea ([84]) sia dell'EDPB.

162. In questo contesto, l'EDPB prende atto che la CEDU, nelle sue recenti decisioni «Big Brother Watch e altri contro Regno Unito» e «Centrum för Rättvisa c. Svezia», ha fornito orientamenti ([85]) relativi alle precauzioni in materia di protezione dei dati da osservare negli Stati contraenti quando comunicano dati personali ad altre parti a fini di applicazione della legge e sicurezza nazionale in casi di raccolta massiva: «*In primo luogo, le circostanze in cui tale trasferimento può avvenire devono essere definite chiaramente nel diritto interno. In secondo luogo, lo Stato trasferente deve assicurarsi che lo Stato ricevente, nel trattamento dei dati, disponga di garanzie in grado di prevenire abusi e interferenze sproporzionate. In particolare, lo Stato ricevente è tenuto a garantire che il materiale sia conservato in modo sicuro e a limitarne la divulgazione successiva. [...] In terzo luogo, saranno necessarie maggiori garanzie laddove sarà evidente che il materiale trasferito richiede una particolare riservatezza, ad esempio nel caso di materiale giornalistico riservato*.» ([86])

([83]) Cfr. l'articolo 4, paragrafo 2, LED.
([84]) Cfr. il considerando 84 e seguenti del progetto di decisione.
([85]) I seguenti elementi sono stati stabiliti in occasione delle cause *Big Brother Watch* e *Centrum för Rättvisa*, che riguardano i regimi di intercettazione massiva. Il requisito relativo alle precauzioni da prendere quando si comunica materiale ad altre parti faceva già parte dei criteri sviluppati dalla CEDU nel contesto delle intercettazioni mirate e non era stato ulteriormente specificato dalla Corte (cfr. *Big Brother Watch e altri contro Regno Unito*, punti 335 e 362).
([86]) CEDU, *Big Brother Watch e altri contro Regno Unito*, 25 maggio 2021, ECLI:CE:ECHR:2021:0525JUD005817013, punto 362.

163. Nell'applicazione di queste norme, la CEDU ha constatato nel caso «Centrum för Rättvisa c. Svezia» che l'assenza nel regime di intercettazione di un requisito giuridico esplicito per valutare la necessità e la proporzionalità della condivisione dell'intelligence per il suo possibile impatto sul diritto alla privacy costituisce una violazione dell'articolo 8 della Convenzione europea dei diritti dell'uomo. La CEDU ha criticato il fatto che, a causa del livello di generalità della legge, il materiale di intercettazione potrebbe essere generalmente inviato all'estero ogni volta che ciò è considerato nell'interesse nazionale, indipendentemente dal fatto che il destinatario straniero offra un livello minimo accettabile di garanzie ([87]).

164. Riconoscendo che il quadro giuridico della Corea del Sud non consente l'intercettazione massiva, sempre alla luce delle implicazioni della giurisprudenza della CEDU illustrata precedentemente l'EDPB ritiene che, oltre ai requisiti derivanti dal diritto dell'UE come interpretato dalla CGUE, la linea di argomentazioni della CEDU dovrebbe essere considerata per valutare se il quadro giuridico in materia di trasferimenti successivi verso un paese terzo preveda norme adeguate sulla protezione dei dati.

4.6.1. Quadro giuridico applicabile ai trasferimenti successivi da parte delle autorità incaricate dell'applicazione della legge

165. Per quanto riguarda i trasferimenti successivi da parte delle autorità competenti a fini di applicazione della legge, l'EDPB comprende dalle spiegazioni della Commissione europea che il punto 2 dell'allegato I del progetto di decisione, concernente la limitazione dei trasferimenti successivi, è applicabile anche quando il trasferimento è effettuato sulla base di una legge diversa dal PIPA. In base a questa norma, «*se le informazioni personali sono fornite a un terzo che si trova all'estero, potrebbero non ricevere il livello di protezione garantito dall'atto legislativo sulla protezione dei dati personali (PIPA) della Corea a causa delle differenze nei sistemi di protezione dei dati personali dei diversi paesi. Di conseguenza, tali casi saranno considerati come «casi in cui l'interessato potrebbe subire svantaggi», come definito all'articolo 17, paragrafo 4, PIPA, o «casi in cui l'interesse di un interessato o di terzi è violato ingiustamente», come definito all'articolo 18, paragrafo 2, PIPA, e all'articolo 14, paragrafo 2, del relativo decreto di applicazione. Per soddisfare i requisiti di queste disposizioni, il titolare del trattamento dei dati personali e i terzi devono quindi garantire in modo esplicito un livello di protezione equivalente a quello garantito dalla legge, compresa la garanzia dell'esercizio dei diritti dell'interessato in documenti giuridicamente vincolanti, come i contratti, anche dopo il trasferimento all'estero dei dati personali» ([88]).*

166. L'EDPB accoglie con favore questa disposizione la quale, presupponendo l'adeguatezza del livello di protezione dei dati in Corea pe tale finalità, garantisce la continuità di un livello di protezione come sostanzialmente previsto ai sensi del diritto dell'UE per i trasferimenti successivi. La Commissione ha confermato che l'interpretazione dell'EDPB, ossia che questo punto dell'allegato I si applica a tutti i trasferimenti successivi effettuati dalle autorità competenti a fini di applicazione della legge, è corretta. Tuttavia, l'EDPB sottolinea che si deve garantire che questo regolamento fornisca un livello continuo di protezione nella pratica, poiché potrebbe esserci incertezza su quali garanzie e obblighi contrattuali o altri meccanismi simili possono essere utilizzati per ottenere tale livello di protezione in caso di trattamento a fini di applicazione della legge. A questo proposito, dovrebbe essere ulteriormente dichiarato, ad esempio, che i dati personali possono essere condivisi soltanto con le autorità competenti del paese terzo.

([87]) Cfr. CEDU, *Centrum för Rättvisa c. Svezia*, 25 maggio 2021, ECLI:CE:ECHR:2021:0525JUD003525208, punto 326.
([88]) Progetto di decisione, allegato I, pag. 7.

167. Fatta salvo il chiarimento richiesto precedentemente in merito al fatto che la KOFIU rientri nel progetto di decisione, l'EDPB osserva che la dichiarazione ufficiale sull'accesso del governo ([89]) spiega che, ai sensi dell'articolo 8, paragrafo 1, dell'ARUSFTI, il commissario della KOFIU può fornire ai servizi di intelligence stranieri informazioni specifiche sulle operazioni finanziarie, se ciò è ritenuto necessario per conseguire le finalità dell'ARUSFTI ([90]). Lo stesso articolo 8 dell'ARUSFTI non prevede l'obbligo di determinare se il paese straniero offra adeguate garanzie di protezione dei dati né di assicurarlo. L'allegato II non fa riferimento al nuovo punto dell'allegato I relativo. Pertanto, l'EDPB invita la Commissione europea a chiarire l'interrelazione tra il punto pertinente dell'allegato I relativo alla limitazione dei trasferimenti successivi e la base giuridica per i trasferimenti successivi ai sensi dell'ARUSFTI.

4.6.2. Quadro giuridico applicabile ai trasferimenti successivi a fini di sicurezza nazionale

168. Il progetto di decisione non contiene alcuna informazione sul quadro giuridico in materia di trasferimenti successivi nell'ambito della sicurezza nazionale. A tale proposito, l'EDPB comprende che, a differenza di quanto avviene per l'applicazione della legge, il punto 2 dell'allegato I non è applicabile ai trasferimenti successivi a fini di sicurezza nazionale. Gli articoli 17 e 18, PIPA, che sono oggetto del punto in questione dell'allegato I, fanno parte del capitolo III del PIPA, che a sua volta non è applicabile al trattamento dei dati personali a fini di sicurezza nazionale (articolo 58, paragrafo 1, PIPA).

169. Tuttavia, l'EDPB parte dal presupposto che la Corea possa avere bisogno di trasmettere, e che trasmetta, dati personali a servizi di intelligence stranieri a fini di sicurezza nazionale, ad esempio per cooperare nella lotta contro le minacce transfrontaliere alla sicurezza nazionale, per avvertire i governi stranieri o per sollecitare il loro aiuto nell'individuazione di tali minacce.

170. L'EDPB ha compreso che, secondo la Commissione europea, i trasferimenti successivi sono sufficientemente disciplinati nel diritto coreano dalle garanzie derivanti dal quadro costituzionale generale, in particolare i principi di necessità e proporzionalità, nonché dai principi fondamentali di protezione dei dati stabiliti dal PIPA, quali la liceità e la correttezza del trattamento, la limitazione della finalità, la minimizzazione dei dati, la sicurezza e gli obblighi generali di prevenire l'abuso e l'utilizzo improprio dei dati personali.

171. L'EDPB riconosce e ammette l'applicabilità generale di questi principi chiave (di protezione dei dati), ma esprime preoccupazione per il fatto che tali garanzie sono di natura molto generale e non citano o affrontano specificamente, in una base giuridica, le circostanze e le condizioni specifiche per i trasferimenti successivi di dati trasferiti dal SEE a fini di sicurezza nazionale. Sebbene questi principi generali siano ampiamente applicabili, l'EDPB si chiede se si possa ritenere che ciò sia conforme ai criteri di norme chiare e precise e che sancisca sufficientemente garanzie efficaci e applicabili. Soprattutto quando l'accesso e il trattamento dei dati personali da parte del governo è esercitato in segreto e le conclusioni che si potrebbero trarre dai dati sono particolarmente gravi, è essenziale disporre di norme chiare e dettagliate. La normativa dovrebbe indicare l'ambito di applicazione di qualsiasi discrezionalità conferita alle autorità competenti e le modalità del suo esercizio con sufficiente chiarezza per fornire alla persona una protezione adeguata. Nella sentenza *Schrems II*, la CGUE ricorda che una base giuridica che consente un'ingerenza nei diritti fondamentali deve, per soddisfare i requisiti dei principi di necessità e proporzionalità, definire essa stessa la portata della

([89]) Cfr. l'allegato II del progetto di decisione.

([90]) Cfr. l'allegato II, punto 2.2.3.2 del progetto di decisione. Se tale scambio può avvenire solo a condizione che il servizio straniero non possa utilizzare le informazioni per una finalità diversa da quella originaria della comunicazione, e in particolare non per un'indagine o un processo penale (articolo 8, paragrafo 2, ARUSFTI), il commissario della KOFIU può, su richiesta da un paese straniero, dare il consenso all'utilizzo di tali dati per indagini o processi penali per reati penali previo consenso del ministro della Giustizia (articolo 8, paragrafo 3, ARUSFTI).

limitazione dell'esercizio del diritto di cui trattasi e prevedere norme chiare e precise che regolino la portata e l'applicazione della misura in questione e impongano garanzie minime ([91]). L'EDPB teme quindi che non sia sufficiente che tali garanzie siano generalmente sancite in leggi di rango superiore senza che sia attuata specificamente la nozione di proporzionalità, ad esempio, nella rispettiva base giuridica stessa.

172. Queste preoccupazioni trovano fondamento nella summenzionata decisione della CEDU, in cui la Corte ha ritenuto che una norma generale priva di alcun requisito esplicito che disponga di valutare la necessità e la proporzionalità o di prendere in considerazione le preoccupazioni relative alla privacy non è compatibile con il diritto alla privacy ai sensi dell'articolo 8 della Convenzione europea dei diritti dell'uomo. A questo proposito, l'EDPB rileva che nell'ordinamento della causa in questione (così come nel diritto della Corea) esistono principi generali (costituzionalmente garantiti) di necessità e proporzionalità, ad esempio sulla base della Carta e attraverso l'adesione alla Convenzione europea dei diritti dell'uomo.

173. L'EDPB invita la Commissione europea a chiarire la base giuridica nonché le modalità e la misura in cui, e a quali condizioni specifiche, le agenzie dei servizi di intelligence sono obbligate a tenere conto delle preoccupazioni relative alla privacy e delle garanzie di protezione dei dati prima di comunicare dati personali a partner stranieri a fini di sicurezza nazionale. Nel caso in cui tale obbligo derivi direttamente dai principi costituzionali, la Commissione europea dovrebbe valutare ulteriormente i requisiti di precisione e chiarezza della normativa pertinente e confermare che i principi generali costituzionali e di protezione dei dati sono adeguatamente applicati e attuati.

4.6.3. Accordi internazionali

174. L'EDPB rileva che la Commissione europea non ha preso in considerazione, nella sua valutazione di adeguatezza, l'esistenza di accordi internazionali conclusi tra la Corea e paesi terzi o organizzazioni internazionali che possono prevedere disposizioni specifiche per il trasferimento internazionale di dati personali a paesi terzi da parte dei servizi preposti all'applicazione della legge e/o di intelligence. L'EDPB ritiene che la conclusione di accordi bilaterali o multilaterali con paesi terzi ai fini dell'applicazione della legge o della cooperazione in materia di intelligence possa incidere sul quadro giuridico in materia di protezione dei dati della Corea, come valutato.

175. L'EDPB invita pertanto la Commissione europea a chiarire se tali accordi esistano, a quali condizioni possano essere conclusi e a valutare se le disposizioni degli accordi internazionali possano incidere sul livello di protezione dei dati personali trasferiti dal SEE alla Corea garantito dal quadro legislativo e dalle prassi in relazione alle comunicazioni all'estero a fini di applicazione della legge e di sicurezza nazionale.

4.7. Controllo

176. L'EDPB nota che il controllo delle autorità incaricate dell'applicazione del diritto penale e della sicurezza nazionale è garantito da un insieme di organismi diversi interni ed esterni.

177. In questo contesto, è opportuno osservare che la CGUE ha ripetutamente sottolineato la necessità di un controllo indipendente come elemento essenziale della protezione delle persone fisiche per quanto riguarda il trattamento dei loro dati personali. La nozione di indipendenza comprende gli ambiti dell'autonomia istituzionale, della libertà da istruzioni e dell'indipendenza materiale. Al fine di garantire un controllo e un'applicazione coerenti della normativa sulla protezione dei dati, le autorità di controllo devono disporre di poteri efficaci, compresi poteri correttivi e riparatori.

([91]) Cfr. *Schrems II*, punti 175 e 180.

178. L'EDPB concorda con la conclusione della Commissione europea secondo cui, in una valutazione complessiva, si può ritenere che la Corea disponga di un sistema di controllo indipendente ed efficace, anche se diversi organismi del sistema di controllo non soddisfano di per sé i requisiti citati sopra. Ad esempio, la maggior parte di essi non ha poteri esecutivi, ma si limita a semplici raccomandazioni, come la commissione nazionale per i diritti umani o la commissione per le revisioni e le ispezioni. Inoltre, i rispettivi enti pubblici non sono, per la maggior parte, esclusivamente istituzioni per la protezione dei dati, ma sono solitamente incaricati di altri compiti nell'ambito della protezione dei diritti fondamentali.

179. Tuttavia, in base ai chiarimenti della Commissione europea, l'EDPB osserva che il controllo delle autorità incaricate dell'applicazione della legge è garantito in modo completo e senza eccezioni dalla PIPC. Pertanto la PIPC possiede poteri investigativi, correttivi ed esecutivi ai sensi del PIPA e di altre leggi sulla protezione dei dati (ad esempio la CPPA) che si applicano all'intero settore dell'accesso ai dati personali da parte delle autorità incaricate dell'applicazione della legge e della sicurezza nazionale.

180. In questo contesto, l'EDPB desidera sottolineare ancora una volta che per esercitare i propri compiti e poteri, le autorità di controllo devono essere dotate di sufficienti risorse umane, tecniche e finanziarie. A tale proposito, si riscontra purtroppo una mancanza di informazioni circa gli organismi di controllo designati, in particolare la PIPC. Pertanto, l'EDPB rinnova la richiesta alla Commissione europea di fornire ulteriori informazioni in materia.

181. Nel complesso, l'EDPB desidera rilevare che nel progetto di decisione le dichiarazioni, gli esempi o le cifre relativi alle attività di controllo e all'applicazione giuridica della normativa sulla protezione dei dati da parte degli organismi di controllo nell'ambito dell'applicazione della legge e della sicurezza nazionale sono pressoché assenti. Elementi di questo tipo sarebbero utili nel contesto della valutazione dell'efficacia delle autorità di controllo.

4.8. Ricorso giurisdizionale

182. L'EDPB ricorda che è essenziale per un adeguato livello di protezione dei dati che le persone interessate dispongano di mezzi di ricorso completi contro l'accesso o il trattamento non autorizzato dei dati. Tali mezzi di ricorso devono essere tali da consentire all'interessato di ottenere l'accesso ai dati conservati che lo riguardano e di chiederne la rettifica o la cancellazione.

183. Alla luce delle sentenze *Schrems I* e *Schrems II* della CGUE, è chiaro che, oltre al diritto di rivolgersi alle autorità competenti, una tutela giurisdizionale effettiva ai sensi dell'articolo 47, paragrafo 1, della Carta è di fondamentale importanza per l'ipotesi di adeguatezza del diritto di un paese terzo.

184. L'EDPB riconosce che la Corea ha definito una serie di modalità per l'esecuzione dei diritti di accesso, conservazione, cancellazione e sospensione delle persone ai sensi del PIPA. Tali diritti possono essere esercitati nei confronti del titolare stesso o tramite un reclamo presentato alla PIPC o ad altri organismi di controllo, ad esempio la commissione nazionale per i diritti umani. Inoltre, l'EDPB riconosce la possibilità di contestare i titolari del trattamento o la decisione delle autorità pubbliche in risposta alla loro richiesta sulla base della legge sulle controversie amministrative.

185. Inoltre, l'EDPB comprende dalle spiegazioni fornite dalla Commissione europea che le persone possono contestare le azioni delle autorità incaricate dell'applicazione della legge e della sicurezza nazionale dinanzi ai tribunali competenti ai sensi della legge sulle controversie amministrative e della legge sulla Corte costituzionale e hanno la possibilità di ottenere il risarcimento dei danni ai sensi della legge sul risarcimento statale ([92]).

([92]) Cfr. l'allegato II, punto 3.2.4 in combinato disposto con il punto 2.4.3.

186. In questo contesto, tuttavia, l'EDPB nutre perplessità circa il ricorso effettivo per le persone dell'UE nei casi di sicurezza nazionale in cui non sono coinvolti cittadini coreani. Come osservato al punto 33 e seguenti, le autorità di sicurezza nazionale non sono tenute a notificare agli interessati la raccolta e il trattamento dei loro dati personali. Poiché è molto più difficile ottenere una protezione giuridica efficace in tali casi, l'EDPB desidera sottolineare che alcune garanzie giuridiche sono necessarie in questo caso se sono coinvolti dati trasferiti dal SEE. Dette garanzie devono consentire agli interessati di intraprendere un'azione efficace e in modo giuridicamente sicuro contro il trattamento illecito dei dati senza essere ostacolati da requisiti procedurali eccessivamente limitanti, come, ad esempio, l'imposizione di un onere della prova che non possono soddisfare senza essere a conoscenza del trattamento. Inoltre, gli interessati devono potersi rivolgere a un organo competente che soddisfi i requisiti dell'articolo 47 della Carta, ossia che sia competente a determinare se un trattamento di dati ha luogo e a verificare la liceità del trattamento e che, in caso di trattamento illecito, sia in grado di esercitare poteri per porre rimedio. In questo contesto, un semplice diritto di reclamo presentato alla commissione nazionale per i diritti umani, ad esempio, non sarebbe sufficiente. L'EDPB invita pertanto la Commissione a spiegare più dettagliatamente in che modo questi requisiti sono attuati in termini procedurali e sostanziali, ad esempio se è possibile per gli interessati rivolgersi alla PIPC, oltre che a un tribunale, senza dover provare il trattamento dei dati in questione.

187. Inoltre, l'EDPB osserva che il progetto di decisione prevede un meccanismo di deferimento dei reclami, vale a dire che le persone dell'UE possono presentare un reclamo alla PIPC attraverso la loro autorità nazionale di protezione dei dati o l'EDPB. La PIPC informerà poi la persona attraverso lo stesso canale una volta che l'indagine è conclusa ([93]). L'EDPB accoglie con favore lo sforzo di facilitare l'accesso al ricorso contro le autorità coreane di sicurezza nazionale. Allo stesso tempo, l'EDPB raccomanda che tale meccanismo di deferimento sia incanalato attraverso le autorità nazionali europee per la protezione dei dati anziché attraverso l'EDPB, poiché esse sono competenti e più vicine al trattamento dei reclami individuali.

188. Inoltre, l'EDPB rileva una possibile contraddizione rispetto alla comunicazione volontaria. Da un lato, il progetto di decisione afferma che le persone possono ottenere riparazione nel caso in cui i loro dati siano divulgati illecitamente a seguito di una richiesta di comunicazione volontaria, anche contro l'autorità incaricata dell'applicazione della legge che ha emesso la richiesta ([94]). Dall'altro, il progetto di decisione fa riferimento al requisito dell'impatto diretto per quanto riguarda il diritto della persona di contestare le azioni delle autorità pubbliche, elencando (solo) le richieste di comunicazione vincolanti come esempio di un caso in cui si ritiene che l'azione amministrativa abbia un impatto diretto sul diritto alla privacy ([95]). L'EDPB comprende dalle spiegazioni della Commissione europea che in realtà non vi è alcuna limitazione delle possibilità di ricorso dinanzi alle richieste di comunicazione volontaria e chiede pertanto alla Commissione europea di chiarire ulteriormente questo punto nella decisione, nell'ambito sia dell'applicazione della legge sia della sicurezza nazionale (a differenza della sezione sull'applicazione della legge, la sezione sulle comunicazioni volontarie a fini di sicurezza nazionale non contiene alcuna dichiarazione esplicita sul ricorso in questo contesto).

([93]) Cfr. il considerando 205 e l'allegato I, pag. 19, del progetto di decisione.
([94]) Cfr. il considerando 166 del progetto di decisione.
([95]) Cfr. il considerando 181 (applicazione della legge) e i considerando 208 e 181 (sicurezza nazionale) del progetto di decisione.