II

(Atti non legislativi)

DECISIONI

DECISIONE DI ESECUZIONE (UE) 2022/254 DELLA COMMISSIONE

del 17 dicembre 2021

a norma del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio sull'adeguata protezione dei dati personali da parte della Repubblica di Corea nel quadro della legge sulla protezione delle informazioni personali

[notificata con il numero C(2021) 9316]

(Testo rilevante ai fini del SEE)

LA COMMISSIONE EUROPEA,

visto il trattato sul funzionamento dell'Unione europea,

visto il regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati) ([1]), in particolare l'articolo 45, paragrafo 3,

considerando quanto segue:

1. INTRODUZIONE

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

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

(3) Come specificato all'articolo 45, paragrafo 2, del regolamento (UE) 2016/679, l'adozione della decisione di adeguatezza deve basarsi su un'analisi completa dell'ordinamento giuridico del paese terzo, per quanto riguarda tanto le norme applicabili agli importatori di dati quanto le limitazioni e le garanzie relative all'accesso ai dati personali da parte delle autorità pubbliche. Nella propria valutazione la Commissione deve stabilire se il paese terzo in questione assicura un livello di protezione "sostanzialmente equivalente" a quello garantito all'interno dell'Unione europea (considerando 104 del regolamento (UE) 2016/679). Tale determinazione deve essere valutata facendo riferimento alla legislazione dell'UE, in particolare al regolamento (UE) 2016/679, nonché alla giurisprudenza della Corte di giustizia dell'Unione europea ([3]).

([1]) GU L 119 del 4.5.2016, pag. 1.
([2]) Cfr. considerando 101 del regolamento (UE) 2016/679.
([3]) Cfr., più di recente, la sentenza della Corte di giustizia del 16 luglio 2020, *Facebook Ireland e Schrems* (*Schrems II*), C-311/18, ECLI:EU:C:2020:559.

(4) Come chiarito dalla Corte di giustizia dell'Unione europea, non è richiesto un livello di protezione identico ([4]). In particolare gli strumenti dei quali il paese terzo in questione si avvale per proteggere i dati personali possono essere diversi da quelli attuati all'interno dell'Unione, purché si rivelino efficaci, nella prassi, al fine di assicurare un livello di protezione adeguato ([5]). Il livello di adeguatezza non comporta pertanto una duplicazione pedissequa delle norme dell'Unione. La prova consiste, piuttosto, nel determinare se, con la sostanza dei diritti alla riservatezza e rendendone l'attuazione, l'azionabilità e il controllo effettivi, il sistema estero, nel suo insieme, offre il necessario livello di protezione ([6]). Anche i criteri di riferimento per l'adeguatezza del comitato europeo per la protezione dei dati, che cercano di chiarire ulteriormente tale livello, forniscono indicazioni al riguardo ([7]).

(5) La Commissione ha analizzato attentamente la legge e la prassi coreane. Sulla base delle conclusioni di cui ai considerando da 8 a 208, la Commissione conclude che la Repubblica di Corea garantisce un livello di protezione adeguato per i dati personali trasferiti da un titolare del trattamento o da un responsabile del trattamento nell'Unione ([8]) a soggetti (ad esempio persone fisiche o giuridiche, organizzazioni, enti pubblici) in Corea rientranti nell'ambito di applicazione della legge sulla protezione delle informazioni personali (legge n. 10465 del 29 marzo 2011, modificata da ultimo dalla legge n. 16930 del 4 febbraio 2020). Rientrano in tale contesto tanto i titolari del trattamento quanto i responsabili del trattamento (denominati "*outsourcee*" ([9]), ossia fornitore esterno) ai sensi del regolamento (UE) 2016/679. L'accertamento di adeguatezza non riguarda il trattamento di dati personali per attività missionarie da parte di organizzazioni religiose e per la nomina di candidati da parte di partiti politici, oppure per il trattamento di informazioni personali creditizie ai sensi della legge sulle informazioni creditizie da parte di titolari del trattamento soggetti a vigilanza ad opera della commissione per i servizi finanziari.

(6) Tale conclusione tiene conto delle garanzie supplementari stabilite nella notifica n. 2021-5 (allegato I) così come delle dichiarazioni, delle garanzie e degli impegni ufficiali del governo coreano presentati alla Commissione (allegato II).

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

2. NORME CHE SI APPLICANO AL TRATTAMENTO DI DATI PERSONALI

2.1 Il quadro in materia di protezione dei dati in vigore nella Repubblica di Corea

(8) Il sistema giuridico che disciplina la protezione dei dati e della vita privata in Corea ha le sue radici nella costituzione coreana promulgata il 17 luglio 1948. Sebbene non sia espressamente previsto dalla costituzione, il diritto alla protezione dei dati personali è tuttavia riconosciuto come diritto fondamentale, derivante dai diritti costituzionali alla dignità umana e al perseguimento della felicità (articolo 10), alla tutela della vita privata (articolo 17) e alla riservatezza delle comunicazioni (articolo 18). Ciò è stato confermato tanto dalla Corte suprema ([10]) quanto dalla Corte costituzionale ([11]). Limitazioni dei diritti e delle libertà fondamentali (compreso il diritto alla tutela della vita privata) possono essere imposte soltanto per legge, laddove ciò sia necessario per la sicurezza nazionale o per il mantenimento dell'ordine pubblico per il benessere pubblico e non possa incidere sull'essenza del diritto o della libertà in questione (articolo 37, secondo comma).

([4]) Sentenza della Corte di giustizia del 6 ottobre 2015, *Maximillian Schrems/Data Protection Commissioner* (*Schrems*), C-362/14, ECLI:EU:C:2015:650, punto 73.
([5]) *Schrems*, punto 74.
([6]) Cfr. Comunicazione della Commissione al Parlamento europeo e al Consiglio, Scambio e protezione dei dati personali in un mondo globalizzato, COM(2017) 7 final del 10.1.2017, sezione 3.1, pag. 7.
([7]) Comitato europeo per la protezione dei dati, Criteri di riferimento per l'adeguatezza, WP 254 rev. 01, disponibile al seguente indirizzo: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614108.
([8]) La presente decisione è rilevante ai fini del SEE. L'accordo sullo Spazio economico europeo (accordo SEE) prevede l'estensione del mercato interno dell'Unione europea ai tre Stati del SEE: Islanda, Liechtenstein e Norvegia. La decisione che ha integrato il regolamento (UE) 2016/679 nell'allegato XI dell'accordo SEE è stata adottata dal Comitato misto SEE il 6 luglio 2018 ed è entrata in vigore il 20 luglio 2018. Il regolamento rientra pertanto nell'ambito di applicazione dell'accordo. Ai fini della decisione, i riferimenti all'UE e agli Stati membri dell'UE dovrebbero quindi essere intesi anche come riferimenti agli Stati del SEE.
([9]) Cfr. sezione 2.2.3 della presente decisione.
([10]) Cfr. ad esempio decisione della Corte suprema 2014Da77970, 15 ottobre 2015 (sintesi in inglese disponibile al collegamento "*Lawmaker's disclosure of teacher's trade union member case*" presente all'indirizzo https://www.privacy.go.kr/eng/enforcement_01.do) e giurisprudenza ivi citata, tra cui la decisione 2012Da49933, 24 luglio 2014.
([11]) Cfr. in particolare decisione della Corte costituzionale 99Hun-ma513, 26 maggio 2005 (sintesi in inglese disponibile all'indirizzo http://www.koreanlii.or.kr/w/index.php/99Hun-Ma513?ckattempt=2) e decisione 2014JHun-ma449 2013 Hun-Ba68 (consolidata), 23 dicembre 2015 (sintesi in inglese disponibile al collegamento "*Change of resident Registration number case*" presente all'indirizzo https://www.privacy.go.kr/eng/enforcement_01.do).

(9) Sebbene in più punti la costituzione faccia riferimento ai diritti dei cittadini coreani, la Corte costituzionale ha stabilito che anche i cittadini stranieri godono di diritti fondamentali ([12]). In particolare la Corte ha ritenuto che la tutela della propria dignità e del proprio valore in qualità di essere umano, così come il diritto alla ricerca della felicità, siano diritti spettanti a qualsiasi essere umano, non soltanto ai cittadini coreani ([13]). Inoltre, secondo le dichiarazioni ufficiali rilasciate dal governo coreano ([14]), è generalmente riconosciuto che gli articoli da 12 a 22 della costituzione (che comprendono i diritti in materia di tutela della vita privata) prevedono diritti umani fondamentali ([15]). Sebbene finora non esista alcuna giurisprudenza specifica in merito al diritto alla tutela della vita privata dei cittadini stranieri, il suo fondamento nella protezione della dignità umana e nel perseguimento della felicità sostiene tale conclusione ([16]).

(10) La Corea ha inoltre emanato una serie di leggi in materia di protezione dei dati che forniscono garanzie a tutte le persone fisiche, indipendentemente dalla loro nazionalità ([17]). Ai fini della presente decisione le leggi pertinenti sono:

— la Personal Information Protection Act (PIPA, legge sulla protezione delle informazioni personali);

— la *Act on the Use and Protection of Credit Information* ([18]) (legge sull'utilizzo e sulla protezione delle informazioni creditizie; in appresso: "legge sulle informazioni creditizie" o "CIA");

— la legge sulla tutela della vita privata nelle comunicazioni (legge sulle comunicazioni).

(11) La legge sulla protezione delle informazioni personali fornisce il quadro giuridico generale per la protezione dei dati nella Repubblica di Corea. È integrata 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 della PIPA") che, come la legge sulla protezione delle informazioni personali, è giuridicamente vincolante ed esecutivo.

(12) Inoltre le "notifiche" normative adottate dalla Personal Information Protection Commission (in appresso "PIPC", commissione per la protezione delle informazioni personali) forniscono ulteriori norme in merito all'interpretazione e all'applicazione della legge sulla protezione delle informazioni personali. Sulla base dell'articolo 5 (Obblighi dello Stato) e dell'articolo 14 (Cooperazione internazionale) della legge sulla protezione delle informazioni personali, la PIPC ha adottato la notifica n. 2021-5 del 1º settembre 2020 (come modificata dalla notifica n. 2021-1 del 21 gennaio 2021 e dalla notifica n. 2021-5 del 16 novembre 2021, in appresso "notifica n. 2021-5") sull'interpretazione, sull'applicazione e sull'esecuzione di talune disposizioni di detta legge. Tale notifica fornisce chiarimenti che si applicano a qualsiasi trattamento di dati personali nell'ambito della legge sulla protezione delle informazioni personali, nonché ulteriori garanzie per i dati personali trasferiti in Corea ai sensi della presente decisione. Tale notifica è legalmente vincolante per i titolari del trattamento delle informazioni personali e tanto la PIPC quanto gli organi giurisdizionali possono farla rispettare ([19]). La violazione delle norme contenute in tale notifica comporta la violazione delle pertinenti disposizioni della legge sulla protezione delle informazioni personali che esse integrano. Il contenuto delle garanzie supplementari viene quindi analizzato nel contesto della valutazione degli articoli pertinenti della legge sulla protezione delle informazioni personali. Infine ulteriori orientamenti in merito alla legge sulla protezione delle informazioni personali e al suo decreto di applicazione, che informano l'applicazione e l'esecuzione delle norme in materia di protezione dei dati da parte della PIPC, sono riportati nel manuale e nelle linee guida su tale legge adottati dalla PIPC ([20]).

([12]) Decisione della Corte costituzionale 93 Hun-MA120, 29 dicembre 1994.

([13]) Decisione della Corte costituzionale 99HeonMa494, 29 novembre 2001.

([14]) Cfr. sezione 1.1 dell'allegato II.

([15]) Cfr. anche l'articolo 1 della legge sulla protezione delle informazioni personali che fa espresso riferimento alle "libertà e diritti delle persone fisiche". Più specificamente in tale articolo si afferma che la finalità di tale legge è "prevedere il trattamento e la protezione delle informazioni personali al fine di tutelare [la] libertà e i diritti delle persone fisiche, nonché di realizzare ulteriormente la dignità e il valore delle stesse". Analogamente l'articolo 5, primo comma, della legge sulla protezione delle informazioni personali stabilisce che è responsabilità dello Stato "formulare politiche destinate a prevenire conseguenze dannose derivanti dalla raccolta al di fuori delle finalità previste, dall'abuso e dall'uso improprio di informazioni personali, dalla sorveglianza indiscreta e dal tracciamento, ecc. nonché a migliorare la dignità degli esseri umani e la vita privata delle persone fisiche".

([16]) Inoltre l'articolo 6, secondo comma, della costituzione prevede che lo status di cittadini stranieri sia garantito come prescritto dal diritto e dai trattati internazionali. La Corea è parte di numerosi accordi internazionali che garantiscono il diritto alla tutela della vita privata, 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 del fanciullo (articolo 16).

([17]) Rientrano in tale contesto norme pertinenti per la protezione dei dati personali ma non si applicano in circostanze nelle quali i dati personali sono raccolti nell'Unione e trasferiti in Corea ai sensi del regolamento (UE) 2016/679, ad esempio nel contesto della legge sulla protezione, sull'utilizzo, ecc. delle informazioni relative all'ubicazione.

([18]) La finalità di tale legge è favorire un'attività affidabile in merito alle informazioni creditizie, promuovendo l'utilizzo efficiente e la gestione sistematica delle informazioni creditizie e proteggendo la vita privata dall'uso improprio e dall'abuso delle informazioni creditizie (articolo 1 della legge in questione).

([19]) Ad esempio gli organi giurisdizionali coreani si sono pronunciati in merito al rispetto delle notifiche di regolamentazione in una serie di cause, considerando altresì i titolari del trattamento coreani responsabili di violazioni di una notifica (cfr. ad esempio la decisione della Corte Suprema 2018Da219406, 25 ottobre 2018, nella quale la Corte ha ordinato a un titolare del trattamento di corrispondere un risarcimento a persone fisiche in ragione di danni subiti a causa di una violazione della "Notifica per la norma per le misure destinate a garantire la sicurezza delle informazioni personali"; cfr. anche: decisione della Corte suprema 2018Da219352, 25 ottobre 2018; decisione della Corte Suprema 2011Da24555, 16 maggio 2016; decisione della Corte distrettuale centrale di Seoul 2014Gahap511956, 13 ottobre 2016; decisione della Corte distrettuale centrale di Seoul 2009GahaP43176, 26 gennaio 2010).

([20]) Articolo 12, primo comma, della legge sulla protezione delle informazioni personali.

(13) Inoltre la legge sulle informazioni creditizie stabilisce norme specifiche che si applicano tanto agli operatori commerciali "ordinari" quanto a soggetti specializzati nel settore finanziario quando trattano informazioni creditizie personali, ossia informazioni necessarie per determinare l'affidabilità creditizia delle parti in operazioni finanziarie o commerciali. Tra tali informazioni figurano, in particolare, il nome, i dettagli di contatto, le operazioni finanziarie, il rating di credito, lo stato assicurativo o il saldo di un prestito quando tali informazioni vengono utilizzate per determinare l'affidabilità creditizia di una persona fisica ([21]). Al contrario, laddove tali informazioni vengano utilizzate per altre finalità (ad esempio nel settore delle risorse umane), la legge sulla protezione delle informazioni personali si applica pienamente. Per quanto concerne le disposizioni specifiche in materia di protezione dei dati di cui alla legge sulle informazioni creditizie, la conformità è controllata in parte dalla PIPC (per le organizzazioni commerciali, cfr. articolo 45-3 di tale legge) e in parte dalla commissione per i servizi finanziari ([22]) (per il settore finanziario, comprese le agenzie di rating del credito, le banche, le compagnie di assicurazione, le casse di risparmio, le imprese finanziarie e creditizie specializzate, le imprese finanziarie che offrono servizi di investimento, le società di finanziamento titoli, le cooperative di credito, ecc., cfr. articolo 45, primo comma, della legge sulle informazioni creditizie in combinato disposto con l'articolo 36-2 del decreto di applicazione della CIA e l'articolo 38 della legge sulla commissione per i servizi finanziari). A questo proposito, l'ambito di applicazione della presente decisione è limitato agli operatori commerciali soggetti alla vigilanza della PIPC ([23]). Le norme specifiche della legge sulle informazioni creditizie che si applicano in questo contesto (le norme generali della legge sulla protezione delle informazioni personali si applicano laddove non esistano norme specifiche) sono descritte nella sezione 2.3.11.

2.2 **Ambito di applicazione materiale e personale della legge sulla protezione delle informazioni personali**

(14) Salvo quanto diversamente previsto da altre leggi, la protezione dei dati personali è disciplinata dalla legge sulla protezione delle informazioni personali (articolo 6). L'ambito materiale e personale della sua applicazione è determinato dai concetti definiti di "informazioni personali", "trattamento" e "titolare del trattamento delle informazioni personali".

2.2.1 *Definizione di dati personali*

(15) L'articolo 2, primo comma, della legge sulla protezione delle informazioni personali definisce le informazioni personali come informazioni relative a una persona fisica in vita che la identificano direttamente, ad esempio tramite il suo nome, il suo numero di registrazione come residente o una sua immagine, oppure indirettamente, ossia quando le informazioni che di per sé non possono identificare una determinata persona fisica possono essere combinate facilmente con altre informazioni. Il fatto che le informazioni possano essere combinate "facilmente" dipende dalla ragionevole probabilità di tale combinazione, tenendo conto della possibilità di ottenere altre informazioni nonché del tempo, dei costi e della tecnologia necessari per identificare una persona fisica.

(16) Inoltre, le informazioni pseudonimizzate, ossia le informazioni che non possono identificare una persona fisica specifica senza utilizzarle o combinarle con informazioni supplementari per ripristinarle allo stato originale, sono considerate dati personali ai sensi della legge sulla protezione delle informazioni personali (articolo 2, primo comma, lettera c), di tale legge). Al contrario le informazioni completamente "anonimizzate" sono escluse dall'ambito di applicazione della legge sulla protezione delle informazioni personali (articolo 58-2 di tale legge). Si tratta di informazioni che non sono in grado di identificare una persona fisica specifica, anche se combinate con altre informazioni, tenendo conto dei tempi, dei costi e della tecnologia ragionevolmente necessari per l'identificazione.

(17) Ciò corrisponde all'ambito di applicazione materiale del regolamento (UE) 2016/679 e alle sue nozioni di "dati personali", "pseudonimizzazione" ([24]) e "informazioni anonimizzate" ([25]).

([21]) Articolo 2, primo comma, della legge sulle informazioni creditizie.

([22]) La commissione per i servizi finanziari è l'autorità di vigilanza della Corea per il settore finanziario e in tale veste fa rispettare altresì la legge sulle informazioni creditizie.

([23]) Qualora tale circostanza dovesse mutare in futuro, ad esempio in caso di estensione della competenza giurisdizionale della PIPC a tutti i trattamenti di informazioni creditizie personali nell'ambito della legge sulle informazioni creditizie, si potrebbe considerare di modificare la decisione di adeguatezza per includere anche i soggetti attualmente sottoposti a vigilanza da parte della commissione per i servizi finanziari.

([24]) Nella legge sulla protezione delle informazioni personali, il "trattamento di pseudonimizzazione" è considerato un trattamento condotto con modalità quali la cancellazione parziale di dati personali o la sostituzione parziale o totale dei dati personali affinché non sia possibile riconoscere alcuna persona fisica specifica senza disporre di informazioni aggiuntive (articolo 2, primo e secondo comma). Ciò corrisponde alla definizione di pseudonimizzazione di cui all'articolo 4, punto 5, del regolamento (UE) 2016/679 che fa riferimento al "trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile".

([25]) In particolare il considerando 26 del regolamento (UE) 2016/679 chiarisce che tale atto non si applica alle informazioni anonimizzate, ossia informazioni non correlate a una persona fisica identificata o identificabile. Ciò a sua volta dipende da tutti i mezzi ragionevolmente utilizzabili, dal titolare del trattamento o da un altro soggetto, per identificare la persona fisica direttamente o indirettamente. Per accertare la ragionevole probabilità di utilizzo di tali mezzi, si dovrebbe prendere in considerazione l'insieme dei fattori obiettivi, tra cui i costi e il tempo necessario per l'identificazione, tenendo conto sia delle tecnologie disponibili al momento del trattamento, sia degli sviluppi tecnologici.

2.2.2 *Definizione di trattamento*

(18) La nozione di "trattamento" è definita in maniera ampia nella legge sulla protezione delle informazioni personali come comprendente "la raccolta, la generazione, il collegamento, l'interconnessione, la registrazione, l'archiviazione, la conservazione, l'elaborazione a valore aggiunto, la modifica, il recupero, la produzione, la correzione, il ripristino, l'uso, la fornitura e la divulgazione, nonché la distruzione di informazioni personali e altre attività analoghe" ([26]). Sebbene alcune disposizioni della legge sulla protezione delle informazioni personali facciano riferimento soltanto a tipi specifici di trattamento, quali "uso", "fornitura" o "raccolta" ([27]), la nozione di "uso" è interpretata come comprendente qualsiasi tipo di trattamento diverso dalla "raccolta" o dalla "fornitura" (a terzi). Questa ampia interpretazione del concetto di "uso" assicura quindi che non vi siano lacune nella protezione rispetto ad attività di trattamento specifiche. Il concetto di trattamento corrisponde quindi alla medesima nozione di cui al regolamento (UE) 2016/679.

2.2.3 *Titolare del trattamento delle informazioni personali e fornitore esterno di servizi di trattamento*

(19) La legge sulla protezione delle informazioni personali si applica ai "titolari del trattamento delle informazioni personali" ("titolari del trattamento"). Analogamente a quanto avviene per il regolamento (UE) 2016/679, in tale nozione rientra qualsiasi ente pubblico, qualsiasi persona giuridica, qualsiasi organizzazione o persona fisica che tratta dati personali direttamente o indirettamente per gestire archivi di informazioni personali nel contesto delle loro attività ([28]). In questo contesto il termine "fascicolo di informazioni personali" indica qualsiasi "insieme o serie di informazioni personali disposte od organizzate in modo sistematico sulla base di una determinata norma per consentire un facile accesso alle informazioni personali" (articolo 2, quarto comma, della legge sulla protezione delle informazioni personali) ([29]). Internamente il titolare del trattamento è tenuto a formare le persone coinvolte nel trattamento soggette alla sua direzione, quali dirigenti o dipendenti dell'impresa, nonché a esercitare un controllo e una supervisione adeguati (articolo 28, primo comma, della legge sulla protezione delle informazioni personali).

(20) Obblighi specifici si applicano nel caso in cui un titolare del trattamento (in questo caso il soggetto che esternalizza, *outsourcer*) esternalizzi il trattamento dei dati personali a un soggetto terzo (il fornitore esterno di servizi di trattamento, l'*outsourcee*, in appresso: "il fornitore esterno"). In particolare l'esternalizzazione deve essere disciplinata da un accordo giuridicamente vincolante (solitamente un contratto) ([30]) che definisca l'ambito di applicazione del lavoro esternalizzato, le finalità del trattamento, le garanzie tecniche e gestionali da applicare, il controllo da parte del titolare, la responsabilità (come nel caso di risarcimento di danni cagionati da inadempimento degli obblighi contrattuali) nonché le limitazioni relative a eventuali sub-trattamenti ([31]) (articolo 26, primo e secondo comma, della legge sulla protezione delle informazioni personali in combinato disposto con l'articolo 28, primo comma, del decreto di applicazione) ([32]).

(21) Inoltre il titolare del trattamento deve pubblicare e aggiornare continuamente i dettagli concernenti l'attività esternalizzata e l'identità del fornitore esterno o, nella misura in cui il trattamento esternalizzato riguardi attività di marketing diretto, notificare direttamente alle persone fisiche le informazioni pertinenti (articolo 26, secondo e terzo comma, della legge sulla protezione delle informazioni personali in combinato disposto con l'articolo 28, dal secondo al quinto comma, del decreto di applicazione) ([33]).

(22) Inoltre, ai sensi dell'articolo 26, quarto comma, della legge sulla protezione delle informazioni personali in combinato disposto con l'articolo 28, sesto comma, del decreto di applicazione, il titolare del trattamento è tenuto a "istruire" il fornitore esterno in merito alle misure di sicurezza necessarie, nonché a controllare, anche mediante ispezioni, che rispetti tutti gli obblighi spettanti al titolare del trattamento ai sensi di tale legge ([34]) e quelli derivanti dal contratto di esternalizzazione. Laddove il fornitore esterno causi danni dovuti a una violazione della legge sulla protezione delle informazioni personali, le sue azioni o le sue omissioni saranno attribuite al titolare del trattamento ai fini della responsabilità come se si trattasse di un dipendente (articolo 26, sesto comma, di tale legge).

([26]) Articolo 2, secondo comma, della legge sulla protezione delle informazioni personali.

([27]) Ad esempio gli articoli da 15 a 19 della legge sulla protezione delle informazioni personali fanno riferimento esclusivamente alla raccolta, all'uso e alla fornitura di informazioni personali.

([28]) Articolo 2, quinto comma, della legge sulla protezione delle informazioni. Ai sensi della legge sulla protezione delle informazioni personali, nella nozione di "enti pubblici" rientrano tutti i dipartimenti o tutte le agenzie amministrative centrali e i loro organi affiliati, le amministrazioni locali, le scuole e le imprese pubbliche locali a partecipazione statale, gli organi amministrativi dell'Assemblea nazionale e la magistratura (compresa la Corte costituzionale) (articolo 2, sesto comma, della legge sulla protezione delle informazioni personali in combinato disposto con l'articolo 2 del decreto di applicazione della PIPA).

([29]) Ciò corrisponde all'ambito di applicazione materiale del regolamento (UE) 2016/679. A norma dell'articolo 2, paragrafo 1, del regolamento (UE) 2016/679, il regolamento stesso "si applica al trattamento interamente o parzialmente automatizzato di dati personali e al trattamento non automatizzato di dati personali contenuti in un archivio o destinati a figurarvi". L'articolo 4, punto 6, del regolamento (UE) 2016/679 definisce un "archivio" come "qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati". In linea con ciò, il considerando 15 spiega che "la protezione delle persone fisiche dovrebbe applicarsi sia al trattamento automatizzato che al trattamento manuale dei dati personali, se i dati personali sono contenuti o destinati a essere contenuti in un archivio. Non dovrebbero rientrare nell'ambito di applicazione del presente regolamento i fascicoli o le serie di fascicoli non strutturati secondo criteri specifici, così come le rispettive copertine".

([30]) Cfr. Manuale sulla legge sulla protezione delle informazioni personali, capo III, sezione 2, sull'articolo 26 (pagg. 203-212), che spiega che il primo comma di tale articolo della legge sulla protezione delle informazioni personali fa riferimento ad accordi vincolanti, quali contratti o accordi analoghi.

([31]) Ai sensi dell'articolo 26, quinto comma, della legge sulla protezione delle informazioni personali, al responsabile del trattamento è vietato utilizzare qualsiasi informazione personale al di fuori dell'ambito di applicazione del lavoro esternalizzato oppure fornire informazioni personali a terzi. Il mancato rispetto di tale obbligo può comportare una sanzione penale ai sensi dell'articolo 71, secondo comma, della legge sulla protezione delle informazioni personali.

([32]) Il mancato rispetto di tale requisito può comportare l'irrogazione di una sanzione pecuniaria, cfr. articolo 75, quarto comma, punto 4, della legge sulla protezione delle informazioni personali.

([33]) Il mancato rispetto di tale requisito può comportare l'irrogazione di una sanzione pecuniaria, cfr. articolo 75, secondo comma, punto 1 e articolo 75, quarto comma, punto 5, della legge sulla protezione delle informazioni personali.

([34]) Cfr. anche articolo 26, settimo comma, della legge sulla protezione delle informazioni personali, ai sensi del quale gli articoli da 15 a 25, da 27 a 31, da 33 a 38 e 50 si applicano mutatis mutandis al responsabile del trattamento.

(23) Sebbene la legge sulla protezione delle informazioni personali non utilizzi quindi concetti diversi per "titolari del trattamento" e "responsabili del trattamento", le norme sull'esternalizzazione prevedono obblighi e garanzie sostanzialmente equivalenti a quelli che disciplinano il rapporto tra titolari e responsabili del trattamento ai sensi del regolamento (UE) 2016/679.

2.2.4 *Disposizioni speciali per i fornitori di servizi di informazione e comunicazione*

(24) Sebbene la legge sulla protezione delle informazioni personali si applichi al trattamento di dati personali da parte di qualsiasi titolare del trattamento, talune disposizioni contengono norme specifiche (come *lex specialis*) per il trattamento di dati personali di "utenti" da parte di "fornitori di servizi di informazione e comunicazione" ([35]). La nozione di "utenti" comprende le persone fisiche che utilizzano servizi di informazione e comunicazione (articolo 2, primo comma, punto 4 della legge sulla promozione dell'utilizzo di reti di informazione e comunicazione e della protezione dei dati, in appresso: "legge sulle reti"). Ciò comporta il fatto che la persona fisica utilizzi direttamente servizi di telecomunicazione forniti da un operatore di telecomunicazioni coreano o utilizzi servizi di informazione ([36]) forniti per finalità commerciali (ossia a scopo di lucro) da un soggetto che a sua volta si affida ai servizi di un operatore di telecomunicazioni autorizzato/registrato in Corea ([37]). In entrambi i casi il soggetto vincolato dalle disposizioni specifiche della legge sulla protezione delle informazioni personali è quello che offre un servizio online direttamente a una persona fisica (ossia un utente).

(25) Al contrario, un accertamento di adeguatezza riguarda esclusivamente il livello di protezione offerto ai dati personali trasferiti da un titolare del trattamento/responsabile del trattamento nell'Unione a un soggetto in un paese terzo (nel caso di specie: la Repubblica di Corea). In quest'ultimo scenario, le persone fisiche nell'Unione avranno di norma un rapporto diretto soltanto con l'"esportatore dei dati" nell'Unione e non con alcun fornitore coreano di servizi di informazione e comunicazione ([38]). Di conseguenza le disposizioni specifiche della legge sulla protezione delle informazioni personali relative ai dati personali degli utenti di servizi di informazione e comunicazione si applicheranno, al massimo, soltanto in situazioni limitate ai dati personali trasferiti ai sensi della presente decisione.

2.2.5 *Esenzione da determinate disposizioni della legge sulla protezione delle informazioni personali*

(26) L'articolo 58, primo comma, della legge sulla protezione delle informazioni personali esclude l'applicazione di parte di tale legge (ossia gli articoli da 15 a 57) in relazione a quattro categorie di trattamento di dati ([39]). In particolare non si applicano le parti della legge sulla protezione delle informazioni personali che trattano 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 da parte del *Personal Information Dispute Mediation Committee* (comitato di mediazione per le controversie sulle informazioni personali). Rimangono applicabili altre disposizioni di base della legge sulla protezione delle informazioni personali, in particolare quelle sui principi di protezione dei dati (articolo 3 di tale legge), compresi ad esempio i principi di liceità, indicazione e limitazione delle finalità, minimizzazione dei dati, esattezza e sicurezza dei dati, e sui diritti individuali (di accesso, rettifica, cancellazione e sospensione, cfr. articolo 4 della medesima legge). Inoltre l'articolo 58, quarto comma, della legge sulla protezione delle informazioni personali impone obblighi specifici per tali attività di trattamento, in particolare per quanto concerne la minimizzazione dei dati, la conservazione limitata dei dati, le misure di sicurezza e la gestione dei reclami ([40]). Di conseguenza le persone fisiche potrebbero comunque promuovere reclamo presso la PIPC laddove tali principi e obblighi non fossero rispettati e la PIPC ha il potere di intraprendere misure di esecuzione in caso di non conformità.

([35]) Cfr. in particolare l'articolo 18, secondo comma e il capo VI della legge sulla protezione delle informazioni personali.

([36]) I servizi di informazione comprendono tanto la fornitura di informazioni quanto servizi di intermediazione per la fornitura di informazioni.

([37]) Cfr. articolo 2, primo comma, punto 3 (in combinato disposto con l'articolo 2, primo comma, punti 2 e 4 della legge sulle reti e con l'articolo 2, sesto e ottavo comma, della legge sulle imprese di telecomunicazione.

([38]) Nella misura in cui i fornitori coreani di servizi di informazione e comunicazione avessero un rapporto diretto con persone fisiche nell'UE (offrendo servizi online), ciò potrebbe portare all'applicazione diretta del regolamento (UE) 2016/679, ai sensi dell'articolo 3, paragrafo 2, lettera a).

([39]) L'articolo 58, secondo comma, della legge sulla protezione delle informazioni personali prevede inoltre che gli articoli 15 e 22, l'articolo 27, primo e secondo comma, e gli articoli 34 e 37 non si applichino alle informazioni personali trattate mediante dispositivi visivi per il trattamento di dati installati e gestiti in luoghi aperti. Dato che tale disposizione riguarda l'uso della videosorveglianza in Corea, ossia la raccolta diretta di informazioni personali da persone fisiche in Corea, non è pertinente ai fini della presente decisione che riguarda i trasferimenti di dati personali da titolari/responsabili del trattamento nell'UE verso soggetti in Corea. Inoltre, ai sensi dell'articolo 58, terzo comma, della legge sulla protezione delle informazioni personali, alle informazioni personali trattate per gestire gruppi o associazioni aventi finalità di amicizia (ad esempio club relativi ad hobby) non si applicano l'articolo 15 (raccolta e utilizzo di informazioni personali), l'articolo 30 (obbligo di disporre di una politica resa pubblica in materia di tutela della vita privata) e l'articolo 31 (obbligo di nominare un responsabile della tutela della vita privata). Dato che tali gruppi sono considerati avere natura personale ed essere privi di collegamenti con attività professionali o commerciali, in tale contesto non è richiesta alcuna base giuridica specifica (come il consenso degli interessati) per raccogliere e utilizzare le informazioni delle persone fisiche coinvolte. Tuttavia tutte le altre disposizioni della legge sulla protezione delle informazioni personali (ad esempio minimizzazione dei dati, limitazione delle finalità, liceità del trattamento, sicurezza e diritti individuali) continuano ad applicarsi. Inoltre qualsiasi trattamento delle informazioni personali che vada oltre le finalità di stabilire un gruppo sociale non beneficerebbe di tale eccezione.

([40]) Più specificamente, l'articolo 58, quarto comma, della legge sulla protezione delle informazioni personali prevede l'obbligo di trattare le informazioni personali nella misura minima necessaria per conseguire la finalità prevista, di trattarle per un periodo minimo nonché di adottare le disposizioni necessarie per la gestione sicura e il trattamento appropriato di tali informazioni personali. Rientrano in quest'ultimo caso garanzie tecniche, gestionali e fisiche, nonché misure destinate a garantire il corretto trattamento di reclami individuali.

(27) Innanzitutto l'esenzione parziale riguarda dati personali raccolti ai sensi della legge sulla statistica per il trattamento da parte di enti pubblici. Secondo i chiarimenti ricevuti dal governo coreano, i dati personali trattati in tale contesto riguardano di norma cittadini coreani e potrebbero includere solo eccezionalmente informazioni in merito a stranieri, in particolare nel caso di statistiche sull'ingresso e sull'uscita dal territorio, o sugli investimenti esteri. Tuttavia, anche in tali situazioni, tali dati di norma non vengono trasferiti da titolari/responsabili del trattamento nell'Unione, ma sono piuttosto raccolti direttamente dalle autorità pubbliche in Corea ([41]). Inoltre, in maniera analoga a quanto previsto dal considerando 162 del regolamento (UE) 2016/679, il trattamento di dati ai sensi della legge sulla statistica è soggetta a diverse condizioni e garanzie. In particolare la legge sulla statistica impone obblighi specifici, tali da garantire esattezza, coerenza e imparzialità; garantire la riservatezza delle persone fisiche; proteggere le informazioni dei rispondenti a quesiti statistici anche al fine di impedire che tali informazioni vengano utilizzate per finalità diverse da quelle della compilazione di statistiche e di assoggettare il personale al rispetto di requisiti in materia di riservatezza ([42]). Le autorità pubbliche che elaborano statistiche devono rispettare tra l'altro altresì i principi di minimizzazione dei dati, limitazione della finalità e sicurezza (articolo 3 e articolo 58, quarto comma, della legge sulla protezione delle informazioni personali) e consentire alle persone fisiche di esercitare i loro diritti (di accesso, rettifica, cancellazione e sospensione; cfr. articolo 4 della legge sulla protezione delle informazioni personali). Infine i dati devono essere trattati in forma anonimizzata o pseudonimizzata laddove ciò consenta il soddisfacimento della finalità del trattamento (articolo 3, settimo comma, della legge sulla protezione delle informazioni personali).

(28) In secondo luogo, l'articolo 58, primo comma, della legge sulla protezione delle informazioni personali fa riferimento ai dati personali raccolti o richiesti per finalità di analisi di informazioni in relazione alla sicurezza nazionale. La portata e le conseguenze di tale esenzione parziale sono descritte più in dettaglio nel considerando 149.

(29) In terzo luogo, l'esenzione parziale si applica al trattamento temporaneo di dati personali laddove sia urgentemente necessario per motivi di sicurezza pubblica, compresa la salute pubblica. Questa categoria è interpretata in senso stretto dalla PIPC e, secondo le informazioni ricevute, non è mai stata utilizzata e si applica soltanto nelle emergenze che richiedono un'azione urgente, ad esempio per rintracciare agenti infettivi, oppure per salvare e aiutare le vittime di disastri naturali ([43]). Anche in tali situazioni, l'esenzione parziale riguarda soltanto il trattamento di dati personali per un periodo di tempo limitato allo svolgimento di tale azione. Le situazioni in cui ciò potrebbe applicarsi ai trasferimenti di dati oggetto della presente decisione sono ancora più limitate, data la bassa probabilità che dati personali trasferiti dall'Unione ad operatori coreani siano del tipo che potrebbe rendere il loro successivo trattamento "urgentemente necessario" per tali emergenze.

(30) Infine l'esenzione parziale si applica ai dati personali raccolti o utilizzati dalla stampa, per le attività missionarie di organizzazioni religiose o per la nomina di candidati da parte di partiti politici. L'esenzione si applica soltanto quando i dati personali sono trattati da stampa, organizzazioni religiose o partiti politici per tali finalità specifiche (ad esempio attività giornalistica, attività missionarie e nomina di candidati politici). Laddove tali soggetti trattino dati personali per altre finalità quali la gestione delle risorse umane o l'amministrazione interna, la legge sulla protezione delle informazioni personali si applica integralmente.

(31) In relazione al trattamento dei dati personali da parte della stampa per attività giornalistiche, la legge sull'arbitrato e sui mezzi di ricorso, ecc. per i danni causati da notizie di stampa (in appresso: "legge sulla stampa") ([44]) prevede un bilanciamento tra libertà di espressione e altri diritti (incluso il diritto alla tutela della vita privata). In particolare l'articolo 5 della legge sulla stampa prevede che gli organi di stampa (ossia qualsiasi organizzazione che si occupa di trasmissione radiotelevisiva, qualsiasi quotidiano, periodico o quotidiano online), qualsiasi servizio di cronaca su internet oppure qualsiasi organismo di trasmissione multimediale su internet non possa violare la vita

([41]) A questo proposito, l'articolo 33 della legge sulla statistica impone agli enti pubblici di proteggere le informazioni dei rispondenti a quesiti statistici, anche al fine di impedire che tali informazioni vengano utilizzate per finalità diverse dalla compilazione di statistiche.

([42]) Articolo 2, secondo e terzo comma, articolo 30, secondo comma, articolo 33 e articolo 34 della legge sulla statistica.

([43]) Manuale sulla legge sulla protezione delle informazioni personali, sezione dedicata all'articolo 58.

([44]) Ad esempio l'articolo 4 della legge sulla stampa prevede che le notizie di stampa debbano essere imparziali e obiettive, nell'interesse pubblico, rispettare la dignità e il valore umano e non possano né diffamare altre persone né violare i loro diritti, la morale pubblica o l'etica sociale.

privata di persone fisiche. Se, ciò nonostante, si verifica una violazione della vita privata, quest'ultima deve essere prontamente sanata secondo procedure specifiche previste in tale legge. A questo proposito la legge riconosce alle persone fisiche che subiscono un danno a causa di notizie di stampa una serie di diritti, quali quello di ottenere la pubblicazione di una rettifica di una dichiarazione falsa, una rettifica mediante una dichiarazione in contraddittorio oppure un'ulteriore notizia (laddove una notizia di stampa riguardi asserzioni di reati dai quali la persona fisica viene successivamente assolta) ([45]). I reclami promossi da persone fisiche possono essere risolti direttamente dagli organi di stampa (ricorrendo a un mediatore) ([46]), attraverso la conciliazione o l'arbitrato (dinanzi a una commissione arbitrale specializzata per la stampa) ([47]) oppure adendo gli organi giurisdizionali. Le persone fisiche possono altresì ottenere un risarcimento quando subiscono un danno pecuniario, una violazione di un diritto della personalità o qualsiasi altro disagio emotivo imputabile a un atto illecito degli organi di stampa (per dolo o negligenza) ([48]). Gli organi di stampa sono esentati da responsabilità ai sensi della legge in questione nella misura in cui una notizia di stampa che interferisce con i diritti di una persona fisica non sia contraria ai valori sociali e venga pubblicata con il consenso dell'interessato o nell'interesse pubblico (e qualora vi siano motivi sufficienti per ritenere che tale comunicazione corrisponda al vero) ([49]).

(32) Mentre il trattamento di dati personali da parte della stampa per attività giornalistiche è quindi soggetto a specifiche garanzie che derivano dalla legge sulla stampa, non esistono tali garanzie supplementari che inquadrano il ricorso alle eccezioni per le attività di trattamento da parte di organizzazioni religiose e partiti politici in modo assimilabile agli articoli 85, 89 e 91 del regolamento (UE) 2016/679. La Commissione ritiene pertanto opportuno escludere dall'ambito di applicazione della presente decisione le organizzazioni religiose nella misura in cui trattano dati personali per le loro attività missionarie e i partiti politici nella misura in cui trattano dati personali nel contesto della nomina di candidati.

2.3 **Garanzie, diritti e obblighi**

2.3.1 *Liceità e correttezza del trattamento*

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

(34) Tale principio è sancito dall'articolo 3, primo e secondo comma, della legge sulla protezione delle informazioni personali ed è rafforzato dall'articolo 59 della medesima legge, che vieta il trattamento di dati personali "in modo fraudolento, con mezzi impropri o ingiusti", "senza disporre del potere giuridico" od "oltre i limiti dell'esercizio di un potere adeguato" ([50]). Tali principi generali di liceità del trattamento sono elaborati negli articoli da 15 a 19 della legge sulla protezione delle informazioni personali che stabiliscono le diverse basi giuridiche per il trattamento (raccolta, utilizzo e fornitura a terzi), comprese le circostanze in cui ciò può comportare una variazione di finalità (articolo 18 di tale legge).

([45]) Articoli da 15 a 17 della legge sulla stampa.

([46]) Ogni organo di stampa o multimediale deve disporre di un proprio mediatore per prevenire e porre rimedio a eventuali danni causati da notizie di stampa (ad esempio raccomandando la correzione di notizie di stampa false o lesive della reputazione altrui) (articolo 6 della legge sulla stampa).

([47]) Tale commissione è costituita da 40 a 90 commissari arbitrali, nominati dal ministro della Cultura, dello sport e del turismo tra persone qualificate quali giudici, avvocati, persone che si occupano di informazione o cronaca da almeno 10 anni, o altre persone aventi competenze legate alla stampa. I commissari arbitrali non possono essere allo stesso tempo funzionari pubblici, membri di partiti politici o giornalisti. Ai sensi dell'articolo 8 della legge sulla stampa, i commissari arbitrali devono svolgere le proprie funzioni in modo indipendente e non possono essere soggetti ad alcuna direzione o istruzione in relazione a tali compiti. Inoltre sono in vigore norme specifiche destinate a prevenire conflitti di interesse, ad esempio escludendo singoli commissari dalla trattazione di casi specifici laddove il coniuge o loro parenti siano parte in causa (articolo 10 della legge sulla stampa). La commissione può gestire le controversie attraverso la conciliazione o l'arbitrato, ma può altresì formulare raccomandazioni per porre rimedio a violazioni (sezione 5 della legge sulla stampa).

([48]) Articolo 30 della legge sulla stampa.

([49]) Articolo 5 della legge sulla stampa.

([50]) L'articolo 59 della legge sulla protezione delle informazioni personali vieta a qualsiasi persona "che tratta o abbia mai trattato informazioni personali" di "acquisire informazioni personali od ottenere il consenso al trattamento di informazioni personali mediante frode, mezzi impropri o ingiusti", "divulgare informazioni personali acquisite nel corso dell'attività aziendale oppure fornirle per l'utilizzo da parte di terzi senza autorizzazione" oppure "danneggiare, distruggere, alterare, falsificare o divulgare le informazioni personali di altri senza disporre del potere giuridico corrispondente oppure agendo oltre i limiti dell'esercizio di un potere adeguato". Una violazione di tale divieto può comportare sanzioni penali, cfr. articolo 71, quinto e sesto comma, e articolo 72, secondo comma, della legge sulla protezione delle informazioni personali. L'articolo 70, secondo comma, della legge sulla protezione delle informazioni personali consente inoltre l'imposizione di una sanzione penale per l'ottenimento di informazioni personali trattate da terzi in maniera fraudolenta o con altri mezzi o modalità ingiuste ovvero per averle fornite a terzi per fini di lucro o ingiusti, nonché in caso di concorso in tale condotta od organizzazione della stessa.

(35) Ai sensi dell'articolo 15, primo comma, della legge sulla protezione delle informazioni personali, un titolare del trattamento può raccogliere dati personali (nell'ambito della finalità prevista per la raccolta) soltanto per un numero limitato di fondamenti giuridici. Si tratta nello specifico dei seguenti: 1) il consenso dell'interessato ([51]) (punto 1); 2) la necessità di dare esecuzione eseguire ed attuare un contratto stipulato con l'interessato (punto 4); 3) un'autorizzazione speciale sancita dalla legge o la necessità di adempiere un obbligo sancito dalla legge (punto 2); la necessità ([52]) per un ente pubblico di svolgere i compiti di sua competenza previsti dalla legge; 4) la manifesta necessità di proteggere la vita, l'incolumità o gli interessi patrimoniali dell'interessato o di una terza parte rispetto a un pericolo imminente (soltanto se l'interessato non è in grado di esprimere la sua intenzione o se non è possibile ottenerne il consenso preventivo) (punto 5); 5) la necessità di conseguire l'"interesse giustificabile" del titolare del trattamento se è "manifestamente prevalente" rispetto agli interessi dell'interessato (e soltanto laddove il trattamento comporti una "relazione sostanziale" con l'interesse legittimo e non vada oltre quanto ragionevole) (punto 6) ([53]). Tali fondamenti per il trattamento sono sostanzialmente equivalenti a quelli di cui all'articolo 6 del regolamento (UE) 2016/679, ivi compreso quello relativo all'"interesse giustificabile" che coincide con il motivo del "legittimo interesse" di cui all'articolo 6, paragrafo 1, lettera f), del regolamento (UE) 2016/679.

(36) Una volta raccolti, i dati personali possono essere utilizzati nell'ambito della finalità prevista dalla raccolta (articolo 15, primo comma, della legge sulla protezione delle informazioni personali), oppure "in un ambito ragionevolmente correlato" alla finalità della raccolta, tenendo conto dei possibili svantaggi causati all'interessato e a condizione che siano state adottate le misure di sicurezza necessarie (ad esempio cifratura) (articolo 15, terzo comma, della medesima legge). Al fine di stabilire se la finalità d'uso è "ragionevolmente correlata" alla finalità originaria della raccolta, il decreto di applicazione stabilisce criteri specifici, analoghi a quelli di cui all'articolo 6, paragrafo 4, del regolamento (UE) 2016/679. In particolare deve esserci una notevole attinenza rispetto alla finalità originaria; l'uso aggiuntivo deve essere prevedibile (ad esempio alla luce delle circostanze in cui le informazioni sono state raccolte); e, ove possibile, i dati devono essere pseudonimizzati ([54]). I criteri specifici utilizzati da un titolare del trattamento nel contesto di tale valutazione devono essere comunicati preventivamente nella politica in materia di protezione della vita privata ([55]). Inoltre il responsabile della tutela della vita privata (cfr. considerando 94) è specificamente tenuto a verificare se l'ulteriore utilizzo avviene nel rispetto di tali parametri.

([51]) Il consenso deve essere liberamente prestato, informato, specifico ed espresso in uno dei diversi modi prestabiliti dalla legge. In ogni caso, il consenso non può essere ottenuto con mezzi fraudolenti, impropri o altrimenti ingiusti (articolo 59, primo comma, della legge sulla protezione delle informazioni personali). Innanzitutto, conformemente all'articolo 4, secondo comma, della legge sulla protezione delle informazioni personali, gli interessati hanno il diritto "di prestare o meno il loro consenso" e "di scegliere l'ambito di applicazione del consenso" e dovrebbero esserne informati (articolo 15, secondo comma, articolo 16, secondo e terzo comma, articolo 17, secondo comma e articolo 18, terzo comma, di tale legge). L'articolo 22, quinto comma, della legge sulla protezione delle informazioni personali contiene un'ulteriore tutela che vieta a un titolare del trattamento di negare la fornitura di beni o servizi qualora ciò possa pregiudicare la libera scelta della persona fisica di concedere il consenso. Rientrano in tale contesto situazioni nelle quali soltanto alcuni tipi di trattamento richiedono il consenso (mentre altri si basano su un contratto) e che riguardano anche l'ulteriore trattamento dei dati personali raccolti nel contesto della fornitura di beni o servizi. In secondo luogo, ai sensi dell'articolo 15, secondo comma, dell'articolo 17, secondo e terzo comma, e dell'articolo 18, terzo comma, della legge sulla protezione delle informazioni personali, quando richiede il consenso il titolare del trattamento deve informare l'interessato in merito ai "determinati dettagli" dei dati personali in questione (ad esempio il fatto che riguardano dati sensibili, cfr. articolo 17, secondo comma, punto 2, lettera a), del decreto di applicazione della PIPA), alle finalità del trattamento, al periodo di conservazione e all'eventuale destinatario dei dati. Qualsiasi richiesta di questo tipo deve essere presentata "in modo esplicitamente riconoscibile" che distingua le questioni che richiedono il consenso da altre questioni (articolo 22, dal primo al quarto comma, della legge sulla protezione delle informazioni personali). In terzo luogo, l'articolo 17, primo comma, punti da 1 a 6 del decreto di applicazione della PIPA stabilisce le modalità specifiche attraverso le quali un titolare del trattamento deve ottenere il consenso, come il consenso scritto con firma dell'interessato o il consenso tramite messaggio di posta elettronica (di ritorno). Sebbene la legge sulla protezione delle informazioni personali non riconosca specificamente alle persone fisiche un diritto generale di revoca del consenso, le persone godono invece del diritto di ottenere la sospensione del trattamento dei dati relativi alla loro persona, che quando esercitato determina la cessazione del trattamento e la cancellazione dei dati (cfr. considerando 78 sul diritto alla sospensione).

([52]) Secondo le informazioni ricevute dalla PIPC, gli enti pubblici possono fare affidamento su questo motivo soltanto se il trattamento delle informazioni personali è inevitabile, ossia deve essere impossibile o irragionevolmente difficile per l'ente in questione svolgere le proprie funzioni senza trattare i dati.

([53]) L'articolo 39-3 della legge sulla protezione delle informazioni personali impone obblighi specifici (più rigorosi) ai fornitori di servizi di informazione e comunicazione per quanto riguarda la raccolta e l'uso delle informazioni personali dei loro utenti. In particolare ciò comporta l'ottenimento da parte del fornitore del consenso dell'utente, dopo aver fornito informazioni sulla finalità della raccolta/dell'uso, sulle categorie di informazioni personali da raccogliere e sul periodo per il quale le informazioni saranno trattate (articolo 39-3, primo comma, della legge sulla protezione delle informazioni personali). Lo stesso vale se uno qualsiasi di tali aspetti cambia. Il mancato ottenimento del consenso alla raccolta delle informazioni è soggetto a sanzioni penali (articolo 71, quarto e quinto comma, della legge sulla protezione delle informazioni personali). In via eccezionale, le informazioni personali degli utenti possono essere raccolte o utilizzate da fornitori di servizi di informazione e comunicazione senza previo consenso. Ciò si verifica: 1) quando è manifestamente difficile ottenere il normale consenso per le informazioni personali necessarie per l'esecuzione del contratto che disciplina la fornitura di servizi di comunicazione e informazione per motivi economici e tecnologici (ad esempio quando i dati personali vengono creati inevitabilmente nel processo di esecuzione di un contratto, come le informazioni di fatturazione, i registri di accesso e le registrazioni dei pagamenti); 2) quando è necessario per il regolamento di oneri in seguito alla fornitura di servizi di informazione e comunicazione; o 3) laddove consentito da altre leggi (ad esempio, l'articolo 21, primo comma, punto 6, della legge sulla protezione dei consumatori nel commercio elettronico prevede che gli operatori economici possano raccogliere informazioni personali sui tutori legali di un minore per confermare se è stato ottenuto un consenso valido a nome del minore) (articolo 39-3, secondo comma, della legge sulla protezione delle informazioni personali). In ogni caso i fornitori di servizi di informazione e comunicazione non possono rifiutarsi di fornire servizi semplicemente perché l'utente non fornisce informazioni personali in misura maggiore al minimo richiesto (ossia le informazioni necessarie per svolgere gli elementi essenziali del servizio in questione), cfr. articolo 39-3, terzo comma, della legge sulla protezione delle informazioni personali.

([54]) Cfr. articolo 14-2 del decreto di applicazione della PIPA.

([55]) Articolo 14-2, secondo comma, del decreto di applicazione della PIPA.

(37) Norme simili (ma un po' più rigorose) si applicano alla fornitura di dati a terzi. Ai sensi dell'articolo 17, primo comma, della legge sulla protezione delle informazioni personali, la fornitura di dati personali a terzi è consentita sulla base del consenso ([56]) o, nel rispetto delle finalità della raccolta, quando le informazioni sono state raccolte in ragione di uno dei fondamenti giuridici di cui all'articolo 15, primo comma, punti 2, 3 e 5, della legge sulla protezione delle informazioni personali. Ciò esclude in particolare qualsiasi divulgazione basata sull'"interesse giustificabile" del titolare del trattamento. Inoltre, l'articolo 17, quarto comma, della legge sulla protezione delle informazioni personali consente la messa a disposizione di terzi "in un ambito di applicazione ragionevolmente correlato" alla finalità della raccolta, sempre tenendo conto dei possibili svantaggi causati all'interessato e purché siano state adottate le necessarie misure di sicurezza (come la cifratura). Ai fini della valutazione dell'eventualità che la messa a disposizione in questione rientri nell'ambito di applicazione ragionevolmente correlato alla finalità della raccolta e nell'applicazione delle medesime garanzie (ossia rispetto della trasparenza attraverso la politica in materia di tutela della vita privata e il coinvolgimento del responsabile della tutela della vita privata) occorre tenere conto dei medesimi fattori descritti nel considerando 36.

(38) La ricezione di dati personali dall'Unione da parte di un titolare del trattamento coreano dei dati è considerata una "raccolta" ai sensi dell'articolo 15 della legge sulla protezione delle informazioni personali. La notifica n. 2021-5 (sezione I dell'allegato I della presente decisione) chiarisce che la finalità per la quale i dati sono stati trasferiti dal soggetto UE interessato costituisce la finalità della raccolta per il titolare del trattamento coreano dei dati. Di conseguenza i titolari coreani del trattamento dei dati che ricevono dati personali dall'Unione sono in linea di principio tenuti a trattare tali informazioni nell'ambito della finalità del trasferimento, ai sensi dell'articolo 17 della legge sulla protezione delle informazioni personali.

(39) Si applicano limitazioni speciali nel caso in cui il titolare del trattamento cerchi di utilizzare i dati personali o di fornirli a terzi per una finalità diversa da quella della raccolta ([57]). Ai sensi dell'articolo 18, secondo comma, della legge sulla protezione delle informazioni personali, un titolare del trattamento privato può eccezionalmente ([58]) utilizzare i dati personali o fornirli a terzi per una finalità diversa: 1) sulla base del consenso aggiuntivo (ossia distinto) dell'interessato; 2) laddove ciò sia previsto da disposizioni speciali di legge; o 3) laddove ciò sia manifestamente necessario per la protezione della vita, dell'incolumità o degli interessi patrimoniali dell'interessato o di terzi rispetto a un pericolo imminente (soltanto se l'interessato non è in grado di esprimere la sua intenzione o se non è possibile ottenerne il consenso preventivo) ([59]).

(40) Anche gli enti pubblici possono utilizzare i dati personali o fornirli a terzi per una finalità diversa in determinate situazioni. Tra tali casi figurano situazioni nelle quali sarebbe altrimenti impossibile per tali enti svolgere i propri compiti statutari come prescritto dalla legge, previa autorizzazione della PIPC. Inoltre gli enti pubblici possono fornire dati personali ad un'altra autorità o a un organo giurisdizionale, laddove ciò sia necessario per l'accertamento e il perseguimento di reati o per un rinvio a giudizio; affinché un organo giurisdizionale possa svolgere le sue funzioni in relazione a procedimenti giudiziari in corso; oppure per l'esecuzione di una sanzione penale oppure di un'ordinanza cautelare o di custodia cautelare ([60]). Gli enti pubblici possono altresì fornire dati personali a un governo straniero o a un'organizzazione internazionale per adempiere a un obbligo giuridico derivante da un trattato o da una convenzione internazionale, nel qual caso devono altresì rispettare i requisiti in materia di trasferimenti transfrontalieri di dati (cfr. considerando 90).

(41) I principi di liceità e correttezza del trattamento trovano quindi attuazione nel quadro giuridico coreano in maniera sostanzialmente equivalente a quanto previsto dal regolamento (UE) 2016/679, consentendo il trattamento soltanto sulla base di motivi legittimi e chiaramente definiti. Inoltre, in tutti i casi menzionati, il trattamento è consentito soltanto se non è suscettibile di "violare ingiustamente" gli interessi dell'interessato o di un terzo, il che richiede un bilanciamento degli interessi. Inoltre l'articolo 18, quinto comma, della legge sulla protezione delle informazioni personali prescrive garanzie supplementari quando il titolare del trattamento fornisce i dati personali a terzi, che possono comprendere una richiesta di limitazione delle finalità e delle modalità di utilizzo o la messa in atto di misure di sicurezza specifiche. La terza parte in questione è a sua volta tenuta ad attuare le misure richieste.

([56]) Violazioni dell'articolo 17, primo comma, punto 1, della legge sulla protezione delle informazioni personali possono comportare l'irrogazione di sanzioni penali (articolo 71, primo comma, della medesima legge).

([57]) La "finalità prevista" è la finalità per la quale le informazioni sono state raccolte. Ad esempio, quando le informazioni sono raccolte sulla base del consenso dell'interessato, la finalità prevista è la finalità comunicata alla persona fisica ai sensi dell'articolo 15, secondo comma, della legge sulla protezione delle informazioni personali.

([58]) Cfr. articolo 18, primo comma, della legge sulla protezione delle informazioni personali. Violazioni dell'articolo 18, primo e secondo comma, possono comportare l'irrogazione di sanzioni penali (articolo 71, primo comma, della medesima legge).

([59]) L'utilizzo di informazioni personali o la loro fornitura a terzi da parte di fornitori di servizi di informazione e comunicazione per una finalità diversa da quella originaria possono avvenire soltanto per i motivi di cui all'articolo 18, secondo comma, punti 1 e 2, della legge sulla protezione delle informazioni personali (ossia laddove si ottenga un consenso aggiuntivo o laddove esistano disposizioni di legge speciali). Cfr. articolo 18, secondo comma, della legge sulla protezione delle informazioni personali.

([60]) Fatto salvo il caso in cui il trattamento sia necessario per l'accertamento di reati, il rinvio a giudizio e il perseguimento, gli enti pubblici che utilizzano dati personali o li forniscono a terzi per una finalità diversa da quella della raccolta (ad esempio laddove ciò sia specificamente consentito dalla legge o necessario per dare esecuzione a un trattato) sono tenuti a pubblicare i fondamenti giuridici per il trattamento, la sua finalità e la sua portata sul proprio sito web o sulla gazzetta ufficiale e a conservare registrazioni in merito (articolo 18, quarto comma, della legge sulla protezione delle informazioni personali in combinato disposto con l'articolo 15 del decreto di applicazione della medesima legge).

(42) Infine l'articolo 28-2 della legge sulla protezione delle informazioni personali consente il (l'ulteriore) trattamento di informazioni pseudonimizzate senza il consenso dell'interessato per finalità di compilazione di statistiche, di ricerca scientifica ([61]) e di archiviazione nell'interesse pubblico, fatte salve garanzie specifiche. Analogamente al regolamento (UE) 2016/679 ([62]), la legge sulla protezione delle informazioni personali facilita pertanto il (l'ulteriore) trattamento di dati personali per tali finalità in un quadro che prevede garanzie adeguate a tutela dei diritti delle persone fisiche. Anziché fare affidamento sulla pseudonimizzazione come possibile garanzia, la legge sulla protezione delle informazioni personali la impone come prerequisito ai fini dello svolgimento di determinate attività di trattamento per finalità di compilazione di statistiche, di ricerca scientifica e di archiviazione nell'interesse pubblico (come ad esempio per poter trattare i dati senza consenso o per combinare serie diverse di dati).

(43) La legge sulla protezione delle informazioni personali impone inoltre una serie di garanzie specifiche, in particolare in termini di misure tecniche e organizzative necessarie, di conservazione di registri, di limitazioni alla condivisione dei dati e di gestione dei possibili rischi di reidentificazione. La combinazione delle varie garanzie di cui ai considerando da 44 a 48 assicura che il trattamento dei dati personali in questo contesto sia soggetto a tutele sostanzialmente equivalenti rispetto a quelle che sarebbero richieste ai sensi del regolamento (UE) 2016/679.

(44) Innanzitutto e come aspetto ancora più importante, l'articolo 28-5, primo comma, della legge sulla protezione delle informazioni personali vieta il trattamento di informazioni pseudonimizzate con la finalità di identificare una determinata persona fisica. Se durante il trattamento di informazioni pseudonimizzate vengono comunque generate informazioni che potrebbero identificare una persona fisica, il titolare del trattamento deve immediatamente sospendere il trattamento e distruggere tali informazioni (articolo 28-5, secondo comma, della legge sulla protezione delle informazioni personali). Il mancato rispetto di tali disposizioni è soggetto a sanzioni amministrative pecuniarie e costituisce reato ([63]). Ciò significa che, anche in quelle situazioni in cui sarebbe *praticamente* possibile identificare nuovamente la persona fisica, tale reidentificazione è *giuridicamente* vietata.

(45) In secondo luogo, quando si trattano (ulteriormente) informazioni pseudonimizzate per tali finalità, il titolare del trattamento è tenuto a mettere in atto misure tecnologiche, gestionali e fisiche specifiche per assicurare la sicurezza delle informazioni (compresa l'archiviazione e la gestione separate delle informazioni necessarie per ripristinare le informazioni pseudonimizzate al loro stato originale) ([64]). Occorre inoltre conservare registrazioni delle informazioni pseudonimizzate trattate, della finalità del trattamento, della cronologia di utilizzo e di eventuali destinatari terzi (articolo 29-5, secondo comma, del decreto di applicazione della PIPA).

(46) In terzo e ultimo luogo, la legge sulla protezione delle informazioni personali prevede garanzie specifiche per impedire l'identificazione di persone fisiche da parte di terzi nel caso in cui le informazioni vengano condivise. In particolare, quando forniscono informazioni pseudonimizzate a terzi per finalità di compilazione di statistiche, di ricerca scientifica o di archiviazione nell'interesse pubblico, i titolari del trattamento non possono includere informazioni che potrebbero essere utilizzate per identificare una persona fisica specifica (articolo 28-2, secondo comma, della legge sulla protezione delle informazioni personali) ([65]).

(47) In particolare sebbene consenta la combinazione di informazioni pseudonimizzate (trattate da titolari del trattamento diversi) per finalità di compilazione di statistiche, di ricerca scientifica o di archiviazione nel pubblico interesse, la legge sulla protezione delle informazioni personali riserva tale facoltà a istituzioni specializzate dotate di sistemi specifici di sicurezza (articolo 28-3, primo comma, della legge sulla protezione delle informazioni personali) ([66]). Nel presentare una richiesta di combinazione di dati pseudonimizzati, un titolare del trattamento

([61]) La ricerca scientifica è definita dall'articolo 2, ottavo comma, della legge sulla protezione delle informazioni personali come la "ricerca che applica metodi scientifici, quali sviluppo e la dimostrazione di tecnologia, la ricerca fondamentale, la ricerca applicata e la ricerca finanziata da soggetti privati". Tali categorie corrispondono a quelle di cui al considerando 159 del regolamento (UE) 2016/679.

([62]) Cfr. articolo 5, paragrafo 1, lettera b), e articolo 89, paragrafi 1 e 2, nonché considerando 50 e 157 del regolamento (UE) 2016/679.

([63]) Cfr. articolo 28-6, primo comma, articolo 71, terzo e quarto comma e articolo 75, secondo comma, punto 4-4, della legge sulla protezione delle informazioni personali.

([64]) Articolo 28-4 della legge sulla protezione delle informazioni personali e 29-5 del decreto di applicazione di tale legge. L'inosservanza di tale obbligo è passibile di sanzioni amministrative e penali, cfr. articolo 73, primo comma, e articolo 75, secondo comma, punto 6, della legge sulla protezione delle informazioni personali.

([65]) La violazione di tali requisiti può comportare l'irrogazione di sanzioni penali (articolo 71, secondo comma, della legge sulla protezione delle informazioni personali). La PIPC ha iniziato immediatamente a far rispettare tali nuove norme, ad esempio nella sua decisione del 28 aprile 2021, in cui ha imposto una sanzione pecuniaria e misure correttive nei confronti di un'impresa che, tra le altre violazioni della legge sulla protezione delle informazioni personali, non ha rispettato il requisito di cui all'articolo 28-2, secondo comma, di tale legge. Cfr. https://www.pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS074&mCode=C020010000&nttId=7298&fbclid=IwAR3SKcMQi6G5pR9k4I7j6GNXtc8aBVDOwcURevvvzQtYI7AS40UKYXoOXo8.

([66]) Per poter ottenere la designazione di istituzione specializzata (una "agenzia specializzata nella combinazione di dati"), occorre presentare una domanda alla PIPC unitamente a documenti giustificativi che dettaglino tra l'altro le strutture e le attrezzature utilizzate per combinare in modo sicuro i dati pseudonimizzati e confermino che il richiedente impiega almeno tre membri del personale a tempo pieno aventi qualifiche o esperienza in materia di protezione dei dati personali (articolo 29-2, primo e secondo comma, del decreto di applicazione della PIPA). Requisiti dettagliati, ad esempio per quanto riguarda le qualifiche del personale, le strutture disponibili, le misure di sicurezza, le politiche e le procedure interne, nonché i requisiti finanziari sono stabiliti nella notifica 2020-9 della PIPC sulla combinazione e sul rilascio di informazioni pseudonimizzate (allegato I). Una designazione in veste di agenzia specializzata nella combinazione di dati può essere revocata dalla PIPC (dopo aver tenuto un'audizione) per determinati motivi, ad esempio se l'agenzia non soddisfa più le norme di sicurezza richieste per la designazione o se si è verificata una violazione dei dati nel contesto della combinazione di dati (articolo 29-2, quinto e sesto comma, del decreto di applicazione della PIPA). La PIPC deve pubblicare ogni designazione (o revoca della designazione) di un'agenzia specializzata nella combinazione di dati (articolo 29-2, settimo comma, del decreto di applicazione della PIPA).

deve fornire documentazione, tra l'altro, in merito ai dati da combinare, alla finalità di tale combinazione, nonché alle misure di sicurezza proposte per il trattamento dei dati combinati ([67]). Per consentire tale combinazione, il titolare del trattamento deve inviare i dati da combinare all'istituzione specializzata e fornire una "chiave di combinazione" (ossia le informazioni che sono state utilizzate per la pseudonimizzazione) all'Agenzia coreana per la sicurezza e internet ([68]). Quest'ultimo genera "dati di collegamento delle chiavi di combinazione" (che consentono di collegare le chiavi di combinazione di richiedenti diversi al fine di ottenere la combinazione delle serie di dati) e li fornisce all'istituzione specializzata ([69]).

(48) Il titolare del trattamento che richiede la combinazione può analizzare le informazioni combinate presso la sede dell'istituzione specializzata, in uno spazio al quale si applicano misure di sicurezza tecniche, fisiche e amministrative specifiche (articolo 29-3 del decreto di applicazione della PIPA). I titolari del trattamento che forniscono una serie di dati per tale combinazione possono portare i dati combinati al di fuori dell'istituto specializzato soltanto a seguito di un'ulteriore pseudonimizzazione o anonimizzazione dei dati combinati e con l'approvazione di tale istituto (articolo 28-3, secondo comma, della legge sulla protezione delle informazioni personali) ([70]). Nel valutare se concedere o meno tale approvazione, l'istituzione valuterà il legame tra i dati combinati e la finalità del trattamento e se è stato predisposto un piano di sicurezza specifico per l'uso di tali dati ([71]). L'esportazione delle informazioni combinate al di fuori dell'istituzione non sarà consentita se le informazioni contengono dati che consentirebbero l'identificazione di una persona fisica ([72]). Infine la combinazione e il rilascio di dati pseudonimizzati da parte dell'istituzione specializzata è controllata dalla PIPC (articolo 29-4, terzo comma, del decreto di applicazione della PIPA).

2.3.2 *Trattamento di categorie particolari di dati personali*

(49) Garanzie specifiche dovrebbero essere applicate al trattamento di "categorie particolari" di dati.

(50) La legge sulla protezione delle informazioni personali contiene norme specifiche per quanto concerne il trattamento di dati sensibili ([73]), definiti come dati personali che rivelano informazioni in merito all'ideologia, alle convinzioni personali, all'adesione o alla revoca di adesione da un sindacato o un partito politico, alle opinioni politiche, alla salute e alla vita sessuale di una persona fisica, nonché altre informazioni personali suscettibili di ledere "in maniera significativa" la vita privata dell'interessato e che sono state prescritte essere informazioni sensibili mediante decreto presidenziale ([74]). Secondo i chiarimenti ricevuti dalla PIPC, il concetto di vita sessuale è interpretato comprendere anche l'orientamento o le preferenze sessuali di una persona fisica ([75]). L'articolo 18 del decreto di applicazione aggiunge inoltre ulteriori categorie all'ambito dei dati sensibili, in particolare le informazioni sul DNA acquisite mediante prove genetiche e i dati che costituiscono un casellario giudiziario. La recente modifica del decreto di applicazione della PIPA ha ampliato ulteriormente la nozione di dati sensibili, includendo anche i dati personali che rivelano l'origine razziale o etnica e le informazioni biometriche ([76]). A seguito di tale modifica, la nozione di dati sensibili ai sensi della legge sulla protezione delle informazioni personali è sostanzialmente equivalente a quella di cui all'articolo 9 del regolamento (UE) 2016/679.

(51) Ai sensi dell'articolo 23, primo comma, della legge sulla protezione delle informazioni personali e analogamente a quanto previsto dall'articolo 9, paragrafo 1, del regolamento (UE) 2016/679, il trattamento dei dati sensibili è in genere vietato, fatto salvo il caso in cui si applichi una delle eccezioni elencate ([77]). Queste ultime limitano il

([67]) Articolo 8, primo e secondo comma, della notifica 2020-9 sulla combinazione e sul rilascio di informazioni pseudonimizzate.
([68]) Articolo 2, terzo e sesto comma, e articolo 9, primo comma, della notifica 2020-9 sulla combinazione e sul rilascio di informazioni pseudonimizzate.
([69]) Articolo 2, quarto comma, e articolo 9, secondo e terzo comma, della notifica 2020-9 sulla combinazione e sul rilascio di informazioni pseudonimizzate. L'istituzione specializzata deve distruggere i dati di collegamento delle chiavi di combinazione immediatamente dopo la combinazione (articolo 9, quarto comma, di tale notifica).
([70]) Le violazioni dei requisiti per la combinazione di serie di dati possono portare all'irrogazione di sanzioni penali (articolo 71, comma 4-2, della legge sulla protezione delle informazioni personali). Cfr. anche articolo 29-2, quarto comma, del decreto di applicazione della PIPA.
([71]) La procedura per approvare un rilascio di dati combinati è stabilita nell'articolo 11 della notifica 2020-9 sulla combinazione e sul rilascio di informazioni pseudonimizzate. In particolare l'istituzione specializzata deve istituire un "comitato di riesame del rilascio", costituito da membri aventi conoscenze ed esperienze sostanziali in materia di protezione dei dati.
([72]) Articolo 29-2, quarto comma, del decreto di applicazione della PIPA e articolo 11 della notifica n. 2020-9.
([73]) La necessità di prevedere tutele specifiche per il trattamento di dati sensibili, quali i dati relativi alla salute o al comportamento sessuale, è stata riconosciuta anche dalla Corte costituzionale coreana, cfr. decisione della Corte costituzionale HunMa 1139, 31 maggio 2007.
([74]) Articolo 23, primo comma, della legge sulla protezione delle informazioni personali.
([75]) Cfr. anche Manuale sulla legge sulla protezione delle informazioni personali, capo III, sezione 2, dedicata all'articolo 23 (pagg. 157-164).
([76]) Ossia informazioni personali risultanti da un trattamento tecnico specifico di dati relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica al fine di identificarla in maniera univoca.
([77]) Il mancato rispetto di tali requisiti può comportare sanzioni ai sensi dell'articolo 71, terzo comma, della legge sulla protezione delle informazioni personali.

trattamento ai casi in cui il titolare del trattamento informi l'interessato ai sensi degli articoli 15 e 17 della legge sulla protezione delle informazioni personali e ottenga un consenso distinto (ossia separato da quello per il trattamento di altri dati personali) oppure laddove il trattamento sia richiesto o consentito per legge. Le autorità pubbliche possono altresì trattare, sulla base dei fondamenti giuridici di cui sopra, informazioni biometriche, informazioni sul DNA acquisite da prove genetiche, informazioni personali che rivelano l'origine razziale o etnica e i dati che costituiscono un casellario giudiziario che sono disponibili in via esclusiva a tali autorità (ad esempio ove necessario per l'accertamento di reati o se necessario affinché un organo giurisdizionale possa procedere con una causa) ([78]). Di conseguenza le basi giuridiche disponibili per il trattamento di dati sensibili sono più limitate rispetto ad altri tipi di dati personali e sono persino più restrittive nel diritto coreano rispetto a quanto non lo siano ai sensi dell'articolo 9, paragrafo 2, del regolamento (UE) 2016/679.

(52) Inoltre, l'articolo 23, secondo comma, della legge sulla protezione delle informazioni personali (il cui mancato rispetto può comportare sanzioni ([79])) sottolinea la particolare importanza di garantire un'adeguata sicurezza durante il trattamento di dati sensibili affinché "non possano andare persi, venire rubati, divulgati, falsificati, alterati o danneggiati". Sebbene si tratti di un requisito generale ai sensi dell'articolo 29 della legge sulla protezione delle informazioni personali, l'articolo 3, quarto comma, chiarisce che il livello di sicurezza deve essere adattato al tipo di dati personali trattati, il che significa che occorre prendere in considerazione i rischi specifici connessi al trattamento di dati sensibili. Inoltre il trattamento dei dati deve essere sempre effettuato "in modo da ridurre al minimo la possibilità di violazione" della vita privata dell'interessato e, se possibile, "in forma anonima" (articolo 3, sesto e settimo comma, della legge sulla protezione delle informazioni personali). Tali requisiti sono particolarmente rilevanti laddove il trattamento riguardi dati sensibili.

2.3.3 *Limitazione delle finalità*

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

(54) Tale principio è garantito dall'articolo 3, primo e secondo comma, della legge sulla protezione delle informazioni personali, secondo il quale il titolare del trattamento "specifica ed esplicita" la finalità del trattamento, tratta i dati personali in maniera adeguata rispetto a tale finalità e non li utilizza al di fuori di tale finalità. Il principio generale della limitazione delle finalità trova conferma anche nell'articolo 15, primo comma, nell'articolo 18, primo comma, nell'articolo 19 nonché, per i responsabili del trattamento (i cosiddetti *outsourcee*, ossia i fornitori esterni), nell'articolo 26, primo comma, punto 1 e nell'articolo 26, quinto e settimo comma, della legge sulla protezione delle informazioni personali. In particolare i dati personali possono in linea di principio essere utilizzati e forniti a terzi soltanto nell'ambito della finalità per la quale sono stati raccolti (articolo 15, primo comma, e articolo 17, primo comma, punto 2). Il trattamento per una finalità compatibile, ossia "all'interno di un contesto ragionevolmente connesso alla finalità iniziale della raccolta", può aver luogo soltanto se ciò non reca pregiudizio agli interessati coinvolti e se sono adottate le misure di sicurezza necessarie (quali la cifratura) (articolo 15, terzo comma, e articolo 17, quarto comma, della legge sulla protezione delle informazioni personali). Al fine di stabilire se l'ulteriore trattamento venga svolto per una finalità compatibile, il decreto di applicazione della PIPA elenca criteri specifici simili a quelli previsti dall'articolo 6, quarto comma, del regolamento (UE) 2016/679, cfr. considerando 36.

(55) Come spiegato nel considerando 38, la finalità della raccolta nel caso in cui i titolari del trattamento coreani ricevano dati personali dall'Unione è la finalità per la quale i dati vengono trasferiti. Una modifica della finalità da parte del titolare del trattamento è consentita soltanto in via eccezionale, in casi specifici (elencati) (articolo 18, secondo comma, punto 1-3, della legge sulla protezione delle informazioni personali, cfr. anche considerando 39). Nella misura in cui una modifica di finalità è autorizzata dalla legge, tali leggi devono a loro volta rispettare il diritto fondamentale alla tutela della vita privata e alla protezione dei dati, nonché i principi di necessità e proporzionalità stabiliti nella costituzione coreana. Inoltre, l'articolo 18, secondo e quinto comma, della legge sulla protezione delle informazioni personali prevede garanzie supplementari, in particolare il requisito secondo il quale tale modifica di finalità non deve "violare ingiustamente l'interesse di un interessato", rendendo quindi sempre necessario un bilanciamento degli interessi. Ciò prevede un livello di protezione sostanzialmente equivalente a quello di cui all'articolo 5, primo comma, lettera b), e di cui all'articolo 6, in combinato disposto con il considerando 50, del regolamento (UE) 2016/679.

2.3.4 *Esattezza e minimizzazione dei dati*

(56) I dati personali dovrebbero essere esatti e, se necessario, dovrebbero essere aggiornati. Dovrebbero essere adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati.

([78]) L'articolo 18 del decreto di applicazione della PIPA prevede che le categorie di dati ivi elencate siano escluse dall'applicazione della disposizione di cui all'articolo 23, primo comma, della legge sulla protezione delle informazioni personali quando sono trattate da un ente pubblico ai sensi dell'articolo 18, secondo comma 2, punto 5-9, di quest'ultima legge.

([79]) Cfr. articolo 73, primo comma, e articolo 75, secondo comma, punto 6, della legge sulla protezione delle informazioni personali.

(57) Il principio di esattezza è analogamente riconosciuto all'articolo 3, terzo comma, della legge sulla protezione delle informazioni personali, che prescrive che i dati personali siano "esatti, completi e aggiornati nella misura necessaria in relazione alle finalità" per le quali sono trattati. La minimizzazione dei dati è prescritta ai sensi dell'articolo 3, primo e sesto comma, e dell'articolo 16, primo comma, della legge sulla protezione delle informazioni personali, che stabiliscono che il titolare del trattamento raccoglie dati personali (soltanto) "nella misura minima necessaria" per la finalità prevista e che a lui spetta l'onere della prova al riguardo. Laddove sia possibile adempiere la finalità della raccolta elaborando le informazioni in forma anonima, i titolari del trattamento dovrebbero sforzarsi di farlo (articolo 3, settimo comma, della legge sulla protezione delle informazioni personali).

2.3.5 *Limitazione della conservazione*

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

(59) Il principio della limitazione della conservazione è analogamente previsto dall'articolo 21, primo comma, della legge sulla protezione delle informazioni personali ([80]), che impone al titolare del trattamento di "distruggere" ([81]) i dati personali senza indugio una volta conseguita la finalità del trattamento o alla scadenza del periodo di conservazione (a seconda di quale circostanza si verifichi per prima), fatto salvo il caso in cui una conservazione ulteriore sia obbligatoria per legge ([82]). In quest'ultimo caso, i dati personali pertinenti "sono archiviati e gestiti separatamente dalle altre informazioni personali" (articolo 21, terzo comma, della legge sulla protezione delle informazioni personali).

(60) L'articolo 21, primo comma, della legge sulla protezione delle informazioni personali non si applica quando i dati pseudonimizzati vengono trattati per finalità statistiche, di ricerca scientifica o di archiviazione nell'interesse pubblico ([83]). Al fine di assicurare il principio della conservazione limitata dei dati anche in questo caso, la notifica 2021-5 impone ai titolari del trattamento di anonimizzare le informazioni conformemente all'articolo 58-2 della legge sulla protezione delle informazioni personali laddove i dati non vengano distrutti una volta conseguita la finalità specifica perseguita dal trattamento ([84]).

2.3.6 *Sicurezza dei dati*

(61) I dati personali dovrebbero essere trattati in maniera da garantirne la sicurezza, compresa la protezione da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali. A tal fine gli operatori economici dovrebbero adottare misure tecniche od organizzative per proteggere i dati personali da possibili minacce. Tali misure dovrebbero essere valutate tenendo conto dello stato dell'arte, dei costi correlati e della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi per i diritti delle persone fisiche.

(62) Un principio analogo di sicurezza è stabilito all'articolo 3, quarto comma, della legge sulla protezione delle informazioni personali, che impone ai titolari del trattamento di gestire le informazioni personali "in maniera sicura secondo i metodi, le tipologie, ecc. di trattamento delle informazioni personali, tenendo conto della possibilità di violazione dei diritti dell'interessato e della gravità dei rischi pertinenti". Inoltre il titolare del trattamento "tratta le informazioni personali in maniera tale da ridurre al minimo la possibilità di violare la vita privata di un interessato" e, in tale contesto, si sforza di trattare i dati personali in formato anonimizzato o pseudonimizzato, se possibile (articolo 3, sesto e settimo comma, della legge sulla protezione delle informazioni personali).

(63) Tali requisiti generali sono ulteriormente elaborati all'articolo 29 della legge sulla protezione delle informazioni personali, ai sensi del quale ciascun titolare del trattamento "adotta misure tecniche, gestionali e fisiche, quali definire un piano di gestione interno e conservare registrazioni di accesso, ecc., che sono necessarie per assicurare

([80]) Articolo 8 (in combinato disposto con l'articolo 8-2 del decreto di applicazione) e articolo 11 (in combinato disposto con l'articolo 12, secondo comma, del decreto di applicazione).

([81]) Sulle modalità di distruzione delle informazioni personali cfr. articolo 16 del decreto di applicazione della PIPA. L'articolo 21, secondo comma, della legge sulla protezione delle informazioni personali chiarisce che ciò comprende "misure necessarie per bloccare il recupero e il riutilizzo".

([82]) Il mancato rispetto di tali requisiti può comportare sanzioni penali (articolo 73, comma 1-2, della legge sulla protezione delle informazioni personali). L'articolo 39-6 della legge sulla protezione delle informazioni personali impone un requisito ulteriore ai fornitori di servizi di informazione e comunicazione che sono tenuti ad eliminare le informazioni personali degli utenti che non utilizzano i servizi offerti di informazione e di comunicazione da almeno un anno (fatto salvo il caso in cui una conservazione ulteriore sia prevista dalla legge o richiesta dalla persona fisica). Le persone fisiche devono essere informate della prevista cancellazione delle loro informazioni 30 giorni prima della scadenza del termine di un anno (articolo 39-6, secondo comma, della legge sulla protezione delle informazioni personali e articolo 48-5, terzo comma, del decreto di applicazione di tale legge). Se per legge è richiesta una conservazione ulteriore, i dati conservati devono essere archiviati separatamente dalle altre informazioni degli utenti e possono essere utilizzati o divulgati soltanto in conformità con tale legge (articolo 48-5, primo e secondo comma, del decreto di applicazione della PIPA).

([83]) Articolo 28-7 della legge sulla protezione delle informazioni personali.

([84]) Notifica 2021-5 (allegato I), sezione 4.

la sicurezza come prescritto mediante decreto presidenziale affinché le informazioni personali non possano andare perse, venire rubate, divulgate, falsificate, alterate o danneggiate". L'articolo 30, primo comma, del decreto di applicazione della PIPA specifica tali misure facendo riferimento a: 1) la formulazione e l'attuazione di un piano di gestione interno per il trattamento sicuro dei dati personali; 2) controlli e limitazioni all'accesso; 3) l'adozione di tecnologia di cifratura per archiviare e trasmettere in maniera sicura i dati personali; 4) registrazioni di accessi informatici; 5) programmi di sicurezza; e 6) misure fisiche quali un sistema sicuro di archiviazione o blocco ([85]).

(64) Si applicano inoltre obblighi specifici qualora si verifichi una violazione dei dati (articolo 34 della legge sulla protezione delle informazioni personali in combinato disposto con gli articoli 39 e 40 del decreto di applicazione di tale legge) ([86]). In particolare il titolare del trattamento è tenuto a notificare senza indugio agli interessati lesi i dettagli della violazione ([87]), comprese informazioni in merito a contromisure (obbligatorie) adottate dal titolare del trattamento e alle azioni che gli interessati possono intraprendere per ridurre al minimo il rischio di danni (articolo 34, primo e secondo comma, della legge sulla protezione delle informazioni personali) ([88]). Laddove la violazione dei dati riguardi almeno 1 000 interessati, il titolare del trattamento deve segnalare senza indugio la violazione dei dati e le contromisure adottate anche alla PIPC e all'Agenzia coreana per la sicurezza e internet, che possono fornire assistenza tecnica (articolo 34, terzo comma, della legge sulla protezione delle informazioni personali in combinato disposto con l'articolo 39 del decreto di applicazione di tale legge). I titolari del trattamento rispondono per eventuali danni derivanti da violazioni dei dati, in conformità con le disposizioni del codice civile sulla responsabilità civile (cfr. altresì sezione 2.5 sul ricorso) ([89]).

(65) Nel rispettare i suoi obblighi in materia di sicurezza, il titolare del trattamento deve essere assistito da un responsabile della tutela della vita privata, i cui compiti comprendono, tra gli altri, la creazione di un sistema di controllo interno destinato a "prevenire la divulgazione, l'abuso e l'uso improprio di informazioni personali" (articolo 31, secondo comma, punto 4, della legge sulla protezione delle informazioni personali). Inoltre il titolare del trattamento è tenuto a condurre "un controllo e una supervisione adeguati" sui membri del suo personale che trattano dati personali, anche per quanto concerne la loro gestione sicura; ciò comprende la formazione necessaria ("istruzione") dei dipendenti (articolo 28, primo e secondo comma, della legge sulla protezione delle informazioni personali). Infine, in caso di sub-trattamento, il titolare del trattamento deve imporre dei requisiti al fornitore esterno, tra l'altro per quanto concerne la gestione sicura dei dati personali ("garanzie tecniche e gestionali"), e deve controllare le corrispondenti modalità di attuazione tramite ispezioni (articolo 26, primo e quarto comma, PIPA in combinato disposto con l'articolo 28, primo comma, punti 3 e 4 e con l'articolo 28, sesto comma, del decreto di applicazione di tale legge).

2.3.7 *Trasparenza*

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

([85]) Per quanto riguarda il trattamento dei dati personali da parte di fornitori di servizi di informazione e comunicazione, l'articolo 39-5 della legge sulla protezione delle informazioni personali prevede esplicitamente che il numero di persone che gestiscono le informazioni personali degli utenti debba essere limitato al minimo. Inoltre i fornitori di servizi di informazione e di comunicazione devono assicurare che le informazioni personali degli utenti non siano esposte al pubblico attraverso la rete di informazioni e comunicazioni (articolo 39-10, primo comma, della legge sulla protezione delle informazioni personali). Le informazioni esposte devono essere cancellate o bloccate su richiesta della PIPC (articolo 39-10, secondo comma, della legge sulla protezione delle informazioni personali). Più in generale, i fornitori di servizi di informazione e di comunicazione (e terzi che ricevono dati personali degli utenti) sono tenuti a rispettare obblighi di sicurezza aggiuntivi, specificati nell'articolo 48-2, del decreto di applicazione della PIPA, ad esempio lo sviluppo e l'attuazione di un piano di gestione interno per quanto riguarda le misure di sicurezza, le misure per assicurare il controllo degli accessi, la cifratura, l'uso di software per rilevare programmi dannosi, ecc.

([86]) Esiste inoltre un divieto generale di danneggiare, distruggere, alterare, falsificare o divulgare informazioni personali senza disporre della legittimazione giuridica, cfr. articolo 59, terzo comma, della legge sulla protezione delle informazioni personali.

([87]) L'obbligo di notifica alla persona fisica non si applica nella misura in cui si verifica una violazione dei dati rispetto a informazioni pseudonimizzate trattate per finalità di compilazione di statistiche, ricerca scientifica o archiviazione nell'interesse pubblico (articolo 28-7 della legge sulla protezione delle informazioni personali, che prevede un'esenzione dall'articolo 34, primo comma, e dall'articolo 39-4 della medesima legge). Garantire la notifica individuale imporrebbe al titolare del trattamento in questione di identificare le persone fisiche a partire dalla serie di dati pseudonimizzata, una circostanza che è espressamente vietata ai sensi dell'articolo 28-5 della legge sulla protezione delle informazioni personali. Tuttavia l'obbligo generale di notifica (alla PIPC) di una violazione dei dati si applica comunque.

([88]) I requisiti in materia di notifica, comprese le rispettive tempistiche e la possibilità di attuare una notifica "per fasi", sono specificati più in dettaglio all'articolo 40 del decreto di applicazione di tale legge. Norme più rigorose si applicano ai fornitori di servizi di informazione e comunicazione che sono tenuti a notificare all'interessato e alla PIPC entro 24 ore dal momento in cui si rendono conto del fatto che le informazioni personali sono state perse, rubate o divulgate (articolo 39-4, primo comma, della legge sulla protezione delle informazioni personali). La presente notifica deve comprendere i dettagli delle informazioni personali che sono state divulgate, il momento in cui ciò è accaduto, le misure che possono essere intraprese dall'utente, le misure di risposta adottate dal fornitore e i dettagli di contatto del dipartimento al quale l'utente può rivolgere domande (articolo 39-4, primo comma, punto 1-5, della legge sulla protezione delle informazioni personali). In presenza di un motivo giustificabile, ad esempio la non disponibilità di dettagli di contatto dell'utente, si può ricorrere ad altri mezzi di notifica, ad esempio rendendo le informazioni pubblicamente disponibili su un sito web (articolo 39-4, primo comma, della legge sulla protezione delle informazioni personali in combinato disposto con l'articolo 48-4, quarto comma, e seguenti del decreto di applicazione di tale legge). In tal caso, la PIPC deve essere informata dei motivi (articolo 34-4, terzo comma, della legge sulla protezione delle informazioni personali).

([89]) Cfr. ad esempio decisioni della Corte suprema 2011Da59834, 2011Da59858 e 2011Da59841, 26 dicembre 2012. Una sintesi in inglese è disponibile al seguente indirizzo: http://library.scourt.go.kr/SCLIB_data/decision/9-69%202012.12.26.2011Da59834.htm.

(67) Il sistema coreano garantisce tale aspetto in diversi modi. A parte il diritto all'informazione ai sensi dell'articolo 4, primo comma (in generale) e dell'articolo 20, primo comma (per i dati personali raccolti da terzi), della legge sulla protezione delle informazioni personali, nonché il diritto di accesso ai sensi dell'articolo 35 della medesima legge, la legge in questione prevede un requisito generale di trasparenza per quanto concerne la finalità del trattamento (articolo 3, primo comma, della medesima legge) e requisiti specifici di trasparenza nel caso in cui il trattamento sia basato sul consenso (articolo 15, secondo comma, articolo 17, secondo comma, e articolo 18, terzo comma, della medesima legge) ([90]). Inoltre l'articolo 20, secondo comma, della legge sulla protezione delle informazioni personali impone a determinati titolari del trattamento (coloro il cui trattamento supera determinate soglie ([91])) di notificare all'interessato quali dati personali hanno ricevuto da una terza parte della fonte di informazione, la finalità del trattamento e il diritto dell'interessato di richiedere una sospensione del trattamento, fatto salvo il caso in cui tale notifica si riveli impossibile in ragione della mancanza di informazioni di contatto. Si applicano eccezioni per determinati archivi di dati personali detenuti da autorità pubbliche, in particolare archivi che contengono dati trattati per finalità di sicurezza nazionale, altri interessi nazionali particolarmente importanti ("gravi") o finalità di contrasto penale oppure nei casi in cui la notifica può minacciare la vita o ledere l'incolumità di un'altra persona oppure ledere ingiustamente gli interessi patrimoniali e di altra natura di qualsiasi altra persona, tuttavia soltanto quando l'interesse pubblico e quello privato in gioco sono "manifestamente superiori" ai diritti degli interessati in questione (articolo 20, quarto comma, della legge sulla protezione delle informazioni personali). Ciò richiede un bilanciamento degli interessi.

(68) L'articolo 3, quinto comma, della legge sulla protezione delle informazioni personali prescrive inoltre che i titolari del trattamento debbano rendere pubblica la loro politica in materia di tutela della vita privata (e altre questioni relative al trattamento dei dati personali). Tale requisito è ulteriormente specificato nell'articolo 30 della legge sulla protezione delle informazioni personali in combinato disposto con l'articolo 31 del decreto di applicazione di tale legge. Secondo tali disposizioni, la politica pubblica in materia di tutela della vita privata deve tra le altre cose comprendere: 1) i tipi di dati personali trattati; 2) la finalità del trattamento; 3) il periodo di conservazione; 4) se i dati personali sono forniti a una terza parte ([92]); 5) qualsiasi sub-trattamento; 6) informazioni sui diritti dell'interessato e sulle modalità per il loro esercizio; e 7) informazioni di contatto (compreso il nome del responsabile della tutela della vita privata o il dipartimento interno competente per l'assicurazione del rispetto delle norme in materia di protezione dei dati e di gestione dei reclami). La politica in materia di tutela della vita privata deve essere resa accessibile al pubblico in modo tale che gli interessati "possano riconoscerla facilmente" (articolo 30, secondo comma, della legge sulla protezione delle informazioni personali) ([93]) e deve essere costantemente aggiornata (articolo 31, secondo comma, del decreto di applicazione della PIPA).

(69) Gli enti pubblici sono soggetti all'obbligo aggiuntivo di registrare in particolare le seguenti informazioni presso la PIPC: 1) il nome dell'ente pubblico; 2) i motivi e le finalità per il trattamento dei fascicoli di dati personali; 3) i dettagli dei dati personali registrati; 4) il metodo di trattamento; 5) il periodo di conservazione; 6) il numero di interessati i cui dati personali vengono conservati; 7) il dipartimento che gestisce le richieste degli interessati e 8) i destinatari dei dati personali quando i dati vengono forniti in maniera regolare o ripetitiva (articolo 32, primo comma, della legge sulla protezione delle informazioni personali) ([94]). I fascicoli dei dati personali registrati sono resi pubblici dalla PIPC e anche gli enti pubblici devono farvi riferimento nella loro politica in materia di tutela della vita privata (articolo 30, primo comma, e articolo 32, quarto comma, della legge sulla protezione delle informazioni personali).

(70) Al fine di migliorare la trasparenza per gli interessati nell'Unione i cui dati personali vengono trasferiti in Corea ai sensi della presente decisione, la sezione 3, punti i) e ii), della notifica 2021-5 (allegato I) impone requisiti supplementari in materia di trasparenza. Innanzitutto nel ricevere dati personali dall'Unione ai sensi della presente decisione i titolari coreani del trattamento devono notificare agli interessati in questione senza indebito ritardo (e in ogni caso non oltre un mese dal trasferimento) il nome e i dettagli di contatto dei soggetti che effettuano il

([90]) In particolare, quando le informazioni personali vengono trattate con il consenso di una persona fisica, il titolare del trattamento deve informare tale persona della finalità del trattamento, fornirle dettagli sulle informazioni da trattare, sul destinatario delle informazioni, sul periodo di conservazione e di utilizzo delle informazioni, nonché in merito al fatto che la persona fisica ha il diritto di negare il consenso (e qualsiasi svantaggio che possa derivarne).

([91]) Ai sensi dell'articolo 15-2, primo comma, del decreto di applicazione della PIPA, ciò riguarda i titolari del trattamento che trattano informazioni sensibili di almeno 50 000 interessati o informazioni personali "normali" di almeno 1 milione di interessati. L'articolo 15-2, secondo comma, del decreto di applicazione della PIPA definisce i metodi e i tempi per la notifica, mentre l'articolo 15-2, terzo comma stabilisce l'obbligo di tenere determinati registri. Inoltre norme specifiche si applicano a determinate categorie di fornitori di servizi di informazione e comunicazione (quelli che hanno generato almeno 10 miliardi di KRW di entrate dalle vendite durante l'anno precedente o quelli che conservano/gestiscono i dati personali di almeno un milione di utenti al giorno in media i tre mesi antecedenti la fine dell'anno precedente), i quali sono tenuti a notificare periodicamente agli utenti la cronologia di utilizzo delle loro informazioni personali, fatto salvo il caso in cui ciò si dimostri impossibile in ragione della mancanza di informazioni di contatto (articolo 39-8 della legge sulla protezione delle informazioni personali e articolo 48-6 del decreto di applicazione di tale legge della PIPA).

([92]) Secondo le informazioni ricevute dal governo coreano, ciò comporta l'obbligo di elencare singolarmente i destinatari nella politica in materia di tutela della vita privata.

([93]) Ulteriori modalità sono definite all'articolo 31, terzo comma, del decreto di applicazione della PIPA.

([94]) L'obbligo di registrazione non si applica a determinati tipi di fascicoli di informazioni personali ad esempio quelli che registrano questioni relative a sicurezza nazionale, segreti diplomatici, indagini criminali, azioni giuridiche, pene, indagini su reati in materia di tassazione oppure i fascicoli che si riferiscono esclusivamente all'esecuzione di un lavoro interno (articolo 32, secondo comma, della legge sulla protezione delle informazioni personali).

trasferimento e che ricevono le informazioni, i dati personali (o le categorie di dati personali) trasferiti, la finalità della raccolta da parte del titolare del trattamento coreano, del periodo di conservazione e dei diritti disponibili ai sensi della legge sulla protezione delle informazioni personali. In secondo luogo, quando forniscono a terzi dati personali ricevuti dall'Unione sulla base della presente decisione, i titolari del trattamento devono informare gli interessati tra l'altro in merito al destinatario, ai dati personali o alle categorie di dati personali oggetto della fornitura, il paese al quale i dati sono forniti (ove applicabile), nonché i diritti disponibili ai sensi della legge sulla protezione delle informazioni personali ([95]). In questo modo la notifica garantisce che le persone fisiche dell'UE continuino ad essere informate in merito ai titolari specifici del trattamento che trattano le loro informazioni e siano in grado di esercitare i loro diritti nei confronti dei soggetti pertinenti.

(71) La sezione 3, punto iii), della notifica (allegato I) consente alcune eccezioni limitate e qualificate a tali obblighi aggiuntivi in materia di trasparenza che sono essenzialmente equivalenti a quelle previste dal regolamento (UE) 2016/679. In particolare la notifica degli interessati nell'Unione non è richiesta: 1) quando e purché sianecessario limitare la notifica per determinate ragioni di interesse pubblico (ad esempio, se le informazioni vengono trattate per finalità di sicurezza nazionale o indagini penali in corso), nella misura in cui tali obiettivi di interesse pubblico prevalgano in maniera manifesta sui diritti dell'interessato; 2) l'interessato dispone già delle informazioni; 3) se e fintantoché la notifica può minacciare la vita o ledere l'incolumità della persona fisica o di un'altra persona o violare ingiustamente gli interessi patrimoniali di un'altra persona, laddove tali diritti o interessi prevalgano manifestamente sui diritti dell'interessato; oppure 4) quando non siano disponibili dettagli di contatto per le persone fisiche interessate o sarebbe necessario uno sforzo sproporzionato per inviare loro una notifica. Ai fini della determinazione della possibilità o meno di contattare l'interessato o dell'eventualità che ciò implichi o meno sforzi eccessivi, è opportuno prendere in considerazione la possibilità di cooperare con l'esportatore di dati nell'UE.

(72) Le norme di cui ai considerando da 67 a 71 assicurano pertanto un livello sostanzialmente equivalente di protezione in materia di trasparenza rispetto a quanto previsto dal regolamento (UE) 2016/679.

2.3.8 *Diritti delle persone fisiche*

(73) Gli interessati dovrebbero disporre di determinati diritti azionabili nei confronti del titolare del trattamento o del responsabile del trattamento, in particolare il diritto di accesso ai dati, il diritto di rettifica, il diritto di opporsi al trattamento e il diritto di far cancellare i dati. Allo stesso tempo tali diritti possono essere soggetti a limitazioni, nella misura in cui tali limitazioni sono necessarie e proporzionate per salvaguardare obiettivi importanti di interesse pubblico generale.

(74) Ai sensi dell'articolo 3, quinto comma, della legge sulla protezione delle informazioni personali, il titolare del trattamento deve garantire i diritti degli interessati di cui all'articolo 4 della medesima legge e come ulteriormente specificato negli articoli da 35 a 37, 39 e 39-2 della medesima legge.

(75) Innanzitutto alle persone fisiche spettano diritti all'informazione e all'accesso. Quando il titolare del trattamento ha raccolto dati personali da una terza parte (come accadrà sempre nel caso in cui i dati vengano trasferiti dall'Unione), in generale gli interessati hanno il diritto di ricevere informazioni in merito a: 1) la "fonte" dei dati personali raccolti (ossia il soggetto cedente); 2) la finalità del trattamento; e 3) il fatto che l'interessato ha il diritto di richiedere la sospensione del trattamento (articolo 20, primo comma, della legge sulla protezione delle informazioni personali). Si applicano eccezioni limitate, ossia laddove tale notifica possa minacciare la vita o compromettere l'incolumità di un'altra persona oppure "leda ingiustamente gli interessi patrimoniali e di altra natura" di un'altra persona, ma soltanto quando tali interessi di terzi "prevalgano esplicitamente" sui diritti dell'interessato (articolo 20, quarto comma, punto 2, della legge sulla protezione delle informazioni personali).

(76) Inoltre l'articolo 35, primo e terzo comma, della legge sulla protezione delle informazioni personali in combinato disposto con l'articolo 41, quarto comma, del decreto di applicazione della medesima legge riconosce agli interessati il diritto di accesso alle loro informazioni personali ([96]). Il diritto di accesso riguarda la conferma del trattamento, informazioni in merito al tipo di dati trattati, la finalità del trattamento, il periodo di conservazione, nonché qualsiasi divulgazione a terzi e la fornitura di una copia delle informazioni personali trattate (articolo 4, terzo comma, della legge sulla protezione delle informazioni personali in combinato disposto con

([95]) Notifica 2021-5, sezione 3, punto ii) (allegato I).

([96]) Ai sensi dell'articolo 35, terzo comma, della legge sulla protezione delle informazioni personali in combinato disposto con l'articolo 42, secondo comma, del decreto di applicazione di tale legge, il titolare del trattamento può rinviare l'accesso per una "buona causa" (ossia per motivi giustificati, ad esempio qualora sia necessario più tempo per valutare se tale accesso può essere concesso), ma deve notificare all'interessato tale giustificazione entro 10 giorni e fornire informazioni sulle modalità di impugnazione di tale decisione; non appena non sussiste più il motivo per tale rinvio, è necessario concedere l'accesso.

l'articolo 41, primo comma, del decreto di applicazione di tale legge) ([97]). L'accesso può essere limitato (accesso parziale) ([98]) o negato soltanto se ciò è previsto dalla legge ([99]), nei casi in cui potrebbe minacciare la vita o ledere l'incolumità di una terza parte oppure una violazione ingiustificata di interessi patrimoniali o di altra natura di un'altra persona (articolo 35, quarto comma, della legge sulla protezione delle informazioni personali) ([100]). Quest'ultima disposizione implica che si dovrebbe stabilire un equilibrio tra i diritti e le libertà protetti dalla costituzione della persona fisica, da un lato, e quelli di altre persone, dall'altro. Quando l'accesso è limitato o negato, il titolare del trattamento deve notificarne i motivi all'interessato e le modalità per impugnare tale decisione (articolo 41, quinto comma, e articolo 42, secondo comma, del decreto di applicazione della PIPA).

(77) In secondo luogo gli interessati hanno il diritto alla correzione o alla cancellazione ([101]) dei loro dati personali "salvo quanto diversamente specificamente stabilito da altre leggi" (articolo 36, primo e secondo comma, della legge sulla protezione delle informazioni personali) ([102]). Al ricevimento di una richiesta, il titolare del trattamento deve esaminare la questione senza indugio, adottare le misure necessarie ([103]) e notificare l'interessato entro 10 giorni; qualora non sia possibile accogliere la richiesta, tale requisito di notifica riguarda i motivi del rifiuto e le modalità di impugnazione (cfr. articolo 36, quarto comma, della legge sulla protezione delle informazioni personali in combinato disposto con l'articolo 43, terzo comma, del decreto di applicazione di tale legge) ([104]).

(78) Infine gli interessati hanno il diritto alla sospensione del trattamento dei loro dati personali, senza indugio ([105]), fatto salvo il caso in cui si applichi una delle eccezioni enumerate (articolo 37, primo e secondo comma, della legge sulla protezione delle informazioni personali) ([106]). Il titolare del trattamento può respingere la richiesta: 1) se ciò è specificamente autorizzato dalla legge o necessario ("inevitabile") per rispettare obblighi giuridici; 2) laddove la sospensione potrebbe minacciare la vita o ledere l'incolumità di una terza parte oppure causare una violazione ingiustificata di interessi patrimoniali e di altra natura di un'altra persona; 3) laddove sarebbe impossibile per un ente pubblico assolvere la sua funzione come prescritto dalla legge in assenza del trattamento delle informazioni in questione; oppure 4) laddove l'interessato non risolva espressamente il contratto sottostante stipulato con il titolare del trattamento anche se sarebbe impossibile dare esecuzione al contratto in assenza di tale trattamento dei dati. In questo caso il titolare del trattamento deve notificare senza indugio all'interessato i motivi del rifiuto e le modalità di impugnazione (articolo 37, secondo comma, della legge sulla protezione delle informazioni personali in combinato disposto con l'articolo 44, secondo comma, del decreto di applicazione di tale legge). Conformemente all'articolo 37, quarto comma, della legge sulla protezione delle informazioni personali, il titolare del trattamento deve, senza indugio, "adottare misure necessarie compresa la distruzione delle informazioni personali pertinenti" quando si conforma alla richiesta di sospensione ([107]).

(79) Il diritto alla sospensione si applica anche nei casi in cui i dati personali vengono utilizzati per finalità di marketing diretto, ossia per promuovere beni o servizi oppure sollecitarne l'acquisto. Inoltre tale ulteriore trattamento richiede in genere il consenso specifico (aggiuntivo) dell'interessato (cfr. articolo 15, primo comma, punto 1, e articolo 17, secondo comma, punto 1, della legge sulla protezione delle informazioni personali) ([108]). Quando richiede tale consenso, il titolare del trattamento deve informare l'interessato in particolare in merito

([97]) L'accesso alle informazioni personali trattate da un ente pubblico può essere ottenuto rivolgendosi direttamente all'ente in questione oppure indirettamente presentando una richiesta alla PIPC, che a sua volta deve trasmetterla senza indugio (articolo 35, secondo comma, della legge sulla protezione delle informazioni personali e articolo 41, terzo comma, del decreto di applicazione di tale legge).

([98]) Ai sensi dell'articolo 42, primo comma, del decreto di applicazione della PIPA, il titolare del trattamento è tenuto a concedere un accesso parziale laddove almeno parte delle informazioni non è interessata dai motivi del rifiuto.

([99]) Tale legge deve a sua volta rispettare il diritto fondamentale della tutela della vita privata e della protezione dei dati, nonché i principi di necessità e proporzionalità stabiliti nella costituzione coreana.

([100]) Gli enti pubblici possono inoltre rifiutarsi di concedere l'accesso qualora ciò causerebbe gravi difficoltà nello svolgimento di determinate funzioni, comprese revisioni in corso oppure l'imposizione, la raccolta o il rimborso di imposte (articolo 35, quarto comma, della legge sulla protezione delle informazioni personali).

([101]) In questo caso, il titolare del trattamento deve adottare misure destinate a prevenire il recupero delle informazioni personali, cfr. articolo 36, terzo comma, della legge sulla protezione delle informazioni personali.

([102]) Tali leggi devono soddisfare i requisiti della costituzione secondo i quali si può limitare un diritto fondamentale soltanto se ciò è necessario per la sicurezza nazionale o il mantenimento dell'ordine pubblico per il benessere pubblico e non è suscettibile di incidere sull'essenza della libertà o del diritto (articolo 37, secondo comma, della costituzione).

([103]) L'articolo 43, secondo comma, del decreto di applicazione della PIPA prevede una procedura speciale nel caso in cui il titolare del trattamento tratti fascicoli di informazioni personali forniti da un altro titolare del trattamento.

([104]) La mancata adozione delle misure necessarie per correggere o cancellare le informazioni personali e l'uso continuato o la fornitura di tali informazioni a una terza parte possono determinare l'irrogazione di sanzioni penali (articolo 73, secondo comma, della legge sulla protezione delle informazioni personali).

([105]) Ai sensi dell'articolo 44, secondo comma, del decreto di applicazione della PIPA, il titolare del trattamento deve informare l'interessato in merito al fatto di aver debitamente sospeso il trattamento entro 10 giorni dal ricevimento della richiesta.

([106]) Per quanto concerne gli enti pubblici, il diritto alla sospensione del trattamento può essere esercitato in relazione alle informazioni contenute nei fascicoli di informazioni personali registrati (articolo 37 in combinato disposto con l'articolo 32 della legge sulla protezione delle informazioni personali). Tale registrazione non è richiesta in un numero limitato di circostanze, ad esempio quando i fascicoli di informazioni personali riguardano la sicurezza nazionale, indagini in merito a reati, relazioni diplomatiche, ecc. (articolo 32, secondo comma, della legge sulla protezione delle informazioni personali).

([107]) La mancata sospensione del trattamento può determinare sanzioni penali (articolo 73, terzo comma, della legge sulla protezione delle informazioni personali).

([108]) Il comitato di mediazione per le controversie (cfr. considerando 133) ha affrontato diversi casi in cui le persone fisiche si sono lamentate in merito all'uso dei loro dati per finalità di marketing diretto in assenza di consenso, che hanno portato ad esempio al versamento di un risarcimento e alla cancellazione dei dati personali da parte del titolare del trattamento corrispondente (cfr. ad esempio comitato di mediazione per le controversie 20R10-024(2020.11.18), 20R08-015(2020.8.28), 20R07-031(2020.9.1)).

all'uso previsto dei dati per finalità di marketing diretto, ossia in merito al fatto che i) può essere contattato per la promozione di beni o servizi o per sollecitarne l'acquisto, in un "modo esplicitamente riconoscibile" (articolo 22, secondo e quarto comma, della legge sulla protezione delle informazioni personali in combinato disposto con l'articolo 17, secondo comma, punto 1, del decreto di applicazione di tale legge).

(80) Al fine di facilitare l'esercizio dei diritti individuali, il titolare del trattamento deve stabilire procedure dedicate ed annunciarle pubblicamente (articolo 38, quarto comma, della legge sulla protezione delle informazioni personali) ([109]). Ciò comprende procedure destinate ad aumentare le obiezioni contro la negazione di una richiesta (articolo 38, quinto comma, della legge sulla protezione delle informazioni personali). Il titolare del trattamento deve assicurare che la procedura per esercitare i diritti sia "agevole per gli interessati" e non sia più difficile rispetto a quella per la raccolta dei dati personali; ciò comporta altresì l'obbligo di fornire informazioni su tale procedura sul suo sito web (articolo 41, secondo comma, articolo 43, primo comma, e articolo 44, primo comma, del decreto di applicazione della PIPA) ([110]). Le persone fisiche possono autorizzare un rappresentante a presentare una tale richiesta (articolo 38, primo comma, della legge sulla protezione delle informazioni personali in combinato disposto con l'articolo 45 del decreto di applicazione di tale legge). Sebbene il titolare del trattamento abbia il diritto di imporre una commissione (e, in caso di richiesta di invio di copie di dati personali a mezzo posta, di addebitare le spese di affrancatura), l'ammontare corrispondente deve essere determinato "nel rispetto delle spese effettive necessarie per l'elaborazione del[la richiesta]"; non può essere imposta alcuna commissione (né spesa di affrancatura) qualora la richiesta sia imputabile al titolare del trattamento (articolo 38, terzo comma, della legge sulla protezione delle informazioni personali in combinato disposto con l'articolo 47 del decreto di applicazione di tale legge).

(81) La legge sulla protezione delle informazioni personali e il suo decreto di applicazione non contengono disposizioni generali che affrontano la questione delle decisioni riguardanti l'interessato basate unicamente sul trattamento automatizzato di dati personali. Tuttavia, per quanto riguarda i dati personali raccolti nell'Unione, qualsiasi decisione basata sul trattamento automatizzato sarà generalmente presa dal titolare del trattamento nell'Unione (che ha un rapporto diretto con l'interessato) ed è, di conseguenza, soggetta al regolamento (UE) 2016/679 ([111]). Ciò comprende i casi di trasferimento in cui il trattamento è effettuato da un operatore economico straniero (ad esempio, coreano) che agisce in qualità di agente (responsabile del trattamento) per conto del titolare del trattamento stabilito nell'Unione (o come responsabile del trattamento in seconda battuta che agisce per conto del responsabile del trattamento dell'Unione, che ha ricevuto i dati dal titolare del trattamento dell'Unione che li ha raccolti) che, su questa base, prende la decisione. È pertanto improbabile che l'assenza di norme specifiche relative al processo decisionale automatizzato nella legge sulla protezione delle informazioni personali incida sul livello di protezione dei dati personali trasferiti ai sensi della presente decisione.

(82) In via eccezionale, le disposizioni relative alla trasparenza su richiesta (articolo 20) e ai diritti individuali (articoli da 35 a 37), nonché il requisito di notifica individuale per i fornitori di servizi di informazione e di comunicazione (articolo 39-8 della legge sulla protezione delle informazioni personali), non si applicano alle informazioni pseudonimizzate, quando queste ultime vengono trattate per finalità di compilazione di statistiche, di ricerca scientifica o di archiviazione nell'interesse pubblico (articolo 28-7 della legge sulla protezione delle informazioni personali) ([112]). In linea con l'approccio di cui all'articolo 11, paragrafo 2, (in combinato disposto con il considerando 57) del regolamento (UE) 2016/679, ciò è giustificato dal fatto che, per garantire la trasparenza o concedere i diritti individuali, il titolare del trattamento dovrebbe stabilire se una parte qualsiasi dei dati (e in caso affermativo, quali) è correlata alla persona che formula la richiesta, una circostanza questa espressamente vietata nella legge sulle imprese di telecomunicazione (articolo 28-5, primo comma). Inoltre, laddove tale reidentificazione comporti l'annullamento della pseudonimizzazione per l'intera serie di dati (pseudonimizzati), ciò esporrebbe le informazioni personali di tutte le altre persone fisiche interessate a un aumento dei rischi. Considerando che il regolamento (UE) 2016/679 fa riferimento a circostanze nelle quali una reidentificazione è praticamente impossibile, la legge sulla protezione delle informazioni personali adotta un approccio più rigoroso vietando espressamente la reidentificazione in tutte le situazioni nelle quali vengono trattate informazioni pseudonimizzate.

(83) Il sistema coreano, come descritto nei considerando da 74 a 82, contiene pertanto norme sui diritti in materia di dati che forniscono un livello di protezione essenzialmente equivalente a quello previsto dal regolamento (UE) 2016/679.

([109]) Cfr. anche articolo 30, primo comma, punto 5, della legge sulla protezione delle informazioni personali concernente la politica in materia di tutela della vita privata che deve contenere tra l'altro informazioni sui diritti a disposizione della persona fisica e sulle modalità per esercitarli.

([110]) Cfr. anche articolo 39-7, secondo comma, della legge sulla protezione delle informazioni personali per quanto riguarda i fornitori di servizi di informazione e comunicazione.

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

([112]) Cfr. anche notifica 2021-5, che conferma che la sezione III della legge sulla protezione delle informazioni personali (incluso l'articolo 28-7) si applica soltanto quando le informazioni pseudonimizzate sono trattate per finalità di ricerca scientifica, di compilazione di statistiche o per l'archiviazione nell'interesse pubblico, cfr. sezione 4 dell'allegato I della presente decisione.

2.3.9 *Trasferimenti successivi*

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

(85) Tali "trasferimenti successivi" costituiscono trasferimenti internazionali dalla Repubblica di Corea dalla prospettiva del titolare del trattamento coreano. A tale riguardo la legge sulla protezione delle informazioni personali distingue tra l'esternalizzazione del trattamento a un fornitore esterno (ossia un responsabile del trattamento) e la fornitura di dati personali a terzi ([113]).

(86) Innanzitutto, quando il trattamento dei dati personali è esternalizzato a un soggetto situato in un paese terzo, il titolare del trattamento coreano deve garantire il rispetto delle disposizioni della legge sulla protezione delle informazioni personali in materia di esternalizzazione (articolo 26). Ciò comprende la messa in atto di uno strumento giuridicamente vincolante che tra gli altri limita il trattamento da parte del fornitore esterno alla finalità del lavoro esternalizzato, impone l'adozione di garanzie tecniche e gestionali e limita il sub-trattamento (cfr. articolo 26, primo comma, della legge sulla protezione delle informazioni personali); nonché la pubblicazione di informazioni in merito al lavoro esternalizzato. Il titolare del trattamento è inoltre tenuto a "istruire" il fornitore esterno in merito alle misure di sicurezza necessarie, nonché a controllare, anche mediante ispezioni, il rispetto di tutti gli obblighi spettanti al titolare del trattamento ai sensi della legge sulla protezione delle informazioni personali ([114]) e quelli derivanti dal contratto di esternalizzazione.

(87) Se il fornitore esterno provoca danni mediante il trattamento di dati personali in violazione della legge sulla protezione delle informazioni personali, tali danni saranno imputati al titolare del trattamento ai fini della responsabilità, come accadrebbe nel caso di dipendenti del titolare del trattamento (articolo 26, sesto comma, di tale legge). Il titolare del trattamento coreano rimane quindi responsabile per i dati personali esternalizzati e deve assicurare che il responsabile del trattamento straniero tratti le informazioni in conformità con legge sulla protezione delle informazioni personali. Se il fornitore esterno tratta le informazioni in violazione della legge sulla protezione delle informazioni personali, il titolare del trattamento coreano può essere ritenuto responsabile per mancato rispetto del suo obbligo di assicurare il rispetto della legge sulla protezione delle informazioni personali, ad esempio esercitando un controllo sul fornitore esterno. Le garanzie incluse nel contratto di esternalizzazione e la responsabilità del titolare del trattamento coreano per le azioni del fornitore esterno garantiscono la continuità della protezione quando il trattamento dei dati personali è esternalizzato a un soggetto situato al di fuori della Corea.

(88) In secondo luogo i titolari del trattamento coreani possono fornire dati personali a una terza parte situata al di fuori della Corea. Sebbene la legge sulla protezione delle informazioni personali comprenda una serie di fondamenti giuridici che consentono la fornitura a terzi in generale, se la terza parte si trova al di fuori della Corea, in linea di principio ([115]) il titolare del trattamento deve ottenere il consenso ([116]) dell'interessato dopo avergli fornito informazioni in merito: 1) al tipo di dati personali; 2) al destinatario dei dati personali; 3) alla finalità del trasferimento nel senso della finalità di trattamento perseguita dal destinatario; 4) al periodo di conservazione per il trattamento da parte del destinatario, nonché 5) al fatto che l'interessato possa negare il consenso (articolo 17, secondo e terzo comma, della legge sulla protezione delle informazioni personali). La notifica 2021-5, nella sua sezione sulla trasparenza (cfr. considerando 70), impone che le persone fisiche vengano informate in merito al paese terzo al quale verranno forniti i loro dati. Ciò garantisce che gli interessati nell'Unione possano adottare una decisione pienamente informata in merito all'eventualità di prestare o meno il consenso a una fornitura dei dati all'estero. Inoltre il titolare del trattamento non deve stipulare un contratto con il destinatario terzo in violazione della legge sulla protezione delle informazioni personali, il che significa che il contratto non deve contenere obblighi in contraddizione con i requisiti imposti da tale legge al titolare del trattamento ([117]).

([113]) Norme specifiche si applicano ai fornitori di servizi di informazione e comunicazione. Conformemente all'articolo 39-12 della legge sulla protezione delle informazioni personali i fornitori di servizi di informazione e comunicazione devono in linea di principio ottenere il consenso dell'utente per qualsiasi trasferimento di informazioni personali all'estero. Nel caso in cui le informazioni personali siano trasferite nel contesto dell'esternalizzazione di trattamenti, anche per fini di conservazione, il consenso non è richiesto se le persone fisiche interessate sono state informate preventivamente, direttamente o tramite avviso pubblico in un modo che consente un facile accesso, in merito: 1) ai dettagli relativi alle informazioni da trasferire; 2) al paese verso il quale le informazioni verranno trasferite (nonché la data e il metodo del trasferimento); 3) il nome del destinatario e 4) la finalità d'uso e la conservazione da parte del destinatario (articolo 39-12, terzo comma, della legge sulla protezione delle informazioni personali). Inoltre in tal caso si applicheranno i requisiti generali per l'esternalizzazione. Per ciascun trasferimento è necessario mettere in atto garanzie specifiche in relazione alla sicurezza, alla gestione dei reclami e delle controversie, nonché altre misure necessarie per proteggere le informazioni degli utenti (articolo 48-10 del decreto di applicazione della PIPA).

([114]) Cfr. anche articolo 26, settimo comma, della legge sulla protezione delle informazioni personali, ai sensi del quale gli articoli da 15 a 25, da 27 a 31, da 33 a 38 e 50 si applicano mutatis mutandis al responsabile del trattamento.

([115]) In caso di fornitura a terzi di informazioni personali di utenti da parte di fornitori di servizi di informazione e comunicazione, ciò richiede sempre il consenso dell'utente (articolo 39-12, secondo comma, della legge sulla protezione delle informazioni personali).

([116]) Come spiegato in modo più dettagliato alla nota 51, affinché tale consenso sia valido, deve essere prestato liberamente, informato e specifico.

([117]) Cfr. anche articolo 39-12, primo comma, della legge sulla protezione delle informazioni personali per quanto concerne i fornitori di servizi di informazione e comunicazione.

(89) Senza il consenso della persona fisica, i dati personali possono essere forniti a una terza parte (all'estero) laddove la finalità della divulgazione rimanga "all'interno di un ambito di applicazione ragionevolmente correlato" alla finalità iniziale della raccolta (articolo 17, quarto comma, della legge sulla protezione delle informazioni personali - cfr. considerando 36). Tuttavia nel decidere se divulgare (o meno) i dati personali per una finalità "correlata", il titolare del trattamento deve valutare se la divulgazione provoca svantaggi alla persona fisica e se sono state adottate le misure di sicurezza necessarie (come la cifratura). Dato che il paese terzo verso il quale i dati personali vengono trasferiti potrebbe non offrire protezioni analoghe a quelle fornite nella legge sulla protezione delle informazioni personali, la sezione 2 della notifica 2021-5 riconosce che tali svantaggi possono insorgere e possono essere evitati soltanto se il titolare del trattamento coreano e il destinatario all'estero, attraverso uno strumento giuridicamente vincolante (come un contratto), assicurano un livello di protezione equivalente a detta legge, anche rispetto ai diritti degli interessati.

(90) Norme speciali si applicano alla divulgazione "al di fuori della finalità", ossia la fornitura di dati a terzi per una finalità nuova (non correlata), che può avvenire soltanto in ragione di uno dei motivi di cui all'articolo 18, secondo comma, della legge sulla protezione delle informazioni personali come illustrato al considerando 39. Tuttavia, anche in tali condizioni, la fornitura a terzi è esclusa se è probabile che "violi ingiustamente" gli interessi dell'interessato o di una terza parte, di conseguenza è necessario stabilire un equilibrio tra gli interessi. Inoltre, ai sensi dell'articolo 18, quinto comma, della legge sulla protezione delle informazioni personali, il titolare del trattamento deve applicare ulteriori garanzie, che possono comprendere il richiedere alla terza parte di limitare la finalità e il metodo di trattamento oppure di mettere in atto misure di sicurezza specifiche. Ancora una volta, dato che il paese terzo verso il quale i dati personali vengono trasferiti potrebbe non offrire protezioni analoghe a quelle fornite nella legge sulla protezione delle informazioni personali, la sezione 2 della notifica 2021-5 riconosce che può verificarsi una "violazione ingiusta" degli interessi della persona fisica o di una terza e che ciò può essere evitato soltanto se il titolare del trattamento coreano e il destinatario all'estero, attraverso uno strumento giuridicamente vincolante (come un contratto), assicurano un livello di protezione equivalente a detta legge, anche rispetto ai diritti degli interessati.

(91) Le norme di cui ai considerando da 86 a 90 assicurano pertanto la continuità della protezione quando i dati personali vengono ulteriormente trasferiti (a un "fornitore esterno" o a una terza parte) dalla Repubblica di Corea in un modo che è essenzialmente equivalente a quanto previsto dal regolamento (UE) 2016/679.

2.3.10 *Responsabilizzazione*

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

(93) Ai sensi dell'articolo 3, sesto e ottavo comma, della legge sulla protezione delle informazioni personali, il titolare del trattamento deve trattare i dati personali "in maniera tale da ridurre al minimo la possibilità di violare" la vita privata dell'interessato e deve sforzarsi di ottenere la fiducia dell'interessato rispettando e adempiendo i doveri e le responsabilità di cui alla legge sulla protezione delle informazioni personali ed altre leggi correlate. Ciò comprende l'istituzione di un piano di gestione interno (articolo 29 della legge sulla protezione delle informazioni personali), nonché una formazione e un controllo adeguati del personale (articolo 28 della medesima legge).

(94) Come mezzo per assicurare la responsabilizzazione, l'articolo 31 della legge sulla protezione delle informazioni personali in combinato disposto con l'articolo 32 del decreto di applicazione di tale legge crea l'obbligo per i titolari del trattamento di designare un responsabile della tutela della vita privata che "si assuma la responsabilità complessiva del trattamento delle informazioni personali". In particolare tale responsabile della tutela della vita privata è incaricato dello svolgimento delle seguenti funzioni: 1) definizione e attuazione di un piano di protezione dei dati personali e redazione della politica in materia di tutela della vita privata; 2) conduzione di indagini periodiche sullo stato e sulle prassi di trattamento dei dati personali, al fine di porre rimedio a eventuali carenze; 3) gestione dei reclami e risarcimento riparatorio; 4) istituzione di un sistema di controllo interno per prevenire la divulgazione, l'abuso o l'uso improprio dei dati personali; 5) preparazione e attuazione di un programma di istruzione; 6) protezione, controllo e gestione di fascicoli di dati personali; e 7) distruzione di dati personali una volta conseguita la finalità prevista per il trattamento o scaduto il periodo di conservazione. Nello svolgere tali compiti, il responsabile della tutela della vita privata può ispezionare lo stato del trattamento dei dati personali e i relativi sistemi e può richiedere informazioni in merito (articolo 31, terzo comma, della legge sulla protezione delle informazioni personali). Se il responsabile della tutela della vita privata viene a conoscenza di qualsiasi violazione di legge sulla protezione delle informazioni personali o di altre leggi pertinenti per la protezione dei dati, attua immediatamente misure correttive e segnala tali misure alla dirigenza ("capo") del titolare del trattamento, se necessario (articolo 31, quarto comma, di tale legge). Ai sensi dell'articolo 31, quinto comma, della legge sulla protezione delle informazioni personali, il responsabile della tutela della vita privata non deve subire svantaggi ingiustificati in conseguenza dello svolgimento di tali funzioni.

(95) Inoltre i titolari del trattamento devono tentare proattivamente di condurre una valutazione dell'impatto sulla vita privata nel caso in cui il funzionamento dei fascicoli di dati personali implichi un rischio per la vita privata (articolo 33, ottavo comma, della legge sulla protezione delle informazioni personali). Sulla base dell'articolo 33, primo e secondo comma, della legge sulla protezione delle informazioni personali in combinato disposto con gli articoli 35, 36 e 38 del decreto di applicazione di tale legge, fattori quali il tipo e la natura dei dati trattati (in particolare se costituiscono informazioni sensibili), il loro volume, il periodo di conservazione e la probabilità di violazioni dei dati saranno rilevanti ai fini della valutazione del grado di rischio per i diritti degli interessati. La valutazione dell'impatto sulla vita privata mira ad assicurare l'analisi dei fattori di rischio per la vita privata nonché di qualsiasi misura di sicurezza o altra contromisura, così come a rilevare le questioni che necessitano di miglioramento (cfr. articolo 33, primo comma, della legge sulla protezione delle informazioni personali in combinato disposto con l'articolo 38 del decreto di applicazione di tale legge).

(96) Gli enti pubblici sono soggetti all'obbligo di svolgere una valutazione d'impatto quando trattano determinati fascicoli di dati personali che presentano un rischio più elevato di possibili violazioni in materia di vita privata (articolo 33, primo comma, del primo comma, della legge sulla protezione delle informazioni personali). Conformemente all'articolo 35 del decreto di applicazione della PIPA, ciò si verifica tra l'altro per i fascicoli che contengono informazioni sensibili riguardanti almeno 50 000 interessati, i fascicoli che saranno associati ad altri fascicoli e, di conseguenza, conterranno informazioni in merito ad almeno 500 000 interessati oppure i fascicoli che contengono informazioni su almeno un milione di interessati. Il risultato di una valutazione d'impatto condotta da un ente pubblico deve essere comunicato alla PIPC (articolo 33, primo comma, della legge sulla protezione delle informazioni personali), che può fornire il suo parere (articolo 33, terzo comma, della medesima legge).

(97) Infine l'articolo 13 della legge sulla protezione delle informazioni personali prevede che la PIPC definisca politiche necessarie per promuovere e sostenere "attività di protezione dei dati in autoregolamentazione" da parte del titolare del trattamento, tra l'altro attraverso l'istruzione in materia di protezione dei dati, la promozione e il sostegno a favore delle organizzazioni impegnate nella protezione dei dati nonché fornendo assistenza ai titolari del trattamento nella definizione e nell'attuazione di norme di autoregolamentazione. Inoltre deve introdurre e facilitare il sistema di marchio ePRIVACY. A tale proposito, l'articolo 32-2 della legge sulla protezione delle informazioni personali in combinato disposto con gli articoli da 34-2 a 34-8 del decreto di applicazione di tale legge prevede la possibilità di certificare che il sistema o i sistemi di protezione e di trattamento dei dati personali del titolare del trattamento rispettano i requisiti di cui a detta legge. Secondo tali norme, una certificazione ([118]) può essere concessa (per un periodo di 3 anni) se il titolare del trattamento soddisfa i criteri di certificazione stabiliti dalla PIPC, compresa la definizione di garanzie gestionali, tecniche e fisiche per proteggere i dati personali ([119]). La PIPC deve esaminare i sistemi del titolare del trattamento pertinenti per la certificazione almeno una volta l'anno per mantenerne l'efficacia, che può portare alla revoca della certificazione (articolo 32, quarto comma, della legge sulla protezione delle informazioni personali in combinato disposto con l'articolo 34-5 del decreto di applicazione di tale legge; la cosiddetta "gestione del seguito").

(98) Il quadro coreano attua pertanto il principio di responsabilizzazione in un modo che garantisce un livello di protezione essenzialmente equivalente a quello del regolamento (UE) 2016/679, anche previa fornitura di meccanismi diversi per garantire e dimostrare la conformità rispetto alla legge sulla protezione delle informazioni personali.

2.3.11 *Norme speciali per il trattamento delle informazioni creditizie personali*

(99) Come illustrato al considerando 13 la legge sulle informazioni creditizie stabilisce norme specifiche per il trattamento di informazioni creditizie personali da parte degli operatori commerciali. Durante il trattamento di informazioni creditizie personali gli operatori commerciali devono quindi rispettare i requisiti generali della legge sulla protezione delle informazioni personali, fatto salvo il caso in cui la legge sulle informazioni creditizie contenga norme più specifiche. Ciò si verificherà ad esempio quando trattano informazioni relative a una carta di credito o un conto bancario nel contesto di un'operazione commerciale con una persona fisica. Come legislazione settoriale per il trattamento di informazioni creditizie (personali e non personali), la legge sulle informazioni creditizie non impone soltanto garanzie specifiche in materia di protezione dei dati (ad esempio in termini di trasparenza e sicurezza), ma anche più in generale le circostanze specifiche nelle quali si possono trattare informazioni creditizie personali. Ciò si rispecchia in particolare nei requisiti dettagliati per l'uso, la fornitura di dati a una terza parte e la conservazione di tali dati.

(100) Come per la legge sulla protezione delle informazioni personali, la legge sulle informazioni creditizie rispecchia il principio di liceità e proporzionalità. Innanzitutto, come requisito generale, l'articolo 15, primo comma, della legge sulle informazioni creditizie consente soltanto la raccolta di informazioni creditizie personali con mezzi ragionevoli ed equi e nella misura minima possibile misura inferiore necessaria per soddisfare una finalità specificata, conformemente all'articolo 3, primo e secondo comma, della legge sulla protezione delle informazioni personali. In secondo luogo, la legge sulle informazioni creditizie disciplina specificamente la liceità del trattamento di informazioni creditizie personali, limitandone la raccolta, l'uso e la fornitura a una terza parte e in generale correlando tali attività di trasformazione al requisito del consenso della persona interessata.

([118]) Inoltre se il titolare del trattamento intende fare riferimento o promuovere la certificazione nelle sue attività aziendali può utilizzare il marchio di protezione delle informazioni personali stabilito dalla PIPC. Cfr. articolo 34-7 del decreto di applicazione della PIPA.

([119]) Dal novembre del 2018 è stato sviluppato il "sistema di gestione delle informazioni personali e della sicurezza delle informazioni" (ISMS-P) che certifica che i titolari del trattamento gestiscono un sistema di gestione completo.

(101) Le informazioni creditizie personali possono essere raccolte in base a uno dei motivi forniti dalla legge sulla protezione delle informazioni personali o su un motivo specifico stabilito nella legge sulle informazioni creditizie. Dato che l'articolo 45 del regolamento (UE) 2016/679 presuppone un trasferimento di dati personali da parte di un titolare o di un responsabile del trattamento nell'Unione, ma non riguarda la raccolta diretta (ad esempio da una persona fisica o tramite un sito web) da un titolare del trattamento in Corea, soltanto il consenso e i motivi previsti nella legge sulla protezione delle informazioni personali sono pertinenti per la presente decisione. Tra tali motivi figurano in particolare gli scenari nei quali il trasferimento è necessario per dare esecuzione a un contratto con la persona fisica o in virtù degli interessi legittimi del titolare del trattamento coreano (articolo 15, primo comma, punti 4 e 6, della legge sulla protezione delle informazioni personali) ([120]).

(102) Una volta raccolte, le informazioni creditizie personali possono essere utilizzate 1) per la finalità originale per la quale erano state fornite (direttamente) dalla persona fisica ([121]); 2) per una finalità compatibile con quella originale della raccolta ([122]); 3) per decidere se stabilire o mantenere una relazione commerciale richiesta dalla persona fisica ([123]); 4) per finalità di compilazione di statistiche, di ricerca e di archiviazione nell'interesse pubblico ([124]) se le informazioni sono pseudonimizzate ([125]); 5) se si ottiene un ulteriore consenso oppure 6) in conformità con la legge.

(103) Se un operatore commerciale intende divulgare informazioni creditizie personali a una terza parte, deve ottenere il consenso della persona fisica ([126]) dopo averla informata in merito al destinatario dei dati, alla finalità del trattamento da parte del destinatario, ai dettagli dei dati da fornire, al periodo di conservazione del destinatario e al diritto di negare il consenso (articolo 32, primo comma, della legge sulle informazioni creditizie e articolo 28, secondo comma, del decreto di applicazione di tale legge) ([127]). Tale requisito di consenso non si applica in situazioni specifiche, ossia laddove vengano divulgate informazioni creditizie personali ([128]): 1) a un fornitore esterno per finalità di esternalizzazione ([129]); 2) a una terza parte in caso di trasferimento, divisione o fusione aziendale; 3) per finalità di compilazione di statistiche, di ricerca e di archiviazione nell'interesse pubblico se le informazioni sono pseudonimizzate; 4) per una finalità compatibile con quella originale della raccolta; 5) a una terza parte che utilizza le informazioni per recuperare un credito vantato nei confronti della persona fisica ([130]); 6) per rispettare l'ordinanza di un organo giurisdizionale; 7) a un pubblico ministero/funzionario della polizia giudiziaria in caso di emergenza, qualora la vita della persona fisica sia in pericolo o si prevede che quest'ultima possa subire lesioni personali e non

([120]) La legge sulle informazioni creditizie contiene altresì altre basi giuridiche per la raccolta, ossia qualora esista un obbligo di legge, qualora le informazioni siano rese pubbliche da un ente pubblico ai sensi della legislazione in materia di libertà di informazione oppure qualora tali informazioni siano disponibili su un social network. Per poter invocare quest'ultimo motivo, l'operatore commerciale deve essere in grado di dimostrare che la raccolta rimane all'interno del consenso dell'interessato, sulla base di un'interpretazione ragionevole ("obiettiva") e tenendo conto della natura dei dati, dell'intento e della finalità del renderli disponibili sul social network, se la finalità della raccolta era "altamente pertinente" a tale finalità, ecc. (articolo 13 del decreto di applicazione della CIA). Tuttavia, come spiegato al considerando 101, in linea di principio tali motivi non saranno pertinenti in uno scenario di trasferimento.

([121]) Ad esempio quando le informazioni creditizie sono generate/fornite nel contesto di una transazione commerciale con la persona fisica. Tuttavia questo motivo non può essere invocato per utilizzare informazioni creditizie personali per finalità di marketing diretto (cfr. articolo 33, primo comma, punto 3, della legge sulle informazioni creditizie).

([122]) Al fine di stabilire se la finalità d'uso sia compatibile con la finalità originale della raccolta, devono essere presi in considerazione i seguenti fattori: 1) la relazione ("pertinenza") tra le due finalità; 2) le modalità di raccolta delle informazioni; 3) l'impatto dell'uso relativo alla persona fisica; e 4) se sono state attuate misure di sicurezza adeguate, quali la pseudonimizzazione (cfr. articolo 32, sesto comma, punto 9-4, della legge sulle informazioni creditizie).

([123]) Ad esempio un titolare del trattamento potrebbe dover tenere conto delle informazioni creditizie personali che ha ricevuto da una persona fisica al fine di decidere se estendere il termine di un prestito concesso a tale persona.

([124]) Articolo 33 della legge sulle informazioni creditizie, in combinato disposto con l'articolo 32, sesto comma, punto 9-2, 9-4, 10 della legge sulle informazioni creditizie.

([125]) La pseudonimizzazione è definita dall'articolo 2, quindicesimo comma, della legge sulle informazioni creditizie come trattamento di informazioni creditizie personali in modo tale che le persone fisiche non possano più essere identificate dalle informazioni fatta eccezione combinandole con informazioni aggiuntive. Sebbene la legge sulle informazioni creditizie contenga garanzie specifiche per il trattamento delle informazioni pseudonimizzate per finalità di compilazione di statistiche, di ricerca e di archiviazione nell'interesse pubblico (articolo 40-2 della legge sulle informazioni creditizie), tali norme non si applicano alle organizzazioni commerciali. Piuttosto queste ultime rimangono soggette ai requisiti specifici di cui alla sezione III della legge sulla protezione delle informazioni personali, come illustrato nei considerando da 42 a 48. L'articolo 40-3 della legge sulle informazioni creditizie esenta inoltre il trattamento di informazioni creditizie pseudonimizzate, laddove sia condotto per finalità di compilazione di statistiche, di ricerca scientifica o di archiviazione nell'interesse pubblico, rispetto ai requisiti in materia di trasparenza e di diritti individuali, in maniera analoga all'eccezione di cui all'articolo 28-7 della legge sulla protezione delle informazioni personali e nel rispetto delle garanzie di cui alla sezione III della medesima legge, come descritto in maggior dettaglio nei considerando da 42 a 48.

([126]) Ciò non si applica se le informazioni sono fornite a terzi per mantenere l'esattezza e l'aggiornamento delle informazioni creditizie personali, a condizione che la disposizione rimanga all'interno della finalità originale del trattamento (articolo 32, primo comma, della legge sulle informazioni creditizie). Ciò può ad esempio verificarsi nel caso in cui informazioni aggiornate vengano fornite ad un'agenzia di rating del credito per assicurare che le sue registrazioni siano esatte.

([127]) Qualora non sia pratico fornire le informazioni summenzionate, potrebbe essere sufficiente rinviare la persona fisica al destinatario terzo per le informazioni richieste.

([128]) Dato che la legge sulle informazioni creditizie non disciplina specificamente le divulgazioni all'estero di informazioni creditizie personali, tali divulgazioni devono essere conformi alle garanzie per i trasferimenti successivi imposte dalla sezione 2 della notifica n. 2021-5.

([129]) L'esternalizzazione del trattamento delle informazioni creditizie personali può avvenire soltanto in base a un contratto scritto e nel rispetto dei requisiti di cui all'articolo 26, dal primo al terzo comma e quinto comma, della legge sulla protezione delle informazioni personali, come illustrato al considerando 20 (articolo 17 della legge sulle informazioni creditizie e articolo 14 del decreto di applicazione di tale legge). Il fornitore esterno non può utilizzare le informazioni al di fuori dell'ambito di applicazione dei compiti esternalizzati e l'impresa che esternalizza deve soddisfare requisiti di sicurezza specifici (ad esempio cifratura) ed istruire il fornitore esterno in merito alle modalità per impedire che le informazioni creditizie vadano perse, vengano rubate, divulgate, alterate o compromesse.

([130]) Cfr. anche articolo 28, decimo comma, punti 1, 2 e 6 del decreto di applicazione della CIA.

vi è il tempo per il rilascio di un mandato giudiziario ([131]); 8) alle autorità fiscali competenti per rispettare le leggi in materia di tassazione; o 9) in conformità con altre leggi. In caso di divulgazione sulla base di uno di questi motivi, l'interessato deve ricevere una notifica preventiva (articolo 32, settimo comma, della legge sulle informazioni creditizie).

(104) La legge sulle informazioni creditizie disciplina inoltre in maniera specifica la durata del trattamento delle informazioni creditizie personali sulla base di uno di tali motivi per l'uso o la fornitura a terzi dopo la fine della relazione commerciale con la persona fisica ([132]). Si possono conservare soltanto le informazioni necessarie per stabilire o mantenere tale relazione, previo rispetto di garanzie supplementari (le informazioni devono essere conservate separatamente dalle informazioni creditizie relative a persone fisiche con le quali è in corso una relazione commerciale, essere protette mediante misure di sicurezza specifiche ed essere accessibili soltanto a persone fisiche autorizzate) ([133]). Tutti gli altri dati devono essere cancellati (articolo 17-2, primo comma, punto 2, del decreto di applicazione della CIA). Ai fini della determinazione dei dati necessari per la relazione commerciale, occorre prendere in considerazione diversi fattori, compresa l'eventualità che sia possibile stabilire la relazione in assenza dei dati in questione e che si faccia riferimento direttamente ai beni o servizi forniti alla persona fisica (articolo 17-2, secondo comma, del decreto di applicazione della CIA).

(105) Anche nei casi in cui possono in linea di principio essere conservate oltre la fine della relazione commerciale, le informazioni creditizie personali devono essere cancellate entro tre mesi dal conseguimento della finalità ulteriore del trattamento ([134]) o, in ogni caso, dopo cinque anni (articolo 20-2 della legge sulle informazioni creditizie). In un numero limitato di circostanze, le informazioni creditizie personali possono essere conservate per più di cinque anni, in particolare laddove ciò sia necessario per adempiere un obbligo legale; laddove ciò sia necessario per gli interessi vitali relativi alla vita, all'incolumità o al patrimonio di una persona fisica; per l'archiviazione di informazioni pseudonimizzate (utilizzate per finalità di ricerca scientifica, di compilazione di statistiche o di archiviazione nell'interesse pubblico); oppure per finalità assicurative (in particolare per i pagamenti assicurativi o per prevenire frodi assicurative) ([135]). In questi casi eccezionali, si applicano garanzie specifiche (quali la notifica alla persona fisica dell'uso ulteriore, la separazione delle informazioni conservate da quelle relative a persone fisiche con le quali è ancora in essere una relazione commerciale o la limitazione di diritti di accesso, cfr. articolo 17-2, primo e secondo comma, del decreto di applicazione della CIA).

(106) La legge sulle informazioni creditizie specifica altresì ulteriormente i principi di esattezza e qualità dei dati, prescrivendo che le informazioni creditizie personali siano "registrate, modificate e gestite" in maniera da preservarne l'esattezza e l'aggiornamento (articolo 18, primo comma, della legge sulle informazioni creditizie e articolo 15, terzo comma, del decreto di applicazione della CIA) ([136]). Quando forniscono informazioni creditizie a determinati altri soggetti (quali le agenzie di rating del credito), gli operatori commerciali sono inoltre specificamente tenuti a verificare l'accuratezza delle informazioni per garantire che soltanto informazioni esatte vengano registrate e gestite dal destinatario (articolo 15, primo comma, del decreto di applicazione della CIA, in combinato disposto con l'articolo 18, primo comma, di tale legge). Più in generale la legge sulle informazioni creditizie prescrive la tenuta di registri sulla raccolta, sull'uso, sulla divulgazione a terzi e sulla distruzione di informazioni creditizie personali (articolo 20, secondo comma, della legge sulle informazioni creditizie) ([137]).

(107) Inoltre il trattamento di informazioni creditizie personali è soggetto a requisiti specifici rispetto alla sicurezza dei dati. In particolare la legge sulle informazioni creditizie richiede l'attuazione di misure tecnologiche, fisiche e organizzative per impedire l'accesso illecito a sistemi informatici nonché l'alterazione, la distruzione o qualsiasi altro rischio per i dati trattati (ad esempio mediante controlli di accesso, cfr. articolo 19 della legge sulle informazioni creditizie e articolo 16 decreto del decreto di applicazione di tale legge). Inoltre, quando si scambiano informazioni creditizie personali con una terza parte, è necessario concludere un accordo che stabilisce misure di sicurezza specifiche (articolo 19, secondo comma, della legge sulle informazioni creditizie). Se si verifica una violazione delle informazioni creditizie personali, è necessario adottare misure per ridurre al minimo qualsiasi danno e le persone fisiche interessate devono riceverne notifica senza indugio (articolo 39-4, primo e secondo comma, della legge sulle informazioni creditizie). Inoltre si deve informare la PIPC in merito alla notifica fornita alle persone fisiche e alle misure che sono state attuate (articolo 39-4, quarto comma, della legge sulle informazioni creditizie).

([131]) In tal caso si deve richiedere un mandato senza indugio. Se il mandato non viene emesso entro 36 ore, i dati ricevuti devono essere cancellati senza indugio (articolo 32, sesto comma, punto 6, della legge sulle informazioni creditizie).

([132]) Ad esempio, dato che le obbligazioni contrattuali sono state soddisfatte, una delle parti ha esercitato il proprio diritto alla risoluzione, ecc., cfr. articolo 17-2, quinto comma, decreto di applicazione della CIA.

([133]) Articolo 20-2, primo comma, della legge sulle informazioni creditizie e articolo 17-2, primo comma, punto 1, del decreto di applicazione della CIA.

([134]) Tale periodo tiene conto del fatto che spesso la cancellazione non sarà possibile immediatamente, ma in genere richiede determinati passaggi (ad esempio la separazione dei dati da eliminare dagli altri dati e l'esecuzione della cancellazione senza influire sulla stabilità dei sistemi di informazione) la cui attuazione può richiedere del tempo.

([135]) Articolo 20-2, secondo comma, della legge sulle informazioni creditizie.

([136]) L'articolo 18, secondo comma, della legge sulle informazioni creditizie e l'articolo 15, quarto comma, del decreto di applicazione di tale legge stabiliscono norme più specifiche rispetto a tale requisito di tenuta di registri, ad esempio in riferimento alle registrazioni relative alle informazioni che possono creare svantaggi a una persona fisica, quali informazioni in merito a reati e fallimenti.

([137]) Per quanto concerne gli altri meccanismi di responsabilizzazione, la legge sulle informazioni creditizie impone a determinate organizzazioni (ad esempio cooperative e imprese pubbliche, cfr. articolo 21, secondo comma, del decreto di applicazione della CIA) di nominare un "amministratore/tutore delle informazioni creditizie" incaricato di controllare il rispetto della legge sulle informazioni creditizie ed svolgere i compiti del "responsabile della tutela della vita privata" ai sensi della legge sulla protezione delle informazioni personali (articolo 20, terzo e quarto comma, della legge sulle informazioni creditizie).

(108) La legge sulle informazioni creditizie impone altresì obblighi di trasparenza specifici quando si ottiene il consenso per l'uso o la fornitura di informazioni creditizie personali (articolo 32, quarto comma, e articolo 34-2, della legge sulle informazioni creditizie nonché articolo 30-3 del decreto di applicazione di tale legge) e, più in generale, prima di fornire informazioni a terzi (articolo 32, settimo comma, della legge sulle informazioni creditizie) ([138]). Inoltre le persone fisiche hanno il diritto, su richiesta, di ottenere informazioni sull'uso e sulla fornitura a terzi di loro informazioni creditizie nei tre anni antecedenti la richiesta (compresa la finalità e le date di tale uso/fornitura) ([139]).

(109) Ai sensi della legge sulle informazioni creditizie, le persone fisiche hanno altresì il diritto di accedere alle loro informazioni creditizie personali (articolo 38, primo comma, della legge sulle informazioni creditizie) e di ottenere una correzione di dati inesatti (articolo 38, secondo e terzo comma, della legge sulle informazioni creditizie) ([140]). Inoltre, oltre al diritto generale alla cancellazione ai sensi della legge sulla protezione delle informazioni personali (cfr. considerando 77), la legge sulle informazioni creditizie prevede un diritto specifico di cancellazione delle informazioni creditizie personali conservate oltre i periodi di conservazione menzionati nel considerando 104, ossia cinque anni (per informazioni creditizie personali necessarie per stabilire o mantenere una relazione commerciale) o tre mesi (per altri tipi di informazioni creditizie personali) ([141]). Una richiesta di cancellazione può essere rifiutata in via eccezionale qualora sia necessaria una conservazione ulteriore nelle circostanze di cui al considerando 105. Se una persona fisica richiede la cancellazione, ma si applica una delle eccezioni, le garanzie specifiche devono essere applicate alle informazioni creditizie interessate (articolo 38-3, terzo comma, della legge sulle informazioni creditizie e articolo 33-3 del decreto di applicazione di tale legge). Ad esempio le informazioni devono essere conservate in maniera separata dalle altre informazioni, possono essere accessibili soltanto da parte di una persona autorizzata e devono essere soggette a misure di sicurezza specifiche.

(110) Oltre ai diritti di cui al considerando 109, la legge sulle informazioni creditizie garantisce alle persone fisiche il diritto di richiedere a un titolare del trattamento di smettere di contattarle per finalità di marketing diretto (articolo 37, secondo comma, di tale legge) e il diritto alla portabilità dei dati. Per quanto concerne quest'ultimo caso, la legge sulle informazioni creditizie consente alle persone fisiche di richiedere la trasmissione delle loro informazioni creditizie personali a sé stesse o a talune terze parti (quali enti finanziari e imprese del rating di credito). Le informazioni creditizie personali devono essere trattate e trasmesse alla terza parte in un formato che può essere trattato da un dispositivo di trattamento delle informazioni (come un computer).

(111) Nella misura in cui la legge sulle informazioni creditizie contiene norme specifiche rispetto alla legge sulla protezione delle informazioni personali, la Commissione ritiene pertanto che anche tali norme garantiscano un livello di protezione sostanzialmente equivalente a quella offerta ai sensi del regolamento (UE) 2016/679.

2.4 **Vigilanza ed esecuzione**

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

2.4.1 *Vigilanza indipendente*

(113) Nella Repubblica di Corea l'autorità indipendente incaricata di monitorare e assicurare il rispetto della legge sulla protezione delle informazioni personali è la PIPC. La PIPC è composta da un presidente, un vicepresidente e sette commissari. Il presidente e il vicepresidente sono nominati dal presidente della Repubblica di Corea su raccomandazione del primo ministro. Per quanto concerne i commissari, due sono nominati dal presidente della Repubblica di Corea su raccomandazione del presidente della commissione mentre cinque sono nominati su raccomandazione dell'Assemblea nazionale (di cui due su raccomandazione del partito politico al quale appartiene il presidente della Repubblica di Corea, mentre i tre membri rimanenti sono nominati su raccomandazione di altri partiti politici (articolo 7-2, secondo comma, della legge sulla protezione delle informazioni personali), una

([138]) Ciò implica un requisito di notifica generale (articolo 32, settimo comma, della legge sulle informazioni creditizie) e un obbligo specifico di trasparenza nel caso in cui informazioni tramite le quali sia possibile determinare l'affidabilità creditizia di una persona fisica siano fornite a determinati soggetti, quali agenzie di rating del credito e agenzie di raccolta di informazioni creditizie (articolo 35-3 della legge sulle informazioni creditizie e articolo 30-3 del decreto di applicazione di tale legge) oppure se una relazione in merito a una transazione commerciale viene rifiutata o risolta sulla base delle informazioni creditizie personali ricevuto da una terza parte (articolo 36 della legge sulle informazioni creditizie e articolo 31 del decreto di applicazione di tale legge).

([139]) Articolo 35 della legge sulle informazioni creditizie. Talune organizzazioni commerciali, ad esempio cooperative e imprese pubbliche (articolo 21, secondo comma, del decreto di applicazione della legge sulle informazioni creditizie) sono soggette a requisiti ulteriori in materia di trasparenza, ad esempio per rendere accessibili al pubblico determinate informazioni (articolo 31 della legge sulle informazioni creditizie) e per informare le persone fisiche in merito a possibili svantaggi per il loro punteggio di rating del credito quando sono coinvolte in operazioni finanziarie che generano rischi di credito (articolo 35-2 della legge sulle informazioni creditizie).

([140]) Per quanto concerne le condizioni e le eccezioni relative ai diritti di accesso e correzione, si applicano le norme di cui alla legge sulla protezione delle informazioni personali (di cui ai considerando 76 e 77). Inoltre ulteriori modalità sono stabilite nell'articolo 38, dal quarto all'ottavo comma, della legge sulle informazioni creditizie e nell'articolo 33 del decreto di applicazione della CIA. In particolare un operatore commerciale che ha corretto o cancellato informazioni creditizie inesatte deve notificarlo alla persona fisica alla quale tali informazioni si riferiscono. Inoltre occorre notificare qualsiasi terza parte alla quale tali informazioni sono state comunicate nei sei mesi precedenti ed occorre informarne la persona fisica interessata. Se una persona fisica non è soddisfatta del modo in cui è stata gestita una richiesta di correzione, può presentare una richiesta presso la PIPC, la quale verifica le azioni del titolare del trattamento e può imporre misure correttive.

([141]) Articolo 38-3 della legge sulle informazioni creditizie.

circostanza questa che contribuisce a contrastare la parzialità del processo di nomina) ([142]). La presente procedura è in linea con i requisiti applicabili alla nomina dei membri delle autorità di protezione dei dati nell'Unione (articolo 53, paragrafo 1, del regolamento (UE) 2016/679). Inoltre tutti i commissari devono astenersi da qualsiasi attività legata a profitti o attività politica, nonché dal rivestire funzioni nella pubblica amministrazione o nell'assemblea nazionale (articolo 7-6 e articolo 7-7, primo comma, punto 3, della legge sulla protezione delle informazioni personali) ([143]). Tutti i commissari sono soggetti a norme specifiche che impediscono loro di partecipare alle deliberazioni in caso di un possibile conflitto di interessi (articolo 7-11 della legge sulla protezione delle informazioni personali). La PIPC è assistita da un segretariato (articolo 7-13) e può stabilire sottocommissioni (composte da tre commissari) incaricate della gestione di violazioni minori e questioni ricorrenti (articolo 7-12 della legge sulla protezione delle informazioni personali).

(114) Ciascun membro della PIPC è nominato per un mandato di tre anni e può essere rinominato una volta (articolo 7-4, primo comma, della legge sulla protezione delle informazioni personali). I commissari possono essere rimossi dal loro incarico soltanto in circostanze specifiche, in particolare se non sono più in grado di svolgere i propri compiti a causa di una disabilità mentale o fisica a lungo termine, qualora abbiano commesso atti in violazione della legge o siano soggetti all'applicazione di uno dei motivi per la rimozione dall'incarico ([144]) (articolo 7-5 della legge sulla protezione delle informazioni personali). Ciò fornisce loro una protezione istituzionale nell'esercizio delle loro funzioni.

(115) Più in generale l'articolo 7, primo comma, della legge sulla protezione delle informazioni personali garantisce esplicitamente l'indipendenza della PIPC e l'articolo 7-5, secondo comma, della medesima legge impone ai commissari di svolgere le loro funzioni in maniera indipendentemente, secondo la legge e la loro coscienza ([145]). Le garanzie istituzionali e procedurali descritte, anche rispetto alla nomina e alla rimozione dall'incarico dei suoi membri, assicurano che la PIPC agisca in assoluta indipendenza, senza essere soggetta a influenze o istruzioni esterne. Inoltre, in veste di agenzia amministrativa centrale, la PIPC propone annualmente il proprio bilancio (che è riesaminato dal ministero delle Finanze nel contesto del bilancio nazionale complessivo prima dell'adozione da parte dell'Assemblea nazionale) ed è competente per la gestione del proprio personale. La PIPC ha un bilancio attuale di circa 35 milioni di EUR e ha 154 membri del personale (di cui 40 dipendenti specializzati in tecnologie dell'informazione e della comunicazione, 32 dipendenti che si concentrano sulle indagini e 40 esperti legali).

(116) I compiti e i poteri della PIPC sono previsti principalmente negli articoli 7-8 e 7-9, nonché negli articoli da 61 a 66 della legge sulla protezione delle informazioni personali ([146]). In particolare i compiti della PIPC comprendono l'erogazione di consulenza in merito a leggi e le normative relative alla protezione dei dati, lo sviluppo di politiche e orientamenti per la protezione dei dati, l'indagine di violazioni dei diritti individuali, la gestione di reclami e la mediazione di controversie, l'assicurazione del rispetto della legge sulla protezione delle informazioni personali, la garanzia dell'istruzione e della promozione nel settore della protezione dei dati nonché lo scambio e la cooperazione con autorità di protezione dei dati di paesi terzi ([147]).

(117) Sulla base dell'articolo 68 della legge sulla protezione delle informazioni personali in combinato disposto con l'articolo 62 del decreto di applicazione di tale legge, alcuni compiti della PIPC sono stati delegati all'Agenzia coreana per la sicurezza e internet, ossia: 1) l'istruzione e le pubbliche relazioni; 2) la formazione di specialisti e lo sviluppo di criteri per le valutazione dell'impatto sulla vita privata; 3) la gestione di richieste di designazione di una cosiddetta istituzione per la valutazione dell'impatto sulla vita privata; 4) il trattamento delle richieste di accesso indiretto ai dati personali detenuti da autorità pubbliche (articolo 35, secondo comma, della legge sulla

([142]) Soltanto le persone fisiche che soddisfano i criteri che seguono possono essere nominate ad agire in veste di commissari della PIPC: funzionari pubblici di alto livello competenti per questioni relative alle informazioni personali; ex giudici, pubblici ministeri o avvocati che hanno esercitato la professione per almeno 10 anni; ex dirigenti aventi esperienza nella protezione dei dati che hanno prestato servizio presso un ente pubblico od organizzazione per oltre tre anni o che sono stati raccomandati da tale ente od organizzazione; ed ex professori associati con conoscenze professionali nel settore della protezione dei dati che abbiano prestato servizio per almeno cinque anni presso un istituto accademico (articolo 7-2 della legge sulla protezione delle informazioni personali).

([143]) Cfr. anche articolo 4-2 del decreto di applicazione della PIPA.

([144]) Cfr. articolo 7-7 della legge sulla protezione delle informazioni personali, secondo il quale i cittadini non coreani e i membri di partiti politici non possono diventare membri della PIPC. Lo stesso si applica alle persone fisiche alle quali sono stati irrogati alcuni tipi di sanzioni penali, che sono state rimosse da un incarico mediante un'azione disciplinare negli ultimi cinque anni, ecc. (articolo 7-7 della legge sulla protezione delle informazioni personali in combinato disposto con l'articolo 33 della legge sui funzionari pubblici).

([145]) Mentre l'articolo 7, secondo comma, della legge sulla protezione delle informazioni personali fa riferimento al potere generale del primo ministro ai sensi dell'articolo 18 della legge sull'organizzazione del governo di sospendere o revocare, previa approvazione del presidente della Repubblica di Corea, qualsiasi disposizione illecita o ingiusta di un'agenzia amministrativa centrale, nessun potere analogo è concesso rispetto ai poteri investigativi o di esecuzione della PIPC (cfr. articolo 7, secondo comma, punti 1 e 2, della legge sulla protezione delle informazioni personali). Secondo le spiegazioni ricevute dal governo coreano, l'articolo 18 della legge sull'organizzazione del governo è destinato a fornire al primo ministro la possibilità di agire in circostanze straordinarie, ad esempio per mediare in caso di disaccordo tra agenzie governative diverse. Tuttavia il primo ministro non è mai ricorso all'esercizio di tale potere dall'adozione di tale disposizione nel 1963.

([146]) Quando è necessario svolgere compiti ai sensi dell'articolo 7-9, primo comma, della legge sulla protezione delle informazioni personali, la PIPC può sollecitare i pareri di funzionari pubblici pertinenti, esperti in materia di protezione dei dati, organizzazioni civiche e operatori economici pertinenti. Inoltre la PIPC può richiedere materiali pertinenti, emettere raccomandazioni per il miglioramento e compiere ispezioni per verificarne l'attuazione (articolo 7-9, secondo e quinto comma, della legge sulla protezione delle informazioni personali).

([147]) Cfr. anche articolo 9 (Piano generale triennale per la protezione delle informazioni personali), articolo 12 (Linee guida per la protezione delle informazioni personali standard) e articolo 13 (Politiche per la promozione e il sostegno dell'autoregolamentazione) della legge sulla protezione delle informazioni personali.

protezione delle informazioni personali); e 5) il compito di richiedere materiali e svolgere ispezioni in relazione ai reclami ricevuti attraverso il cosiddetto call centre per la tutela della vita privata. Nel contesto della gestione dei reclami attraverso il call centre per la tutela della vita privata, l'agenzia coreana per la sicurezza e internet trasmette il caso alla PIPC o al pubblico ministero laddove constati che si è verificata una violazione della legge. La possibilità di promuovere reclamo presso il call centre per la tutela della vita privata non impedisce alle persone fisiche di presentare un reclamo direttamente alla PIPC o dal rivolgersi alla PIPC qualora ritengano che il loro reclamo non sia stato gestito in modo soddisfacente dall'agenzia coreana per la sicurezza e internet.

2.4.2 *Applicazione, sanzioni comprese*

(118) Al fine di garantire il rispetto della legge sulla protezione delle informazioni personali, il legislatore ha conferito alla PIPC tanto poteri di indagine quanto quelli di esecuzione, che spaziano dalle raccomandazioni alle sanzioni amministrative pecuniarie. Tali poteri sono ulteriormente integrati da un regime di sanzioni penali.

(119) Per quanto riguarda i poteri di indagine, in caso di sospetta violazione della legge sulla protezione delle informazioni personali o di segnalazione di una tale violazione oppure, ove necessario, per la protezione dei diritti degli interessati in relazione a violazioni, la PIPC può condurre ispezioni in loco e richiedere tutti i materiali pertinenti (quali articoli e documenti) dai titolari del trattamento dei dati personali (articolo 63 della legge di cui sopra in combinato disposto con l'articolo 60 del decreto di applicazione della stessa) ([148]).

(120) In termini di esecuzione, ai sensi dell'articolo 61, secondo comma, della legge sulla protezione delle informazioni personali, la PIPC può fornire un parere ai titolari del trattamento dei dati in merito alle modalità per migliorare il livello della protezione dei dati personali di attività specifiche di trattamento. I titolari del trattamento dei dati devono effettuare sforzi in buona fede per attuare tale parere e sono tenuti a informare la PIPC in merito all'esito. Inoltre qualora vi siano motivi ragionevoli per ritenere che si sia verificata una violazione della legge sulla protezione delle informazioni personali e l'inazione potrebbe causare danni ai quali è difficile porre rimedio, la PIPC può imporre misure correttive (articolo 64, primo comma, della legge sulla protezione delle informazioni personali) ([149]). La sezione 5 della notifica 2021-5 (allegato I) chiarisce, con effetto vincolante, che tali condizioni sono soddisfatte in relazione alla violazione di qualsiasi disposizione della legge sulla protezione delle informazioni personali che protegge i diritti alla vita privata delle persone fisiche in merito alle informazioni personali ([150]). Le misure che la PIPC è autorizzata ad adottare comprendono ordinare la cessazione della condotta che causa la violazione, la sospensione temporanea del trattamento dei dati o qualsiasi altra misura necessaria. Il mancato rispetto di una misura correttiva può portare a una sanzione con irrogazione di una multa per un importo massimo di 50 milioni di KRW (articolo 75, secondo comma, punto 13, della legge sulla protezione delle informazioni personali).

(121) Per quanto concerne determinate autorità pubbliche (quali l'Assemblea nazionale, le agenzie amministrative centrali, gli organi dell'amministrazione locale e gli organi giurisdizionali), l'articolo 64, quarto comma, della legge sulla protezione delle informazioni personali prevede che la PIPC possa "raccomandare" una qualsiasi delle misure correttive menzionate nel considerando 120 e che tali autorità siano tenute a rispettare detta raccomandazione fatto salvo il caso in cui vi siano circostanze straordinarie. Secondo la sezione 5 della notifica 2021-5, ciò fa riferimento a circostanze di fatto o di diritto straordinarie di cui la PIPC non era a conoscenza nel momento in cui ha formulato la sua raccomandazione. L'autorità pubblica interessata può invocare tali circostanze straordinarie soltanto se dimostra chiaramente che non si è verificata alcuna violazione e la PIPC constata che in effetti è così. Altrimenti l'autorità pubblica è tenuta a seguire la raccomandazione della PIPC e ad "adottare una misura correttiva, anche per fermare immediatamente l'azione e compensare i danni nel caso eccezionale in cui sia stato comunque commesso un atto illegale".

(122) La PIPC può altresì richiedere ad altre agenzie amministrative aventi competenza specifica ai sensi della legislazione settoriale (ad esempio salute, istruzione) di svolgere indagini, in maniera indipendente o congiuntamente con la PIPC, in merito a violazioni (sospette) della tutela della vita privata da parte di titolari del trattamento che operano in tali settori soggetti alla loro competenza giurisdizionale, nonché di imporre misure correttive (articolo 63, quarto e quinto comma, della legge sulla protezione delle informazioni personali). In tal caso la PIPC stabilisce i motivi, l'oggetto e la portata dell'indagine ([151]). A sua volta l'agenzia amministrativa pertinente deve presentare un piano di ispezione alla PIPC e informare quest'ultima in merito all'esito dell'ispezione. La PIPC può raccomandare l'adozione di una misura correttiva specifica, che l'agenzia pertinente deve sforzarsi di attuare. In ogni caso tale richiesta non limita la competenza della PIPC in termini di svolgimento di indagini proprio o irrogazione di sanzioni.

([148]) La PIPC può inoltre accedere ai locali del titolare del trattamento per ispezionare lo stato delle operazioni commerciali, i registri, i documenti, ecc. (articolo 63, secondo comma, della legge sulla protezione delle informazioni personali). Cfr. anche l'articolo 45-3 della legge sulle informazioni creditizie e l'articolo 36-4 del decreto di applicazione di tale legge in relazione ai poteri della PIPC ai sensi di tale atto legislativo.

([149]) Cfr. anche articolo 45-4 della legge sulle informazioni creditizie in relazione ai poteri della PIPC ai sensi di tale atto legislativo.

([150]) La sezione 5 della notifica prevede che un "motivo sostanziale per ritenere che vi sia stata una violazione rispetto alle informazioni personali e un'inazione potrebbe causare danni a cui è difficile porre rimedio di cui al primo e secondo comma dell'articolo 64 della legge sulla protezione delle informazioni personali faccia riferimento a una violazione di qualsiasi principio, diritto e dovere incluso nella legge per proteggere i diritti delle persone sulle informazioni personali". Lo stesso vale per i poteri della PIPC di cui all'articolo 45-4 della legge sulle informazioni creditizie.

([151]) Articolo 60 del decreto di applicazione della PIPA.

(123) Oltre ai suoi poteri correttivi, la PIPC può imporre sanzioni amministrative pecuniarie tra 10 e 50 milioni di KRW per violazioni di vari requisiti della legge sulla protezione delle informazioni personali (articolo 75 di tale legge) ([152]). Tra l'altro in tale contesto rientrano il mancato rispetto dei requisiti per la liceità del trattamento, la mancata adozione delle misure di sicurezza necessarie, la mancata notifica agli interessati in caso di violazione dei dati, il mancato rispetto dei requisiti per il sub-trattamento, la mancata definizione e divulgazione di una politica in materia di tutela della vita privata, la mancata designazione di un responsabile della tutela della vita privata o l'inazione a fronte di una richiesta dell'interessato di esercizio dei suoi diritti individuali, nonché determinate violazioni procedurali (omessa cooperazione nel corso di un'indagine). In caso di violazione di diverse disposizioni della PIPA da parte del medesimo titolare del trattamento, può essere imposta una sanzione pecuniaria per ciascuna violazione e il numero di persone fisiche interessate sarà preso in considerazione ai fini della fissazione dell'ammontare di tale sanzione pecuniaria.

(124) Inoltre, laddove vi siano motivi ragionevoli per sospettare una violazione della legge sulla protezione delle informazioni personali o di qualsiasi altra "legge in materia di protezione dei dati", la PIPC può presentare una denuncia penale all'agenzia investigativa competente (quale un pubblico ministero, cfr. articolo 65, primo comma, della legge sulla protezione delle informazioni personali). Inoltre la PIPC può consigliare al titolare del trattamento di adottare azioni disciplinari nei confronti della persona responsabile (compreso il dirigente incaricato, cfr. articolo 65, secondo comma, della legge sulla protezione delle informazioni personali). Dopo aver ricevuto tale parere, il titolare del trattamento deve conformarvisi ([153]) e deve notificare alla PIPC per iscritto il risultato (articolo 65 della legge sulla protezione delle informazioni personali in combinato disposto con l'articolo 58 del decreto di applicazione della PIPA).

(125) Per quanto riguarda il parere ai sensi dell'articolo 61, misure correttive ai sensi dell'articolo 64, l'accusa o la consulenza per azioni disciplinari ai sensi dell'articolo 65 e l'imposizione di sanzioni amministrative pecuniarie ai sensi dell'articolo 75 della legge sulla protezione delle informazioni personali, la PIPC può pubblicizzare i fatti, ossia la violazione, il soggetto che ha violato la legge e le misure imposte, pubblicandoli sul proprio sito web o in un quotidiano generale, nazionale giornaliero (articolo 66 della legge sulla protezione delle informazioni personali in combinato disposto con l'articolo 61, primo comma, del decreto di applicazione di tale legge) ([154]).

(126) Infine il rispetto dei requisiti di protezione dei dati di cui alla legge sulla protezione delle informazioni personali (nonché ad altre "leggi in materia di protezione dei dati") è sostenuto da un regime di sanzioni penali. A tale riguardo gli articoli da 70 a 73 della legge sulla protezione delle informazioni personali contengono disposizioni in merito a sanzioni che possono determinare l'irrogazione di una sanzione pecuniaria (compresa tra 20 e 100 milioni di KRW) oppure una pena detentiva (con una pena massima compresa tra 2 e 10 anni). Le violazioni pertinenti comprendono, tra le altre, l'uso di dati personali o la fornitura di tali dati a terzi in assenza del necessario consenso, il trattamento di informazioni sensibili in maniera contraria al divieto di cui all'articolo 23, primo comma, della legge sulla protezione delle informazioni personali, il mancato rispetto dei requisiti di sicurezza applicabili che si traduce nella perdita, nel furto, della falsificazione, nella modifica o nel danneggiamento dei dati personali, la mancata adozione delle misure necessarie per rettificare, cancellare o sospendere i dati personali o il trasferimento illecito dei dati personali a un paese terzo ([155]). Ai sensi dell'articolo 74 della legge sulla protezione delle informazioni personali, in ciascuno di questi casi la responsabilità ricade sul dipendente, sull'agente o sul rappresentante del titolare del trattamento e sul titolare del trattamento stesso ([156]).

(127) Oltre alle sanzioni penali previste nella legge sulla protezione delle informazioni personali, l'uso improprio di dati personali può costituire un reato anche ai sensi del codice penale. Ciò si verifica in particolare per quanto riguarda la violazione della segretezza di lettere, atti o registrazioni elettroniche (articolo 316), la divulgazione di informazioni soggette a segreto professionale (articolo 317), la frode mediante l'uso di computer (articolo 347-2) nonché il peculato e la violazione della fiducia (articolo 355).

(128) Di conseguenza il sistema coreano combina diversi tipi di sanzioni, che spaziano da misure correttive e sanzioni amministrative fino a sanzioni penali, che possono avere un effetto deterrente particolarmente marcato sui titolari

([152]) Inoltre, laddove i sistemi di trattamento e protezione delle informazioni personali gestiti da un titolare del trattamento siano stati certificati essere conformi alla legge sulla protezione delle informazioni personali, ma in realtà i criteri di certificazione ai sensi dell'articolo 34-2, primo comma, del decreto di applicazione della PIPA non siano stati soddisfatti, oppure in caso di una violazione grave di qualsiasi "legge correlata alla protezione delle informazioni [personali]", la PIPC può revocare tale certificazione (articolo 32-2, terzo e quinto comma, della legge sulla protezione delle informazioni personali). La PIPC deve notificare al titolare del trattamento tale revoca e annunciarla pubblicamente o pubblicarla sul proprio sito web o nella gazzetta ufficiale (articolo 34-4 del decreto di applicazione della PIPA). Per le violazioni della legge sulle informazioni creditizie sono inoltre previste sanzioni amministrative (articolo 52 di tale legge) e sanzioni penali (articolo 50 di tale legge).

([153]) Conformemente all'articolo 58, secondo comma, del decreto di applicazione della PIPA, nel caso in cui circostanze particolari rendano il rispetto del parere "impraticabile", il titolare del trattamento deve fornire una giustificazione motivata alla PIPC.

([154]) Nel decidere se effettuare tale divulgazione pubblica, la PIPC tiene conto della sostanza e della gravità della violazione, della sua lunghezza e della sua frequenza, nonché delle sue conseguenze (estensione del danno). Al soggetto in questione deve essere concesso un preavviso e la possibilità di difendersi. Cfr. articolo 61, secondo e terzo comma, del decreto di applicazione della PIPA.

([155]) Cfr. articolo 71, punto 2, in combinato disposto con l'articolo 18, primo comma, della legge sulla protezione delle informazioni personali (mancato rispetto delle condizioni di cui all'articolo 17, terzo comma, di tale legge a cui l'articolo 18, primo comma, fa riferimento). Cfr. anche articolo 75, secondo comma, punto 1, in combinato disposto con l'articolo 17, secondo comma, della legge sulla protezione delle informazioni personali (mancata fornitura delle informazioni necessarie alla persona fisica in questione ai sensi dell'articolo 17, secondo comma, di tale legge, a cui l'articolo 17, terzo comma, fa riferimento).

([156]) Inoltre l'articolo 74-2 della legge sulla protezione delle informazioni personali consente la confisca di qualsiasi somma di denaro, bene o altro profitto acquisita/o come conseguenza della violazione oppure, laddove una confisca sia impossibile, la "riscossione" del beneficio ottenuto in maniera illegittima.

del trattamento e sulle persone fisiche che gestiscono i dati. Subito dopo la sua istituzione nel 2020, la PIPC ha iniziato a utilizzare i propri poteri. Dalla relazione annuale del 2021 della PIPC emerge che tale commissione ha già emesso una serie di raccomandazioni, sanzioni amministrative pecuniarie e ordini per misure correttive, tanto nei confronti del settore pubblico (circa 34 autorità pubbliche) quanto di operatori privati (circa 140 imprese) ([157]). Tra i casi degni di nota figurano ad esempio l'irrogazione di una sanzione pecuniaria di 6,7 miliardi di KRW nel dicembre del 2020 a un'impresa che agiva in violazione di diverse disposizioni della legge sulla protezione delle informazioni personali (compresi i requisiti di sicurezza, i requisiti per il consenso per la fornitura a terzi e la trasparenza) ([158]) e una sanzione pecuniaria di 103,3 milioni di KRW nell'aprile del 2021 ad un'impresa tecnologica attiva nel settore dell'intelligenza artificiale (colpevole di aver violato tra l'altro le norme sulla liceità del trattamento, in particolare quelle sul consenso, e sul trattamento di informazioni pseudonimizzate) ([159]). Nell'agosto del 2021 la PIPC ha finalizzato un'ulteriore indagine sulle attività di tre imprese che ha portato all'adozione di misure correttive e all'irrogazione di sanzioni pecuniarie per un importo fino a 6,47 miliardi di KRW (tra l'altro, per non aver informato le persone fisiche in merito alla divulgazione dei loro dati personali a terzi, compresi trasferimenti verso paesi terzi) ([160]). Inoltre, già prima della recente riforma, la Corea del Sud aveva registrato uno storico notevole in materia di esecuzione, dato che le autorità competenti avevano fanno uso dell'intera gamma di misure di contrasto, comprese le sanzioni amministrative pecuniarie, le misure correttive e la "denominazione e condivisione" rispetto a una varietà di titolari del trattamento, compresi i fornitori di servizi di comunicazione (commissione coreana per le comunicazioni), nonché operatori commerciali, enti finanziari, autorità pubbliche, università ed ospedali (ministero degli Interni e della sicurezza) ([161]). Su tale base la Commissione conclude che il sistema coreano garantisce l'applicazione efficace delle norme sulla protezione dei dati, assicurando in tal modo un livello di protezione sostanzialmente equivalente a quello previsto dal regolamento (UE) 2016/679.

2.5 **Ricorso**

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

(130) Il sistema coreano offre alle persone fisiche diversi meccanismi per far valere efficacemente i loro diritti e ottenere un ricorso (in sede giudiziaria).

(131) Innanzitutto le persone fisiche che ritengono che i loro diritti o i loro interessi in materia di protezione dei dati siano stati violati possono rivolgersi al titolare del trattamento pertinente. Ai sensi dell'articolo 30, primo comma, punto 5, della legge sulla protezione delle informazioni personali, la politica in materia di tutela della vita privata del titolare del trattamento deve contenere tra l'altro informazioni sui diritti degli interessati e sulle modalità per esercitarli. Inoltre deve fornire informazioni di contatto, quali il nome e il numero di telefono del responsabile della tutela della vita privata o dell'ufficio competente per la protezione dei dati, al fine di consentire la presentazione di reclami (nell'atto legislativo coreano in inglese: *grievances*). All'interno dell'organizzazione del titolare del trattamento, il responsabile della tutela della vita privata è competente per la gestione dei reclami, l'adozione di misure correttive in caso di violazione della vita privata e il risarcimento riparatorio (articolo 31, secondo comma, punto 3 e articolo 31, quarto comma, della legge sulla protezione delle informazioni personali). Quest'ultimo aspetto è rilevante ad esempio in caso di una violazione dei dati in quanto il titolare del trattamento deve informare l'interessato in merito ai suoi dati di contatto per la segnalazione tra l'altro di eventuali danni (articolo 34, primo comma, punto 5, della legge sulla protezione delle informazioni personali).

(132) Inoltre la legge sulla protezione delle informazioni personali offre diversi mezzi di ricorso alle persone fisiche nei confronti dei titolari del trattamento. Innanzitutto qualsiasi persona fisica che ritenga che i suoi diritti o i suoi interessi in materia di protezione dei dati siano stati violati dal titolare del trattamento può segnalare tale violazione direttamente alla PIPC e/o a una delle istituzioni specializzate da essa designate per ricevere e gestire i reclami; tra queste figura l'agenzia coreana per la sicurezza e internet che a tale fine gestisce un call centre sulle informazioni personali (il cosiddetto "call centre per la tutela della vita privata") (articolo 62, primo e secondo comma, della legge sulla protezione delle informazioni personali in combinato disposto con l'articolo 59 del decreto di applicazione di tale legge). Il call centre per la tutela della vita privata indaga, constata le violazioni e fornisce consulenza in relazione al trattamento dei dati personali (articolo 62, terzo comma, della legge sulla protezione delle informazioni personali) e può segnalare violazioni alla PIPC ma non può adottare provvedimenti di esecuzione in prima persona). Il call centre per la tutela della vita privata riceve numerosissimi reclami/richieste

([157]) Cfr. relazione annuale del 2021 della PIPC, pagg. 50-55 disponibile (soltanto in coreano) all'indirizzo: https://www.pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS074&mCode=C020010000&nttId=7511#LINK

([158]) Cfr. l'indirizzo (disponibile soltanto in coreano): https://www.pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS074&mCode=C020010000&nttId=6954#LINK.

([159]) Cfr. l'indirizzo (disponibile soltanto in coreano): https://www.pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS074&mCode=C020010000&nttId=7298&fbclid=IwAR3SKcMQi6G5pR9k4l7j6GNXtc8aBVDOwcURevvvzQtYI7AS40UKYXoOXo8.

([160]) Cfr. pagina web (disponibile soltanto in coreano): https://www.pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS074&mCode=C020010000&nttId=7497#LINK.

([161]) Cfr. ad esempio la relazione annuale 2020 (disponibile solo in coreano) all'indirizzo: https://www.pipc.go.kr/np/cop/bbs/selectBoardList.do?bbsId=BS079&mCode=D070020000 e gli esempi forniti in inglese all'indirizzo: https://www.privacy.go.kr/eng/enforcement_02.do.

(ad esempio 177 457 nel 2020, 159 255 nel 2019 e 164 497 nel 2018) ([162]). Secondo le informazioni ricevute dalla PIPC, alla stessa sono pervenuti circa 1 000 reclami tra agosto del 2020 e agosto del 2021. In risposta a un reclamo la PIPC può emettere un parere per l'adozione di miglioramenti, misure correttive, una "accusa" all'agenzia investigativa competente (compreso un pubblico ministero) oppure un parere in merito ad azioni disciplinari (cfr. articoli 61, 64 e 65 della legge sulla protezione delle informazioni personali). Le decisioni della PIPC (quali un rifiuto a gestire un reclamo o un rifiuto sulla sostanza di un reclamo) possono essere impugnate ai sensi della legge sui contenziosi amministrativi ([163]).

(133) In secondo luogo, conformemente agli articoli da 40 a 50 della legge sulla protezione delle informazioni personali in combinato disposto con gli articoli da 48 a 57 del decreto di applicazione della PIPA, gli interessati possono proporre reclamo presso un cosiddetto "comitato di mediazione per le controversie", costituito da rappresentanti nominati dal presidente della PIPC, da membri del servizio esecutivo di alto grado di tale commissione e persone fisiche nominate in base alla loro esperienza nel settore della protezione dei dati tra determinati gruppi ammissibili (cfr. articolo 40, secondo, terzo e settimo comma, della legge sulla protezione delle informazioni personali e articolo 48-14 del decreto di applicazione di quest'ultima legge) ([164]). La possibilità di fare ricorso alla mediazione dinanzi al comitato di mediazione per le controversie offre un metodo alternativo per ottenere riparazione, ma non limita il diritto della persona fisica a rivolgersi piuttosto alla PIPC o agli organi giurisdizionali. Al fine di esaminare il caso, il comitato può richiedere alle parti coinvolte nella controversia di fornire materiali necessari e/o invitare i testimoni pertinenti a comparire dinanzi al comitato stesso (articolo 45 della legge sulla protezione delle informazioni personali). Una volta chiarita la questione, il comitato prepara un progetto di decisione di mediazione ([165]) sulla quale una maggioranza dei suoi membri deve essere concorde. Il progetto di mediazione può comprendere la sospensione della violazione, i rimedi necessari (compresa la restituzione o il risarcimento) nonché tutte le misure necessarie per prevenire la reiterazione della medesima violazione o di una violazione analoga (articolo 47, primo comma, della legge sulla protezione delle informazioni personali). Nel caso in cui entrambe le parti concordino in merito alla decisione di mediazione, quest'ultima avrà il medesimo effetto di una transazione giudiziale (articolo 47, quinto comma, della legge sulla protezione delle informazioni personali). A nessuna delle parti è vietato avviare un'azione giudiziaria mentre la mediazione è in corso, nel qual caso quest'ultima sarà sospesa (cfr. articolo 48, secondo comma, della legge sulla protezione delle informazioni personali) ([166]). I dati annuali pubblicati dalla PIPC mostrano che le persone fisiche ricorrono regolarmente all'uso della procedura dinanzi il comitato di mediazione per le controversie che porta spesso ad un esito positivo. Ad esempio nel 2020 tale comitato ha gestito 126 casi, di cui 89 sono stati risolti dinanzi al comitato stesso (con 77 casi in cui le parti avevano già raggiunto un accordo prima della conclusione della procedura di mediazione e 12 casi in cui le parti hanno accettato la proposta di mediazione), facendo registrare un tasso di mediazione pari al 70,6 % ([167]). Analogamente nel 2019 il comitato ha gestito 139 casi, di cui 92 sono stati risolti, portando a registrare un tasso di mediazione del 62,2 %.

(134) Inoltre, qualora almeno 50 persone fisiche subiscano danni, o i loro diritti di protezione dei dati siano stati violati nello stesso modo o in modo analogo a seguito del medesimo (tipo di) incidente ([168]), un interessato o un'organizzazione che si occupa di protezione dei dati può richiedere la mediazione collettiva della controversia per conto di tale collettività; altri interessati possono presentare domanda di adesione a tale mediazione, che sarà annunciata pubblicamente dal comitato di mediazione delle controversie (articolo 49, primo e terzo comma, della legge sulla protezione delle informazioni personali in combinato disposto con gli articoli da 52 a 54 del decreto di applicazione della PIPA) ([169]). Il comitato di mediazione per le controversie può selezionare almeno una persona che rappresenti in modo più adeguato l'interesse comune affinché agisca da parte rappresentante

([162]) Cfr. relazione annuale del 2021 della PIPC, pag. 174. Nel 2020 tali reclami hanno interessato ad esempio la raccolta di dati in assenza di consenso, il mancato rispetto degli obblighi di trasparenza, violazioni della PIPA da parte di responsabili del trattamento, misure di sicurezza insufficienti, la mancata risposta a richieste di interessati, nonché richieste di informazioni generali.

([163]) In particolare le persone fisiche possono impugnare l'esercizio o il rifiuto dell'esercizio di un potere pubblico da parte di un'agenzia amministrativa (articolo 2, primo comma, punto 1 e articolo 3, punto 1, della legge sui contenziosi amministrativi). Informazioni più dettagliate sugli aspetti procedurali, compresi i requisiti di ammissibilità sono riportate nel considerando 181.

([164]) Tutti i membri hanno un mandato di durata fissa e possono essere rimossi dal loro incarico soltanto per giusta causa (cfr. articolo 40, quinto comma, e articolo 41 della legge sulla protezione delle informazioni personali). Inoltre l'articolo 42 della legge sulla protezione delle informazioni personali contiene garanzie per la protezione contro conflitti di interesse.

([165]) Cfr. articolo 44 della legge sulla protezione delle informazioni personali. Inoltre può proporre un progetto di transazione e raccomandare il regolamento senza ricorrere alla mediazione (cfr. articolo 46 della legge sulla protezione delle informazioni personali).

([166]) Il comitato può inoltre respingere la mediazione qualora ritenga inappropriato mediare la controversia in considerazione della sua natura o perché la domanda di mediazione è stata depositata per una finalità ingiusta (articolo 48 della legge sulla protezione delle informazioni personali).

([167]) Cfr. relazione annuale del 2021 della PIPC, pagg. 179 e 180. Tali casi hanno riguardato tra l'altro violazioni dell'obbligo di ottenere il consenso per la raccolta di dati, del principio di limitazione della finalità e dei diritti degli interessati.

([168]) Cfr. articolo 49, primo comma, della legge sulla protezione delle informazioni personali, secondo il quale gli interessati devono subire danni o una violazione dei loro diritti "in modo identico o simile" e l'articolo 52, punto 2, del decreto di applicazione della PIPA che rende un requisito il fatto che "[q]uestioni importanti degli incidenti siano comuni di fatto o di diritto".

([169]) Inoltre anche i soggetti che non sono parte del contenzioso possono beneficiare di una decisione di mediazione nel contesto di una controversia collettiva accolta dal titolare del trattamento dato che il comitato di mediazione per le controversie può consigliare al titolare del trattamento di preparare e presentare un piano di risarcimento che includa (anche) tali soggetti (articolo 49, quinto comma, della legge sulla protezione delle informazioni personali).

(articolo 49, quarto comma, della legge sulla protezione delle informazioni personali). Laddove il titolare del trattamento rifiuti la mediazione collettiva della controversia o non accetti la decisione di mediazione, alcune organizzazioni ([170]) possono promuovere un'azione collettiva risarcitoria per affrontare la violazione (articoli da 51 a 57 della legge sulla protezione delle informazioni personali).

(135) In terzo luogo, nel caso di una violazione della vita privata che causa "danni" a una persona fisica, l'interessato ha diritto a un ricorso effettivo nel contesto di una "procedura rapida ed equa" (articolo 4, punto 5 e articolo 39 della legge sulla protezione delle informazioni personali) ([171]). Il titolare del trattamento può liberarsi dall'accusa dimostrando l'assenza di colpa ("intento doloso" o negligenza). Laddove l'interessato subisca danni in ragione della perdita, del furto, della divulgazione, della falsificazione, dell'alterazione o del danneggiamento dei suoi dati personali, un organo giurisdizionale può stabilire un risarcimento pari a fino a tre volte il danno effettivo, tenendo conto di una serie di fattori (articolo 39, terzo e quarto comma, della legge sulla protezione delle informazioni personali). In alternativa l'interessato può richiedere un "ammontare ragionevole" di risarcimento non superiore a 3 milioni di KRW (articolo 39-2, primo e secondo comma, della legge sulla protezione delle informazioni personali). Inoltre, conformemente al codice civile, il risarcimento può essere richiesto nei confronti di qualsiasi persona "che causa perdite o infligge lesioni a un'altra persona in ragione di un atto illecito, intenzionalmente o per negligenza" ([172]) oppure nei confronti di una persona "che ha leso l'integrità, la libertà o la fama di un'altra persona o ha inflitto qualsiasi angoscia mentale a un'altra persona" ([173]). Tale responsabilità civile a seguito della violazione delle norme in materia di protezione dei dati è stata confermata dalla Corte suprema ([174]). Se il danno è stato causato da un'azione illecita di un'autorità pubblica, è possibile presentare una richiesta di risarcimento anche ai sensi della *State Compensation Act* (legge sul risarcimento da parte dello Stato) ([175]). Una tale richiesta può essere depositata presso un "consiglio per il risarcimento" specializzato oppure direttamente adendo gli organi giurisdizionali coreani ([176]). La responsabilità dello Stato si applica anche a danni non materiali (quali la sofferenza mentale) ([177]). Se la vittima è un cittadino straniero, la legge sul risarcimento da parte dello Stato si applica nella misura in cui il suo paese di origine garantisce allo stesso modo un risarcimento da parte dello Stato a favore di cittadini coreani ([178]).

(136) In quarto luogo la Corte suprema ha riconosciuto che le persone fisiche hanno il diritto di richiedere un provvedimento ingiuntivo per violazioni dei loro diritti ai sensi della costituzione, compreso il diritto alla protezione dei dati personali ([179]). In tale contesto un organo giurisdizionale può ad esempio ordinare ai titolari del trattamento di sospendere o interrompere qualsiasi attività illecita. Inoltre si può chiedere l'esecuzione di diritti di protezione dei dati, compresi quelli protetti dalla legge sulla protezione delle informazioni personali, tramite azioni civili. Tale applicazione orizzontale della tutela costituzionale della vita privata alle relazioni tra parti private è stata riconosciuta dalla Corte suprema ([180]).

([170]) In particolare i gruppi di consumatori o le ONG senza scopo di lucro di una certa dimensione in termini di adesione la cui finalità dichiarata è la protezione dei dati (anche se nel caso di quest'ultima circostanza si applica il requisito aggiuntivo secondo il quale almeno 100 interessati che hanno subito lo stesso (tipo di) violazione devono aver presentato una richiesta di avvio di un'azione collettiva risarcitoria). Cfr. articolo 51 della legge sulla protezione delle informazioni personali.

([171]) Gli articoli da 43 a 43-3 della legge sulle informazioni creditizie stabiliscono anche la responsabilità di compensare i danni a seguito di violazioni di tale legge.

([172]) Articolo 750 del codice civile.

([173]) Articolo 751, primo comma, del codice civile.

([174]) Cfr. ad esempio la decisione della Corte suprema 2015Da251539, 251546, 251553, 251560, 251577, 30 maggio 2018. Inoltre la Corte suprema ha confermato che le violazioni dei dati possono determinare il riconoscimento di un risarcimento dei danni ai sensi del codice civile, cfr. decisione della Corte suprema 2011Da59834, 59858, 59841, 26 dicembre 2012 (sintesi in inglese disponibile all'indirizzo: http://library.scourt.go.kr/SCLIB_data/decision/9-69%202012.12.26.2011Da59834.htm). In questo caso, la Corte suprema ha chiarito che, ai fini della valutazione dell'eventualità che una persona fisica abbia subito una sofferenza emotiva che si qualifica come un danno risarcibile, si dovrebbero considerare diversi fattori quali il tipo e le caratteristiche delle informazioni divulgate, l'identificabilità della persona fisica in ragione della violazione, la possibilità di accedere ai dati da parte di terzi, la misura in cui le informazioni personali sono state diffuse, se ciò ha portato a eventuali ulteriori violazioni di diritti individuali, in che modo le informazioni personali sono state gestite e protette, ecc.

([175]) Ai sensi della legge sul risarcimento da parte dello Stato, le persone fisiche possono presentare domanda di risarcimento dei danni causati da funzionari pubblici nello svolgimento delle loro funzioni ufficiali in violazione della legge (articolo 2, primo comma, di tale legge).

([176]) Articoli 9 e 12 della legge sul risarcimento da parte dello Stato. Tale legge istituisce i consigli distrettuali (presieduti dal vice pubblico ministero del corrispondente ufficio della procura), un consiglio centrale (presieduto dal vice ministro della Giustizia) e un consiglio speciale (competente per le richieste di risarcimento di danni causati da personale militare o dipendenti civili delle forze armate, presieduto dal vice ministro della Difesa nazionale). Le richieste di risarcimento sono in linea di principio gestite dai consigli distrettuali che, in determinate circostanze, devono rinviare i casi al consiglio centrale/speciale, ad esempio se il risarcimento supera un determinato importo o nel caso in cui una persona fisica presenti una domanda di nuova deliberazione. Tutti i consigli sono costituiti da membri nominati dal ministro della Giustizia (ad esempio tra i funzionari pubblici del ministero della Giustizia, degli ufficiali giudiziari, degli avvocati e delle persone che hanno esperienza in relazione al risarcimento da parte dello Stato) e sono soggetti a norme specifiche in materia di conflitti di interesse (cfr. articolo 7 del decreto di applicazione della legge sul risarcimento da parte dello Stato).

([177]) Cfr. articolo 8 della legge sul risarcimento da parte dello Stato (che fa riferimento al codice civile), nonché l'articolo 751 del codice civile.

([178]) Articolo 7 della legge sul risarcimento da parte dello Stato.

([179]) Decisione della Corte suprema 93Da40614, 12 aprile 1996 e decisione 2008Da42430, 2 settembre 2011 (sintesi in inglese disponibile all'indirizzo: https://www.scourt.go.kr/eng/supreme/decisions/NewDecisionsView.work?seq=696&pageIndex=1&mode=6&searchWord).

([180]) Cfr. ad esempio la decisione della Corte suprema 2008Da42430, 2 settembre 2011 (sintesi in inglese disponibile all'indirizzo: https://www.scourt.go.kr/eng/supreme/decisions/NewDecisionsView.work?seq=696&pageIndex=1&mode=6&searchWord).

(137) Infine le persone fisiche possono presentare una denuncia penale ai sensi del codice penale (articolo 223) presso un pubblico ministero o un funzionario della polizia giudiziaria ([181]).

(138) Il sistema coreano offre pertanto svariati modi per ottenere risarcimento che spaziano da opzioni facilmente accessibili e a basso costo (ad esempio contattando il call centre per la tutela della vita privata oppure tramite la mediazione (collettiva)) fino alle opzioni amministrative (rivolgendosi alla PIPC) e alle vie giudiziarie, disponendo altresì della possibilità di ottenere un risarcimento dei danni.

3. ACCESSO E USO DEI DATI PERSONALI TRASFERITI DALL'UNIONE EUROPEA DA PARTE DI AUTORITÀ PUBBLICHE NELLA REPUBBLICA DI COREA

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

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

(141) Innanzitutto qualsiasi limitazione nell'esercizio del diritto alla protezione dei dati personali deve essere prevista dalla legge e implica che la base giuridica che consente l'ingerenza in tali diritti deve definire essa stessa la portata della limitazione dell'esercizio del diritto considerato ([182]).

(142) In secondo luogo, per soddisfare il requisito di proporzionalità secondo cui le deroghe e le limitazioni alla protezione dei dati personali devono operare nei limiti dello stretto necessario in una società democratica per soddisfare gli obbiettivi specifici di interesse generale equivalenti a quelli riconosciuti dall'Unione, la legislazione del paese terzo in questione che consente tale ingerenza deve prevedere regole chiare e precise che disciplinino la portata e l'applicazione della misura in questione e impongano requisiti minimi in modo che le persone i cui dati sono trasferiti dispongano di garanzie sufficienti che permettano di proteggere efficacemente i loro dati personali contro il rischio di abusi ([183]). In particolare, essa deve indicare in quali circostanze e a quali condizioni possa essere adottata una misura che prevede il trattamento di siffatti dati ([184]) nonché assoggettare il soddisfacimento di tali requisiti alla vigilanza indipendente ([185]).

(143) In terzo luogo tale legislazione e i suoi requisiti devono essere legalmente vincolanti ai sensi del diritto interno. Ciò riguarda innanzitutto tutte le autorità del paese terzo in questione, ma tali requisiti giuridici devono altresì poter essere fatti valere dinanzi agli organi giurisdizionali nei confronti di tali autorità ([186]). In particolare gli interessati devono disporre della possibilità di esperire mezzi di ricorso dinanzi a un giudice indipendente e imparziale al fine di avere accesso a dati personali che li riguardano, o di ottenere la rettifica o la soppressione di tali dati ([187]).

3.1 Quadro giuridico generale

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

([181]) Come illustrato al considerando 127, l'uso improprio di dati può costituire un reato ai sensi del codice penale.

([182]) Cfr. *Schrems II*, punti 174 e 175 e giurisprudenza citata. Cfr. anche, per quanto riguarda l'accesso da parte di autorità pubbliche di Stati membri, sentenza della Corte di giustizia del 6 ottobre 2020, *Privacy International*, C-623/17, ECLI:EU:C:2020:790, punto 65; e sentenza della Corte di giustizia del 6 ottobre 2020, *La Quadrature du Net e a.*, cause riunite C-511/18, C-512/18 e C-520/18, ECLI:EU:C:2020:791, punto 175.

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

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

([185]) Cfr. *Schrems II*, punto 179.

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

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

(145) Innanzitutto l'accesso ai dati personali da parte delle autorità pubbliche coreane è disciplinato da principi generali di legalità, necessità e proporzionalità che derivano dalla costituzione coreana ([188]). In particolare diritti e libertà fondamentali (compreso il diritto alla tutela della vita privata e il diritto alla tutela della vita privata della corrispondenza) ([189]) possono essere limitati soltanto per legge e laddove necessario per la sicurezza nazionale o il mantenimento dell'ordine pubblico per il benessere pubblico. Tali limitazioni non possono incidere sull'essenza del diritto o della libertà in questione. Per quanto riguarda nello specifico le perquisizioni e i sequestri, la costituzione prevede che tali attività possano essere condotte soltanto come previsto dalla legge, sulla base di un mandato emesso da un giudice e in relazione a un giusto processo ([190]). Infine le persone fisiche possono invocare i loro diritti e le loro libertà dinanzi alla Corte costituzionale se ritengono che siano stati violati dalle autorità pubbliche nell'esercizio delle loro funzioni ([191]). Analogamente le persone fisiche che hanno subito danni in ragione di un atto illecito commesso da un funzionario pubblico nello svolgimento delle sue funzioni ufficiali hanno il diritto di richiedere un risarcimento equo ([192]).

(146) In secondo luogo, come descritto in maggior dettaglio nelle sezioni 3.2.1 e 3.3.1, i principi generali di cui al considerando 145 si rispecchiano altresì nelle leggi specifiche che disciplinano i poteri delle autorità di contrasto e di quelle di sicurezza nazionale. Ad esempio, per quanto concerne le indagini penali, il codice di procedura penale prevede che misure obbligatorie possano essere adottate soltanto se esplicitamente previste in tale codice, e nella minima misura necessaria ai fini del conseguimento della finalità dell'indagine ([193]). Analogamente l'articolo 3 della legge sulla tutela della vita privata nelle comunicazioni (in appresso: "legge sulle comunicazioni") vieta l'accesso a comunicazioni private, fatta eccezione in base alla legge e nel rispetto di limitazioni e garanzie ivi stabilite. Nel settore della sicurezza nazionale, la *National Intelligence Service Act* (legge sul servizio nazionale di intelligence, in appresso: "legge sul NIS") prevede che qualsiasi accesso a comunicazioni o informazioni relative all'ubicazione debba rispettare la legge e assoggetta l'abuso di potere e violazioni della legge a sanzioni penali ([194]).

(147) In terzo luogo il trattamento dei dati personali da parte delle autorità pubbliche, anche per finalità di contrasto e di sicurezza nazionale, è soggetto alle norme in materia di protezione dei dati di cui alla legge sulla protezione delle informazioni personali ([195]). Come principio generale, l'articolo 5, primo comma, della legge sulla protezione delle informazioni personali impone alle autorità pubbliche di sviluppare politiche destinate a prevenire "l'abuso e l'uso improprio di informazioni personali, la sorveglianza e il tracciamento indiscreti, ecc. nonché a migliorare la dignità degli esseri umani e la vita privata individuale". Inoltre, qualsiasi titolare del trattamento deve trattare i dati personali in modo tale da ridurre al minimo la possibilità di violazione della tutela della vita privata dell'interessato (articolo 3, sesto comma, della legge sulla protezione delle informazioni personali).

(148) Tutti i requisiti della legge sulla protezione delle informazioni personali, come descritti in dettaglio nella sezione 2, si applicano al trattamento dei dati personali per finalità di contrasto. Rientrano in tale contesto i principi fondamentali (quali la liceità e la correttezza, la limitazione della finalità, l'esattezza, la minimizzazione dei dati, la limitazione della conservazione, la sicurezza e la trasparenza), le obbligazioni (ad esempio in relazione alla notifica di violazioni di dati ed a dati sensibili) e i diritti (di ottenere accesso, di rettifica, di cancellazione e di sospensione).

(149) Mentre il trattamento di dati personali per finalità di sicurezza nazionale è soggetto a una serie più limitata di disposizioni ai sensi della legge sulla protezione delle informazioni personali, si applicano i principi fondamentali, nonché le norme in materia di vigilanza, esecuzione e ricorso ([196]). Più in particolare, gli articoli 3 e 4 della legge sulla protezione delle informazioni personali stabiliscono i principi generali in materia di protezione dei dati (liceità e correttezza, limitazione della finalità, correttezza, minimizzazione dei dati, sicurezza e trasparenza) e diritti individuali (il diritto di essere informato, il diritto di accesso e i diritti di rettifica, cancellazione e sospensione) ([197]). L'articolo 4, quinto comma, della legge sulla protezione delle informazioni personali riconosce inoltre alle persone fisiche il diritto a un risarcimento adeguato per i danni derivanti dal trattamento dei loro dati

([188]) Cfr. allegato II, sezione 1.1.
([189]) Articolo 37, secondo comma, della costituzione.
([190]) Articolo 16 e articolo 12, terzo comma, della costituzione. L'articolo 12, terzo comma, della costituzione, stabilisce altresì le circostanze eccezionali nelle quali potrebbero verificarsi perquisizioni o sequestri in assenza di mandato (sebbene sia comunque richiesto un mandato ex post), ossia in caso di flagranza di reato oppure per i reati soggetti a pena detentiva di almeno tre anni, laddove vi sia il rischio che elementi di prova vengano distrutti o che l'indiziato sparisca.
([191]) Articolo 68, primo comma, della legge sulla Corte costituzionale.
([192]) Articolo 29, primo comma, della costituzione.
([193]) Articolo 199, primo comma, del codice di procedura penale. Più in generale, nell'esercizio dei loro poteri ai sensi del codice di procedura penale, le autorità pubbliche devono rispettare i diritti fondamentali dei presunti autori di reati e di qualsiasi altra persona interessata (articolo 198, secondo comma, di tale codice).
([194]) Articolo 14 della legge sul NIS.
([195]) Cfr. allegato II, sezione 1.2.
([196]) Articolo 58, primo comma, punto 2, della legge sulla protezione delle informazioni personali. Cfr. anche sezione 6 della notifica n. 2021-5 (allegato I). Tale esenzione da talune disposizioni della legge sulla protezione delle informazioni personali si applica soltanto quando i dati personali vengono trattati "per finalità di sicurezza nazionale". Quando la circostanza relativa alla sicurezza nazionale che giustificava il trattamento si è conclusa, l'esenzione non può più essere invocata e si applicano tutti i requisiti della legge sulla protezione delle informazioni personali.
([197]) Tali diritti possono essere limitati soltanto laddove previsto dalla legge nella misura e per il tempo necessari e proporzionati per proteggere un obiettivo importante di interesse pubblico oppure quando la concessione del diritto può causare un danno alla vita o all'incolumità di una terza parte oppure la violazione ingiustificata di interessi patrimoniali e di altra natura di una terza parte. Cfr. sezione 6 della notifica n. 2021-5.

personali nel contesto di una procedura rapida ed equa. Ciò è integrato da obblighi più specifici che impongono di trattare i dati personali esclusivamente nella misura minima necessaria per il conseguimento della finalità prevista e per il periodo minimo, di mettere in atto le misure necessarie per garantire una gestione sicura dei dati e un trattamento adeguato (quali garanzie tecniche, gestionali e fisiche), oltre a mettere in atto misure per la gestione adeguata di reclami ([198]). Infine i principi generali di legalità, necessità e proporzionalità derivanti dalla costituzione coreana (cfr. considerando 145) si applicano anche al trattamento dei dati personali per finalità di sicurezza nazionale.

(150) Tali limitazioni e garanzie generali possono essere invocate da persone fisiche rivolgendosi all'organismo indipendente di vigilanza (ad esempio la PIPC e/o la *National Human Rights Commission*, (NHRC, commissione nazionale per i diritti umani), cfr. considerando 177 e 178) e adendo organi giurisdizionali (cfr. considerando da 179 a 183) per ottenere risarcimento.

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

(151) Il diritto della Repubblica di Corea impone una serie di limitazioni in materia di accesso e uso di dati personali per finalità di contrasto penale e prevede meccanismi di vigilanza e ricorso che sono in linea con i requisiti di cui ai considerando da 141 a 143 della presente decisione. Le condizioni in cui tale accesso può avvenire e le garanzie applicabili all'uso di tali poteri sono valutate in dettaglio nelle sezioni che seguono.

3.2.1 *Basi giuridiche, limitazioni e garanzie*

(152) I dati personali trattati dai titolari del trattamento coreani che sarebbero trasferiti dall'Unione ai sensi della presente decisione ([199]) possono essere raccolti dalle autorità coreane per finalità di contrasto penale nel contesto di una perquisizione o di un sequestro (ai sensi del codice di procedura penale), accedendo a informazioni sulle comunicazioni (sulla base della legge sulle comunicazioni) oppure ottenendo i dati dell'abbonato attraverso richieste di divulgazione volontaria (sulla base della legge sulle imprese di telecomunicazione) ([200]).

3.2.1.1 Perquisizioni e sequestri

(153) Il codice di procedura penale prevede che una perquisizione o un sequestro possa avvenire soltanto se una persona è sospettata della commissione di un reato, se ciò è necessario ai fini dell'indagine e se è stato stabilito un legame tra l'indagine e la persona da sottoporre a perquisizione o ai beni da ispezionare e sequestrare ([201]). Inoltre una perquisizione o un sequestro (come qualsiasi misura obbligatoria) può essere autorizzato/a o condotta/o soltanto nella minima misura necessaria ([202]). Se una perquisizione riguarda il disco rigido di un computer o un altro supporto di memorizzazione dati, in linea di principio saranno sequestrati soltanto i dati necessari (copiati o stampati) anziché l'intero supporto ([203]). Quest'ultimo può essere sequestrato soltanto quando viene considerato sostanzialmente impossibile stampare o copiare i dati richiesti separatamente o quando è considerato sostanzialmente impraticabile conseguire diversamente la finalità della perquisizione ([204]). Il codice di procedura penale stabilisce quindi norme chiare e precise sull'ambito di applicazione e sull'applicazione di tali misure, garantendo così che l'ingerenza nei diritti delle persone in caso di perquisizione o sequestro sia limitata/o a quanto necessario per una specifica indagine penale e proporzionata/o alla finalità perseguita.

([198]) Articolo 58, quarto comma, della legge sulla protezione delle informazioni personali.

([199]) Cfr. allegato II, sezione 2.1. La dichiarazione ufficiale del governo coreano (sezione 2.1 dell'allegato II) fa riferimento altresì alla possibilità di raccogliere informazioni sulle operazioni finanziarie al fine di prevenire il riciclaggio di denaro e il finanziamento del terrorismo sulla base della *Act on Reporting and Using Specified Financial Transaction Information* (legge sulla segnalazione e l'utilizzo di informazioni specifiche sulle operazioni finanziarie). Tale legge impone tuttavia obblighi di divulgazione soltanto ai titolari del trattamento che trattano informazioni creditizie personali ai sensi della legge sulle informazioni creditizie e sono soggetti a vigilanza da parte della commissione per i servizi finanziari (cfr. considerando 13). Dato che il trattamento di informazioni creditizie personali da parte di tali titolari del trattamento è escluso dall'ambito di applicazione della presente decisione, la legge sulla segnalazione e l'utilizzo di informazioni specifiche sulle operazioni finanziarie non è pertinente ai fini della presente valutazione.

([200]) L'articolo 3 della legge sulle comunicazioni menziona altresì la legge sugli organi giurisdizionali militari come possibile base giuridica per la raccolta di dati relativi alle comunicazioni. Tuttavia tale legge disciplina la raccolta di informazioni concernenti il personale militare e può applicarsi ai civili soltanto in un numero limitato di casi (ad esempio, nel caso in cui membri del personale militare e civili commettessero un reato congiuntamente oppure se una persona fisica commette un reato nei confronti di militari, il procedimento corrispondente può essere avviato dinanzi un organo giurisdizionale militare, cfr. articolo 2 della legge sugli organi giurisdizionali militari). In ogni caso, stabilisce disposizioni generali che disciplinano le perquisizioni e i sequestri che sono simili al codice di procedura penale (cfr. articoli da 146 a 149 e da 153 a 156 della legge sugli organi giurisdizionali militari) e prevede ad esempio che la corrispondenza postale possa essere raccolta soltanto se necessario a un'indagine e sulla base di un mandato di un organo giurisdizionale militare. Nella misura in cui comunicazioni elettroniche vengano raccolte sulla base di tale legge, si applicano le limitazioni e le garanzie di cui alla legge sulle comunicazioni. Cfr. allegato II, sezione 2.2.2 e nota 50.

([201]) Articolo 215, primo e secondo comma, del codice di procedura penale. Cfr. anche l'articolo 106, primo comma, l'articolo 107 e l'articolo 109 del codice di procedura penale, che prevedono che gli organi giurisdizionali possano effettuare perquisizioni e sequestri a condizione che gli articoli o le persone interessati siano considerati legati a un caso specifico. Cfr. allegato II, sezione 2.2.1.2.

([202]) Articolo 199, primo comma, del codice di procedura penale.

([203]) Articolo 106, terzo comma, del codice di procedura penale.

([204]) Articolo 106, terzo comma, del codice di procedura penale.

(154) In termini di garanzie procedurali, il codice di procedura penale prescrive che per effettuare una perquisizione o un sequestro sia necessario ottenere un mandato ([205]). Una perquisizione o un sequestro in assenza di mandato è consentita/o soltanto in via eccezionale, ossia in circostanze urgenti ([206]), in loco al momento dell'arresto o del trattenimento di un indiziato per un reato ([207]) oppure laddove un oggetto sia gettato o prodotto volontariamente da un indiziato per un reato o una terza persona (per quanto concerne i dati personali, dalla persona fisica in questione) ([208]). Perquisizioni e sequestri illegali sono soggetti a sanzioni penali ([209]) e qualsiasi elemento di prova ottenuto in violazione del codice di procedura penale è considerato inammissibile ([210]). Infine occorre sempre notificare senza indugio ([211]) le persone fisiche interessate in merito a una perquisizione o a un sequestro (anche in caso di sequestro dei loro dati); una circostanza questa che a sua volta faciliterà l'esercizio dei diritti sostanziali della persona fisica e il diritto al ricorso (cfr. in particolare la possibilità di impugnare l'esecuzione di un mandato di sequestro, cfr. considerando 180).

3.2.1.2 Accesso alle informazioni sulle comunicazioni

(155) Sulla base della legge sulle comunicazioni, le autorità coreane di contrasto in materia penale possono adottare due tipi di misure ([212]): da un lato, la raccolta di "dati di conferma di comunicazioni" ([213]), che comprende la data delle telecomunicazioni, il loro orario di inizio e di fine, il numero di chiamate in uscita e in arrivo, nonché il numero dell'abbonato dell'altro capo, la frequenza d'uso, i file di registro sull'uso dei servizi di telecomunicazione e le informazioni relative all'ubicazione (ad esempio dalle torri di trasmissione presso le quali vengono ricevuti i segnali); e, dall'altro, "misure di limitazione delle comunicazioni", relative tanto alla raccolta del contenuto della corrispondenza per posta tradizionale quanto l'intercettazione diretta del contenuto di telecomunicazioni ([214]).

(156) I dati di conferma di comunicazioni possono essere accessibili soltanto quando necessario per condurre un'indagine penale o dare esecuzione a una sentenza ([215]), sulla base di un mandato rilasciato da un organo giurisdizionale ([216]). A tale riguardo, la legge sulle comunicazioni richiede la fornitura di informazioni dettagliate tanto nella domanda per l'ottenimento di un mandato (ad esempio in merito ai motivi della richiesta, alla relazione con la persona/l'abbonato in questione e ai dati necessari) quanto nel mandato stesso (ad esempio in merito all'obiettivo, all'oggetto e alla portata della misura) ([217]). La raccolta in assenza di mandato può verificarsi soltanto quando motivi di urgenza rendono impossibile ottenere l'autorizzazione da parte dell'organo giurisdizionale, nel qual caso

([205]) Articolo 215, primo e secondo comma, e articolo 113 del codice di procedura penale. Al momento della richiesta di mandato, l'autorità interessata deve presentare materiali che dimostrino i motivi per sospettare una persona fisica della commissione di un reato, la necessità della perquisizione, dell'ispezione o del sequestro, nonché l'esistenza di oggetti pertinenti da sequestrare (articolo 108, primo comma, del regolamento sulla procedura penale). Il mandato stesso deve specificare, tra l'altro, i nomi dell'indiziato e il reato; il luogo, la persona o gli oggetti da sottoporre a perquisizione o gli oggetti da sequestrare; la data di emissione; e il periodo efficace per l'applicazione (articolo 114, primo comma, in combinato disposto con l'articolo 219 del codice di procedura penale). Cfr. allegato II, sezione 2.2.1.2.

([206]) Ossia, laddove sia impossibile ottenere un mandato in ragione dell'urgenza sulla scena di un reato (articolo 216, terzo comma, del codice di procedura penale), nel qual caso un mandato deve comunque essere ottenuto successivamente senza indugio (articolo 216, terzo comma, del medesimo codice).

([207]) Articolo 216, primo e secondo comma, del codice di procedura penale.

([208]) Articolo 218 del codice di procedura penale. Inoltre, come spiegato nella sezione 2.2.1.2 dell'allegato II, gli oggetti prodotti volontariamente sono ammessi come elementi di prova nei procedimenti giudiziari soltanto se non vi è alcun dubbio ragionevole circa la natura volontaria della divulgazione, aspetto che spetta al pubblico ministero dimostrare.

([209]) Articolo 321 del codice penale.

([210]) Articolo 308-2 del codice di procedura penale. Inoltre una persona fisica (e il suo legale) può essere presente quando viene data esecuzione a un mandato di perquisizione o di sequestro e può quindi altresì sollevare un'obiezione nel momento in cui il mandato viene eseguito (articoli 121 e 219 del codice di procedura penale).

([211]) Articolo 121 e 122 del codice di procedura penale (in relazione a perquisizioni) e articolo 219 in combinato disposto con l'articolo 106, quarto comma, del codice di procedura penale (in relazione ai sequestri).

([212]) Cfr. anche allegato II, sezione 2.2.2.1. Tali misure possono essere adottate con l'assistenza che deve essere obbligatoriamente fornita dagli operatori di telecomunicazioni nel momento in cui a tali operatori viene presentata un'autorizzazione scritta ottenuta da un organo giurisdizionale (articolo 9, secondo comma, della legge sulle comunicazioni), che deve essere conservata dagli operatori (articolo 15-2 della medesima legge e articolo 12 del decreto di applicazione di tale legge). I fornitori di servizi di telecomunicazione possono rifiutare la cooperazione quando le informazioni sulla persona fisica in questione indicata nell'autorizzazione scritta dell'organo giurisdizionale (ad esempio il suo numero di telefono) non sono corrette; inoltre a tali fornitori è vietato in qualsiasi circostanza divulgare le password utilizzate per le telecomunicazioni (articolo 9, quarto comma, della legge sulle comunicazioni).

([213]) Articolo 2, undicesimo comma, della legge sulle comunicazioni.

([214]) Cfr. articolo 2, sesto comma, della legge sulle comunicazioni, riferito alla "censura" (apertura di corrispondenza senza il consenso della parte in questione o l'acquisizione di conoscenza, la registrazione o il trattenimento dei rispettivi contenuti attraverso altri mezzi) e articolo 2, settimo comma, della medesima legge, concernente l'"intercettazione" (acquisizione o registrazione di contenuti di telecomunicazioni ascoltando o leggendo in associazione suoni, parole, simboli o immagini delle comunicazioni attraverso dispositivi elettronici e meccanici senza il consenso della parte interessata oppure interferenza con la loro trasmissione e ricezione).

([215]) Articolo 13, primo comma, della legge sulle comunicazioni. Cfr. anche allegato II, sezione 2.2.2.3. Inoltre i dati di monitoraggio dell'ubicazione in tempo reale e i dati di conferma di comunicazioni relativi a una stazione base specifica possono essere raccolti soltanto per un'indagine in merito a reati gravi o laddove sarebbe altrimenti difficile prevenire la commissione di un reato oppure per la raccolta di elementi di prova (articolo 13, secondo comma, della legge sulle comunicazioni). Ciò rispecchia la necessità di prevedere garanzie supplementari in caso di misure particolarmente intrusive in relazione alla vita privata, in linea con il principio di proporzionalità.

([216]) Articoli 13 e 6 della legge sulle comunicazioni.

([217]) Cfr. articolo 13, terzo e nono comma, in combinato disposto con l'articolo 6, quarto e sesto comma, della legge sulle comunicazioni.

il mandato deve essere ottenuto e comunicato al fornitore di servizi di telecomunicazione immediatamente dopo aver richiesto i dati ([218]). Laddove l'organo giurisdizionale rifiuti la concessione dell'autorizzazione conseguente, le informazioni raccolte devono essere distrutte ([219]).

(157) In termini di garanzie supplementari rispetto alla raccolta dei dati di conferma di comunicazioni, la legge sulle comunicazioni impone requisiti specifici in materia di tenuta di registri e trasparenza ([220]). In particolare tanto le autorità di contrasto in materia penale ([221]) quanto i fornitori di servizi di telecomunicazione ([222]) devono tenere registri delle richieste e delle divulgazioni effettuate. Inoltre, in linea di principio, le autorità di contrasto penale devono notificare alle persone fisiche la raccolta dei loro dati di conferma di comunicazioni ([223]). Tale notifica può essere differita soltanto in circostanze eccezionali, sulla base di un'autorizzazione del direttore di un ufficio distrettuale del pubblico ministero competente ([224]). Tale autorizzazione può essere rilasciata soltanto quando è probabile che la notifica: 1) comprometta la sicurezza nazionale, nonché la sicurezza e l'ordine pubblici; 2) causi decessi o lesioni personali; 3) ostacoli procedimenti giudiziari equi (ad esempio determinando la distruzione di elementi di prova o minacce ai testimoni); oppure 4) diffami l'indiziato, le vittime o altre persone collegate al caso oppure invada la loro vita privata. In tali casi la notifica deve essere fornita entro 30 giorni dal momento in cui motivo o i motivi per il differimento cessano di esistere ([225]). All'atto della notifica, le persone fisiche hanno il diritto di ottenere informazioni sui motivi della raccolta dei loro dati ([226]).

(158) Norme più severe si applicano per quanto concerne le misure di limitazione delle comunicazioni, che possono essere utilizzate soltanto quando esiste un motivo sostanziale per sospettare che siano stati pianificati o commessi o che saranno commessi determinati reati gravi specificatamente elencati nella legge sulle comunicazioni ([227]). Misure di limitazione delle comunicazioni possono inoltre essere adottate soltanto come misura di ultima istanza e laddove sia altrimenti difficile prevenire la commissione di un reato, arrestare un criminale o raccogliere elementi di prova ([228]). Tali misure devono essere interrotte immediatamente non appena non sono più necessarie, in maniera da assicurare che la violazione della vita privata delle comunicazioni sia limitata il più possibile ([229]). Le informazioni che sono state ottenute illecitamente mediante misure di limitazione delle comunicazioni non sono ammesse come elementi di prova nel contesto di procedimenti giudiziari o disciplinari ([230]).

(159) In termini di garanzie procedurali, la legge sulle comunicazioni prescrive che per attuare misure di limitazione delle comunicazioni sia necessario ottenere un mandato ([231]). Ancora una volta la legge sulle comunicazioni richiede che la domanda di rilascio di un mandato e il mandato stesso contengano informazioni dettagliate ([232]), anche in merito alla giustificazione della richiesta, nonché alle comunicazioni da raccogliere (che devono essere quelle della persona sospettata soggetta ad indagine) ([233]). Tali misure possono essere adottate in assenza di un mandato soltanto in caso di una minaccia imminente di un atto di criminalità organizzata o qualora sia imminente un altro reato grave che può causare direttamente la morte o lesioni gravi, nonché in presenza di

([218]) Articolo 13, secondo comma, della legge sulle comunicazioni.
([219]) Articolo 13, terzo comma, della legge sulle comunicazioni.
([220]) Cfr. allegato II, sezione 2.2.2.3.
([221]) Articolo 13, quinto e sesto comma, della legge sulle comunicazioni.
([222]) Articolo 13, settimo comma, della legge sulle comunicazioni. Inoltre i fornitori di servizi di telecomunicazione devono comunicare due volte l'anno informazioni sulla divulgazione di dati di conferma di comunicazioni al ministero della Scienza e delle TIC.
([223]) Articolo 13-3, settimo comma, in combinato disposto con l'articolo 9-2, della legge sulle comunicazioni. In particolare occorre notificare alle persone fisiche entro 30 giorni dall'adozione di una decisione di procedere (o meno) con l'azione giudiziaria o entro 30 giorni trascorso un anno dalla decisione di sospendere il rinvio a giudizio (sebbene la notifica debba essere fornita in ogni caso entro 30 giorni trascorso un anno dalla raccolta delle informazioni), cfr. articolo 13-3, primo comma, della legge sulle comunicazioni.
([224]) Articolo 13-3, secondo e terzo comma, della legge sulle comunicazioni.
([225]) Articolo 13-3, quarto comma, della legge sulle comunicazioni.
([226]) Articolo 13-3, quinto comma, della legge sulle comunicazioni. Su richiesta della persona fisica, un pubblico ministero o un funzionario della polizia giudiziario deve fornire per iscritto le motivazioni entro 30 giorni dalla ricezione della richiesta, fatto salvo il caso in cui si applichi una delle eccezioni per il differimento della notifica (articolo 13-3, sesto comma, della legge sulle comunicazioni).
([227]) Ad esempio insurrezioni, reati legati alla droga, reati che coinvolgono esplosivi, nonché reati relativi alla sicurezza nazionale, a relazioni diplomatiche o basi e installazioni militari, cfr. articolo 5, primo comma, della legge sulle comunicazioni. Cfr. anche allegato II, sezione 2.2.2.2.
([228]) Articolo 3, secondo comma, e articolo 5, primo comma, della legge sulle comunicazioni.
([229]) Articolo 2 del decreto di applicazione della legge sulle comunicazioni.
([230]) Articolo 4 della legge sulle comunicazioni.
([231]) Articolo 6, primo e secondo comma e dal quinto al sesto comma, della legge sulle comunicazioni.
([232]) Una domanda di rilascio di un mandato deve descrivere: 1) i motivi sostanziali per sospettare (prima facie) che uno dei reati elencati sia stato pianificato o che la sua commissione sia in atto o che sia stato commesso, unitamente a qualsiasi materiale giustificativo; 2) le misure di limitazione delle comunicazioni, unitamente all'oggetto, alla portata, all'obiettivo e alla durata di efficacia delle stesse; e 3) il luogo in cui le misure verrebbero eseguite e le modalità di attuazione (articolo 6, quarto comma, della legge sulle comunicazioni e articolo 4, primo comma, del decreto di applicazione della legge sulle comunicazioni). Il mandato in sé deve specificare le misure e il loro oggetto, la loro portata, il loro periodo di efficacia, il loro luogo di esecuzione e le corrispondenti modalità di attuazione (articolo 6, sesto comma, della legge sulle comunicazioni).
([233]) L'oggetto di una misura di limitazione delle comunicazioni deve essere costituito da comunicazioni tramite posta o telecomunicazioni specifiche inviate o ricevute da un indiziato oppure comunicazioni tramite posta o telecomunicazioni inviate o ricevute da un indiziato entro un periodo di tempo fisso (articolo 5, secondo comma, della legge sulle comunicazioni).

un'emergenza che rende impossibile seguire la procedura normale ([234]). Tuttavia, in tal caso, occorre presentare una domanda di rilascio di un mandato immediatamente dopo l'adozione della misura ([235]). Le misure di limitazione delle comunicazioni possono essere attuate soltanto per un periodo massimo di due mesi ([236]) e la loro durata può essere prorogata soltanto con l'approvazione dell'organo giurisdizionale laddove continuino ad essere soddisfatte le condizioni per l'attuazione delle misure ([237]). La durata prorogata non può superare complessivamente un anno oppure tre anni per alcuni reati particolarmente gravi (quali i reati relativi a insurrezione, aggressione straniera, sicurezza nazionale) ([238]).

(160) Come nel caso della raccolta di dati di conferma di comunicazioni, la legge sulle comunicazioni impone ai fornitori di servizi di telecomunicazione ([239]) e alle autorità di contrasto ([240]) di tenere registri relativi all'esecuzione di misure di limitazione delle comunicazioni e prevede la notifica alla persona fisica interessata, che può essere differita in via eccezionale laddove necessario sulla base di importanti motivi di interesse pubblico ([241]).

(161) Infine il mancato rispetto di diverse limitazioni e garanzie della legge sulle comunicazioni (nonché ad esempio degli obblighi di ottenimento di un mandato, di tenuta di registri e di notifica alla persona fisica), per quanto concerne tanto la raccolta di dati di conferma di comunicazioni quanto il ricorso a misure di limitazione delle comunicazioni, è soggetto a sanzioni penali ([242]).

(162) I poteri delle autorità di contrasto in materia penale in relazione alla raccolta di dati relativi alle comunicazioni ai sensi della legge sulle comunicazioni (in termini tanto di contenuto di comunicazioni quanto di dati di conferma di comunicazioni) sono quindi circoscritti da norme chiare e precise e sono soggetti a numerose garanzie. Tali garanzie assicurano in particolare la vigilanza sull'esecuzione di tali misure, tanto ex ante (attraverso l'approvazione giudiziaria preventiva) quanto ex post (attraverso requisiti di tenuta di registri e di segnalazione), e facilitano l'accesso da parte delle persone fisiche a mezzi di ricorso effettivi (garantendo che siano informati in merito alla raccolta dei loro dati).

3.2.1.3 Richieste di divulgazione volontaria di dati di abbonati

(163) Oltre a fare affidamento sulle misure obbligatorie illustrate nei considerando da 153 a 162, le autorità di contrasto coreane possono chiedere ai fornitori di servizi di telecomunicazione di trasmettere loro "dati relativi alle comunicazioni" su base volontaria, a sostegno di un procedimento penale, di un'indagine o dell'esecuzione di una sentenza (articolo 83, terzo comma, della legge sulle imprese di telecomunicazione). Questa possibilità esiste soltanto in relazione a serie limitate di dati, ossia il nome, il numero di registrazione come residente, l'indirizzo e il numero di telefono di utenti, le date nelle quali gli utenti si abbonano o disdicono il loro abbonamento nonché i codici di identificazione utente (ossia i codici utilizzati per identificare l'utente legittimo di sistemi informatici o reti di comunicazione) ([243]). Dato che soltanto le persone fisiche che acquistano direttamente servizi da un fornitore di servizi di telecomunicazione coreano sono considerati "utenti" ([244]), le persone fisiche dell'UE i cui dati vengono trasferiti alla Repubblica di Corea non rientrano di norma in tale categoria ([245]).

(164) A tali divulgazioni volontarie si applicano diverse limitazioni, tanto in termini di esercizio dei poteri da parte dell'autorità di contrasto quanto di risposta dell'operatore di telecomunicazioni. Come requisito generale, le autorità di contrasto devono agire nel rispetto dei principi costituzionali di necessità e proporzionalità (articolo 12, primo comma, e articolo 37, secondo comma, della costituzione), anche quando richiedono informazioni su base volontaria. Inoltre devono rispettare la legge sulla protezione delle informazioni personali, in particolare raccogliere dati personali in misura minima, ossia nella misura necessaria al conseguimento di una finalità legittima, in maniera da ridurre al minimo l'impatto sulla vita privata delle persone fisiche (come previsto ad

([234]) Articolo 8, primo comma, della legge sulle comunicazioni. Tuttavia la raccolta di informazioni in situazioni di emergenza deve sempre avvenire in conformità con una "dichiarazione di censura/intercettazione di emergenza" e l'autorità che effettua la raccolta deve tenere un registro di tutte le misure di emergenza (articolo 8, quarto comma, della legge sulle comunicazioni).

([235]) La raccolta deve essere interrotta immediatamente se l'agenzia di contrasto non riesce a ottenere l'autorizzazione da parte dell'organo giurisdizionale entro 36 ore (articolo 8, secondo comma, della legge sulle comunicazioni), nel qual caso, come spiegato nella sezione 2.2.2.2 dell'allegato II, le informazioni raccolte saranno in linea di principio distrutte. Occorre notificare l'organo giurisdizionale altresì nel caso in cui le misure di emergenza siano state completate in tale breve arco di tempo al fine di ovviare alla necessità di autorizzazione (ad esempio se l'indiziato viene arrestato subito dopo l'avvio dell'intercettazione, cfr. articolo 8, quinto comma, della legge sulle comunicazioni). In tal caso si devono fornire informazioni all'organo giurisdizionale in merito all'obiettivo, all'oggetto, alla portata, al periodo, al luogo di esecuzione e al metodo di raccolta nonché ai motivi che giustificano la mancata presentazione di una richiesta di autorizzazione dell'organo giurisdizionale (articolo 8, sesto e settimo comma, della legge sulle comunicazioni).

([236]) Articolo 6, settimo comma, della legge sulle comunicazioni. Se l'obiettivo delle misure viene conseguito prima, entro tale termine, le misure devono essere interrotte immediatamente.

([237]) Articolo 6, settimo e ottavo comma, della legge sulle comunicazioni.

([238]) Articolo 6, ottavo comma, della legge sulle comunicazioni.

([239]) Articolo 9, terzo comma, della legge sulle comunicazioni.

([240]) Articolo 18, primo comma, della legge sulle comunicazioni.

([241]) In particolare il pubblico ministero deve inviare una notifica alla persona fisica entro 30 giorni dall'emissione di un rinvio a giudizio o di una disposizione a non procedere con un rinvio a giudizio o l'arresto (articolo 9-2, primo comma, della legge sulle comunicazioni). Tale notifica può essere differita con l'approvazione del capo dell'ufficio distrettuale del pubblico ministero qualora sia suscettibile di compromettere seriamente la sicurezza nazionale o perturbare la sicurezza e l'ordine pubblici oppure se è probabile che comporti danni sostanziali alla vita e all'incolumità di altri (articolo 9-2, dal quarto al sesto comma, della legge sulle comunicazioni).

([242]) Articoli 16 e 17 della legge sulle comunicazioni.

([243]) Articolo 83, terzo comma, della legge sulle imprese di telecomunicazione. Cfr. anche allegato II, sezione 2.2.3.

([244]) Articolo 2, nono comma, della legge sulle imprese di telecomunicazione.

([245]) Cfr. anche allegato II, sezione 2.2.3.

esempio dall'articolo 3, primo e sesto comma, della legge sulla protezione delle informazioni personali). Più specificamente, le richieste di ottenimento di dati relativi alle comunicazioni ai sensi della legge sulle imprese di telecomunicazione devono essere formulate per iscritto e indicare i motivi della richiesta, il legame con l'utente pertinente e la portata dei dati richiesti ([246]).

(165) I fornitori di servizi di telecomunicazione non sono tenuti a ottemperare a tali richieste e possono farlo solo in conformità con la legge sulla protezione delle informazioni personali. Ciò significa, segnatamente, che devono trovare un equilibrio tra i diversi interessi in gioco e non possono fornire i dati qualora farlo potrebbe violare ingiustamente gli interessi della persona fisica in questione o di una terza parte ([247]). Ciò si verificherebbe ad esempio nel caso in cui sia evidente che l'autorità richiedente ha abusato della propria autorità ([248]). Gli operatori di telecomunicazioni devono tenere registri delle divulgazioni ai sensi della legge sulle imprese di telecomunicazione e riferire due volte l'anno al ministro della Scienza e delle tecnologie dell'informazione e della comunicazione (ministro della Scienza e delle TIC) ([249]).

(166) Inoltre, in conformità con la sezione 3 della notifica n. 2021-5 (allegato I), i fornitori di servizi di telecomunicazione devono in linea di principio inviare una notifica alla persona fisica in questione qualora si conformino volontariamente a una richiesta ([250]). Ciò consentirà a sua volta alla persona fisica di esercitare i propri diritti e, nel caso in cui i propri dati vengano divulgati illecitamente, di ottenere un risarcimento, dal titolare del trattamento (ad esempio per aver divulgato dati in violazione di legge sulla protezione delle informazioni personali o per aver risposto a una richiesta che era palesemente sproporzionata) oppure nei confronti dell'autorità di contrasto (ad esempio per aver agito oltre i limiti di quanto necessario e proporzionato oppure per non aver rispettato i requisiti procedurali della legge sulle imprese di telecomunicazione).

3.2.2 *Ulteriore utilizzo delle informazioni raccolte*

(167) Il trattamento dei dati personali raccolti dalle autorità coreane di contrasto in materia penale è soggetto a tutti i requisiti di cui alla legge sulla protezione delle informazioni personali, inclusi quelli concernenti la limitazione della finalità (articolo 3, primo e secondo comma), la liceità dell'uso e della fornitura di dati a terzi (articoli 15, 17 e 18), i trasferimenti internazionali (articoli 17 e 18 della legge, in combinato disposto con la sezione 2 della notifica 2021-5) ([251]), la proporzionalità/minimizzazione dei dati (articolo 3, primo e sesto comma) e la limitazione della conservazione (articolo 21) ([252]).

(168) Per quanto concerne il contenuto di comunicazioni acquisite attraverso l'esecuzione di misure di limitazione delle comunicazioni, la legge sulle comunicazioni limita specificamente il loro possibile utilizzo a: un'indagine, un'azione giudiziaria o la prevenzione di reati gravi ([253]); procedimenti disciplinari per i medesimi reati; richieste di risarcimento danni avanzate da una parte coinvolta nelle comunicazioni o laddove ciò sia specificamente consentito da altre leggi ([254]). Inoltre il contenuto raccolto delle telecomunicazioni trasmesse tramite internet può essere conservato soltanto previa approvazione dell'organo giurisdizionale che ha autorizzato le misure di limitazione delle comunicazioni ([255]), in vista di utilizzarlo per l'indagine, l'azione giudiziaria o la prevenzione di reati gravi ([256]). Più in generale la legge sulle comunicazioni vieta la divulgazione di informazioni riservate ottenute tramite misure di limitazione delle comunicazioni e l'uso di tali informazioni per danneggiare la reputazione di coloro che erano soggetti a tali misure ([257]).

3.2.3 *Vigilanza*

(169) In Corea, le attività delle autorità di contrasto in materia penale sono soggette a vigilanza da parte di diversi organismi ([258]).

([246]) Articolo 83, quarto comma, della legge sulle imprese di telecomunicazione. Laddove sia impossibile fornire una richiesta scritta per motivi di urgenza, tale richiesta deve essere presentata non appena il motivo di urgenza cessa di applicarsi (articolo 83, quarto comma, della legge sulle imprese di telecomunicazione).

([247]) Articolo 18, secondo comma, della legge sulla protezione delle informazioni personali.

([248]) Decisione della Corte suprema n. 2012Da105482, 10 marzo 2016. Cfr. anche allegato II, sezione 2.2.3, su tale decisione della Corte suprema.

([249]) Articolo 83, quinto e sesto comma, della legge sulle imprese di telecomunicazione.

([250]) Tale requisito è soggetto a eccezioni limitate e qualificate, in particolare se e per tutto il tempo per il quale la notifica comprometterebbe un'indagine penale in corso o potrebbe minacciare la vita o ledere l'incolumità di un'altra persona, laddove tali diritti o interessi prevalgano manifestamente sui diritti dell'interessato. Cfr. sezione 3, punto iii), sottopunto 1), della notifica.

([251]) In particolare le autorità pubbliche coreane sono tenute a garantire, attraverso uno strumento giuridicamente vincolante, un livello di protezione equivalente alla legge sulla protezione delle informazioni personali, cfr. anche considerando 90.

([252]) Cfr. anche allegato II, sezione 1.2.

([253]) Cfr. considerando 158.

([254]) Articolo 12 della legge sulle comunicazioni. Cfr. allegato II, sezione 2.2.2.2.

([255]) Il pubblico ministero o il funzionario di polizia che dà esecuzione alle misure di limitazione delle comunicazioni deve selezionare le telecomunicazioni da conservare entro 14 giorni dalla cessazione delle misure e richiedere l'approvazione da parte dell'organo giurisdizionale (nel caso di un funzionario di polizia, la domanda deve essere presentata a un pubblico ministero, il quale a sua volta presenta la richiesta all'organo giurisdizionale) (cfr. articolo 12-2, primo e secondo comma, della legge sulle comunicazioni).

([256]) Una domanda volta a richiedere tale autorizzazione deve contenere informazioni in merito alle misure di limitazione delle comunicazioni, una sintesi dei risultati delle misure, i motivi per la conservazione (unitamente a materiali a sostegno) e le telecomunicazioni da conservare (articolo 12-2, terzo comma, della legge sulle comunicazioni). Qualora non venga presentata alcuna domanda, i dati acquisiti devono essere cancellati entro 14 giorni dalla cessazione delle misure di limitazione delle comunicazioni (articolo 12-2, quinto comma, della legge sulle comunicazioni); se la domanda viene invece respinta, tali dati devono essere cancellati entro sette giorni (articolo 12-2, quinto comma, della medesima legge). In entrambi i casi, entro sette giorni, occorre presentare una relazione di cancellazione all'organo giurisdizionale che aveva autorizzato la raccolta.

([257]) Articolo 11, secondo comma, della legge sulle comunicazioni.

([258]) Cfr. allegato II, sezione 2.3.

(170) Innanzitutto, la polizia è soggetta a vigilanza interna da parte di un ispettore generale ([259]), il quale attua un controllo della legalità, anche in relazione a possibili violazioni dei diritti umani. L'ispettore generale è stato istituito per attuare l'*Act on Public Sector Audits* (legge sulle attività di revisione nel settore pubblico), che incoraggia la creazione di organismi di controllo interno e stabilisce requisiti specifici per la loro composizione nonché i loro compiti. In particolare, tale legge prescrive che il capo di un organismo di controllo interno sia nominato dall'esterno dell'autorità competente (come nel caso di ex giudici, professori) per un periodo da due a cinque anni ([260]), possa essere rimosso dall'incarico soltanto per ragioni giustificate (ad esempio quando non riesce a svolgere le proprie funzioni in ragione di motivi di salute oppure quando è soggetto ad azioni disciplinari) ([261]) e disponga di un'indipendenza garantita nella misura massima possibile ([262]). L'ostruzione di un controllo interno è soggetta sanzioni amministrative pecuniarie ([263]). Le relazioni di controllo interno (che possono comprendere raccomandazioni, richieste di azione disciplinare e richieste di risarcimento o rettifica) sono comunicate al capo dell'autorità pubblica pertinente, al *Board of Audit and Inspection* (BAI, consiglio di revisione e ispezione) ([264]) e, in genere, rese pubbliche ([265]). Anche i risultati dell'attuazione della relazione devono essere notificati al consiglio di revisione e ispezione ([266]) (cfr. considerando 173 sul ruolo di vigilanza e sui poteri di tale organismo).

(171) In secondo luogo, la PIPC vigila sul rispetto da parte del trattamento di dati condotto dalle autorità di contrasto in materia penale della legge sulla protezione delle informazioni personali e di altre leggi che tutelano la vita privata delle persone fisiche, comprese le leggi che disciplinano la raccolta di elementi di prova (elettronici) per finalità di contrasto penale, come descritto nella sezione 3.2. 1 ([267]). In particolare, dato che la vigilanza della PIPC si estende alla liceità e alla correttezza della raccolta e del trattamento dei dati (articolo 3, primo comma, della legge sulla protezione delle informazioni personali), che verrà violata qualora i dati personali siano accessibili e utilizzati in violazione di tali leggi ([268]), la PIPC può altresì indagare e far rispettare le limitazioni e le garanzie di cui sezione 3.2.1 ([269]). Nell'esercizio di tale ruolo di vigilanza, la PIPC può esercitare tutti i suoi poteri di indagine e di imposizione di misure correttive, come descritto in dettaglio nella sezione 2.4.2. Già prima della recente riforma della legge sulla protezione delle informazioni personali (ossia nel suo precedente ruolo di vigilanza per il settore pubblico), la PIPC ha svolto diverse attività di vigilanza nel contesto del trattamento dei dati personali da parte delle autorità di contrasto in materia penale, ad esempio nel contesto dell'esame di indiziati (caso n. 2013-16, 26 agosto 2013), in merito alla fornitura di notifiche a persone fisiche circa l'imposizione di sanzioni amministrative pecuniarie (caso n. 2015-02-04, 26 gennaio 2015), la condivisione di dati con altre autorità (caso n. 2018-15-146, 9 luglio 2018, caso n. 2018-25-308, 10 dicembre 2018; caso n. 2019-02-015, 29 gennaio 2019), la raccolta di impronte digitali o fotografie (caso n. 2019-17-273, 9 settembre 2019), l'uso di droni (caso n. 2020-01-004, 13 gennaio 2020). In tali casi la PIPC ha esaminato il rispetto di diverse disposizioni della legge sulla protezione delle informazioni personali (ad esempio liceità del trattamento, principi di limitazione e minimizzazione dei dati), ma anche le disposizioni pertinenti di altre leggi quali il codice di procedura penale e, ove necessario, ha emesso raccomandazioni per allineare il trattamento ai requisiti in materia di protezione dei dati.

(172) In terzo luogo, la commissione nazionale per i diritti umani ("NHRC") ([270]) attua una vigilanza indipendente. Tale organismo può infatti indagare in merito a violazioni dei diritti alla tutela della vita privata e della vita privata nella corrispondenza nel contesto del suo mandato generale di tutelare i diritti fondamentali di cui agli articoli da 10 a 22 della costituzione. La NHRC è costituita da 11 commissari che devono soddisfare qualifiche specifiche ([271]) e sono nominati dal presidente della Repubblica di Corea in conformità con le procedure stabilite dalla legge. In particolare, quattro commissari assumono il loro incarico su nomina dell'Assemblea nazionale, quattro su nomina del presidente della Repubblica di Corea e tre su nomina del giudice capo della Corte suprema ([272]). Il presidente della commissione è nominato dal presidente della Repubblica di Corea tra i commissari e deve essere confermato dall'Assemblea nazionale ([273]). I commissari (compreso il presidente della commissione) sono nominati per un termine rinnovabile di tre anni e possono essere rimossi dall'incarico

([259]) Cfr. allegato II, sezione 2.3.1. Cfr. anche https://www.police.go.kr/eng/knpa/org/org01.jsp.
([260]) Analogamente i revisori sono nominati sulla base di condizioni specifiche stabilite nella legge menzionata; cfr. articoli 16 e seguenti della legge sulle attività di revisione nel settore pubblico.
([261]) Articoli da 8 a 11 della legge sulle attività di revisione nel settore pubblico.
([262]) Articolo 7 della legge sulle attività di revisione nel settore pubblico.
([263]) Articolo 41 della legge sulle attività di revisione nel settore pubblico.
([264]) Articolo 23, primo comma, della legge sulle attività di revisione nel settore pubblico.
([265]) Articolo 26 della legge sulle attività di revisione nel settore pubblico.
([266]) Articolo 23, terzo comma, della legge sulle attività di revisione nel settore pubblico.
([267]) Cfr. articolo 7-8, terzo e quarto comma, e articolo 7-9, quinto comma, della legge sulla protezione delle informazioni personali.
([268]) Cfr. notifica n. 2021-5 della PIPC, sezione 6 (allegato I).
([269]) Cfr. anche allegato II, sezione 2.3.4.
([270]) Articolo 1 della legge sulla commissione per i diritti umani (in appresso: "legge sulla NHRC").
([271]) Per essere nominato un commissario deve: 1) aver prestato servizio per almeno dieci anni presso un'università o un istituto di ricerca autorizzato, quanto meno come professore associato; 2) aver prestato servizio come giudice, pubblico ministero o avvocato per almeno dieci anni; 3) essere stato impegnato in attività a tutela dei diritti umani per almeno dieci anni (ad esempio per un'organizzazione non governativa senza scopo di lucro o un'organizzazione internazionale); oppure 4) essere stato raccomandato da gruppi della società civile (articolo 5, terzo comma, della legge sulla NHRC). Inoltre, una volta nominati, i commissari non possono detenere un incarico simultaneo in seno all'Assemblea nazionale, a consigli locali, a qualsiasi amministrazione statale o governativa locale (in veste di funzionario pubblico) (cfr. articolo 10 della legge sulla NHRC).
([272]) Articolo 5, primo e secondo comma, della legge sulla NHRC.
([273]) Articolo 5, quinto comma, della legge sulla NHRC.

soltanto se vengono condannati a una pena detentiva o non sono più in grado di adempiere le loro funzioni in ragione di una debolezza fisica o mentale prolungata (nel qual caso due terzi dei commissari devono concordate con la rimozione dall'incarico) ([274]). Nel contesto di un'indagine, la NHRC può richiedere la presentazione di materiali pertinenti, condurre ispezioni e convocare persone fisiche affinché prestino testimonianza ([275]). In termini di poteri di imposizione di misure correttive, la NHRC può emettere raccomandazioni (pubbliche) destinate a migliorare o correggere politiche e pratiche specifiche, alle quali le autorità pubbliche devono rispondere proponendo un piano di attuazione ([276]). Se l'autorità interessata non attua le raccomandazioni, deve informarne la commissione ([277]), che può a sua volta riferire tale mancanza all'Assemblea nazionale e/o renderla pubblica. Secondo la dichiarazione ufficiale del governo coreano (sezione 2.3.5 dell'allegato II), in genere le autorità coreane si conformano alle raccomandazioni della NHRC e sono fortemente incentivate a farlo in quanto la loro attuazione è stata esaminata nel contesto di una valutazione generale e continua condotta sotto l'egida dell'ufficio del primo ministro. Dai dati annuali sulle sue attività emerge che la NHRC vigila attivamente sulle attività delle autorità di contrasto in materia penale, sulla base di istanze individuali o tramite indagini d'ufficio ([278]).

(173) In quarto luogo, la vigilanza generale in merito alla liceità delle attività delle autorità pubbliche è condotta dal BAI, che esamina le entrate e le spese dello Stato, ma che, più in generale, vigila sull'adempimento dei doveri delle autorità pubbliche al fine di migliorare il funzionamento della pubblica amministrazione ([279]). Il BAI si colloca formalmente al di sotto del presidente della Repubblica di Corea, ma mantiene uno stato indipendente per quanto concerne i suoi doveri ([280]). Inoltre, è concessa piena indipendenza rispetto alla nomina, alla revoca dell'incarico e all'organizzazione del suo personale, nonché alla compilazione del suo bilancio ([281]). Il BAI è costituito da un presidente (nominato dal presidente della Repubblica di Corea, con il consenso dell'Assemblea nazionale) ([282]) e sei commissari (nominati dal presidente della Repubblica di Corea su raccomandazione del presidente del BAI) ([283]), che devono soddisfare le qualifiche specifiche stabilite dalla legge ([284]) e possono essere rimossi dall'incarico soltanto in caso di messa in stato di accusa, condanna a una pena detentiva o incapacità di adempiere le proprie funzioni in ragione di una debolezza mentale o fisica prolungata ([285]). Il BAI conduce una revisione generale su base annuale, ma può altresì effettuare revisioni specifiche in merito a questioni di interesse speciale. Nello svolgere una revisione o un'ispezione, il BAI può richiedere la presentazione dei documenti e la partecipazione di persone fisiche ([286]). Il BAI può emettere raccomandazioni, richiedere l'adozione di azioni disciplinari oppure depositare una denuncia penale ([287]).

(174) Infine l'Assemblea nazionale svolge attività di vigilanza parlamentare delle autorità pubbliche attraverso indagini e ispezioni ([288]) delle loro attività ([289]). Può richiedere la divulgazione di documenti, imporre la comparizione di testimoni ([290]), raccomandare misure correttive (laddove concluda che hanno avuto luogo attività illecite o

([274]) Articolo 7, primo comma, e articolo 8, della legge sulla NHRC.

([275]) Articolo 36 della legge sul NHRC. Conformemente all'articolo 6, settimo comma, di tale legge, la presentazione di materiali od oggetti può essere respinta qualora sia suscettibile di compromettere la riservatezza dello Stato, qualora possa avere un effetto sostanziale sulla sicurezza dello Stato o sulle relazioni diplomatiche oppure qualora costituisca un grave ostacolo a un'indagine penale o un procedimento in sospeso. In tali casi la commissione può richiedere ulteriori informazioni al capo dell'agenzia pertinente (che deve rispettare la buona fede) ove necessario per consentire il riesame dell'eventualità o meno che il rifiuto di fornire le informazioni sia giustificato.

([276]) Articolo 25, primo e terzo comma, della legge sulla NHRC.

([277]) Articolo 25, quarto comma, della legge sulla NHRC.

([278]) Ad esempio, tra il 2015 e il 2019, alla NHRC sono pervenute annualmente tra 1 380 e 1 699 istanze contro autorità di contrasto in materia penale dell'ordine che sono state affrontate in un numero parimenti elevato di casi (ad esempio, tale commissione ha gestito 1 546 reclami contro la polizia nel 2018 e 1 249 nel 2019); ha inoltre condotto diverse indagini d'ufficio, come descritto più dettagliatamente nella relazione annuale del 2018 (disponibile all'indirizzo in inglese https://www.humanrights.go.kr/site/program/board/basicboard/view?menuid=002003003001&pagesize=10&boardtypeid=7017&boardid=7602641) e nella relazione annuale del 2019 (disponibile all'indirizzo in inglese https://www.humanrights.go.kr/site/program/board/basicboard/view?menuid=002003003001&pagesize=10&boardtypeid=7017&boardid=7606217) della NHRC.

([279]) Articoli 20 e 24 della *Board of Audit and Inspection Act* (legge sul consiglio di revisione e ispezione, in appresso: "legge sul BAI"). Cfr. allegato II, punto 2.3.2.

([280]) Articolo 2, primo comma, della legge sul BAI.

([281]) Articolo 2, secondo comma, della legge sul BAI.

([282]) Articolo 4, primo comma, della legge sul BAI.

([283]) Articolo 5, primo comma, e articolo 6 della legge sul BAI.

([284]) Ad esempio aver prestato servizio in veste di giudice, pubblico ministero o avvocato per almeno dieci anni, aver lavorato come funzionario pubblico o professore oppure aver occupato una posizione di livello superiore presso un'università per almeno otto anni, oppure aver lavorato per almeno dieci anni in una società quotata in borsa o un'istituzione a partecipazione statale (di cui almeno cinque anni in veste di alto dirigente) (cfr. articolo 7 della legge sul BAI). Inoltre ai commissari è vietato partecipare alle attività politiche e detenere contemporaneamente incarichi in seno all'Assemblea nazionale, ad agenzie amministrative, a organizzazioni soggette a revisione e ispezione da parte del BAI oppure qualsiasi altro incarico o assumere qualsiasi altra posizione che comporti una remunerazione (articolo 9 della legge sul BAI).

([285]) Articolo 8 della legge sul BAI.

([286]) Cfr. ad esempio articolo 27 della legge sul BAI.

([287]) Articolo 24 e articoli da 31 a 35, della legge sul BAI.

([288]) Articolo 128 della legge sull'assemblea nazionale e articoli 2, 3 e 15 della legge sull'ispezione e sull'indagine dell'amministrazione dello Stato. Rientrano in tale contesto ispezioni annuali di questioni governative nel loro complesso, ma anche indagini su questioni specifiche.

([289]) Cfr. allegato II, sezione 2.2.3.

([290]) Articolo 10, primo comma, della legge sull'ispezione e sull'indagine dell'amministrazione dello Stato. Cfr. anche articoli 128 e 129 della legge sull'assemblea nazionale.

improprie) ([291]) e rendere pubblici i risultati delle sue conclusioni ([292]). Se l'Assemblea nazionale richiede l'adozione di misure correttive che possono ad esempio comprendere il riconoscimento di un risarcimento, l'adozione di azioni disciplinari o il miglioramento delle procedure interne, l'autorità pubblica interessata è tenuta ad agire senza indugio e a riferire in merito all'esito all'Assemblea nazionale ([293]).

3.2.4 *Ricorso*

(175) Il sistema coreano offre diversi mezzi (giudiziari) per ottenere ricorso, compreso il risarcimento dei danni.

(176) Innanzitutto la legge sulla protezione delle informazioni personali fornisce alle persone fisiche un diritto di accesso, di rettifica, di cancellazione e di sospensione rispetto ai dati personali trattati per finalità di contrasto penale ([294]).

(177) In secondo luogo, le persone fisiche possono fare ricorso ai diversi meccanismi di ricorso offerti da legge sulla protezione delle informazioni personali qualora i loro dati siano trattati da un'autorità di contrasto in materia penale in violazione di tale legge oppure in violazione delle limitazioni e delle garanzie che disciplinano la raccolta di dati personali in altre leggi (ossia il codice di procedura penale o la legge sulle comunicazioni, cfr. considerando 171). In particolare le persone fisiche possono promuovere un reclamo presso la PIPC (anche attraverso il call centre per la tutela della vita privata gestito dall'agenzia coreana per la sicurezza e internet ([295])) o il comitato di mediazione per le controversie sui dati ([296]). Tali possibilità di ricorso non sono soggette a ulteriori requisiti di ammissibilità. Ai sensi della legge sui contenziosi amministrativi, le persone fisiche possono inoltre impugnare le decisioni o l'inazione della PIPC (cfr. considerando 132).

(178) In terzo luogo, qualsiasi persona fisica ([297]) può promuovere un reclamo presso la NHRC in relazione a una violazione del diritto alla vita privata e alla protezione dei dati da parte di un'autorità coreana di contrasto in materia penale. La NHRC può raccomandare la rettifica o il miglioramento di qualsiasi statuto, istituzione, politica o pratica pertinente ([298]) oppure l'attuazione di mezzi di ricorso quali la mediazione ([299]), la cessazione della violazione di diritti umani, il risarcimento dei danni e misure destinate a prevenire la reiterazione della stessa violazione o di violazioni analoghe ([300]). Secondo la dichiarazione ufficiale rilasciata dal governo coreano (sezione 2.4.2 dell'allegato II), in tale contesto può figurare anche la cancellazione di dati personali raccolti in maniera illecita. Sebbene la NHRC non disponga del potere di rilasciare decisioni vincolanti, offre un mezzo di ricorso più informale, a basso costo e facilmente accessibile, in particolare dato che, come spiegato all'allegato II, sezione 2.4.2, non richiede la dimostrazione di un pregiudizio a livello fattuale affinché un reclamo sia oggetto di indagine ([301]). Ciò assicura che i reclami promossi da persone fisiche in relazione alla raccolta dei loro dati possano essere soggette a indagine, anche se una persona fisica non è in grado di dimostrare che i suoi dati sono stati in effetti raccolti (ad esempio perché la notifica alla persona fisica non ha ancora avuto luogo). Dalle relazioni annuali di attività della NHRC emerge che le persone fisiche utilizzano questo mezzo di ricorso nella pratica anche per impugnare attività delle autorità di contrasto in materia penale, anche in relazione alla gestione di dati personali ([302]). Se una persona fisica non è soddisfatta dell'esito di una procedura dinanzi la NHRC, può

([291]) Articolo 16, secondo comma, della legge sull'ispezione e sull'indagine dell'amministrazione dello Stato.

([292]) Articolo 12-2 della legge sull'ispezione e sull'indagine dell'amministrazione dello Stato.

([293]) Articolo 16, terzo comma, della legge sull'ispezione e sull'indagine dell'amministrazione dello Stato.

([294]) Tale diritto può essere esercitato direttamente nei confronti dell'autorità competente oppure indirettamente tramite la PIPC (articolo 35, secondo comma, della legge sulla protezione delle informazioni personali). Come descritto in maniera più dettagliata nei considerando da 76 a 78, le eccezioni a tali diritti si applicano soltanto quando ciò è necessario per tutelare interessi (pubblici) importanti.

([295]) Articolo 62 della legge sulla protezione delle informazioni personali.

([296]) Articoli da 40 a 50 della legge sulla protezione delle informazioni personali e articoli da 48-2 a 57 del decreto di applicazione di tale legge. Cfr. anche allegato II, sezione 2.4.1.

([297]) Come spiegato nell'allegato II, sezione 2.4.2, sebbene l'articolo 4 della legge sulla NHRC faccia riferimento ai cittadini e agli stranieri residenti nella Repubblica di Corea, il termine "residente" rispecchia un concetto di competenza giurisdizionale piuttosto che di territorio. Di conseguenza se i diritti fondamentali di uno straniero al di fuori della Corea sono violati dalle istituzioni nazionali in Corea, la persona fisica in questione può promuovere un reclamo presso la NHRC. Ciò si verificherebbe qualora le autorità pubbliche coreane avessero accesso in maniera illecita ai dati personali di uno straniero trasferiti in Corea. Cfr. in particolare le spiegazioni fornite all'indirizzo: https://www.humanrights.go.kr/site/program/board/basicboard/list?boardtypeid=7025&menuid=002004005001&pagesize=10&currentpage=2.

([298]) Articolo 44 della legge sul NHRC.

([299]) Una persona fisica può altresì richiedere di risolvere il reclamo attraverso la mediazione, cfr. articoli 42 e seguenti della legge sulla NHRC.

([300]) Articolo 42, quarto comma, della legge sulla NHRC. Inoltre la NHRC può adottare misure di riparazione urgenti in caso di violazione in corso che potrebbe causare danni cui sarebbe difficile porre rimedio qualora non venisse trattata (cfr. articolo 48 della legge sulla NRHC).

([301]) In linea di massima un reclamo va depositato entro un anno dalla violazione, ma la NHRC può comunque decidere di indagare in merito a un reclamo che viene presentato trascorso tale termine fintantoché non sia scaduto il termine di prescrizione previsto dal diritto penale o civile (articolo 32, primo comma, punto 4, della legge sulla NHRC).

([302]) Ad esempio in passato la NHRC ha gestito denunce e ha emesso raccomandazioni in merito a sequestri illeciti e a una violazione dell'obbligo di informare le persone fisiche in merito a un sequestro (cfr. pagg. 80 e 91 della relazione annuale del 2018 della NHRC, disponibile all'indirizzo: https://www.humanrights.go.kr/site/program/board/basicboard/view?menuid=002003003001&pagesize=10&boardtypeid=7017&boardid=7604746), nonché il trattamento illecito di dati personali da parte della polizia, dell'ufficio del pubblico ministero e degli organi giurisdizionali (cfr. pagg. 157 e 158 della relazione annuale del 2019 della NHRC, disponibile all'indirizzo https://www.humanrights.go.kr/site/program/board/basicboard/view?menuid=002003003001&pagesize=10&boardtypeid=7017&boardid=7603308, e pag. 76 della relazione annuale del 2019, disponibile all'indirizzo https://www.humanrights.go.kr/site/program/board/basicboard/view?menuid=002003003001&pagesize=10&boardtypeid=7017&boardid=7606217).

impugnare le decisioni (ad esempio una decisione di non continuare l'indagine in merito a un reclamo ([303])) e le raccomandazioni di quest'ultima adendo gli organi giurisdizionali coreani ai sensi della legge sui contenziosi amministrativi (cfr. considerando 181) ([304]). Inoltre, una procedura dinanzi la NHRC può facilitare ulteriormente l'accesso agli organi giurisdizionali, dato che una persona fisica potrebbe chiedere ulteriormente ricorso contro l'autorità pubblica che ha trattato i suoi dati in maniera illecita sulla base delle constatazioni della NHRC, in conformità con le procedure illustrate ai considerando da 181 a 183.

(179) Infine sono disponibili diversi ricorsi giurisdizionali che consentono alle persone fisiche di invocare le limitazioni e le garanzie di cui alla sezione 3.2.1 per ottenere riparazione ([305]).

(180) Per quanto concerne i sequestri (anche di dati), il codice di procedura penale prevede la possibilità di opporsi all'esecuzione di un mandato o di impugnare tale esecuzione attraverso un "quasi-reclamo", presentando un'istanza presso l'organo giurisdizionale competente contenente una richiesta di annullamento o di modifica di una disposizione formulata da un pubblico ministero o un funzionario di polizia ([306]).

(181) Più in generale, le persone fisiche possono impugnare le azioni ([307]) o le omissioni ([308]) di autorità pubbliche (comprese quelle delle autorità di contrasto in materia penale) ai sensi della legge sui contenziosi amministrativi ([309]). Un'azione amministrativa è considerata una "disposizione impugnabile" se incide direttamente sui diritti e sugli obblighi civili ([310]), una circostanza questa che, come confermato dal governo coreano (sezione 2.4.3 dell'allegato II), si verifica per le misure destinate a raccogliere dati personali, direttamente (ad esempio tramite l'intercettazione di comunicazioni), tramite richieste di divulgazione obbligatoria (ad esempio rivolte a fornitori di servizi) oppure richieste di cooperazione volontaria. Affinché un'impugnazione ai sensi della legge sui contenziosi amministrativi sia ammissibile, una persona fisica deve avere un interesse giuridico nel perseguire l'istanza ([311]). Secondo la giurisprudenza della Corte suprema, la nozione di "interesse giuridico" è interpretata come un "interesse protetto dalla legge", ossia un interesse diretto e specifico protetto da leggi e normative sulle quali si basano disposizioni amministrative (il che significa interessi non generali, indiretti e astratti di interessi del pubblico) ([312]). Le persone fisiche hanno un tale interesse giuridico in caso di violazione delle limitazioni e delle garanzie che si applicano alla raccolta dei loro dati personali per finalità di contrasto penale (a norma di leggi specifiche o della legge sulla protezione delle informazioni personali). Ai sensi della legge sui contenziosi amministrativi, un organo giurisdizionale può decidere di revocare o modificare una disposizione illecita, emettere una constatazione di nullità (ossia una decisione che constati l'assenza di effetto giuridico di una disposizione oppure la sua non esistenza nell'ordinamento giuridico) oppure emettere una constatazione che attesti l'illegalità di un'omissione ([313]). Una sentenza definitiva ai sensi della legge sui contenziosi amministrativi è vincolante sulle parti ([314]).

([303]) Ad esempio qualora eccezionalmente la NHRC non fosse in grado di ispezionare determinati materiali o strutture perché riguardano segreti di Stato passibili di avere un effetto sostanziale sulla sicurezza dello Stato o sulle relazioni diplomatiche, oppure qualora l'ispezione costituisse un grave ostacolo a un'indagine penale o un procedimento in sospeso, e qualora ciò impedisse alla NHRC di svolgere l'indagine necessaria per valutare i meriti dell'istanza pervenuta, tale commissione informerà la persona fisica dei motivi per i quali la denuncia è stata respinta, in conformità con l'articolo 39 della legge sulla NHRC. In tal caso la persona fisica potrebbe impugnare la decisione della NHRC ai sensi della legge sui contenziosi amministrativi.

([304]) Cfr. ad esempio decisione della *Seoul High Court* (Alta Corte di Seoul) 2007Nu27259, 18 aprile 2008, confermata dalla decisione della Corte suprema 2008Du7854 del 9 ottobre 2008; Decisione dell'Alta Corte di Seoul 2017Nu69382, 2 febbraio 2018.

([305]) Cfr. allegato II, punto 2.4.3.

([306]) Articolo 417 del codice di procedura penale, in combinato disposto con l'articolo 414, secondo comma, del medesimo codice. Cfr. anche decisione della Corte suprema n. 97Mo66, 29 settembre 1997.

([307]) La legge sui contenziosi amministrativi fa riferimento a una "disposizione", ossia all'esercizio, o al rifiuto dell'esercizio, di un pubblico potere in un caso specifico.

([308]) Ai sensi della legge sui contenziosi amministrativi, ciò fa riferimento alla mancata adozione, per un periodo prolungato, da parte di un'agenzia amministrativa di una determinata disposizione contraria a un obbligo giuridico a procedere in tal senso.

([309]) Un'impugnazione di sede amministrativa può essere promossa innanzitutto dinanzi le commissioni di ricorso amministrativo istituite in seno a determinate autorità pubbliche (ad esempio il servizio nazionale di intelligence o la NHRC) oppure dinanzi la *Central Administrative Appeals Commission* (commissione centrale per gli appelli amministrativi) istituita in seno alla commissione anticorruzione e per i diritti civili (articolo 6 della legge sui ricorsi amministrativi e articolo 18, primo comma, della legge sui contenziosi amministrativi), come procedura di riparazione più informale. Tuttavia è possibile proporre reclamo anche direttamente presso gli organi giurisdizionali coreani ai sensi della legge sui contenziosi amministrativi.

([310]) Decisione della Corte suprema 98Du18435, 22 ottobre 1999, decisione della Corte suprema 99Du1113, 8 settembre 2000 e decisione della Corte suprema 2010Du3541 del 27 settembre 2012.

([311]) Articoli 12, 35 e 36 della legge sui contenziosi amministrativi. Inoltre una richiesta di revoca/modifica di una disposizione e una richiesta di constatazione dell'illegalità di un'omissione deve essere depositata entro 90 giorni dalla data in cui la persona fisica viene a conoscenza della disposizione/dell'omissione e, in linea di principio, entro e non oltre un anno dalla data in cui viene emessa la disposizione o in cui si è verificata l'omissione, fatto salvo il caso in cui vi siano motivi giustificabili (articolo 20 e articolo 38, secondo comma, della legge sui contenziosi amministrativi). La nozione di "motivi giustificabili" è stata interpretata in senso ampio dalla Corte suprema e richiede la valutazione dell'eventualità che sia socialmente accettabile consentire la presentazione di un reclamo tardivo, alla luce di tutte le circostanze del caso (decisione della Corte suprema 90Nu6521, 28 giugno 1991). Come confermato dal governo coreano nella sezione 2.4.3 dell'allegato II, ciò comprende (a titolo esemplificativo ma non esaustivo) motivi di ritardo non imputabili alla parte interessata (ossia imputabili a circostanze al di fuori del controllo della parte che presenta il reclamo, ad esempio, nel caso in cui tale parte non abbia ricevuto notifica della raccolta delle sue informazioni personali) oppure cause di forza maggiore (ad esempio un disastro naturale, una guerra).

([312]) Decisione della Corte suprema n. 2006Du330, 26 marzo 2006.

([313]) Articoli 2 e 4 della legge sui contenziosi amministrativi.

([314]) Articolo 30, primo comma, della legge sui contenziosi amministrativi.

(182) Oltre a impugnare un'azione di un soggetto governativo tramite un contenzioso amministrativo, le persone fisiche possono altresì promuovere un reclamo costituzionale presso la Corte costituzionale in merito a qualsiasi violazione dei loro diritti fondamentali imputabile all'esercizio o al mancato esercizio di un potere governativo (escludendo le sentenze di organi giurisdizionali) ([315]). Se sono disponibili altri mezzi di ricorso, occorre che vengano esperiti prima di adire la Corte costituzionale. Secondo la giurisprudenza della Corte costituzionale, i cittadini stranieri possono presentare un reclamo costituzionale nella misura in cui i loro diritti fondamentali siano riconosciuti nel contesto della costituzione coreana (cfr. spiegazioni di cui alla sezione 1.1) ([316]). La Corte costituzionale può invalidare l'esercizio del potere governativo che ha causato l'infrazione o confermare che una determinata inazione è incostituzionale ([317]). In tal caso, l'autorità competente è tenuta ad adottare misure per conformarsi alla decisione della Corte.

(183) Inoltre le persone fisiche possono ottenere un risarcimento per danni adendo gli organi giurisdizionali coreani. In tale contesto figura innanzitutto la possibilità di richiedere un risarcimento per violazioni della legge sulla protezione delle informazioni personali commesse da autorità di contrasto in materia penale, conformemente all'articolo 39 (cfr. anche considerando 135). Più in generale le persone fisiche possono richiedere un risarcimento per danni causati da funzionari pubblici nello svolgimento delle loro funzioni ufficiali in violazione della legge, ai sensi della legge sul risarcimento da parte dello Stato (cfr. anche considerando 135) ([318]).

(184) I meccanismi illustrati ai considerando da 176 a 183 offrono agli interessati mezzi di ricorso effettivi in sede amministrativa e giudiziale che consentono loro in particolare di ottenere l'applicazione dei loro diritti, compreso il diritto di avere accesso ai propri dati personali o di ottenerne la rettifica o la cancellazione.

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

(185) Il diritto della Repubblica di Corea contempla una serie di limitazioni e garanzie in relazione all'accesso e all'uso di dati personali per finalità di sicurezza nazionale e prevede meccanismi di vigilanza e ricorso in questo settore che sono in linea con i requisiti di cui ai considerando da 141 a 143 della presente decisione. Le condizioni in cui tale accesso può avvenire e le garanzie applicabili all'uso di tali poteri sono valutate in dettaglio nelle sezioni che seguono.

3.3.1 *Basi giuridiche, limitazioni e garanzie*

(186) Nella Repubblica di Corea, è possibile accedere a dati personali per finalità di sicurezza nazionale ai sensi della legge sulle comunicazioni, della legge sulle imprese di telecomunicazione e della legge antiterrorismo per la protezione dei cittadini e della sicurezza pubblica ("legge antiterrorismo") ([319]). L'autorità principale ([320]) avente competenze nel settore della sicurezza nazionale è il Servizio nazionale di intelligence (*National Intelligence Service*, NIS) ([321]). La raccolta e l'uso dei dati personali da parte del NIS devono rispettare i requisiti giuridici pertinenti

([315]) Articolo 68, primo comma, della legge sulla Corte costituzionale. I reclami costituzionali devono essere depositati entro 90 giorni dal momento in cui una persona fisica viene a conoscenza della violazione ed entro un anno dal verificarsi di quest'ultima. Come illustrato anche nell'allegato II, sezione 2.4.3, dato che la procedura di cui alla legge sui contenziosi amministrativi si applica a un contenzioso ai sensi della legge sulla Corte costituzionale a norma dell'articolo 40 di quest'ultima legge, un reclamo è comunque ricevibile qualora vi siano "motivi giustificabili", come interpretati in conformità con la giurisprudenza della Corte suprema descritta nella nota 312. Qualora sia necessario esperire prima altri mezzi di ricorso, un reclamo costituzionale deve essere depositato entro 30 giorni dalla decisione finale in merito a un tale mezzo di ricorso (articolo 69 della legge sulla Corte costituzionale).

([316]) Decisione della Corte costituzionale n. 99HeonMa194, 29 novembre 2001.

([317]) Articolo 75, terzo comma, della legge sulla Corte costituzionale.

([318]) Articolo 2, primo comma, della legge sul risarcimento da parte dello Stato.

([319]) Cfr. allegato II, sezione 3.1.

([320]) Eccezionalmente la polizia e il pubblico ministero possono altresì raccogliere informazioni personali per finalità di sicurezza nazionale (cfr. nota 327 e allegato II, sezione 3.2.1.2). Inoltre l'agenzia di intelligence militare coreana (il *Defense Security Support Command*, comando di sostegno alla protezione della difesa, istituito in seno al ministero della Difesa), ha poteri nel settore della sicurezza nazionale. Tuttavia, come spiegato nell'allegato II, sezione 3.1, tale agenzia è competente soltanto per l'intelligence militare e svolge azioni di sorveglianza sui civili soltanto laddove ciò sia necessario per svolgere le proprie funzioni militari. In particolare tale agenzia può indagare esclusivamente in merito al personale militare, a dipendenti civili di forze armate, a persone soggette a formazione militare, a persone appartenenti alla riserva militare o attive nel servizio di reclutamento nonché prigionieri di guerra (articolo 1 della legge sugli organi giurisdizionali militari). Quando raccoglie informazioni sulle comunicazioni per finalità di sicurezza nazionale, il comando di sostegno alla protezione della difesa è soggetto alle limitazioni e alle garanzie stabilite dalla legge sulle comunicazioni e dal suo decreto di applicazione.

([321]) Il mandato del NIS prevede: la raccolta, la compilazione e la distribuzione di informazioni in merito a paesi stranieri (ossia informazioni generali sulle tendenze e sugli sviluppi in relazione a paesi stranieri o alle attività di attori statali); attività di intelligence relativa al contrasto dello spionaggio (incluso lo spionaggio militare e industriale), del terrorismo e di attività della criminalità internazionale; attività di intelligence su determinati tipi di criminalità rivolta contro la sicurezza pubblica e nazionale (ad esempio insurrezioni interne, aggressioni straniere) nonché di intelligence relative al compito di garantire la cibersicurezza e o di contrastare gli attacchi informatici e le minacce (articolo 4, secondo comma, della legge sul NIS). Cfr. anche allegato II, sezione 3.1.

(compresa la legge sulla protezione delle informazioni personali e la legge sulle comunicazioni) ([322]) nonché le linee guida generali preparate dal presidente della Repubblica di Corea e riviste dall'Assemblea nazionale ([323]). Come principio generale, il NIS deve mantenere la neutralità politica e proteggere la libertà e i diritti delle persone fisiche ([324]). Inoltre il personale del NIS non deve abusare della sua autorità ufficiale per costringere alcuna istituzione, organizzazione o persona fisica a compiere alcuna azione che non sia tenuta a compiere (ai sensi della legge), né ostacolare l'esercizio da parte di qualsiasi persona dei suoi diritti ([325]).

3.3.1.1 Accesso alle informazioni sulle comunicazioni

(187) Ai sensi della legge sulle comunicazioni, le autorità pubbliche coreane ([326]) possono raccogliere dati di conferma di comunicazioni (ossia la data di telecomunicazioni, il loro orario di inizio e fine, il numero di chiamate in uscita e in arrivo nonché il numero dell'abbonato dall'altro capo, la frequenza di utilizzo, i file di registro sull'uso dei servizi di telecomunicazione nonché informazioni relative all'ubicazione, cfr. considerando 155 e il contenuto di comunicazioni (mediante misure di limitazione delle comunicazioni, cfr. considerando 155) per finalità di sicurezza nazionale (come stabilito dal mandato del NIS, cfr. nota 332). Tali poteri si estendono a due tipi di informazioni: 1) comunicazioni nel contesto delle quali una o entrambe parti sono cittadini coreani ([327]); e 2) comunicazioni di a) paesi ostili alla Repubblica di Corea, b) agenzie, gruppi o cittadini stranieri sospettati di essere coinvolti in attività anti-coreane ([328]) oppure c) membri di gruppi che operano all'interno della penisola coreana ma di fatto al di fuori della sovranità della Repubblica di Corea e i loro gruppi ombrello con sede in paesi stranieri ([329]). Le comunicazioni di persone fisiche dell'UE trasferite dall'Unione verso la Repubblica di Corea sulla base della presente decisione possono pertanto essere raccolte soltanto ai sensi della legge sulle comunicazioni per finalità di sicurezza nazionale (fatte salve le condizioni di cui ai considerando da 188 a 192) se avvengono tra una persona fisica dell'UE e un cittadino coreano oppure se riguardano comunicazioni esclusivamente tra cittadini non coreani e rientrano in una delle tre categorie menzionate alle lettere a), b) e c) del punto 2.

(188) In entrambi gli scenari, la raccolta di dati di conferma di comunicazioni può avvenire soltanto allo scopo di prevenire minacce alla sicurezza nazionale ([330]) mentre misure di limitazione delle comunicazioni possono essere adottate soltanto in presenza di un rischio grave per la sicurezza nazionale e quando tale raccolta è necessaria per prevenirlo ([331]). Inoltre è possibile accedere al contenuto di comunicazioni soltanto come misura di ultima istanza e si devono compiere sforzi per ridurre al minimo la violazione della vita privata delle comunicazioni ([332]), garantendo in tal modo che tale attività sia proporzionata all'obiettivo di sicurezza nazionale perseguito. La raccolta tanto del contenuto di comunicazioni quanto dei dati di conferma di comunicazioni può durare soltanto per un periodo massimo di quattro mesi e deve essere interrotta immediatamente qualora l'obiettivo perseguito sia conseguito prima ([333]). Se le condizioni pertinenti continuano ad essere soddisfatte, tale termine può essere prorogato, con la preventiva autorizzazione di un organo giurisdizionale (per le misure di cui al considerando 189) o del presidente della Repubblica di Corea (per le misure di cui al considerando 190) ([334]), per un massimo di quattro mesi.

(189) Le stesse garanzie procedurali si applicano alla raccolta di dati di conferma di comunicazioni e del contenuto di comunicazioni ([335]). In particolare qualora almeno una delle persone coinvolte nella comunicazione sia un cittadino coreano, l'agenzia di intelligence deve presentare una richiesta scritta all'Ufficio dell'Alta Procura, che

([322]) Cfr. anche articoli 14, 22 e 23, della legge sul NIS.
([323]) Articolo 4, secondo comma, della legge sul NIS.
([324]) Articolo 3, primo comma, articolo 6, secondo comma e articoli 11 e 21 della legge sul NIS. Cfr. anche norme sui conflitti di interesse, in particolare gli articoli 10 e 12 della legge sul NIS.
([325]) Articolo 13 della legge sul NIS.
([326]) Tra queste figurano le agenzie di intelligence (ossia il NIS e il comando di sostegno alla protezione della difesa) nonché la polizia/il pubblico ministero.
([327]) Articolo 7, primo comma, punto 1, della legge sulle comunicazioni.
([328]) Come spiegato dal governo coreano nella nota 244 dell'allegato II, ciò si riferisce ad attività che minacciano l'esistenza e la sicurezza nazionali, l'ordine democratico o la sopravvivenza e la libertà della popolazione.
([329]) Articolo 7, primo comma, punto 2, della legge sulle comunicazioni.
([330]) Articolo 13-4, della legge sulle comunicazioni.
([331]) Articolo 7, primo comma, della legge sulle comunicazioni.
([332]) Articolo 3, secondo comma, della legge sulle comunicazioni. Inoltre le misure di limitazione delle comunicazioni devono essere interrotte immediatamente una volta che non sono più necessarie, garantendo così che qualsiasi violazione dei segreti delle comunicazioni della persona fisica sia limitata al minimo (articolo 2 del decreto di applicazione della legge sulle comunicazioni).
([333]) Articolo 7, secondo comma, della legge sulle comunicazioni.
([334]) La domanda per l'ottenimento dell'approvazione della proroga delle misure di sorveglianza deve essere presentata per iscritto, indicando i motivi per cui si chiede la proroga e fornendo materiali a sostegno (articolo 7, secondo comma, della legge sulle comunicazioni e articolo 5 del decreto di applicazione di tale legge).
([335]) Cfr. articolo 13-4, secondo comma, della legge sulle comunicazioni e articolo 37, quarto comma, del decreto di applicazione di tale legge, secondo cui le procedure applicabili alla raccolta del contenuto di comunicazioni si applicano anche alla raccolta di dati di conferma di comunicazioni. Cfr. anche allegato II, sezione 3.2.1.1.1.

a sua volta deve richiedere l'emissione di un mandato da parte di un giudice di alto livello dell'Alta Corte ([336]). La legge sulle comunicazioni elenca le informazioni che devono essere fornite nella richiesta al pubblico ministero, nella domanda di mandato e nel mandato stesso, che comprendono in particolare la giustificazione della richiesta e i motivi principali del sospetto nutrito, i materiali a sostegno, nonché informazioni sull'obiettivo, sull'oggetto (ossia la persona o le persone oggetto della misura), la portata e la durata della misura proposta ([337]). Una raccolta in assenza di mandato può avvenire soltanto in presenza di un atto di cospirazione che minaccia la sicurezza nazionale ed esista un'emergenza che rende impossibile l'espletamento delle procedure di cui sopra ([338]). Tuttavia, anche in tal caso, occorre presentare una domanda di rilascio di un mandato immediatamente dopo l'adozione della misura ([339]). La legge sulle comunicazioni definisce chiaramente la portata e le condizioni di tali tipi di raccolta e le assoggetta a garanzie (procedurali) specifiche (inclusa l'approvazione giudiziaria preventiva), che garantisce che l'uso di tali misure sia limitato a quanto necessario e proporzionato. Inoltre l'obbligo di fornire informazioni dettagliate tanto nella domanda di rilascio di un mandato quanto nel mandato stesso esclude la possibilità di un accesso indiscriminato.

(190) Per le comunicazioni tra cittadini non coreani che rientrano in una delle tre categorie specifiche di cui al considerando 187, occorre presentare una domanda al direttore del NIS che, dopo un riesame dell'adeguatezza delle misure proposte, deve richiedere l'approvazione scritta preventiva al presidente della Repubblica di Corea ([340]). La domanda preparata dall'agenzia di intelligence deve comprendere le medesime informazioni dettagliate di una domanda per il rilascio di un mandato da parte dell'organo giurisdizionale (cfr. considerando 189), in particolare in merito alla giustificazione della richiesta e ai motivi principali del sospetto nutrito, materiali di sostegno e informazioni su obiettivi, persone fisiche interessate, portata e durata delle misure proposte ([341]). In situazioni di emergenza ([342]), occorre ottenere l'approvazione preventiva da parte del ministro al quale l'agenzia di intelligence pertinente fa riferimento, sebbene l'agenzia di intelligence debba richiedere l'approvazione del presidente della Repubblica di Corea immediatamente dopo l'adozione di misure di emergenza ([343]). Anche rispetto alla raccolta di comunicazioni tra cittadini esclusivamente non coreani, la legge sulle comunicazioni limita pertanto l'uso di tali misure a quanto necessario e proporzionato, circoscrivendo in maniera chiara le categorie limitate di persone fisiche che possono essere soggette a tali misure e definendo i criteri dettagliati che le agenzie di intelligence devono dimostrare per giustificare una domanda per la raccolta di informazioni. Inoltre ciò esclude ancora una volta la possibilità di accesso indiscriminato. Sebbene non vi sia alcuna approvazione preventiva indipendente di tali misure, la vigilanza indipendente è garantita ex post, in particolare, dalla PIPC e dalla NHRC (cfr. considerando 199 e 200).

(191) La legge sulle comunicazioni impone altresì diverse garanzie supplementari che contribuiscono alla vigilanza ex post e facilitano l'accesso alle persone fisiche a rimedi efficaci. Innanzitutto, per quanto riguarda qualsiasi tipo di raccolta per finalità di sicurezza nazionale, la legge sulle comunicazioni prevede diversi requisiti in materia di tenuta di registri e segnalazione. In particolare quando richiedono la cooperazione di operatori privati, le agenzie di intelligence devono fornire il mandato dell'organo giurisdizionale/l'autorizzazione presidenziale o una copia della copertina di una dichiarazione di censura di emergenza, che il soggetto tenuto a cooperare deve conservare nei suoi registri ([344]). Se gli operatori privati sono tenuti a cooperare, tanto

([336]) Articolo 6, quinto e ottavo comma, articolo 7, primo comma, punto 1 e articolo 7, terzo comma, della legge sulle comunicazioni in combinato disposto con l'articolo 7, terzo e quarto comma, del decreto di applicazione di tale legge.

([337]) Cfr. articolo 7, terzo comma, e articolo 6, quarto comma, della legge sulle comunicazioni (per la domanda dell'agenzia di intelligence), articolo 4 del decreto di applicazione di tale legge (per la domanda da parte del pubblico ministero) e articolo 7, terzo comma e articolo 6, sesto comma, della legge sulle comunicazioni (per il mandato).

([338]) Articolo 8 della legge sulle comunicazioni.

([339]) Articolo 8, secondo e ottavo comma, della legge sulle comunicazioni. La raccolta deve essere interrotta immediatamente qualora non si ottenga l'autorizzazione dell'organo giurisdizionale entro 36 ore dal momento in cui vengono adottate le misure. Nei casi in cui la sorveglianza viene completata in breve tempo, escludendo l'autorizzazione dell'organo giurisdizionale, il capo dell'Ufficio dell'Alta Procura competente deve inviare una notifica di misura di emergenza predisposta dall'agenzia di intelligence al capo dell'organo giurisdizionale competente, il quale su tale base può esaminare la legalità della raccolta (articolo 8, quinto e settimo comma, della legge sulle comunicazioni). Tale notifica deve indicare l'obiettivo, l'oggetto, la portata, il periodo, il luogo di esecuzione e il metodo di sorveglianza nonché i motivi che giustificano la mancata presentazione di una richiesta prima dell'adozione della misura (articolo 8, sesto comma, della legge sulle comunicazioni). Più in generale le agenzie di intelligence possono adottare misure di emergenza soltanto in conformità con una "dichiarazione di censura/intercettazione di emergenza" e devono tenere registrazioni di tali misure (articolo 8, quarto comma, della legge sulle comunicazioni).

([340]) Articolo 8, primo e secondo comma. dl decreto di applicazione della legge sulle comunicazioni.

([341]) Articolo 8, terzo comma, del decreto di applicazione della legge sulle comunicazioni, in combinato disposto con l'articolo 6, quarto comma, di tale legge.

([342]) Ossia nei casi in cui la misura riguarda un atto di cospirazione che minaccia la sicurezza nazionale, in cui non vi è sufficiente tempo per ottenere l'approvazione del presidente della Repubblica di Corea e la mancata adozione di misure di emergenza può compromettere la sicurezza nazionale (articolo 8, ottavo comma, della legge sulle comunicazioni).

([343]) Articolo 8, nono comma, della legge sulle comunicazioni. La raccolta deve essere interrotta immediatamente qualora non si ottenga l'autorizzazione entro 36 ore dal momento in cui viene presentata la domanda.

([344]) Articolo 9, secondo comma, della legge sulle comunicazioni e articolo 12 del decreto di applicazione di tale legge. Cfr. articolo 13 del decreto di applicazione della legge sulle comunicazioni relativo alla possibilità di imporre la fornitura di assistenza a uffici postali e fornitori di servizi di telecomunicazione. Gli operatori privati tenuti a divulgare informazioni potrebbero rifiutarsi di farlo laddove il mandato/l'autorizzazione o la dichiarazione di censura di emergenza faccia riferimento all'identificatore errato (ad esempio un numero di telefono appartenente a una persona fisica diversa da quella identificata). In ogni caso a tali soggetti è vietato rivelare password utilizzate per le comunicazioni (articolo 9, quarto comma, della legge sulle comunicazioni).

l'autorità pubblica richiedente quanto l'operatore pertinente devono tenere registrazioni in merito alla finalità e all'oggetto delle misure, nonché alla data di esecuzione ([345]). Inoltre le agenzie di intelligence devono riferire al direttore del NIS in merito alle informazioni che hanno raccolto e all'esito dell'attività di sorveglianza ([346]).

(192) In secondo luogo occorre notificare alle persone fisiche la raccolta dei loro dati (dati di conferma di comunicazioni o contenuto di comunicazioni) per finalità di sicurezza nazionale laddove ciò riguardi comunicazioni nel contesto delle quali almeno una delle parti è un cittadino coreano ([347]). Tale notifica deve essere effettuata per iscritto entro 30 giorni dalla data in cui la raccolta è terminata (anche laddove i dati siano stati ottenuti in conformità con la procedura di emergenza) e può essere differita soltanto se e nella misura in cui metterebbe a rischio la sicurezza nazionale o la vita e la sicurezza fisica della popolazione ([348]). Indipendentemente da tale notifica, le persone fisiche possono ottenere una riparazione in modi diversi, come spiegato in maniera più dettagliata nella sezione 3.3.4.

3.3.1.2 Raccolta di informazioni su sospetti terroristi

(193) La legge antiterrorismo prevede che il NIS possa raccogliere dati su sospetti terroristici ([349]) in conformità con le limitazioni e le garanzie stabilite in altre leggi ([350]). In particolare il NIS può ottenere dati relativi alle comunicazioni (ai sensi della legge sulle comunicazioni) e altre informazioni personali (attraverso una richiesta di divulgazione volontaria) ([351]). Per quanto concerne la raccolta di informazioni sulle comunicazioni (ossia contenuto di comunicazioni o dati di conferma di comunicazioni), si applicano le limitazioni e le garanzie di cui alla sezione 3.3.1.1, compreso il requisito di ottenere un mandato omologato da un organo giurisdizionale. Per quanto concerne le richieste di divulgazione volontaria di altri tipi di dati personali di sospetti terroristi, il NIS deve rispettare i requisiti di cui alla costituzione e alla legge sulla protezione delle informazioni personali in materia di necessità e proporzionalità (cfr. considerando 164) ([352]). I titolari del trattamento che ricevono tali richieste possono conformarvisi volontariamente nel rispetto delle condizioni di cui alla legge sulla protezione delle informazioni personali (ad esempio in conformità con il principio di minimizzazione dei dati e limitando l'impatto sulla vita privata della persona fisica in questione) ([353]). In tal caso devono altresì rispettare il requisito di notifica alla persona fisica interessata derivante dalla notifica n. 2021-5 (cfr. considerando 166).

([345]) Per le misure di limitazione delle comunicazioni, tali registrazioni devono essere conservate per tre anni, cfr. articolo 9, terzo comma, della legge sulle comunicazioni e articolo 17, secondo comma, del decreto di applicazione di tale legge. Per quanto concerne i dati di conferma di comunicazioni, le agenzie di intelligence devono tenere registri attestanti la presentazione di una richiesta di tali dati, nonché la richiesta scritta stessa e l'istituzione che vi ha fatto affidamento (articolo 13, quinto comma, e articolo 13-4, terzo comma, della legge sulle comunicazioni). I fornitori di servizi di telecomunicazione devono conservare i registri per sette anni e riferire due volte l'anno al ministro della Scienza e delle TIC in merito alla frequenza di tali divulgazioni (articolo 9, terzo comma, della legge sulle comunicazioni in combinato disposto con l'articolo 13, settimo comma, della stessa legge e l'articolo 37, quarto comma, e l'articolo 39 del decreto di applicazione di tale legge).

([346]) Articolo 18, terzo comma, della legge sulle comunicazioni.

([347]) Articolo 9-2, terzo comma, e articolo 13-4, della legge sulle comunicazioni. La notifica deve includere: 1) il fatto che le informazioni sono state raccolte; 2) l'agenzia che ha dato esecuzione alla misura; e 3) il periodo di esecuzione.

([348]) Articolo 9-2, quarto comma, della legge sulle comunicazioni. In tal caso, la notifica deve essere effettuata entro 30 giorni una volta che i motivi per il differimento cessano di sussistere (cfr. articolo 13-4, secondo comma, e articolo 9-2, sesto comma, della legge sulle comunicazioni).

([349]) Ossia i membri di un gruppo terroristico (come designato dalle Nazioni Unite, cfr. articolo 2, secondo comma, della legge antiterrorismo); persone che promuovono e diffondono idee o tattiche di un gruppo terroristico, raccolgono fondi o forniscono contributi per il terrorismo o si impegnano in altre attività di preparazione, cospirazione e propaganda del terrorismo o di istigazione al terrorismo; oppure persone in relazione alle quali esistono buoni motivi per sospettare che abbiano svolto tali attività (articolo 2, terzo comma, della legge antiterrorismo). Il concetto di "terrorismo" è definito dall'articolo 2, primo comma, della legge antiterrorismo come una condotta attuata al fine di ostacolare l'esercizio dell'autorità dello Stato, di un'amministrazione locale o di un governo straniero (comprese le organizzazioni internazionali) oppure al fine di costringere tali soggetti ad agire senza alcun obbligo giuridico a farlo oppure al fine di minacciare il pubblico. Tale condotta può ad esempio includere omicidi, rapimenti o la presa di ostaggi; il dirottamento/il sequestro, la distruzione o il danneggiamento di una nave o di un aeromobile; l'uso di armi biochimiche, esplosive o incendiarie con l'intenzione di causare decessi, lesioni gravi o danni; nonché l'uso abusivo di materiali nucleari o radioattivi.

([350]) Articolo 9, primo e terzo comma, della legge antiterrorismo.

([351]) Sebbene la legge antiterrorismo faccia riferimento anche alla possibilità di raccogliere informazioni sull'ingresso nella Repubblica di Corea e sull'uscita dal paese sulla base della legge sull'immigrazione e della legge sulle dogane, tali leggi attualmente non prevedono l'attribuzione di tale potere (cfr. sezione 3.2.2.1 dell'allegato II). In ogni caso, in linea di principio tali disposizioni non si applicano ai dati trasferiti sulla base della presente decisione, dato che in linea di massima riguardano informazioni raccolte direttamente dalle autorità coreane (piuttosto che dall'accesso a dati precedentemente trasferiti dall'Unione verso titolari del trattamento coreani). Inoltre la legge antiterrorismo menziona la legge sulla segnalazione e l'utilizzo di informazioni specifiche sulle operazioni finanziarie come base giuridica per la raccolta di informazioni sulle operazioni finanziarie. Tuttavia, come spiegato nella nota 200, i tipi di dati che potrebbero essere ottenuti sulla base di tale legge non rientrano nell'ambito di applicazione della presente decisione. Infine la legge antiterrorismo prevede altresì che il NIS possa raccogliere informazioni relative all'ubicazione attraverso richieste non vincolanti, nel qual caso i soggetti che forniscono tali informazioni potrebbero divulgare volontariamente tali informazioni nel rispetto delle condizioni di cui alla legge sulla protezione delle informazioni personali (come illustrato al considerando 193) e alla legge sulle informazioni relative all'ubicazione. Tuttavia, come spiegato anche nella nota 17, le informazioni relative all'ubicazione non sarebbero state trasferite dall'Unione verso titolari del trattamento coreani sulla base della presente decisione, ma sarebbero piuttosto generate all'interno della Corea.

([352]) Cfr. allegato II, sezione 3.2.2.2.

([353]) Cfr. articolo 58, quarto comma, della legge sulla protezione delle informazioni personali, che prescrive che le informazioni personali siano trattate nella misura minima necessaria al conseguimento della finalità prevista e articolo 3, sesto comma, della legge sulla protezione delle informazioni personali, che prescrive che le informazioni personali debbano essere trattate in maniera tale da ridurre al minimo la possibilità di violazione della vita privata della persona fisica in questione. Cfr. anche articolo 59, punti 2 e 3, della legge sulla protezione delle informazioni personali, secondo il quale ai titolari del trattamento è fatto divieto divulgare informazioni personali a terzi senza legittimazione a procedere in tal senso.

3.3.1.3 Richieste di divulgazione volontaria di dati di abbonati

(194) Sulla base della legge sulle imprese di telecomunicazione, i fornitori di servizi di telecomunicazione possono divulgare volontariamente i dati degli abbonati (cfr. considerando 163) su richiesta di un'agenzia di intelligence che intende raccogliere tali informazioni per prevenire una minaccia per la sicurezza nazionale ([354]). Per quanto concerne tali richieste del NIS, si applicano le stesse limitazioni (derivanti dalla costituzione, dalla legge sulla protezione delle informazioni personali e dalla legge sulle imprese di telecomunicazione) applicate nel settore delle attività di contrasto penale, come indicato al considerando 164 ([355]). I fornitori di servizi di telecomunicazione non sono tenuti a conformarsi a tali richieste e possono farlo nel rispetto delle condizioni di cui alla legge sulla protezione delle informazioni personali (in particolare in conformità con il principio di minimizzazione dei dati nonché limitando l'impatto sulla vita privata della persona fisica in questione; cfr. anche considerando 193). Gli stessi requisiti per quanto riguarda la tenuta di registri e la notifica alla persona fisica in questione si applicano come nel settore delle attività di contrasto penale (cfr. considerando 165 e 166).

3.3.2 *Ulteriore utilizzo delle informazioni raccolte*

(195) Il trattamento di dati personali raccolti dalle autorità coreane per finalità di sicurezza nazionale è soggetto ai principi di limitazione della finalità (articolo 3, primo e secondo comma, della legge sulla protezione delle informazioni personali), di liceità e correttezza del trattamento (articolo 3, primo comma, della medesima legge), di proporzionalità/minimizzazione dei dati (articolo 3, primo e sesto comma, e articolo 58 della medesima legge), esattezza (articolo 3, terzo comma, della medesima legge), trasparenza (articolo 3, quinto comma, della medesima legge), sicurezza (articolo 58, quarto comma, della medesima legge) e limitazione della conservazione (articolo 58, quarto comma, della medesima legge) ([356]). La possibile divulgazione di dati personali a terzi (compresi paesi terzi) può avvenire soltanto nel rispetto di tali principi (in particolare di limitazione della finalità e minimizzazione dei dati), dopo aver valutato il rispetto dei principi di necessità e proporzionalità (articolo 37, secondo comma, della costituzione) e tenendo conto dell'impatto sui diritti delle persone fisiche interessate (articolo 3, sesto comma, della legge sulla protezione delle informazioni).

(196) Per quanto concerne il contenuto di comunicazioni e i dati di conferma di comunicazioni, la legge sulle comunicazioni limita ulteriormente l'uso di tali dati ai procedimenti giudiziari, nel contesto dei quali una parte coinvolta nella comunicazione fa affidamento su tali informazioni per avanzare una richiesta di risarcimento dei danni; oppure usi consentiti ai sensi di altre leggi ([357]).

3.3.3 *Vigilanza*

(197) Le attività delle autorità di sicurezza nazionale coreane sono soggette a vigilanza da parte di organismi diversi ([358]).

(198) Innanzitutto la legge antiterrorismo prevede meccanismi di vigilanza specifici per le attività di antiterrorismo, compresa la raccolta di dati su persone sospettate di atti di terrorismo. In particolare, a livello dell'esecutivo, le attività di antiterrorismo sono soggette a vigilanza da parte della commissione antiterrorismo ([359]), alla quale il direttore del NIS è tenuto a riferire in merito alle indagini e al tracciamento di sospetti terroristi per raccogliere informazioni o materiali necessari per le attività antiterrorismo ([360]). Inoltre il responsabile della tutela dei diritti umani vigila specificamente sulla conformità delle attività antiterrorismo rispetto ai diritti fondamentali ([361]). Tale responsabile è nominato dal presidente della commissione antiterrorismo tra persone fisiche che soddisfano qualifiche specifiche elencate nel decreto di applicazione di tale legge ([362]) per un termine (rinnovabile) di due anni e può essere rimosso dal suo incarico soltanto per motivi specifici e limitati e per giusta causa ([363]). Nell'esercizio della sua funzione di vigilanza, il responsabile della tutela dei diritti umani può emettere raccomandazioni

([354]) Articolo 83, terzo comma, della legge sulle imprese di telecomunicazione.
([355]) Cfr. anche allegato II, sezione 3.2.3.
([356]) Cfr. allegato II, sezione 1.2.
([357]) Articolo 5, primo e secondo comma, e articolo 13-5 della legge sulle comunicazioni.
([358]) Cfr. allegato II, sezione 3.3.
([359]) Articolo 5, terzo comma, della legge antiterrorismo. La commissione è presieduta dal primo ministro e composta da diversi ministri e capi di agenzie governative, quali i ministri degli Affari esteri, della Giustizia, della Difesa nazionale e degli Interni e della Sicurezza, il direttore del NIS e il commissario generale dell'agenzia di polizia nazionale (articolo 3, primo comma, del decreto di applicazione della legge antiterrorismo).
([360]) Articolo 9, quarto comma, della legge antiterrorismo.
([361]) Articolo 7 della legge antiterrorismo.
([362]) Ossia chiunque abbia la qualifica di avvocato con almeno dieci anni di esperienza lavorativa oppure con conoscenza a livello di esperto nel settore dei diritti umani e che stia prestando o abbia prestato servizio (quanto meno) come professore associato da/per almeno dieci anni oppure abbia prestato servizio in veste di funzionario pubblico di livello più alto in seno ad agenzie statali o in amministrazioni locali, oppure abbia almeno dieci anni di esperienza lavorativa nel settore dei diritti umani, ad esempio in seno ad un'organizzazione non governativa (articolo 7, primo comma, del decreto di applicazione della legge antiterrorismo).
([363]) Ad esempio in caso di rinvio a giudizio in riferimento a un procedimento penale in relazione alle sue funzioni, in caso di divulgazione di informazioni riservate oppure a causa di incapacità mentale o fisica a lungo termine (articolo 7, terzo comma, del decreto di applicazione della legge antiterrorismo).

generali destinate a migliorare la tutela dei diritti umani ([364]) nonché raccomandazioni specifiche relative a misure correttive qualora sia stata constata una violazione dei diritti umani ([365]). Le autorità pubbliche sono tenute a informare tale responsabile in merito al seguito dato alle sue raccomandazioni ([366]).

(199) In secondo luogo la PIPC vigila sul rispetto da parte delle autorità di sicurezza nazionale rispetto alle norme in materia di protezione dei dati; tale contesto comprende tanto le disposizioni applicabili della legge sulla protezione delle informazioni personali (cfr. considerando 149) quanto le limitazioni e le garanzie che si applicano alla raccolta di dati personali nel contesto di altre leggi (la legge sulle comunicazioni, la legge antiterrorismo e la legge sulle imprese di telecomunicazione; cfr. anche considerando 171) ([367]). Nell'esercizio di tale ruolo di vigilanza, la PIPC può esercitare tutti i suoi poteri di indagine e di imposizione di misure correttive, come descritto in dettaglio nella sezione 2.4.2.

(200) In terzo luogo le attività delle autorità di sicurezza nazionale sono soggette alla vigilanza indipendente della NHRC, in conformità con le procedure di cui al considerando 172 ([368]).

(201) In quarto luogo, la funzione di vigilanza del BAI si estende anche alle autorità di sicurezza nazionale, sebbene, in circostanze eccezionali, il NIS possa rifiutarsi di fornire determinate informazioni o determinati materiali, ossia quando costituiscono segreti di Stato e la loro conoscenza da parte del pubblico inciderebbe in maniera significativa sulla sicurezza nazionale ([369]).

(202) Infine la vigilanza parlamentare sulle attività del NIS è svolta dall'Assemblea nazionale (attraverso un comitato specializzato per l'intelligence) ([370]). La legge sulle comunicazioni stabilisce un ruolo specifico di vigilanza per l'Assemblea nazionale in merito al ricorso a misure di limitazione delle comunicazioni per finalità di sicurezza nazionale ([371]). In particolare l'Assemblea nazionale può condurre ispezioni in loco di apparecchiature di intercettazione e può richiedere al NIS e agli operatori di telecomunicazioni che hanno divulgato il contenuto di comunicazioni di riferire in merito a tali divulgazioni. L'Assemblea nazionale può altresì svolgere le sue funzioni generali di vigilanza (in conformità con le procedure di cui al considerando 174). La legge sul NIS prescrive che il direttore del NIS risponda senza indugio quando il comitato per l'intelligence richiede una relazione su una questione specifica ([372]), prevedendo norme specifiche per talune informazioni particolarmente sensibili. Concretamente il direttore del NIS può rifiutarsi di rispondere o di testimoniare dinanzi il comitato soltanto in circostanze eccezionali, ossia se la richiesta riguarda segreti di Stato relativi a questioni militari, diplomatiche o concernenti la Corea del Nord che potrebbero avere un grave impatto sul "destino nazionale" del paese qualora diventassero di dominio pubblico ([373]). In tal caso il comitato per l'intelligence può richiedere al primo ministro di fornire una spiegazione e, in assenza di tale spiegazione entro sette giorni, la risposta o la testimonianza non può essere rifiutata.

3.3.4 *Ricorso*

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

(204) Innanzitutto, ai sensi dell'articolo 3, quinto comma, dell'articolo 4, primo, terzo e quarto comma, della legge sulla protezione delle informazioni personali, le persone fisiche possono esercitare i loro diritti di accesso, di rettifica, di cancellazione e di sospensione nei confronti delle autorità di sicurezza nazionale. La sezione 6 della notifica n. 2021-5 (allegato I della presente decisione) chiarisce ulteriormente le modalità di applicazione di tali diritti nel contesto del trattamento di dati per finalità di sicurezza nazionale. In particolare un'autorità di sicurezza nazionale può limitare o negare l'esercizio di un tale diritto soltanto nella misura e per il tempo necessari e

([364]) Articolo 8, primo comma, del decreto di applicazione della legge antiterrorismo.
([365]) Articolo 9, primo comma, del decreto di applicazione della legge antiterrorismo. Il responsabile della tutela dei diritti umani decide autonomamente in merito all'adozione di raccomandazioni, ma è tenuto a segnalarle al presidente della commissione antiterrorismo.
([366]) Articolo 9, secondo comma, del decreto di applicazione della legge antiterrorismo. Stando alla dichiarazione ufficiale del governo coreano, la mancata attuazione di una raccomandazione del responsabile della tutela dei diritti umani verrebbe portata all'attenzione della commissione antiterrorismo, che comprende il primo ministro, sebbene finora non vi siano stati casi in cui le raccomandazioni del responsabile della tutela dei diritti umani non siano state implementate (cfr. sezione 3.3.1 dell'allegato II).
([367]) Allegato II, sezione 3.3.4.
([368]) Specificamente rispetto al NIS, la NHRC ha in passato effettuato indagini d'ufficio e ha gestito diversi reclami individuali. Cfr. ad esempio la relazione annuale del 2018 della NHRC, pag. 128 (disponibile all'indirizzo: https://www.humanrights.go.kr/site/program/board/basicboard/view?menuid=002003003001&pagesize=10&boardtypeid=7017&boardid=7604746) e la relazione annuale del 2019 della NHRC, pag. 70 (disponibile all'indirizzo: https://www.humanrights.go.kr/site/program/board/basicboard/view?menuid=002003003001&pagesize=10&boardtypeid=7017&boardid=7606217).
([369]) Articolo 13, primo comma, della legge sul NIS.
([370]) Articolo 36 e articolo 37, primo comma, punto 15, della legge sull'assemblea nazionale.
([371]) Articolo 15 della legge sulle comunicazioni.
([372]) Articolo 15, secondo comma, della legge sul NIS.
([373]) Articolo 17, secondo comma, della legge sul NIS. I "segreti di Stato" sono definiti come fatti, beni o conoscenze (classificati) che non saranno divulgati a nessun altro paese o a nessun'altra organizzazione al fine di evitare un grave svantaggio per la sicurezza nazionale e ai quali è consentito soltanto un accesso limitato. Cfr. articolo 13, quarto comma, della legge sul NIS.

proporzionati a proteggere un importante obiettivo di interesse pubblico (ad esempio nella misura in cui e per il tempo per il quale la concessione del diritto in questione comprometterebbe un'indagine in corso o costituirebbe una minaccia per la sicurezza nazionale) oppure qualora concedere il diritto in questione possa minacciare la vita o compromettere l'incolumità di una terza parte. Invocare tale limitazione richiede quindi la definizione di un equilibrio tra i diritti e gli interessi della persona fisica rispetto all'interesse pubblico pertinente e non può, in alcun caso, incidere sull'essenza del diritto in questione (articolo 37, secondo comma, della costituzione). Laddove la richiesta venga negata o limitata, la persona fisica deve ricevere una notifica dei motivi senza indugio.

(205) In secondo luogo, le persone fisiche hanno il diritto di ottenere una riparazione ai sensi della legge sulla protezione delle informazioni personali qualora i loro dati siano stati trattati da un'autorità di sicurezza nazionale in violazione di tale legge o delle limitazioni e delle garanzie stabilite in altre leggi che disciplinano la raccolta di dati personali (in particolare la legge sulle comunicazioni, cfr. considerando 171) ([374]). Tale diritto può essere esercitato attraverso un reclamo presentato alla PIPC (anche tramite il call centre per la tutela della vita privata gestito dall'agenzia coreana per la sicurezza e internet) ([375]). Inoltre, al fine di facilitare l'accesso a una riparazione nei confronti di autorità coreane di sicurezza nazionale, le persone fisiche dell'UE possono presentare un reclamo alla PIPC attraverso la loro autorità nazionale di protezione dei dati ([376]). In tal caso la PIPC invierà una notifica alla persona fisica attraverso quest'ultima autorità una volta conclusa l'indagine (fornendo altresì, laddove applicabile, informazioni in merito a misure correttive imposte). Ai sensi della legge sui contenziosi amministrativi, le persone fisiche possono inoltre impugnare le decisioni o l'inazione della PIPC (cfr. considerando 132).

(206) In terzo luogo le persone fisiche possono promuovere un reclamo presso il responsabile della tutela dei diritti umani in merito alla violazione del loro diritto alla vita privata/alla protezione dei dati nel contesto di attività di antiterrorismo (ossia ai sensi della legge antiterrorismo) ([377]), il quale può raccomandare azioni correttive. Dato che non vi sono requisiti di ammissibilità per rivolgersi al responsabile della tutela dei diritti umani, un reclamo verrà gestito anche se la persona fisica in questione non è in grado di dimostrare di aver subito in effetti un pregiudizio (ad esempio in ragione della presunta raccolta illecita dei suoi dati da parte di un'autorità di sicurezza nazionale) ([378]). L'autorità pertinente deve informare il responsabile della tutela dei diritti umani di eventuali misure adottate per attuare le sue raccomandazioni.

(207) In quarto luogo le persone fisiche possono presentare un reclamo presso la NHRC in relazione alla raccolta dei loro dati da parte delle autorità di sicurezza nazionale e ottenere una riparazione in conformità con la procedura di cui al considerando 178 ([379]).

(208) Infine sono disponibili diversi ricorsi giurisdizionali ([380]) che consentono alle persone fisiche di invocare le limitazioni e le garanzie di cui alla sezione 3.3.1 per ottenere una riparazione. In particolare le persone fisiche possono contestare la legalità delle azioni delle autorità di sicurezza nazionale ai sensi della legge sui contenziosi amministrativi (secondo la procedura illustrata al considerando 181 o la legge sulla Corte costituzionale (cfr. considerando 182). Possono inoltre ottenere un risarcimento dei danni ai sensi della legge sul risarcimento da parte dello Stato (come illustrato in maggior dettaglio al considerando 183).

4. **CONCLUSIONI**

(209) La Commissione ritiene che la Repubblica di Corea, attraverso la legge sulla protezione delle informazioni personali, le norme speciali applicabili a determinati settori (come analizzate nella sezione 2) e le garanzie supplementari di cui alla notifica n. 2021-5 (allegato I), assicuri un livello di protezione dei dati personali trasferiti dall'Unione europea sostanzialmente equivalente a quello garantito dal regolamento (UE) 2016/679.

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

([374]) Articolo 58, quarto comma, e articolo 4, quinto comma, della legge sulla protezione delle informazioni personali. Cfr. allegato II, sezione 3.4.2.
([375]) Articolo 62 e articolo 63, secondo comma, della legge sulla protezione delle informazioni personali.
([376]) Notifica n. 2021-5 (sezione 6, allegato I).
([377]) Articolo 8, primo comma, punto 2, del decreto di applicazione della legge antiterrorismo.
([378]) Cfr. allegato II, sezione 3.4.1.
([379]) Ad esempio la NHRC riceve regolarmente reclami contro il servizio nazionale di intelligence, cfr. dati riportati nella relazione annuale del 2019 della NHRC in merito al numero di reclami ricevuti tra il 2015 e il 2019, pag. 70 (disponibile in inglese all'indirizzo: https://www.humanrights.go.kr/site/program/board/basicboard/view?menuid=002003003001&pagesize=10&boardtypeid=7017&boardid=7606217).
([380]) Cfr. allegato II, sezione 3.4.4.

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

(212) Di conseguenza, in considerazione delle risultanze di cui alla presente decisione, si dovrebbe decidere che la Repubblica di Corea garantisce un livello di protezione adeguato ai sensi dell'articolo 45 del regolamento (UE) 2016/679, interpretato alla luce della Carta dei diritti fondamentali dell'Unione europea, per i dati personali trasferiti dall'Unione europea alla Repubblica di Corea a titolari del trattamento di dati personali in tale Stato soggetti alla legge sulla protezione delle informazioni personali, fatta eccezione per le organizzazioni religiose nella misura in cui trattano dati personali per le loro attività missionarie, i partiti politici nella misura in cui trattano dati personali nel contesto della nomina di candidati e i titolari del trattamento che sono soggetti a vigilanza da parte della commissione per i servizi finanziari per il trattamento delle informazioni creditizie personali ai sensi della legge sulle informazioni creditizie, nella misura in cui trattino tali informazioni.

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

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

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

(215) È opportuno ricordare che, ai sensi dell'articolo 58, paragrafo 5, del regolamento (UE) 2016/679, e come spiegato dalla Corte di giustizia nella sentenza *Schrems* ([381]), quando un'autorità nazionale di protezione dei dati mette in dubbio, anche in seguito a un reclamo, la compatibilità di una decisione di adeguatezza della Commissione con i diritti fondamentali della persona fisica concernenti la tutela della vita privata e la protezione dei dati, il diritto nazionale deve prevedere mezzi di ricorso per l'affermazione di tali obiezioni dinanzi un organo giurisdizionale nazionale, che può essere tenuto a effettuare un rinvio pregiudiziale alla Corte di giustizia ([382]).

6. MONITORAGGIO E RIESAME DELLA PRESENTE DECISIONE

(216) Secondo la giurisprudenza della Corte di giustizia ([383]), e come riconosciuto dall'articolo 45, paragrafo 4, del regolamento (UE) 2016/679, la Commissione dovrebbe monitorare costantemente gli sviluppi nel paese terzo registrati dopo l'adozione di una decisione di adeguatezza, al fine di valutare se il paese terzo continui a garantire un livello di protezione sostanzialmente equivalente. Tale verifica è in ogni caso obbligatoria quando la Commissione riceve informazioni che fanno sorgere un dubbio giustificato al riguardo.

(217) La Commissione dovrebbe pertanto controllare su base continuativa la situazione nella Repubblica di Corea per quanto riguarda il quadro giuridico e la prassi effettiva del trattamento dei dati personali valutati dalla presente decisione, compreso il rispetto da parte delle autorità coreane delle dichiarazioni, delle garanzie e degli impegni figuranti nell'allegato II. Per agevolare tale processo, le autorità coreane dovrebbero essere invitate a informare prontamente la Commissione degli sviluppi sostanziali rilevanti ai fini della presente decisione, per quanto concerne il trattamento dei dati personali da parte degli operatori economici e delle autorità pubbliche, nonché le limitazioni e le garanzie applicabili all'accesso ai dati personali da parte delle autorità pubbliche.

([381]) *Schrems*, punto 65.

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

([383]) *Schrems*, punto 76.

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

(219) In applicazione dell'articolo 45, paragrafo 3, del regolamento (UE) 2016/679 ([384]) e alla luce del fatto che il livello di protezione assicurato dall'ordinamento giuridico coreano può evolversi, la Commissione, successivamente all'adozione della presente decisione, dovrebbe riesaminare periodicamente se le constatazioni relative al livello di protezione assicurato dalla Repubblica di Corea continuino ad essere giustificate in fatto e in diritto.

(220) A tal fine la presente decisione dovrebbe essere oggetto di un primo riesame entro tre anni dall'entrata in vigore. A seguito del primo riesame, e tenuto conto del suo esito, la Commissione deciderà, in stretta consultazione con il comitato istituito a norma dell'articolo 93, paragrafo 1, del regolamento (UE) 2016/679, se mantenere il ciclo di tre anni. In ogni caso i successivi riesami dovrebbero avvenire almeno ogni quattro anni ([385]). Detto riesame dovrebbe riguardare tutti gli aspetti del funzionamento della presente decisione, in particolare: l'applicazione delle garanzie supplementari di cui all'allegato I della presente decisione, con particolare riguardo alle tutele offerte in caso di trasferimenti successivi; gli sviluppi pertinenti della giurisprudenza; le norme sul trattamento di informazioni pseudonimizzate per finalità di compilazione di statistiche, di ricerca scientifica e di archiviazione nell'interesse pubblico, nonché l'applicazione delle eccezioni di cui all'articolo 28, settimo comma, della legge sulla protezione delle informazioni personali; l'efficacia dell'esercizio dei diritti individuali, anche dinanzi la PIPC riformata di recente, nonché l'applicazione di eccezioni a tali diritti; l'applicazione di esenzioni parziali nel contesto della legge sulla protezione delle informazioni personali; così come le limitazioni e le garanzie per quanto concerne l'accesso da parte di pubbliche amministrazioni (come indicato nell'allegato II della presente decisione), compresa la cooperazione della PIPC con le autorità di protezione dei dati dell'UE in merito a reclami da parte di persone fisiche. Dovrebbe inoltre includere l'efficacia della vigilanza e delle attività di contrasto, per quanto riguarda la legge sulla protezione delle informazioni personali nonché nel settore delle attività di contrasto penale e della sicurezza nazionale (in particolare da parte della PIPC e della NHRC).

(221) Per effettuare il riesame, la Commissione dovrebbe incontrare la PIPC, accompagnata, se del caso, da altre autorità coreane competenti per l'accesso delle pubbliche amministrazioni, compresi i pertinenti organismi di vigilanza. Alla riunione dovrebbero poter partecipare i rappresentanti dei membri del comitato europeo per la protezione dei dati. Nel quadro del riesame la Commissione dovrebbe chiedere alla PIPC di fornire informazioni complete su tutti gli aspetti pertinenti alla constatazione di adeguatezza, incluse le limitazioni e le garanzie relativamente all'accesso delle pubbliche amministrazioni ([386]). La Commissione dovrebbe inoltre chiedere delucidazioni in merito a qualsiasi informazione ricevuta risultata pertinente ai fini della presente decisione, comprese le relazioni pubbliche delle autorità coreane o di altri portatori di interessi in Corea, del comitato europeo per la protezione dei dati, delle singole autorità di protezione dei dati e dei gruppi della società civile, le informazioni dei mezzi di comunicazione o qualsiasi altra fonte di informazioni disponibile.

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

7. SOSPENSIONE, ABROGAZIONE O MODIFICA DELLA PRESENTE DECISIONE

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

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

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

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

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

([386]) Cfr. allegato II della presente decisione.

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

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

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

8. **CONSIDERAZIONI FINALI**

(229) Il comitato europeo per la protezione dei dati ha pubblicato il proprio parere ([387]), del quale si è tenuto conto nell'elaborazione della presente decisione.

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

HA ADOTTATO LA PRESENTE DECISIONE:

Articolo 1

1. Ai fini dell'articolo 45 del regolamento (UE) 2016/679, la Repubblica di Corea garantisce un livello di protezione adeguato dei dati personali trasferiti dall'Unione europea ai soggetti nella Repubblica di Corea ai quali si applica la legge sulla protezione delle informazioni personali, quale integrata dalle garanzie supplementari di cui all'allegato I, unitamente alle dichiarazioni, alle garanzie e agli impegni ufficiali figuranti nell'allegato II.

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

(a) organizzazioni religiose, nella misura in cui trattino i dati personali per le loro attività missionarie;

(b) partiti politici, nella misura in cui trattino i dati personali nel contesto della nomina di candidati;

(c) soggetti sopposti a vigilanza da parte della commissione per i servizi finanziari per il trattamento delle informazioni creditizie personali ai sensi della legge sulle informazioni creditizie, nella misura in cui trattino tali informazioni.

Articolo 2

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

Articolo 3

1. La Commissione monitora costantemente l'applicazione del quadro giuridico su cui si basa la presente decisione, comprese le condizioni in cui sono effettuati i trasferimenti successivi, sono esercitati i diritti individuali e le autorità pubbliche coreane hanno accesso ai dati trasferiti sulla base della presente decisione, al fine di valutare se la Repubblica di Corea continui a garantire un livello di protezione adeguato ai sensi dell'articolo 1.

([387]) Parere 32/2021 concernente il 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, disponibile al seguente indirizzo: https://edpb.europa.eu/our-work-tools/our-documents/opinion-art-70/opinion-322021-regarding-european-commission-draft_en.

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

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

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

5. In presenza di indicazioni del fatto che non è più assicurato un livello di protezione adeguato la Commissione informa le autorità coreane competenti. Se necessario, essa può decidere di sospendere, modificare o abrogare la presente decisione o di limitarne l'ambito di applicazione, conformemente all'articolo 45, paragrafo 5, del regolamento (UE) 2016/679, in particolare in presenza di indicazioni del fatto che:

(a) i titolari del trattamento in Corea che hanno ricevuto dati personali dall'Unione europea nell'ambito della presente decisione non rispettano le garanzie supplementari figuranti nell'allegato I, ovvero del fatto che la vigilanza e il controllo del rispetto in questo senso sono insufficienti;

(b) le autorità pubbliche coreane non rispettano le dichiarazioni, le garanzie e gli impegni figuranti nell'allegato II, in particolare per quanto riguarda le condizioni e le limitazioni alla raccolta dei dati personali trasferiti nell'ambito della presente decisione e all'accesso agli stessi da parte delle autorità pubbliche coreane per finalità di contrasto penale o di sicurezza nazionale.

La Commissione può inoltre adottare tali misure se la mancanza di collaborazione del governo coreano le impedisce di stabilire se la Repubblica di Corea continua ad assicurare un livello di protezione adeguato.

Articolo 4

Gli Stati membri sono destinatari della presente decisione.

Fatto a Bruxelles, il 17 dicembre 2021

Per la Commissione
Didier REYNDERS
Membro della Commissione

ALLEGATO I

NORME SUPPLEMENTARI PER L'INTERPRETAZIONE E L'APPLICAZIONE DELLA LEGGE SULLA PROTEZIONE DELLE INFORMAZIONI PERSONALI IN RELAZIONE AL TRATTAMENTO DI DATI PERSONALI TRASFERITI IN COREA

Contenuto

I. **Sintesi**

La Corea e l'Unione europea (in appresso denominata "UE") sono state impegnate in discussioni in materia di adeguatezza, a seguito delle quali la Commissione europea ha stabilito che la Corea garantisce un livello adeguato di protezione dei dati personali ai sensi dell'articolo 45 del regolamento generale sulla protezione dei dati.

In tale contesto la *Personal Information Protection Commission* (PIPC, commissione per la protezione delle informazioni personali) ha adottato la presente notifica sulla base dell'articolo 5 (obblighi dello Stato, ecc.) e dell'articolo 14 (Cooperazione internazionale) [1] della legge sulla protezione delle informazioni personali al fine di chiarire l'interpretazione, l'applicazione e l'esecuzione di talune disposizioni di tale legge, anche per quanto concerne il trattamento di dati personali trasferiti in Corea ai sensi della decisione di adeguatezza dell'UE.

Dato che la presente notifica gode dello status di una norma amministrativa che l'agenzia amministrativa competente stabilisce e annuncia per chiarire le norme per l'interpretazione, l'applicazione e l'esecuzione della legge sulla protezione delle informazioni personali nel sistema giuridico della Corea, si tratta di un documento giuridicamente vincolante per il titolare del trattamento delle informazioni personali nel senso che qualsiasi violazione della presente notifica può essere considerata una violazione delle disposizioni pertinenti di tale legge. Inoltre, laddove diritti e interessi personali siano lesi in ragione di una violazione della presente notifica, le persone fisiche in questione hanno il diritto di ottenere riparazione dalla commissione per la protezione delle informazioni personali o da un organo giurisdizionale.

Di conseguenza, ai sensi dell'articolo 64, primo e secondo comma, della legge sulla protezione delle informazioni personali, laddove il titolare del trattamento delle informazioni personali, che tratta tali informazioni trasferite in Corea ai sensi della decisione di adeguatezza dell'UE, non adotti misure conformi alla presente notifica, tale circostanza sarà considerata "costituire un motivo sostanziale per ritenere che vi sia stata una violazione in relazione alle informazioni personali e che l'inazione possa causare danni a cui è difficile porre rimedio". In tali casi la commissione per la

[1] L'articolo 14 della legge sulla protezione delle informazioni personali sancisce il potere del governo coreano di stabilire politiche destinate a migliorare il livello di protezione delle informazioni personali nel contesto internazionale e a impedire la violazione dei diritti degli interessati dovuta al trasferimento transfrontaliero di informazioni personali.

protezione delle informazioni personali o le relative agenzie amministrative centrali possono ordinare al titolare del trattamento delle informazioni personali corrispondente di adottare misure correttive, ecc. in maniera conforme ai poteri conferiti dalla presente disposizione e, a seconda delle violazioni specifiche della legge, può imporre anche sanzioni corrispondenti (sanzioni, sanzioni amministrative pecuniarie, ecc.).

II. **Definizioni**

Le definizioni dei termini utilizzate nella presente disposizione sono specificate in appresso.

(i) Legge sulla protezione delle informazioni personali: legge n. 16930, modificata il 4 febbraio 2020 e applicata dal 5 agosto 2020.

(ii) Decreto presidenziale: decreto di applicazione della legge sulla protezione delle informazioni personali (decreto presidenziale n. 30509, del 3 marzo 2020, che modifica altre leggi).

(iii) Interessato: una persona fisica identificabile tramite le informazioni trattate che diventa così il soggetto cui tali informazioni sono riferite.

(iv) Titolare del trattamento delle informazioni personali: un ente pubblico, una persona giuridica, un'organizzazione, una persona fisica, ecc. che tratta informazioni personali direttamente o indirettamente nel contesto delle sue attività;

(v) UE: l'Unione europea (a partire dalla fine di febbraio del 2020, costituita da 27 paesi membri [2], compresi Belgio, Bulgaria, Cechia, Danimarca, Germania, Estonia, Irlanda, Grecia, Spagna, Francia, Croazia, Italia, Cipro, Lettonia, Lituania, Lussemburgo, Ungheria, Malta, Paesi Bassi, Austria, Polonia, Portogallo, Romania, Slovenia, Slovacchia, Finlandia e Svezia) e i paesi associati all'UE attraverso l'accordo sullo Spazio economico europeo (Islanda, Liechtenstein e Norvegia).

(vi) Regolamento generale sulla protezione dei dati: il regolamento generale sulla protezione dei dati dell'UE, ossia il regolamento (UE) 2016/679.

(vii) Decisione di adeguatezza: conformemente all'articolo 45, paragrafo 3, del regolamento generale sulla protezione dei dati, la Commissione europea ha deciso che un paese terzo, un territorio o uno o più settori specifici all'interno di un paese terzo, o un'organizzazione internazionale garantiscono un livello di protezione adeguato per le informazioni personali.

III. **Norme supplementari**

1. **Limitazione all'uso e alla fornitura di informazioni personali al di fuori della finalità prevista (articoli 3, 15 e 18 della legge sulla protezione delle informazioni personali)**

<Legge sulla protezione delle informazioni personali

(legge n. 16930, parzialmente modificata il 4 febbraio 2020)>

Articolo 3 (Principi per la protezione delle informazioni personali) 1) Il titolare del trattamento delle informazioni personali specifica esplicitamente le finalità per le quali le informazioni personali vengono trattate; e raccoglie informazioni personali in maniera lecita e corretta, nella misura minima necessaria per il conseguimento di tali finalità.

2) Il titolare del trattamento delle informazioni personali tratta le informazioni personali in maniera appropriata a quanto necessario per le finalità per le quali tali informazioni personali vengono trattate e non le utilizza in maniera diversa da tali finalità.

Articolo 15 (Raccolta e utilizzo di informazioni personali) 1) Un titolare del trattamento delle informazioni personali può raccogliere informazioni personali in una delle seguenti circostanze, e utilizzarle nel contesto della finalità prevista per la loro raccolta:

1. laddove sia stato ottenuto il consenso da un interessato;

2. laddove esistano disposizioni particolari in atti legislativi oppure laddove ciò sia inevitabile ai fini del rispetto di obblighi giuridici;

3. laddove ciò sia inevitabile per l'adempimento da parte di un ente pubblico dei suoi doveri nel contesto della sua competenza giurisdizionale come prescritto da leggi, ecc.;

4. laddove ciò sia inevitabilmente necessario per dare esecuzione e attuare un contratto stipulato con un interessato;

[2] Fino alla fine del periodo transitorio, il presente documento comprende anche il Regno Unito, come previsto dagli articoli 126, 127 e 132 dell'accordo sul recesso del Regno Unito di Gran Bretagna e Irlanda del Nord dall'Unione europea e dalla Comunità europea dell'energia atomica (GU C 384I del 12.11.2019, pag. 1).

5. laddove ciò sia ritenuto manifestamente necessario per la protezione della vita, dell'incolumità o degli interessi patrimoniali dell'interessato o di una terza parte rispetto a un pericolo imminente nel caso in cui l'interessato o il suo rappresentante legale non sia in grado di esprimere un'intenzione oppure qualora non sia possibile ottenerne il consenso preventivo per mancanza di un indirizzo noto, ecc.;
6. laddove ciò sia necessario ai fini del conseguimento dell'interesse giustificabile di un titolare del trattamento delle informazioni personali, che è manifestamente superiore ai diritti dell'interessato. In tali casi il trattamento è consentito soltanto nella misura in cui è sostanzialmente correlato all'interesse giustificabile del titolare del trattamento delle informazioni personali e non va oltre una portata ragionevole.

Articolo 18 (Limitazione all'uso e fornitura di informazioni personali al di fuori della finalità prevista) 1) Un titolare del trattamento delle informazioni personali non utilizza informazioni personali al di fuori dell'ambito di applicazione di cui all'articolo 15, primo comma, e all'articolo 39-3, primo e secondo comma, né le fornisce a qualsiasi terza parte al di fuori dell'ambito di applicazione di cui all'articolo 17, primo e terzo comma.

2) In deroga al primo comma, laddove si applichi uno dei seguenti punti, un titolare del trattamento delle informazioni personali può utilizzare tali informazioni oppure fornirle a una terza parte per finalità diverse, fatto salvo il caso in cui procedere in tal senso possa violare ingiustamente l'interesse di un interessato o di una terza parte - considerando che i fornitori di servizi di informazione e comunicazione [come stabilito all'articolo 2, primo comma, punto 3, della legge sulla promozione dell'utilizzo di reti di informazione e comunicazione e della protezione dei dati in appresso si applicano le stesse disposizioni] che trattano le informazioni personali degli utenti [come stabilito all'articolo 2, primo comma, punto 4, della legge sulla promozione dell'utilizzo di reti di informazione e comunicazione e della protezione dei dati in appresso si applicano le stesse disposizioni] sono tenuti a rispettare soltanto i punti 1 e 2, mentre i punti da 5 a 9 sono applicabili soltanto agli enti pubblici:

1. laddove sia stato ottenuto il consenso aggiuntivo dall'interessato;
2. laddove esistano altre disposizioni speciali di legge;
3. laddove ciò sia ritenuto manifestamente necessario per la protezione della vita, dell'incolumità o degli interessi patrimoniali dell'interessato o di una terza parte rispetto a un pericolo imminente nel caso in cui l'interessato o il suo rappresentante legale non sia in grado di esprimere un'intenzione oppure qualora non sia possibile ottenerne il consenso preventivo per mancanza di un indirizzo noto;
4. soppresso; <mediante legge n. 16930, 4 febbraio 2020>
5. laddove non sia possibile svolgere i compiti rientranti nella rispettiva competenza giurisdizionale previsti in qualsiasi legge, fatto salvo il caso in cui il titolare del trattamento non utilizzi informazioni personali per altre finalità rispetto a quella prevista oppure le fornisca a una terza parte, e sia soggetto a deliberazione e risoluzione da parte della commissione;
6. laddove sia necessario fornire informazioni personali a un governo straniero o a un'organizzazione internazionale per dare esecuzione a un trattato o un'altra convenzione internazionale;
7. laddove ciò sia necessario ai fini di indagini in merito a un reato, un rinvio a giudizio o un'azione giudiziaria;
8. laddove ciò sia necessario per consentire a un organo giurisdizionale di adempiere i suoi compiti in relazione a un procedimento giudiziario;
9. laddove ciò sia necessario ai fini dell'esecuzione di una pena, della libertà vigilata o della custodia cautelare.

Terzo e quarto comma omessi.

5) Qualora fornisca informazioni personali a una terza parte per altre finalità rispetto a quella prevista in ciascuno dei casi di cui al secondo comma, un titolare del trattamento delle informazioni personali è tenuto a richiedere al destinatario delle informazioni personali di limitare la finalità e il metodo di utilizzo e altre questioni necessarie oppure a prevedere le garanzie necessarie al fine di assicurare la sicurezza delle informazioni personali. In tali casi, il soggetto che riceve tale richiesta è tenuto ad adottare le misure necessarie per assicurare la sicurezza delle informazioni personali.

i) Il primo e secondo comma dell'articolo 3 della legge sulla protezione delle informazioni personali prescrivono il principio secondo il quale un titolare del trattamento delle informazioni personali deve raccogliere soltanto le informazioni personali minime necessarie per adempiere la finalità del trattamento di informazioni personali in maniera lecita e legale e non dovrebbe utilizzarle per finalità diverse da quella prevista ([3]).

ii) Secondo tale principio, il primo comma dell'articolo 15 della legge sulla protezione delle informazioni personali prescrive che quando un titolare del trattamento delle informazioni personali raccoglie tali informazioni queste ultime possono essere utilizzate nel rispetto della finalità per la quale sono state raccolte, mentre il primo comma dell'articolo 18 prescrive che le informazioni personali non dovrebbero essere utilizzate al di fuori della finalità della loro raccolta o fornite a una terza parte.

([3]) Dato che tali disposizioni stabiliscono principi generali che si applicano a qualsiasi trattamento di informazioni personali, anche quando tale trattamento è specificamente disciplinato da altre leggi, i chiarimenti di cui alla presente sezione si applicano anche quando i dati personali vengono trattati sulla base di altre leggi (cfr. ad esempio articolo 15, primo comma, della legge sulle informazioni creditizie, che fa specificamente riferimento a tali disposizioni).

iii) Inoltre, anche se le informazioni personali possono essere utilizzate per finalità diverse da quella prevista o fornite a una terza parte nei casi eccezionali ([4]) di cui ai vari punti del secondo comma dell'articolo 18 della legge sulla protezione delle informazioni personali, occorre richiedere la limitazione della finalità o del metodo di utilizzo affinché le informazioni personali possano essere trattate in sicurezza conformemente al quinto comma oppure adottare misure necessarie per assicurare la sicurezza delle informazioni personali.

iv) Le disposizioni di cui sopra si applicano parimenti al trattamento di tutte le informazioni personali ricevute nel contesto della competenza giurisdizionale della Corea da un paese terzo, indipendentemente dalla nazionalità dell'interessato.

v) Se ad esempio un titolare del trattamento di dati personali nell'UE trasferisce informazioni personali a un titolare del trattamento delle informazioni personali coreano a norma della decisione di adeguatezza della Commissione europea, la finalità per la quale il titolare del trattamento di dati personali dell'UE trasferisce tali informazioni deve essere considerata dal titolare del trattamento delle informazioni personali coreano costituire la finalità per la raccolta di informazioni personali e in tali casi, quest'ultimo soggetto può utilizzare le informazioni personali o fornirle a una terza parte esclusivamente nel rispetto della finalità della raccolta, fatta eccezione per i casi eccezionali di cui all'articolo 18, secondo comma, della legge sulla protezione delle informazioni personali.

2. **Limitazione al trasferimento successivo di dati personali (articolo 17, terzo e quarto comma, e articolo 18 della legge sulla protezione delle informazioni personali)**

<Legge sulla protezione delle informazioni personali
(legge n. 16930, parzialmente modificata il 4 febbraio 2020)>

Articolo 17 (Fornitura di informazioni personali) 1) omesso.

2) Un titolare del trattamento delle informazioni personali informa un interessato in merito alle seguenti questioni quando ottiene il consenso ai sensi del primo comma, punto 1. Lo stesso vale in caso di modifica di uno qualsiasi dei seguenti aspetti:

1. il destinatario delle informazioni personali;
2. la finalità per la quale il destinatario delle informazioni personali utilizza tali informazioni;
3. dettagli in merito alle informazioni personali da fornire;
4. il periodo durante il quale il destinatario conserva e utilizza informazioni personali;
5. il fatto che l'interessato abbia il diritto di negare il consenso e gli svantaggi, se presenti, derivanti dalla negazione del consenso.

3) Un titolare del trattamento delle informazioni personali informa un soggetto in merito alle questioni di cui al punto 2 e ottiene il consenso da tale soggetto al fine di fornire informazioni personali a una terza parte all'estero; e non stipula un contratto per il trasferimento transfrontaliero delle informazioni personali in violazione alla presente legge.

4) Un titolare del trattamento delle informazioni personali può fornire informazioni personali senza il consenso di un interessato all'interno di un ambito di applicazione ragionevolmente connesso alle finalità per le quali tali informazioni sono state inizialmente raccolte, conformemente alle questioni prescritte dal decreto presidenziale tenendo conto dell'eventualità che possano essere causati svantaggi all'interessato, se sono state prese misure necessarie per assicurare la sicurezza, quali la cifratura, ecc.

※ Cfr. pagine 3, 4 e 5 per l'articolo 18.

<Decreto di applicazione della legge sulla protezione delle informazioni personali

([Data di entrata in vigore: 5 febbraio 2021] [Decreto presidenziale n. 30892, 4 agosto 2020, che modifica altri atti])>

Articolo 14-2 (Norme sull'uso aggiuntivo/sulla fornitura aggiuntiva di informazioni personali, ecc.)

1) Se un titolare del trattamento delle informazioni personali utilizza o fornisce informazioni personali (in appresso "uso o fornitura di informazioni personali") senza disporre del consenso dell'interessato conformemente all'articolo 15, terzo comma, della legge sulla protezione delle informazioni personali o all'articolo 17, quarto comma, della medesima legge, il titolare del trattamento delle informazioni personali è tenuto a considerare le seguenti questioni:

1. se tali attività sono ragionevolmente correlate alla finalità originale per la quale sono state raccolte le informazioni personali;
2. se l'uso aggiuntivo o la fornitura aggiuntiva di informazioni personali è un'attività prevedibile alla luce delle circostanze in cui le informazioni personali sono state raccolte e delle prassi di trattamento;
3. se l'uso aggiuntivo o la fornitura aggiuntiva di informazioni personali non viola ingiustamente gli interessi dell'interessato; e
4. se sono state adottate le misure necessarie per assicurare la sicurezza quali la pseudonimizzazione o la cifratura.

([4]) I fornitori di servizi di informazione e comunicazione sono soggetti soltanto all'applicazione dell'articolo 18, secondo comma, punti 1 e 2. I punti da 5 a 9 sono applicabili soltanto agli enti pubblici.

2) Il titolare del trattamento delle informazioni personali divulga preventivamente i criteri per la valutazione delle questioni di cui ai punti del primo comma nella propria politica in materia di tutela della vita privata ai sensi dell'articolo 30, primo comma, della legge sulla protezione delle informazioni personali, e il responsabile della tutela della vita privata ai sensi dell'articolo 31, primo comma, della medesima legge deve verificare se il titolare del trattamento delle informazioni personali utilizza o fornisce informazioni personali aggiuntive in maniera conforme alle norme pertinenti.

i) Se il titolare del trattamento delle informazioni personali fornisce informazioni personali a una terza parte all'estero, deve informare gli interessati preventivamente in merito a tutte le questioni di cui all'articolo 17, secondo comma, della legge sulla protezione delle informazioni personali e ottenerne il consenso, fatta eccezione per i casi di cui al primo 1 o al punto 2. Non si dovrebbe stipulare alcun contratto in merito alla fornitura transfrontaliera di dati personali in violazione della presente legge.

(1) Qualora le informazioni personali siano fornite all'interno di un ambito di applicazione ragionevolmente correlato alla finalità iniziale della raccolta ai sensi dell'articolo 17, quarto comma, della legge sulla protezione delle informazioni personali. Tuttavia i casi a cui la presente disposizione può essere applicata sono limitati a quelli in cui sono soddisfatte le norme per l'uso aggiuntivo e la fornitura aggiuntiva di informazioni personali, di cui all'articolo 14-2 del decreto di applicazione. Inoltre, il titolare del trattamento delle informazioni personali deve considerare se la fornitura di tali informazioni può causare svantaggi agli interessati e se ha adottato misure necessarie per assicurare la sicurezza, quali la cifratura;

(2) se le informazioni personali possono essere fornite a terzi nei casi eccezionali di cui all'articolo 18, secondo comma, della legge sulla protezione delle informazioni personali (cfr. pagine 3~5). Tuttavia, anche in tali casi, qualora sia probabile che la fornitura di tali informazioni personali violi ingiustamente gli interessi dell'interessato o di una terza parte, le informazioni personali non possono essere fornite a terzi. Inoltre il fornitore di informazioni personali deve richiedere al destinatario delle informazioni personali di limitare la finalità o il metodo di utilizzo delle informazioni personali oppure adottare misure necessarie per assicurare la sicurezza di tali informazioni affinché possano essere trattate in maniera sicura.

ii) Se le informazioni personali sono fornite a una terza parte all'estero, potrebbero non ricevere il livello di protezione assicurato dalla legge sulla protezione delle informazioni personali della Corea in ragione di differenze nei sistemi di protezione delle informazioni personali di diversi paesi. Di conseguenza tali casi saranno considerati come "casi nei quali è possibile causare svantaggi all'interessato" di cui all'articolo 17, quarto comma, dalla legge sulla protezione delle informazioni personali o i "casi in cui l'interesse di un interessato o di una terza parte viene violato ingiustamente" di cui all'articolo 18, secondo comma, della medesima legge e all'articolo 14-2 del decreto di applicazione di tale legge ([5]). Al fine di soddisfare i requisiti di cui a tali disposizioni, il titolare del trattamento delle informazioni personali e la terza parte devono pertanto garantire esplicitamente un livello di protezione equivalente a quello sancito dalla legge sulla protezione delle informazioni personali, compresa la garanzia dell'esercizio da parte dell'interessato dei suoi diritti nel contesto di documenti legalmente vincolanti quali contratti, anche dopo che le informazioni personali vengono trasferite all'estero.

3. **Notifica relativa ai dati qualora i dati personali non siano stati ottenuti dall'interessato (articolo 20 della legge sulla protezione delle informazioni personali)**

<Legge sulla protezione delle informazioni personali

(legge n. 16930, parzialmente modificata il 4 febbraio 2020)>

Articolo 20 (notifica sulle fonti, ecc. di informazioni personali raccolte da terzi) 1) Quando un titolare del trattamento delle informazioni personali elabora informazioni personali raccolte da terze parti, il titolare del trattamento delle informazioni personali notifica immediatamente all'interessato, su richiesta di quest'ultimo, le questioni che seguono:

1. la fonte delle informazioni personali raccolte;
2. la finalità delle informazioni personali trattate;
3. il fatto che l'interessato abbia diritto a chiedere la sospensione del trattamento delle informazioni personali, come prescritto all'articolo 37.

2) In deroga al primo comma, quando un titolare del trattamento delle informazioni personali che soddisfi i criteri prescritti dal decreto presidenziale tenendo conto dei tipi e della quantità di informazioni personali trattate, del numero di dipendenti, della quantità di vendite, ecc., raccoglie informazioni personali da terzi e le tratta a norma dell'articolo 17, primo comma, detto titolare del trattamento delle informazioni personali notifica agli interessati le questioni di cui al primo comma. Tale disposizione non si applica se le informazioni raccolte dal titolare del trattamento delle informazioni personali non contengono alcuna informazione personale, quali informazioni di contatto, tramite le quali è possibile inviare notifiche all'interessato.

([5]) Ai sensi dell'articolo 18, secondo comma, punto 2, della legge sulla protezione delle informazioni personali, ciò si applica anche quando le informazioni personali sono divulgate a terze parti all'estero sulla base di disposizioni contenute in altri atti (come ad esempio la legge sulle informazioni creditizie).

3) Le questioni necessarie in relazione a tempi, metodi e procedure per la notifica all'interessato, ai sensi della frase principale di cui al secondo comma, sono prescritte dal decreto presidenziale.

4) Il primo comma e la frase principale del secondo comma non si applicano ad alcuna delle seguenti circostanze (ciò si applica comunque soltanto qualora prevalga in maniera manifesta sui diritti degli interessati ai sensi della presente legge):

1. laddove le informazioni personali, soggette a una richiesta di notifica, sono incluse nei fascicoli di informazioni personali indicati in uno qualsiasi dei punti di cui all'articolo 32, secondo comma;
2. laddove tale notifica possa causare danni alla vita o all'incolumità di qualsiasi altra persona oppure leda ingiustamente gli interessi patrimoniali e di altra natura di qualsiasi altra persona.

(i) Se riceve informazioni personali trasferite dall'UE ai sensi della decisione di adeguatezza di quest'ultima ([6]), il titolare del trattamento delle informazioni personali deve notificare le informazioni che seguono ai punti da 1 a 5 all'interessato senza indebito ritardo e in ogni caso non oltre un mese dal trasferimento.

(1) il nome e le informazioni di contatto delle persone che trasferiscono e ricevono le informazioni personali;

(2) le tipologie o le categorie di informazioni personali trasferite;

(3) la finalità della raccolta e dell'uso delle informazioni personali (come stabilito dall'esportatore di dati ai sensi del punto 1 della presente notifica);

(4) il periodo di conservazione delle informazioni personali;

(5) informazioni sui diritti dell'interessato in merito al trattamento delle informazioni personali, al metodo e alla procedura per l'esercizio dei diritti nonché agli eventuali svantaggi laddove tale esercizio ne crei.

(ii) Inoltre, qualora fornisca le informazioni personali di cui al punto i) a una terza parte nella Repubblica di Corea o all'estero, il titolare del trattamento delle informazioni personali deve notificare le informazioni di cui ai punti da 1 a 5 all'interessato prima della fornitura delle informazioni personali.

(1) il nome e le informazioni di contatto delle persone che forniscono e ricevono le informazioni personali;

(2) le tipologie o le categorie di informazioni personali fornite;

(3) il paese al quale devono essere fornite le informazioni personali, la data e le modalità previste per la fornitura (limitatamente ai casi in cui le informazioni personali devono essere fornite ad una terza parte all'estero);

(4) la finalità del fornitore di informazioni personali e la base giuridica della fornitura di tali informazioni;

(5) informazioni sui diritti dell'interessato in merito al trattamento delle informazioni personali, al metodo e alla procedura per l'esercizio dei diritti nonché agli eventuali svantaggi laddove tale esercizio ne crei.

(iii) Il titolare del trattamento delle informazioni personali potrebbe non applicare il punto i) o ii) in alcuno dei seguenti casi da 1 a 4.

(1) Se le informazioni personali che devono essere comunicate sono incluse in uno dei seguenti fascicoli di informazioni personali di cui all'articolo 32, secondo comma, della legge sulla protezione delle informazioni personali, nella misura in cui gli interessi tutelati da tale disposizione sono manifestamente superiori ai diritti dell'interessato e soltanto fintantoché la notifica minacci il perseguimento degli interessi in gioco, ad esempio mettendo a rischio indagini penali in corso o minacciando la sicurezza nazionale;

(2) se e fintantoché la notifica può minacciare la vita o ledere l'incolumità di un'altra persona o violare ingiustamente gli interessi patrimoniali di un'altra persona, laddove tali diritti o interessi prevalgano manifestamente sui diritti dell'interessato;

(3) se l'interessato possiede già le informazioni che il titolare del trattamento delle informazioni personali deve notificare ai sensi del punto i) o ii);

(4) se il titolare del trattamento delle informazioni personali non dispone di informazioni di contatto dell'interessato o se contattare l'interessato comporta sforzi eccessivi, anche nel contesto del trattamento nel rispetto delle condizioni di cui alla sezione 3 della legge sulla protezione delle informazioni personali. Ai fini della determinazione della possibilità o meno di contattare l'interessato o dell'eventualità che ciò implichi o meno sforzi eccessivi, è opportuno prendere in considerazione la possibilità di cooperare con l'esportatore di dati nell'UE.

([6]) Gli obblighi di cui ai punti i), ii) e iii) si applicano parimenti quando il titolare del trattamento che riceve informazioni personali dall'UE ai sensi della decisione di adeguatezza tratta tali informazioni sulla base di altri atti, come ad esempio la legge sulle informazioni creditizie.

4. **Ambito di applicazione dell'esenzione speciale al trattamento di informazioni pseudonimizzate (articoli 28-2, 28-3, 28-4, 28-5, 28-6 e 28-7, articolo 3 e articolo 58-2 della legge sulla protezione delle informazioni personali)**

<Legge sulla protezione delle informazioni personali

(legge n. 16930, parzialmente modificata il 4 febbraio 2020)>

Capo III Trattamento di informazioni personali

SEZIONE 3 Casi speciali concernenti dati pseudonimizzati

Articolo 28-2 (trattamento di dati pseudonimizzati) 1) Un titolare del trattamento delle informazioni personali può trattare informazioni pseudonimizzate senza il consenso degli interessati per finalità statistiche, di ricerca scientifica e di archiviazione nell'interesse pubblico, ecc.

2) Un titolare del trattamento delle informazioni personali non include informazioni che possono essere utilizzate per identificare una determinata persona fisica quando si forniscono informazioni pseudonimizzate a una terza parte ai sensi del primo comma.

Articolo 28-3 (Limitazione della combinazione di dati pseudonimizzati) 1) In deroga all'articolo 28-2, la combinazione di informazioni pseudonimizzate trattate da titolari diversi del trattamento di informazioni personali per finalità statistiche, di ricerca scientifica e conservazione di registri nell'interesse pubblico, ecc. deve essere condotta da un'istituzione specializzata designata dalla commissione per la protezione o dal capo dell'agenzia amministrativa centrale correlata.

2) Un titolare del trattamento delle informazioni personali che intende rilasciare le informazioni combinate al di fuori dell'organizzazione che ha combinato le informazioni deve ottenere l'approvazione a procedere in tal senso dal capo dell'istituzione specializzata dopo aver trattato le informazioni trasformandole in informazioni pseudonimizzate o nella forma di cui all'articolo 58-2.

3) Le questioni necessarie comprese le procedure e i metodi di combinazione ai sensi del primo comma, le norme e le procedure per designare o annullare la designazione di un'istituzione specializzata, nonché per la gestione e il controllo, così come le norme e le procedure per l'esportazione e l'approvazione ai sensi del secondo comma sono prescritte mediante decreto presidenziale.

Articolo 28-4 (Obbligo di adozione di misure di sicurezza per i dati pseudonimizzati) 1) Durante il trattamento di informazioni pseudonimizzate, un titolare del trattamento delle informazioni personali adotta misure tecniche, organizzative e fisiche quali la conservazione e la gestione separata di ulteriori informazioni necessarie per il ripristino allo stato originale, nella misura necessaria per assicurare la sicurezza come prescritto dal decreto presidenziale affinché le informazioni personali non possano andare perse, venire rubate, divulgate, falsificate, alterate o danneggiate.

2) Ai fini della gestione del trattamento di informazioni pseudonimizzate un titolare del trattamento delle informazioni personali che intende trattare tali informazioni si prepara e conserva registri relativi a questioni prescritte mediante decreto presidenziale, compresa la finalità del trattamento di tali informazioni e l'identificazione di un destinatario terzo quando tali informazioni sono oggetto di fornitura.

Articolo 28-5 (Atti vietati per il trattamento di informazioni pseudonimizzate) 1) Nessun soggetto può trattare informazioni pseudonimizzate con la finalità di identificare una determinata persona fisica.

2) Qualora vengano generate informazioni che identificano una determinata persona fisica mentre vengono trattate informazioni pseudonimizzate, il titolare del trattamento delle informazioni personali cessa di trattare tali informazioni e recupera e distrugge immediatamente le informazioni in questione.

Articolo 28-6 (Imposizione di maggiorazioni amministrative per il trattamento di informazioni pseudonimizzate) 1) La commissione può irrogare una sanzione pecuniaria inferiore al 3 % delle vendite totali al titolare del trattamento dei dati che abbia trattato dati con la finalità di identificare una persona fisica specifica in violazione dell'articolo 28-5, primo comma: in assenza di vendite o qualora si rilevino difficoltà nel calcolo delle entrate generate dalle vendite, al titolare del trattamento dei dati può essere irrogata una sanzione pecuniaria non superiore a 400 milioni di KRW o al 3 % dell'importo del capitale, a seconda di quale dei due importi sia superiore.

2) L'articolo 34-2, dal terzo al quinto comma, si applica mutatis mutandis a questioni necessarie per l'imposizione e la riscossione di maggiorazioni amministrative.

Articolo 28-7 (ambito di applicazione) Gli articoli 20, 21 e 27, l'articolo 34, primo comma, gli articoli da 35 a 37, gli articoli 39-3 e 39-4 e gli articoli da 39-6 a 39-8 non si applicano alle informazioni pseudonimizzate.

Capo I Disposizioni generali

Articolo 3 (Principi per la protezione delle informazioni personali) 1) Il titolare del trattamento delle informazioni personali specifica esplicitamente le finalità per le quali le informazioni personali vengono trattate; e raccoglie informazioni personali in maniera lecita e corretta, nella misura minima necessaria per il conseguimento di tali finalità.

2) Il titolare del trattamento delle informazioni personali tratta le informazioni personali in maniera appropriata a quanto necessario per le finalità per le quali tali informazioni personali vengono trattate e non le utilizza in maniera diversa da tali finalità.

3) Il titolare del trattamento delle informazioni personali garantisce che tali informazioni siano esatte, complete e aggiornate nella misura necessaria in relazione alle finalità per le quali dette informazioni vengono trattate.

4) Il titolare del trattamento delle informazioni personali gestisce tali informazioni in maniera sicura secondo i metodi, le tipologie, ecc. di trattamento delle informazioni personali, tenendo conto della possibilità di violazione dei diritti dell'interessato e della gravità dei rischi pertinenti.

5) Il titolare del trattamento delle informazioni personali rende pubblica la propria politica in materia di tutela della vita privata nonché altre questioni relative al trattamento delle informazioni personali; garantisce altresì il rispetto dei diritti dell'interessato, come quello di accesso alle informazioni personali relative alla sua persona.

6) Il titolare del trattamento delle informazioni personali tratta tali informazioni in maniera tale da ridurre al minimo la possibilità di violare la vita privata di un interessato.

7) Qualora sia comunque possibile soddisfare le finalità della raccolta di informazioni personali trattando informazioni personali anonimamente o pseudonimizzate, il titolare del trattamento delle informazioni personali si sforza di trattare tali informazioni ricorrendo all'anonimizzazione, laddove possibile, oppure attraverso la pseudonimizzazione, qualora sia impossibile soddisfare le finalità della raccolta di informazioni personali attraverso l'anonimizzazione.

8) Il titolare del trattamento delle informazioni personali si sforza di ottenere la fiducia degli interessati rispettando e dando esecuzione agli obblighi e alle responsabilità sanciti dalla presente legge e in altre leggi correlate.

Capo IX Disposizioni supplementari

Articolo 58-2 (Esenzione dall'applicazione) La presente legge non si applica alle informazioni che non identificano più una determinata persona fisica se combinate con altre informazioni, considerando ragionevolmente i tempi, i costi, la tecnologia, ecc. <Questo articolo è stato inserito di recente con la legge n. 16930, 4 febbraio 2020>

i) Il capo III, sezione 3 Casi speciali concernenti dati pseudonimizzati (articoli da 28-2 a 28-7) consente il trattamento delle informazioni pseudonimizzate senza il consenso dell'interessato per finalità di compilazione di statistiche, di ricerca scientifica, di conservazione dei registri pubblici, ecc. (articolo 28-2), ma in tali casi sono obbligatori garanzie e divieti adeguati necessari per la protezione degli interessati (articoli 28-4 e 28-5), possono essere imposte maggiorazioni di sanzioni ai violatori (articolo 28-6) e non si applicano determinate garanzie altrimenti disponibili ai sensi della legge sulla protezione delle informazioni personali (articolo 28-7).

ii) Tali disposizioni non si applicano ai casi in cui le informazioni pseudonimizzate sono trattate per finalità diverse dalla compilazione di statistiche, dalla ricerca scientifica, dalla conservazione di registri pubblici, ecc. Ad esempio, se le informazioni personali di una persona fisica dell'UE, che sono state trasferite in Corea ai sensi della decisione di adeguatezza della Commissione europea, vengono pseudonimizzate per finalità diverse dalla compilazione di statistiche, della ricerca scientifica, della conservazione di registri pubblici, ecc., non si applicano le disposizioni speciali di cui al capo III, sezione 3 ([7]).

iii) Laddove un titolare del trattamento delle informazioni personali tratti informazioni pseudonimizzate per finalità di compilazione die statistiche, ricerca scientifica, conservazione di registri pubblici, ecc. e se le informazioni pseudonimizzate non sono state distrutte in seguito all'adempimento della finalità specifica del trattamento in linea con l'articolo 37 della costituzione e l'articolo 3 (Principi per la protezione delle informazioni personali) della legge sulla protezione delle informazioni personali, tale titolare è tenuto ad anonimizzare le informazioni al fine di garantire che non identifichino più una persona fisica specifica, da sole o se combinate con altre informazioni, considerando in maniera ragionevole i tempi, i costi, le tecnologie, ecc., conformemente all'articolo 58-2 della legge sulla protezione delle informazioni personali.

5. **Misure correttive, ecc. (articolo 64, primo, secondo e quarto comma, della legge sulla protezione delle informazioni personali)**

<Legge sulla protezione delle informazioni personali

(legge n. 16930, parzialmente modificata il 4 febbraio 2020)>

Articolo 64 (Misure correttive) 1) Laddove ritenga che vi sia un motivo sostanziale per ritenere che vi sia stata una violazione rispetto alle informazioni personali e un'inazione potrebbe causare danni a cui è difficile porre rimedio, la commissione per la protezione può ordinare al soggetto che ha violato la presente legge (escluse le agenzie amministrative centrali, le amministrazioni locali, l'Assemblea nazionale, un organo giurisdizionale, la Corte costituzionale e la commissione elettorale nazionale) di adottare una delle seguenti misure:

1. sospendere la violazione rispetto alle informazioni personali;

2. sospendere temporaneamente il trattamento di informazioni personali;

([7]) Analogamente l'eccezione di cui all'articolo 40-3 della legge sulle informazioni creditizie si applica soltanto al trattamento di informazioni creditizie pseudonimizzate per finalità di compilazione di statistiche, di ricerca scientifica e di conservazione di registri pubblici.

3. altre misure necessarie per proteggere le informazioni personali e per prevenire una loro violazione.

2) Quando è del parere che vi sia un motivo sostanziale per ritenere che vi sia stata una violazione delle informazioni personali e un'inazione potrebbe causare danni ai quali è difficile porre rimedio, a norma della legge corrispondente, il capo di un'agenzia amministrativa centrale correlata può ordinare a un titolare del trattamento delle informazioni personali, soggetto alla competenza giurisdizionale di tale agenzia, di adottare una delle misure di cui al primo comma.

4) Quando un'agenzia amministrativa centrale, un'amministrazione locale, l'Assemblea nazionale, un organo giurisdizionale, la Corte costituzionale o la commissione elettorale nazionale viola la presente legge, la commissione per la protezione può raccomandare al capo dell'agenzia pertinente di adottare una delle misure di cui al primo comma. In tali casi, dopo aver ricevuto la raccomandazione, detta agenzia si conforma alla stesse fatto salvo il caso in cui sussistano circostanze straordinarie.

i) Innanzitutto la giurisprudenza ([8]) ([9]) interpreta un "danno a cui è difficile porre rimedio" come una circostanza che potrebbe ledere i diritti personali o la tutela della vita privata di una persona fisica.

ii) Di conseguenza il "motivo sostanziale per ritenere che vi sia stata una violazione rispetto alle informazioni personali e un'inazione potrebbe causare danni a cui è difficile porre rimedio" di cui al primo e secondo comma dell'articolo 64 fa riferimento ai casi in cui si ritiene che una violazione della legge possa violare i diritti e la libertà di persone fisiche per quanto concerne le informazioni personali. Ciò sarà applicabile ad ogni violazione di uno qualsiasi dei principi, dei diritti e dei doveri, di cui alla legge sulla protezione delle informazioni personali ([10]).

iii) Conformemente al quarto comma dell'articolo 64 della legge sulla protezione delle informazioni personali si tratta di una misura in merito a "una violazione della presente legge", ossia un'azione contro una violazione della legge sulla protezione delle informazioni personali.

Un'agenzia amministrativa centrale, ecc., in qualità di autorità pubblica vincolata al rispetto dello Stato di diritto, non può violare alcuna legge ed è tenuta ad adottare una misura correttiva, anche per fermare immediatamente l'azione e compensare i danni nel caso eccezionale in cui sia stato comunque commesso un atto illegale.

Di conseguenza, anche senza alcun intervento della commissione per la protezione conformemente al quarto comma dell'articolo 64 della legge sulla protezione delle informazioni personali, un'agenzia amministrativa centrale ecc. deve adottare una misura correttiva contro eventuali violazioni qualora venga a conoscenza di qualsiasi violazione della legge.

In particolare, laddove la commissione per la protezione abbia raccomandato una misura correttiva, di norma sarà oggettivamente evidente per l'agenzia amministrativa centrale, ecc. che ha violato la legge. Di conseguenza, al fine di giustificare il motivo per cui ritiene che una raccomandazione formulata dalla commissione per la protezione non dovrebbe essere seguita, un'agenzia amministrativa centrale, ecc. deve addurre motivi chiari capaci di dimostrare che non ha violato la legge. La raccomandazione deve essere seguita fatto salvo il caso in cui la commissione per la protezione stabilisca che tale circostanza non sia constatata.

In considerazione di ciò, le "circostanze straordinarie" di cui all'articolo 64, quarto comma, della legge sulla protezione delle informazioni personali devono essere strettamente limitate a circostanze straordinarie nelle quali sussistano motivi evidenti che le agenzie amministrative centrali ecc. possono addurre per dimostrare che "la presente legge non è stata di fatto violata" come avviene nei "casi in cui vi sono circostanze straordinarie (fattuali o giuridiche)" non note alla commissione per la protezione nel momento in cui ha formulato inizialmente la propria raccomandazione e detta commissione constata che non si è in effetti verificata alcuna violazione.

6. **Applicazione della legge sulla protezione delle informazioni personali al trattamento di dati personali per finalità di sicurezza nazionale, compresa l'indagine in merito a infrazioni e le attività di contrasto in conformità con la legge sulla protezione delle informazioni personali (articoli 7-8, 7-9, 58, 3, 4 e 62 della legge sulla protezione delle informazioni personali)**

<Legge sulla protezione delle informazioni personali

(legge n. 16930, parzialmente modificata il 4 febbraio 2020)>

Articolo 7-8 (Lavoro della commissione per la protezione) 1) La commissione per la protezione deve svolgere le seguenti attività: […]

3. gestire questioni riguardanti l'indagine in merito a violazioni dei diritti degli interessati e le disposizioni derivanti;

4. gestire i reclami o le procedure di riparazione relative al trattamento delle informazioni personali, nonché la mediazione delle controversie in materia di informazioni personali;

[…]

([8]) (Sentenza della Corte suprema 97Da10215,10222 del 26 gennaio 1999). Se i fatti criminali attribuiti all'imputato sono stati divulgati attraverso i mezzi di stampa, è probabile che ciò causi danni mentali e fisici irreparabili non soltanto alla vittima, ossia la parte attrice, ma anche alle persone intorno a lei, comprese le famiglie.

([9]) (Sentenza della *Seoul High Court* (Alta Corte di Seoul) 2006Na92006 del 16 gennaio 2008) Se è pubblicato un articolo diffamatorio, è probabile che provochi gravi danni irreparabili alla persona coinvolta.

([10]) I medesimi principi di cui al punto ii) si applicano all'articolo 45-4 della legge sulle informazioni creditizie.

Articolo 7-9 (Questioni soggette a deliberazione e risoluzione da parte della commissione per la protezione) 1) La commissione per la protezione delibera e risolve le seguenti questioni: […]

5. questioni relative all'interpretazione e al funzionamento della legge in relazione alla protezione delle informazioni personali;

[…]

Articolo 58 (Esclusione parziale dell'applicazione) 1) I capi da III a VII non si applicano ad alcuna delle seguenti informazioni personali:

1. informazioni personali raccolte ai sensi della legge sulla statistica per il trattamento da parte di enti pubblici;
2. informazioni personali raccolte o la cui fornitura è richiesta per l'analisi delle informazioni in relazione alla sicurezza nazionale;
3. informazioni personali trattate temporaneamente laddove siano urgentemente necessarie per la sicurezza pubblica, la salute pubblica, ecc.;
4. informazioni personali raccolte o utilizzate rispettivamente per finalità proprie di segnalazione da parte di organi di stampa, attività missionarie da parte di organizzazioni religiose e la nomina di candidati da parte di partiti politici.

[Secondo e terzo comma omessi].

4) In caso di trattamento di informazioni personali ai sensi del primo comma, un titolare del trattamento delle informazioni personali tratta le informazioni personali nella misura minima necessaria ai fini del conseguimento della finalità prevista per il periodo minimo di tempo; prevede inoltre disposizioni necessarie, quali garanzie tecniche, gestionali e fisiche, la gestione di reclami individuali e altre misure necessarie per la gestione sicura e un trattamento adeguato di tali informazioni personali.

Articolo 3 (Principi per la protezione delle informazioni personali) 1) Il titolare del trattamento delle informazioni personali specifica esplicitamente le finalità per le quali le informazioni personali vengono trattate; e raccoglie informazioni personali in maniera lecita e corretta, nella misura minima necessaria per il conseguimento di tali finalità.

2) Il titolare del trattamento delle informazioni personali tratta le informazioni personali in maniera appropriata a quanto necessario per le finalità per le quali tali informazioni personali vengono trattate e non le utilizza in maniera diversa da tali finalità.

3) Il titolare del trattamento delle informazioni personali garantisce che tali informazioni siano esatte, complete e aggiornate nella misura necessaria in relazione alle finalità per le quali dette informazioni vengono trattate.

4) Il titolare del trattamento delle informazioni personali gestisce tali informazioni in maniera sicura secondo i metodi, le tipologie, ecc. di trattamento delle informazioni personali, tenendo conto della possibilità di violazione dei diritti dell'interessato e della gravità dei rischi pertinenti.

5) Il titolare del trattamento delle informazioni personali rende pubblica la propria politica in materia di tutela della vita privata nonché altre questioni relative al trattamento delle informazioni personali; garantisce altresì il rispetto dei diritti dell'interessato, come quello di accesso alle informazioni personali relative alla sua persona.

6) Il titolare del trattamento delle informazioni personali tratta tali informazioni in maniera tale da ridurre al minimo la possibilità di violare la vita privata di un interessato.

7) Qualora sia comunque possibile soddisfare le finalità della raccolta di informazioni personali trattando informazioni personali anonimamente o pseudonimizzate, il titolare del trattamento delle informazioni personali si sforza di trattare tali informazioni ricorrendo all'anonimizzazione, laddove possibile, oppure attraverso la pseudonimizzazione, qualora sia impossibile soddisfare le finalità della raccolta di informazioni personali attraverso l'anonimizzazione.

8) Il titolare del trattamento delle informazioni personali si sforza di ottenere la fiducia degli interessati rispettando e dando esecuzione agli obblighi e alle responsabilità sanciti dalla presente legge e in altre leggi correlate.

Articolo 4 (Diritti degli interessati) Un interessato dispone dei seguenti diritti in relazione al trattamento delle proprie informazioni personali:

1. il diritto di essere informati in merito al trattamento di tali informazioni personali;
2. il diritto di stabilire se prestare o meno il consenso nonché la portata del consenso riguardante il trattamento di tali informazioni personali;
3. il diritto di confermare se le informazioni personali siano state trattate e di richiedere l'accesso (anche tramite la fornitura di copie; in appresso si applica lo stesso) a tali informazioni personali;
4. il diritto di sospendere il trattamento e di richiedere la correzione, la cancellazione e la distruzione di tali informazioni personali;
5. il diritto ad un risarcimento adeguato per eventuali danni derivanti dal trattamento di tali informazioni personali, attraverso una procedura rapida ed equa.

Articolo 62 (Segnalazione di violazioni) 1) Chiunque subisca una violazione di diritti o interessi in relazione alle proprie informazioni personali nel corso del trattamento delle informazioni personali da parte di un titolare del trattamento delle informazioni personali può segnalare tale violazione alla commissione per la protezione.

2) La commissione per la protezione può designare un'istituzione specializzata affinché riceva e gestisca in maniera efficiente le segnalazioni di reclami ai sensi del primo comma, come prescritto dal decreto presidenziale. In tali casi, detta istituzione specializzata istituisce e gestisce un call centre per le violazioni di informazioni personali (in appresso: "call centre per la tutela della vita privata").

3) Il call centre per la tutela della vita privata assolve i seguenti compiti:

1. ricezione di segnalazioni di reclami ed erogazione di consulenza in relazione al trattamento delle informazioni personali;
2. indagine in merito a incidenti e loro conferma, nonché esame dei pareri delle parti correlate;
3. doveri incidentali in relazione al primo e secondo comma.

4) Se necessario, la commissione per la protezione può inviare un suo funzionario pubblico presso l'istituzione specializzata, designato ai sensi secondo comma dell'articolo 32-4 della legge sui funzionari pubblici statali, affinché indaghi in maniera efficace e confermi gli incidenti ai sensi del terzo comma, punto 2.

i) La raccolta di informazioni personali per finalità di sicurezza nazionale è disciplinata da leggi specifiche che autorizzano le autorità competenti (ad esempio il servizio di intelligence nazionale) ad intercettare le comunicazioni o richiedere la divulgazione nel rispetto di determinate condizioni e garanzie (in appresso: "leggi in materia di sicurezza nazionale"). Tali leggi in materia di sicurezza nazionale comprendono ad esempio la legge sulla tutela della vita privata nelle comunicazioni, la legge antiterrorismo per la protezione dei cittadini e della sicurezza pubblica oppure la legge sulle imprese di telecomunicazione. Inoltre la raccolta e l'ulteriore trattamento di informazioni personali devono essere conformi ai requisiti della legge sulla protezione delle informazioni personali. A questo proposito, l'articolo 58, primo comma, punto 2, della legge sulla protezione delle informazioni personali prevede che i capi da III a VII non si applichino alle informazioni personali raccolte o la cui fornitura è necessaria per l'analisi di informazioni relative alla sicurezza nazionale. Tale eccezione parziale si applica quindi al trattamento di informazioni personali per finalità di sicurezza nazionale.

Allo stesso tempo il capo I (Disposizioni generali), il capo II (Istituzione di politiche in materia di protezione delle informazioni personali, ecc.), il capo VIII (Azione collettiva risarcitoria in relazione a una violazione dei dati), il capo IX (Disposizioni supplementari) e il capo X (Disposizioni in merito alle sanzioni) della legge sulla protezione delle informazioni personali si applicano al trattamento di tali informazioni personali. Rientrano in tale contesto i principi generali di protezione dei dati di cui all'articolo 3 (Principi per la protezione delle informazioni personali) e dei diritti individuali garantiti dall'articolo 4 della legge sulla protezione delle informazioni personali (Diritti degli interessati).

Inoltre l'articolo 58, quarto comma, della legge sulla protezione delle informazioni personali prevede che tali informazioni debbano essere trattate nella misura minima necessaria per il conseguimento della finalità prevista e per il periodo minimo necessario; impone altresì al titolare del trattamento delle informazioni personali di mettere in atto misure necessarie per assicurare una gestione sicura dei dati e un trattamento adeguato, quali garanzie tecniche, gestionali e fisiche, nonché misure per la gestione adeguata di singoli reclami.

Infine si applicano le disposizioni che disciplinano i compiti e i poteri della PIPC (compreso l'articolo 60-65 della legge sulla protezione delle informazioni personali sulla gestione dei reclami e l'adozione di raccomandazioni e misure correttive) nonché le disposizioni sulle sanzioni amministrative e penali (articolo 70 e successivi della legge sulla protezione delle informazioni personali). Ai sensi dell'articolo 7-8, primo comma, punti 3 e 4, e dell'articolo 7-9, primo comma, punto 5, della legge sulla protezione delle informazioni personali, tali poteri investigativi e correttivi, anche se esercitati nel contesto della gestione di reclami, riguardano anche possibili violazioni delle norme contenute in leggi specifiche che stabiliscono limitazioni e garanzie rispetto alla raccolta di informazioni personali, quali le leggi in materia di sicurezza nazionale. Dati i requisiti di cui all'articolo 3, primo comma, della legge sulla protezione delle informazioni personali per la raccolta lecita ed equa di tali informazioni, tale violazione costituisce una violazione della "presente legge" ai sensi degli articoli 63 e 64 che consente alla PIPC di svolgere un'indagine e adottare misure correttive ([11]). L'esercizio di tali poteri da parte della PIPC integra ma non sostituisce i poteri della *National Human Rights Commission* (NHRC, commissione nazionale per i diritti umani) di cui alla legge relativa a tale commissione. L'applicazione dei principi, dei diritti e degli obblighi principali della legge sulla protezione delle informazioni personali al trattamento di informazioni personali per finalità di sicurezza nazionale riflette le garanzie sancite nella costituzione a sostegno della protezione del diritto individuale di controllare le proprie informazioni personali. Come riconosciuto dalla Corte costituzionale rientra in tale contesto anche il diritto di una persona fisica ([12]) di "decidere personalmente quando, a chi o da chi, e in che misura le sue informazioni saranno divulgate o utilizzate. Si tratta di un diritto fondamentale ([13]), […], che esiste per proteggere la libertà personale di decisione in relazione al rischio causato dall'ampliamento delle funzioni statali e della tecnologia in materia di informazione e comunicazione". Qualsiasi limitazione a tale diritto, ad esempio se necessaria ai fini della protezione della sicurezza nazionale, richiede la definizione di un equilibrio tra i diritti e gli interessi della persona fisica e l'interesse pubblico pertinente e non può incidere sull'essenza del diritto (articolo 37, secondo comma, della costituzione).

([11]) Per quanto concerne le misure correttive ai sensi dell'articolo 64, cfr. anche la sezione 5.
([12]) Sentenza della Corte costituzionale, 99HunMa513, 2004HunMa190, 26 maggio 2005.
([13]) Sentenza della Corte costituzionale, 2003HunMa282, 21 luglio 2005.

Di conseguenza, quando tratta informazioni personali per finalità di sicurezza nazionale, il titolare del trattamento (ad esempio il *National Intelligence Service*, NIS, ossia il servizio di intelligence nazionale) tra l'altro:

1) specifica esplicitamente le finalità per le quali vengono trattate e raccolte le informazioni personali in maniera lecita ed equa nella misura minima necessaria per il conseguimento di tali finalità (articolo 3, primo comma, della legge sulla protezione delle informazioni personali); in particolare, tale soggetto raccoglie e tratta ulteriormente le informazioni personali soltanto al fine di assolvere i propri doveri ai sensi delle normative pertinenti come nel caso della legge sui servizi di intelligence nazionale;

2) tratta le informazioni personali nella misura minima e per il periodo minimo, necessari per il conseguimento della finalità prevista (articolo 58, quarto comma, della legge sulla protezione delle informazioni personali); una volta conseguita la finalità del trattamento, il titolare del trattamento deve distruggere in maniera irreversibile le informazioni personali, fatto salvo il caso in cui una conservazione ulteriore sia imposta specificamente per legge, nel qual caso le informazioni personali pertinenti devono essere conservate e gestite separatamente da altre informazioni personali, non essere utilizzate per alcuna finalità diversa da quella specificata nella legge ed essere distrutte al termine del periodo di conservazione;

3) tratta le informazioni personali in maniera appropriata a quanto necessario per le finalità per le quali tali informazioni personali vengono trattate e non le utilizza in maniera diversa da tali finalità (articolo 3, secondo comma, della legge sulla protezione delle informazioni personali);

4) garantisce che tali informazioni siano esatte, complete e aggiornate nella misura necessaria in relazione alle finalità per le quali dette informazioni vengono trattate (articolo 3, terzo comma, della legge sulla protezione delle informazioni personali);

5) gestisce le informazioni personali in maniera sicura secondo i metodi, i tipi, ecc. di trattamento delle informazioni personali, tenendo conto della possibilità di violazioni dei diritti degli interessati e della gravità dei rischi pertinenti (articolo 3, quarto comma, della legge sulla protezione delle informazioni personali);

6) rende pubblica la propria politica in materia di tutela della vita privata e altre questioni relative al trattamento di informazioni personali (articolo 3, quinto comma, della legge sulla protezione delle informazioni personali);

7) elabora le informazioni personali in maniera tale da ridurre al minimo la possibilità di violare la vita privata di un interessato (articolo 3, sesto comma, della legge sulla protezione delle informazioni personali).

ii) Conformemente all'articolo 58, quarto comma, della legge sulla protezione delle informazioni personali, il titolare del trattamento (ad esempio le autorità competenti per la sicurezza nazionale quali il servizio di intelligence nazionale) deve adottare le disposizioni necessarie, quali mettere in atto garanzie tecniche, gestionali e fisiche, per assicurare il rispetto di tali principi e il trattamento adeguato delle informazioni personali. Ciò può comprendere ad esempio misure specifiche destinate ad assicurare la sicurezza delle informazioni personali, quali limitazioni all'accesso alle informazioni personali, ai controlli di accesso, ai registri, nonché fornire ai dipendenti una formazione dedicata sulla gestione delle informazioni personali, ecc.

Inoltre, conformemente all'articolo 3, quinto comma, e all'articolo 4, della legge sulla protezione delle informazioni personali, gli interessati dispongono tra l'altro dei seguenti diritti rispetto alle informazioni personali trattate per finalità di sicurezza nazionale:

1) il diritto di ottenere la conferma in merito al fatto che le loro informazioni personali siano o meno oggetto di trattamento, nonché in merito alle informazioni interessate da tale trattamento, anche fornendo copie di tali informazioni (articolo 4, primo e quarto comma, della legge sulla protezione delle informazioni personali);

2) il diritto alla sospensione del trattamento nonché alla raccolta, alla cancellazione e alla distruzione delle informazioni personali (articolo 4, quarto comma, della legge sulla protezione delle informazioni personali).

iii) Un interessato può presentare una richiesta nell'esercizio di tali diritti direttamente presso il titolare del trattamento oppure indirettamente tramite la commissione per la protezione e può autorizzare un proprio rappresentante a procedere in tal senso. Se l'interessato presenta una richiesta, il titolare del trattamento garantisce l'esercizio del diritto in questione senza indugio; è tuttavia previsto che egli possa ritardare, limitare o negare l'esercizio del diritto in questione laddove ciò sia specificamente previsto o inevitabile per rispettare altre leggi nella misura e per il tempo necessari e proporzionati a tutelare un obiettivo importante dell'interesse pubblico (ad esempio nella misura in cui e per il tempo per il quale la concessione del diritto in questione comprometterebbe un'indagine in corso o minaccerebbe la sicurezza nazionale) oppure laddove la concessione di tale diritto possa causare danni alla vita o all'incolumità di una terza parte o una violazione ingiustificata di interessi patrimoniali o di altra natura di una terza parte. Laddove la richiesta venga negata o limitata, il titolare del trattamento deve notificare senza indugio i motivi all'interessato. Il titolare del trattamento deve preparare il metodo e la procedura per consentire agli interessati di presentare richieste e annunciarli pubblicamente affinché gli interessati possano venirne a conoscenza.

Inoltre, conformemente all'articolo 58, quarto comma, della legge sulla protezione delle informazioni personali (requisito per garantire la gestione adeguata dei reclami individuali) e all'articolo 4, quinto comma, della medesima legge (il diritto a un ricorso adeguato in relazione a qualsiasi danno derivante dal trattamento delle informazioni personali attraverso una procedura tempestiva ed equa), gli interessati hanno il diritto di ottenere un risarcimento. Rientra in tale contesto il diritto di segnalare una violazione presunta al centro di segnalazione di violazioni delle informazioni personali (conformemente all'articolo 62, terzo comma, della legge sulla protezione delle informazioni personali), di proporre un reclamo presso la PIPC a cui all'articolo 62 della medesima legge in merito a qualsiasi diritto o interesse in relazione a informazioni personali di una persona fisica nonché di ottenere un ricorso in sede giudiziaria contro decisioni o l'inazione della PIPC ai sensi della legge sui contenziosi amministrativi. Inoltre gli interessati possono ottenere un ricorso in sede giudiziaria ai sensi di quest'ultima legge in caso di violazione dei loro diritti o interessi a causa di una disposizione o di un'omissione da parte del titolare del trattamento (ad esempio una raccolta illecita di dati personali) oppure ottenere un risarcimento per i danni subiti conformemente alla *State Compensation Act* (legge sul risarcimento da parte dello Stato). Tali mezzi di ricorso sono disponibili in caso di possibili violazioni tanto delle norme contenute in leggi specifiche che definiscono limitazioni e garanzie rispetto alla raccolta di informazioni personali, quali le leggi in materia di sicurezza nazionale quanto della legge sulla protezione delle informazioni personali.

Una persona fisica dell'UE può proporre un reclamo alla PIPC attraverso la propria autorità nazionale di protezione dei dati. In tal caso la PIPC informerà la persona fisica attraverso l'autorità nazionale di protezione dei dati, in seguito alla conclusione dell'indagine e della misura correttiva (se applicabile).

ALLEGATO II

18 maggio 2021

Sua Eccellenza signor Didier Reynders, Commissario per la Giustizia della Commissione europea

Signor Commissario,

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

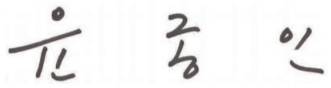
A seguito della richiesta trasmessa dalla Commissione europea al governo della Corea, allego un documento che traccia una panoramica del quadro giuridico in materia di accesso alle informazioni da parte del governo coreano.

Tale documento riguarda numerosi ministeri e agenzie del governo della Corea, e per quanto concerne i contenuti del documento, i ministeri e le agenzie competenti (Commissione per la protezione delle informazioni personali, ministero della Giustizia, Servizio di intelligence nazionale, Commissione nazionale per i diritti umani, Centro nazionale antiterrorismo nazionale, Unità di informazione finanziaria della Corea) sono competenti per le attività rientranti nell'ambito delle rispettive competenze. I pertinenti ministeri e agenzie sono indicati qui di seguito con le rispettive firme.

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

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

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

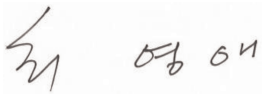


Yoon Jong In
Presidente della Commissione per la protezione delle informazioni personali

Il presente documento è stato redatto dalla Commissione per la protezione delle informazioni personali e dai ministeri e agenzie competenti, elencati qui di seguito.

Park Jie Won
Presidente (direttore), Servizio di intelligence nazionale

Lee Jung Soo
Direttore generale, Ministero della Giustizia



Choi Young Ae
Presidente, Commissione nazionale per i diritti umani della Corea

Kim Hyuck Soo
Direttore, Centro nazionale antiterrorismo

Kim, Jeong Kag
Commissario, Unità di informazione finanziaria della Corea

Quadro giuridico per la raccolta e l'uso di dati personali da parte delle autorità pubbliche coreane per finalità di contrasto e di sicurezza nazionale

Il presente documento fornisce una panoramica del quadro giuridico per la raccolta e l'uso delle informazioni personali da parte delle autorità pubbliche coreane per motivi di contrasto penale e di sicurezza nazionale (in appresso denominato "*accesso da parte delle pubbliche amministrazioni*"), in particolare per quanto riguarda le basi giuridiche disponibili e le condizioni (limitazioni) e le garanzie applicabili, incluse la vigilanza indipendente e le possibilità di ricorso individuale.

1. PRINCIPI GIURIDICI GENERALI IN MATERIA DI ACCESSO DA PARTE DELLE PUBBLICHE AMMINISTRAZIONI

1.1. Quadro costituzionale

La costituzione della Repubblica di Corea stabilisce il diritto alla tutela della vita privata in generale (articolo 17) e il diritto alla tutela della vita privata della corrispondenza in particolare (articolo 18). Spetta allo Stato garantire tali diritti fondamentali ([1]). La costituzione stabilisce inoltre che i diritti e le libertà dei cittadini possano essere limitati soltanto per legge e laddove necessario per la sicurezza nazionale o il mantenimento dell'ordine pubblico per il benessere pubblico ([2]). Anche laddove tali limitazioni vengano imposte, potrebbero non incidere sull'essenza della libertà o del diritto ([3]) in questione. Gli organi giurisdizionali coreani hanno applicato tali disposizioni in cause concernenti l'ingerenza del governo nella vita privata. Ad esempio la Corte suprema ha constatato che il monitoraggio di civili violava il diritto fondamentale alla vita privata, sottolineando che i cittadini hanno "*il diritto all'autodeterminazione delle informazioni personali*" ([4]). In un altro caso la Corte costituzionale ha dichiarato che la vita privata è un diritto fondamentale che fornisce protezione nei confronti dell'intervento e dell'osservazione dello Stato nella vita privata dei cittadini ([5]).

La costituzione coreana assicura altresì che nessuna persona venga arrestata, detenuta, sottoposta a perquisizione, interrogata o che nessun bene venga sequestrato fatta eccezione per quanto previsto dalla legge ([6]). Inoltre le perquisizioni e i sequestri possono essere condotti soltanto sulla base di un mandato rilasciato da un giudice, su richiesta di un pubblico ministero, e in relazione a un giusto processo ([7]). In circostanze eccezionali, ossia quando viene arrestato un sospetto criminale mentre commette un reato (*flagrante delicto*) oppure qualora vi sia il rischio che una persona sospettata di aver commesso un reato punibile con una pena detentiva di almeno tre anni possa fuggire o distruggere elementi di prova, le autorità inquirenti possono condurre una perquisizione o un sequestro in assenza di mandato, nel qual caso devono richiedere un mandato ex post ([8]). Tali principi generali sono ulteriormente sviluppati in leggi specifiche che si occupano di procedura penale e della protezione delle comunicazioni (cfr. in appresso per una panoramica dettagliata).

Per quanto riguarda i cittadini stranieri, la costituzione stabilisce che il loro status è garantito come prescritto dal diritto e dai trattati internazionali ([9]). Diversi accordi internazionali di cui la Corea è parte garantiscono diritti alla tutela della vita privata, 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 del fanciullo (articolo 16). Inoltre, sebbene la costituzione in linea di principio faccia riferimento ai diritti dei "*cittadini*", la Corte costituzionale ha sostenuto che anche i cittadini stranieri godono di diritti fondamentali ([10]). In particolare la Corte ha ritenuto che la tutela della dignità e del valore di una persona in qualità di essere umano, così come il diritto alla ricerca della felicità, siano diritti spettanti a qualsiasi

([1]) Articolo 10 della costituzione della Repubblica di Corea, promulgata il 17 luglio 1948 (di seguito "la costituzione").
([2]) Articolo 37, secondo comma, della costituzione.
([3]) Articolo 37, secondo comma, della costituzione.
([4]) Decisione della Corte suprema della Corea n. 96DA42789, 24 luglio 1998.
([5]) Decisione della Corte costituzionale n. 2002Hun-Ma51, 30 ottobre 2003. Analogamente, nella decisione 99Hun-Ma513 e 2004Hun-Ma190 (consolidata), 26 maggio 2005, la Corte costituzionale ha chiarito che "*il diritto di controllare le proprie informazioni personali consiste nel diritto da parte del soggetto cui le informazioni si riferiscono di decidere personalmente quando, a chi o da chi, e in che misura le sue informazioni saranno divulgate o utilizzate. Si tratta di un diritto fondamentale, sebbene non specificato nella costituzione, che esiste per proteggere la libertà personale di decisione in relazione al rischio causato dall'ampliamento delle funzioni statali e della tecnologia in materia di informazione e comunicazione*".
([6]) Articolo 12, primo comma, prima frase, della costituzione.
([7]) Articoli 16 e articolo 12, terzo comma, della costituzione.
([8]) Articolo 12, terzo comma, della costituzione.
([9]) Articolo 6, secondo comma, della costituzione.
([10]) Decisione della Corte costituzionale n. 93Hun-MA120, 29 dicembre 1994. Cfr. anche ad esempio una decisione della Corte costituzionale n. 2014Hun-Ma346 (31 maggio 2018), nel contesto della quale la Corte ha constatato che il diritto costituzionale di un cittadino sudanese trattenuto all'aeroporto di ricevere assistenza da parte di un consulente legale fosse stato violato. In un'altra causa, la Corte costituzionale ha constatato che la libertà di scegliere il proprio posto di lavoro legale è strettamente correlata al diritto di perseguire la felicità nonché a quello di dignità e valore umani, ed è quindi riservata soltanto ai cittadini ma può essere garantita anche agli stranieri che sono legalmente occupati nella Repubblica di Corea (decisione della Corte costituzionale n. 2007Hun-Ma1083, 29 settembre 2011).

essere umano e non soltanto ai cittadini coreani ([11]). La Corte ha altresì chiarito che il diritto di controllare le proprie informazioni è considerato un diritto fondamentale, che ha il proprio fondamento nel diritto alla dignità e al perseguimento della felicità e nel diritto alla tutela della vita privata ([12]). Sebbene la giurisprudenza non abbia finora trattato il diritto alla tutela della vita privata di cittadini non coreani, è comunque ampiamente accettato tra i ricercatori che gli articoli da 12 a 22 della costituzione (che includono il diritto alla tutela della vita privata e alla libertà personale) stabiliscono i "*diritti degli esseri umani*".

Infine la costituzione prevede altresì il diritto di richiedere un risarcimento equo dalle autorità pubbliche ([13]). Inoltre, ai sensi della legge sulla Corte costituzionale, qualsiasi persona i cui diritti fondamentali garantiti dalla costituzione siano violati dall'esercizio del potere governativo (escludendo le sentenze di organi giurisdizionali) possono presentare un reclamo costituzionale presso la Corte costituzionale ([14]).

1.2. **Norme generali in materia di protezione dei dati personali**

La legge generale sulla protezione dei dati nella Repubblica di Corea, la *Personal Information Protection Act* (PIPA, in appresso: "legge sulla protezione delle informazioni personali" o "PIPA"), si applica tanto al settore privato quanto a quello pubblico. Per quanto concerne le autorità pubbliche, la legge sulla protezione delle informazioni personali fa riferimento all'obbligo di formulare politiche destinate a prevenire "l'*abuso e l'uso improprio di informazioni personali, la sorveglianza e il tracciamento indiscreti, ecc. nonché a migliorare la dignità degli esseri umani e la vita privata individuale*" ([15]).

Il trattamento dei dati personali per finalità di contrasto è soggetto a tutti i requisiti della legge sulla protezione delle informazioni personali. Ciò significa ad esempio che le autorità di contrasto in materia penale devono rispettare gli obblighi per un trattamento lecito, ossia fare affidamento su una delle basi giuridiche elencate nella legge sulla protezione delle informazioni personali per la raccolta, l'uso o la fornitura di informazioni personali (articoli da 15 a 18), nonché i principi di limitazione della finalità (articolo 3, primo e secondo comma), di proporzionalità/minimizzazione dei dati (articolo 3, primo e sesto comma), di limitazione della conservazione dei dati (articolo 21), di sicurezza dei dati, compresa la notifica di violazioni dei dati (articolo 3, quarto comma e articoli 29 e 34), nonché di trasparenza (articolo 3, primo e quinto comma e articoli 20, 30 e 32). Alle informazioni sensibili si applicano garanzie specifiche (articolo 23 della legge sulla protezione delle informazioni personali). Inoltre, ai sensi dell'articolo 3, quinto comma, dell'articolo 4, nonché degli articoli da 35 a 39-2 della legge sulla protezione delle informazioni personali, le persone fisiche possono esercitare i loro diritti di accesso, di rettifica, di cancellazione e di sospensione nei confronti delle autorità di contrasto.

Sebbene si applichi pertanto integralmente al trattamento di dati personali per finalità di contrasto penale, la legge sulla protezione delle informazioni personali contiene un'eccezione quando i dati personali vengono trattati per finalità di sicurezza nazionale. Ai sensi dell'articolo 58, primo comma, punto 2, della legge sulla protezione delle informazioni personali, gli articoli da 15 a 50 della medesima legge non si applicano alle informazioni personali raccolte o richieste per l'analisi di informazioni relative alla sicurezza nazionale ([16]). Di contro, il capo I (Disposizioni generali), il capo II (Istituzione di politiche in materia di protezione delle informazioni personali, ecc.), il capo VIII (Azione collettiva risarcitoria in relazione a una violazione dei dati), il capo IX (Disposizioni supplementari) e il capo X (Disposizioni in merito alle sanzioni) della legge sulla protezione delle informazioni personali rimangono applicabili. Rientrano in tale contesto i principi generali di protezione dei dati di cui all'articolo 3 (Principi per la protezione delle informazioni personali) e dei diritti individuali garantiti dall'articolo 4 della legge sulla protezione delle informazioni personali (Diritti degli interessati). Ciò significa che i principi e i diritti principali sono garantiti anche in questo settore. Inoltre l'articolo 58, quarto comma, della legge sulla protezione delle informazioni personali prevede che tali informazioni debbano essere trattate nella misura minima necessaria per il conseguimento della finalità prevista e per il periodo minimo necessario; Tale disposizione impone inoltre al titolare del trattamento delle informazioni personali di mettere in atto misure necessarie per assicurare una gestione sicura dei dati e un trattamento adeguato, quali garanzie tecniche, gestionali e fisiche, nonché misure per la gestione adeguata di singoli reclami.

Nella notifica n. 2021-1 sulle norme supplementari per l'interpretazione e l'applicazione della legge sulla protezione delle informazioni personali, la commissione per la protezione delle informazioni personali (in appresso: "*PIPC*") ha chiarito ulteriormente le modalità con cui tale legge si applica al trattamento di dati personali per finalità di sicurezza nazionale, alla luce di tale esenzione parziale ([17]). Rientrano in tale contesto in particolare i diritti delle persone fisiche (accesso, rettifica, sospensione e cancellazione) e i motivi nonché le limitazioni per eventuali limitazioni in merito. Secondo la notifica, l'applicazione dei principi, dei diritti e degli obblighi principali della legge sulla protezione delle informazioni personali al trattamento di dati personali per finalità di sicurezza nazionale riflette le garanzie sancite nella costituzione a sostegno della protezione del diritto individuale di controllare le proprie informazioni personali. Qualsiasi

([11]) Decisione della Corte costituzionale n. 99HeonMa494, 29 novembre 2001.
([12]) Cfr. ad esempio la decisione della Corte costituzionale n. 99HunMa513.
([13]) Articolo 29, primo comma, della costituzione.
([14]) Articolo 68, primo comma, della legge sulla Corte costituzionale.
([15]) Articolo 5, primo comma, della legge sulla protezione delle informazioni personali.
([16]) Articolo 58, primo comma, punto 2, della legge sulla protezione delle informazioni personali.
([17]) Notifica n. 2021-1 della PIPC sulle norme supplementari per l'interpretazione e l'applicazione della legge sulla protezione delle informazioni personali, sezione III, punto 6.

limitazione a tale diritto, ad esempio se necessaria ai fini della protezione della sicurezza nazionale, richiede la definizione di un equilibrio tra i diritti e gli interessi della persona fisica e l'interesse pubblico pertinente e non può incidere sull'essenza del diritto (articolo 37, secondo comma, della costituzione).

2. ACCESSO DA PARTE DELLE PUBBLICHE AMMINISTRAZIONI PER FINALITÀ DI CONTRASTO

2.1. Autorità pubbliche competenti nel settore del contrasto

Ai sensi del codice di procedura penale (in appresso «*CPP*»), della legge sulla tutela della vita privata nelle comunicazioni (in appresso: «*legge sulle comunicazioni*») e della legge sulle imprese di telecomunicazione, la polizia, i pubblici ministeri e gli organi giurisdizionali possono raccogliere dati personali per finalità di contrasto penale. Nella misura in cui la *National Intelligence Service Act* (legge sul servizio nazionale di intelligence, in appresso: «legge sul NIS») conferisce tale potere anche al servizio di intelligence nazionale (in appresso: «*NIS*»), tale organismo deve rispettare le leggi di cui sopra ([18]). Infine la *Act on Reporting and Using Specified Financial Transaction Information* (in appresso: «ARUSFTI»; legge sulla segnalazione e l'utilizzo di informazioni specifiche sulle operazioni finanziarie) fornisce una base giuridica sulla quale gli enti finanziari possono fare affidamento per divulgare le informazioni alla *Korea Financial Intelligence Unit* (unità di informazione finanziaria della Corea) al fine di prevenire il riciclaggio di denaro e il finanziamento del terrorismo. Questa agenzia specializzata potrebbe a sua volta fornire tali informazioni alle autorità di contrasto. Tuttavia tali obblighi di divulgazione si applicano soltanto ai titolari del trattamento dei dati che trattano informazioni creditizie personali ai sensi della legge sulle informazioni creditizie e sono soggetti a vigilanza da parte della commissione per i servizi finanziari. Dato che il trattamento di informazioni creditizie personali da parte di tali titolari del trattamento è escluso dall'ambito di applicazione della decisione di adeguatezza, le limitazioni e le garanzie che si applicano nel quadro dell'ARUSFTI non sono descritte in maniera più dettagliata nel presente documento.

2.2. Basi giuridiche e limitazioni

Il codice di procedura penale (cfr. 2.2.1), la legge sulle comunicazioni (cfr. 2.2.2) e la legge sulle imprese di telecomunicazione (cfr. 2.2.3) forniscono basi giuridiche per la raccolta di informazioni personali per finalità di contrasto e stabiliscono le limitazioni e le garanzie applicabili.

2.2.1. *Perquisizioni e sequestri*

2.2.1.1. Base giuridica

I pubblici ministeri e i funzionari di alto livello della polizia giudiziaria possono ispezionare oggetti, perquisire persone e sequestrare oggetti soltanto: 1) se una persona è sospettata di aver commesso un reato (un sospetto criminale); 2) se ciò è necessario ai fini dell'indagine; e 3) gli oggetti da ispezionare, le persone da perquisire e tutti gli oggetti sequestrati sono considerati connessi al caso ([19]). Analogamente gli organi giurisdizionali possono condurre perquisizioni e sequestrare qualsiasi oggetto da utilizzare come elemento di prova o passibile di confisca, purché tali oggetti o persone siano considerati connessi a un caso specifico ([20]).

2.2.1.2. Limitazioni e garanzie

Come obbligo generale, i pubblici ministeri e i funzionari della polizia giudiziaria devono rispettare i diritti umani del sospetto criminale e quelli di qualsiasi altra persona interessata ([21]). Inoltre misure obbligatorie per il conseguimento della finalità dell'indagine possono essere adottate soltanto se previsto in modo esplicito nel codice di procedura penale e nella misura minore necessaria ([22]).

Perquisizioni, ispezioni o sequestri da parte di funzionari di polizia o pubblici ministeri nel contesto di un'indagine penale possono aver luogo soltanto sulla base di un mandato di mandato emesso da un organo giurisdizionale ([23]). L'autorità che richiede il mandato deve presentare materiali che dimostrino i motivi per sospettare una persona fisica della commissione di un reato, la necessità della perquisizione, dell'ispezione o del sequestro, nonché l'esistenza di oggetti pertinenti da sequestrare ([24]). Per quanto riguarda il mandato, tra gli altri elementi deve contenere il nome del sospetto criminale e l'indicazione del reato; il luogo, la persona o gli oggetti da sottoporre a perquisizione o gli oggetti da sequestrare; la data di emissione; nonché il periodo effettivo di applicazione ([25]). Analogamente, quando nel contesto di procedimenti giudiziari in corso perquisizioni e sequestri vengono effettuati in circostanze diverse da un'udienza pubblica, è necessario ottenere preventivamente un mandato da un organo giurisdizionale ([26]). La persona fisica interessata e il suo consulente legale per la difesa ricevono una notifica preventiva della perquisizione o del sequestro e possono essere presenti quando il mandato viene eseguito ([27]).

([18]) Cfr. articolo 3 della legge sul NIS (legge n. 12948), che si riferisce a indagini penali in merito a determinati reati, quali l'insurrezione, la ribellione e reati relativi alla sicurezza nazionale (ad esempio lo spionaggio). In un tale contesto si applicano le procedure di cui al codice di procedura penale in merito a perquisizioni e sequestri, mentre la legge sulle comunicazioni disciplinerebbe la raccolta di dati relativi alle comunicazioni (cfr. parte 3 sulle disposizioni che si occupano di accesso alle comunicazioni per finalità di sicurezza nazionale).

([19]) Articolo 215, primo e secondo comma, del codice di procedura penale.

([20]) Articolo 106, primo comma e articoli 107 e 109, del codice di procedura penale.

([21]) Articolo 198, secondo comma, del codice di procedura penale.

([22]) Articolo 199, primo comma, del codice di procedura penale.

([23]) Articolo 215, primo e secondo comma, del codice di procedura penale.

([24]) Articolo 108, primo comma, del codice di procedura penale.

([25]) Articolo 114, primo comma, del codice di procedura penale in combinato disposto con l'articolo 219 del medesimo codice.

([26]) Articolo 113 del codice di procedura penale.

([27]) Articoli 121 e 122 del codice di procedura penale.

Durante lo svolgimento di perquisizioni o sequestri e laddove l'oggetto da perquisire sia il disco rigido di un computer o un altro supporto di memorizzazione dati, in linea di principio saranno sequestrati soltanto i dati (copiati o stampati) anziché l'intero supporto ([28]). Quest'ultimo può essere sequestrato soltanto quando viene considerato sostanzialmente impossibile stampare o copiare i dati richiesti separatamente o quando è considerato sostanzialmente impraticabile conseguire diversamente la finalità della perquisizione ([29]). La persona fisica interessata deve ricevere notifica del sequestro senza indugio ([30]). Il codice di procedura penale non prevede eccezioni a tale requisito di notifica.

Perquisizioni, ispezioni e sequestri in assenza di mandato possono avvenire soltanto in circostanze limitate. Innanzitutto ciò si verifica quanto non è possibile ottenere un mandato in ragione dell'urgenza presso la scena di un reato ([31]). Tuttavia successivamente occorre ottenere un mandato senza indugio ([32]). In secondo luogo perquisizioni e ispezioni in assenza di mandato possono aver luogo in loco quando un sospetto criminale viene arrestato o trattenuto ([33]). Infine, un pubblico ministero o un alto funzionario della polizia giudiziaria può sequestrare un oggetto in assenza di mandato quando tale oggetto sia stato gettato da un sospetto criminale o una terza persona, oppure sia stato prodotto volontariamente ([34]).

Gli elementi di prova ottenuti in violazione del codice di procedura penale saranno considerati inammissibili ([35]). Il codice penale stabilisce altresì che perquisizioni illegali di persone o del luogo di residenza, dell'edificio custodito, della struttura, dell'automobile, della nave, dell'aeromobile o della stanza occupata da una persona sono punibili con una pena detentiva per un massimo di tre anni ([36]). Di conseguenza questa disposizione si applica anche nelle circostanze in cui oggetti, quali dispositivi di archiviazione dati, vengono sequestrati durante una perquisizione illegale.

2.2.2. *Raccolta di informazioni relative alle comunicazioni*

2.2.2.1. Base giuridica

La raccolta di informazioni relative alle comunicazioni è disciplinata da una legge specifica, la legge sulle comunicazioni. In particolare la legge sulle comunicazioni stabilisce un divieto per chiunque di censurare qualsiasi comunicazione postale, intercettare qualsiasi telecomunicazione, fornire dati di conferma di comunicazioni oppure registrare o ascoltare qualsiasi conversazione tra altri che non sono resi pubblici, fatta eccezione ai sensi del codice di procedura penale, della legge sulle comunicazioni o della legge sugli organi giurisdizionali militari ([37]). Il termine «*comunicazione*» ai sensi del significato della legge sulle comunicazioni comprende tanto la corrispondenza ordinaria quanto le telecomunicazioni ([38]). A tale riguardo la legge sulle comunicazioni distingue tra "*misure di limitazione delle comunicazioni*" ([39]) e la raccolta di "*dati di conferma di comunicazioni*".

La nozione di misure di limitazione delle comunicazioni comprende la "*censura*", ossia la raccolta del contenuto della corrispondenza postale tradizionale, nonché l'"*intercettazione*", ossia l'intercettazione diretta (acquisizione o registrazione) del contenuto di telecomunicazioni ([40]). La nozione di dati di conferma di comunicazioni riguarda "*dati sulle registrazioni di telecomunicazioni*", che comprendono la data delle telecomunicazioni, il loro orario di inizio e di fine, il numero di chiamate in uscita e in arrivo, nonché il numero dell'abbonato dell'altro capo, la frequenza d'uso, i file di registro sull'uso dei servizi di telecomunicazione e le informazioni relative all'ubicazione (ad esempio dalle torri di trasmissione presso le quali vengono ricevuti i segnali) ([41]).

([28]) Articolo 106, terzo comma, del codice di procedura penale.
([29]) Articolo 106, terzo comma, del codice di procedura penale.
([30]) Articolo 219 del codice di procedura penale, in combinato disposto con l'articolo 106, quarto comma, del codice di procedura penale.
([31]) Articolo 216, terzo comma, del codice di procedura penale.
([32]) Articolo 216, terzo comma, del codice di procedura penale.
([33]) Articolo 216, primo e secondo comma, del codice di procedura penale.
([34]) Articolo 218 del codice di procedura penale. Per quanto concerne le informazioni personali, ciò riguarda soltanto la produzione volontaria da parte della persona fisica interessata stessa, non da parte di un titolare del trattamento delle informazioni personali che detiene tali informazioni (una circostanza questa che richiederebbe una base giuridica specifica ai sensi della legge sulla protezione delle informazioni personali). Gli oggetti prodotti volontariamente sono ammessi come elementi di prova nei procedimenti giudiziari soltanto se non vi è alcun dubbio ragionevole per quanto riguarda la natura volontaria della divulgazione, aspetto che spetta al pubblico ministero dimostrare. Cfr. decisione della Corte suprema 2013Do11233, 10 marzo 2016.
([35]) Articolo 308-2 del codice di procedura penale.
([36]) Articolo 321 del codice penale.
([37]) Articolo 3 della legge sulle comunicazioni. La legge sugli organi giurisdizionali militari disciplina in linea di principio la raccolta di informazioni concernenti il personale militare e può applicarsi ai civili soltanto in un numero limitato di casi (ad esempio, nel caso in cui membri del personale militare e civili commettessero un reato congiuntamente oppure se una persona fisica commette un reato nei confronti di militari, il procedimento corrispondente può essere avviato dinanzi un organo giurisdizionale militare, cfr. articolo 2 di tale legge). Le disposizioni generali che disciplinano le perquisizioni e i sequestri sono analoghe a quanto previsto dal codice di procedura penale (cfr. ad esempio articoli da 146 a 149 e da 153 a 156 della legge sugli organi giurisdizionali militari). Ad esempio la corrispondenza postale può essere raccolta soltanto quando ciò è necessario ai fini di un'indagine e sulla base di un mandato emesso da un organo giurisdizionale militare. Qualora vengano raccolte delle comunicazioni elettroniche sulla base di tale legge, si applicano le limitazioni e le garanzie di cui alla legge sulle comunicazioni.
([38]) Articolo 2, primo comma, della legge sulle comunicazioni, ossia «*trasmissione o ricezione di tutti i tipi di suoni, parole, simboli o immagini tramite cablaggio, senza cablaggio, con cablaggio in fibra o altro sistema elettromagnetico, inclusi telefono, posta elettronica, servizi di informazione associativa, facsimile e paging radiofonico*».
([39]) Articolo 2, settimo comma, e articolo 3, secondo comma, della legge sulle comunicazioni.
([40]) La "censura" è definita come l'"*apertura di corrispondenza senza il consenso della parte in questione o l'acquisizione di conoscenza, la registrazione o il trattenimento dei rispettivi contenuti attraverso altri mezzi*" (articolo 2, sesto comma, della legge sulle comunicazioni). "Intercettazione" indica "*l'acquisizione o la registrazione di contenuti di telecomunicazioni ascoltando o leggendo in associazione suoni, parole, simboli o immagini delle comunicazioni attraverso dispositivi elettronici e meccanici senza il consenso della parte interessata oppure l'interferenza con la loro trasmissione e ricezione*" (articolo 2, settimo comma, della legge sulle comunicazioni).
([41]) Articolo 2, undicesimo comma, della legge sulle comunicazioni.

La legge sulle comunicazioni stabilisce le limitazioni e le garanzie per la raccolta di entrambi i tipi di dati e il mancato rispetto di diversi di questi requisiti è soggetta a sanzioni penali ([42]).

2.2.2.2. Limitazioni e garanzie applicabili alla raccolta del contenuto di comunicazioni (misure di limitazione delle comunicazioni)

La raccolta del contenuto di comunicazioni può avvenire soltanto come mezzo supplementare per facilitare un'indagine penale (ossia come misura di ultima istanza) e si devono compiere sforzi per ridurre al minimo le interferenze con i segreti delle comunicazioni delle persone ([43]). In linea con questo principio generale, si può ricorrere a misure di limitazione delle comunicazioni soltanto laddove sia difficile prevenire altrimenti la commissione di un reato, arrestare il criminale o raccogliere elementi di prova ([44]). Le agenzie di contrasto che raccolgono il contenuto di comunicazioni devono immediatamente cessare tale attività una volta che l'accesso continuo non sia più ritenuto necessario, garantendo così che la violazione della vita privata delle comunicazioni sia limitata nella massima misura possibile ([45]).

Inoltre le misure di limitazione delle comunicazioni possono essere utilizzate soltanto quando esiste un motivo sostanziale per sospettare che siano stati pianificati o commessi o che saranno commessi determinati reati gravi specificatamente elencati nella legge sulle comunicazioni. Rientrano in tale contesto reati quali insurrezioni, reati legati alla droga o che coinvolgono esplosivi, nonché reati relativi alla sicurezza nazionale, a relazioni diplomatiche o basi e installazioni militari ([46]). L'oggetto di una misura di limitazione delle comunicazioni deve essere costituito da comunicazioni tramite posta o telecomunicazioni specifiche inviate o ricevute da un indiziato oppure comunicazioni tramite posta o telecomunicazioni inviate o ricevute da un indiziato entro un periodo di tempo fisso ([47]).

Anche quando tali requisiti sono soddisfatti, la raccolta di dati relativi ai contenuti può avvenire soltanto sulla base di un mandato emesso da un organo giurisdizionale. In particolare un pubblico ministero può chiedere a un organo giurisdizionale di consentire la raccolta dei dati relativi ai contenuti riguardanti l'indiziato o la persona oggetto di indagine ([48]). Analogamente un funzionario della polizia giudiziaria può richiedere l'autorizzazione a un pubblico ministero, il quale a sua volta può richiedere a un organo giurisdizionale di emettere un mandato ([49]). Una richiesta di rilascio di un mandato deve essere effettuata per iscritto e deve contenere elementi specifici. In particolare deve stabilire: 1) i motivi sostanziali per sospettare che uno dei reati elencati sia stato pianificato o che la sua commissione sia in atto o che sia stato commesso, unitamente a qualsiasi materiale giustificativo stabilendo un caso di sospetto prima facie; 2) le misure di limitazione delle comunicazioni, unitamente all'oggetto, alla portata, all'obiettivo e alla durata di efficacia delle stesse; e 3) il luogo in cui le misure verrebbero eseguite e le modalità di attuazione ([50]).

Se i requisiti giuridici sono soddisfatti, l'organo giurisdizionale può concedere l'autorizzazione scritta di attuare misure di limitazione delle comunicazioni in relazione all'indiziato o alla persona soggetta a indagine ([51]). Tale mandato specifica le tipologie di misure nonché il loro oggetto, la loro portata, il loro periodo di efficacia, il loro luogo di esecuzione e le corrispondenti modalità di attuazione ([52]).

Le misure di limitazione delle comunicazioni possono essere attuate soltanto per un periodo di due mesi ([53]). Se l'obiettivo delle misure viene conseguito prima, entro tale termine, le misure devono essere interrotte immediatamente. Al contrario, se le condizioni necessarie continuano ad essere soddisfatte, è possibile presentare una richiesta di proroga del periodo di efficacia delle misure di limitazione delle comunicazioni entro un termine di due mesi. Tale richiesta deve comprendere materiali che stabiliscono un caso prima facie per la proroga delle misure ([54]). Il periodo prorogato non può superare complessivamente un anno o tre anni per determinati reati particolarmente gravi (ad esempio reati relativi a insurrezione, aggressione straniera, sicurezza nazionale, ecc.) ([55]).

Le autorità di contrasto possono imporre la fornitura di assistenza da parte degli operatori di comunicazioni fornendo loro l'autorizzazione scritta dell'organo giurisdizionale ([56]). Gli operatori di comunicazioni sono tenuti a cooperare e a conservare l'autorizzazione ricevuta nei loro archivi ([57]). Possono rifiutare la cooperazione quando le informazioni sulla persona fisica oggetto della misura come indicate nell'autorizzazione scritta dell'organo giurisdizionale (ad esempio il numero di telefono di tale persona) non sono corrette. Inoltre, in qualsiasi circostanza, sono soggetti a divieto di divulgazione delle password utilizzate per le telecomunicazioni ([58]).

([42]) Articoli 16 e 17 della legge sulle comunicazioni. Ciò si applica ad esempio alla raccolta in assenza di mandato, alla mancata tenuta di registri, alla mancata interruzione della raccolta nel momento in cui un'emergenza cessa di sussistere oppure alla mancata notifica alla persona fisica interessata.
([43]) Articolo 3, secondo comma, della legge sulle comunicazioni.
([44]) Articolo 5, primo comma, della legge sulle comunicazioni.
([45]) Articolo 2 del decreto di applicazione della legge sulle comunicazioni.
([46]) Articolo 5, primo comma, della legge sulle comunicazioni.
([47]) Articolo 5, secondo comma, della legge sulle comunicazioni.
([48]) Articolo 6, primo comma, della legge sulle comunicazioni.
([49]) Articolo 6, secondo comma, della legge sulle comunicazioni.
([50]) Articolo 6, quarto comma, della legge sulle comunicazioni e articolo 4, primo comma, del decreto di applicazione di tale legge.
([51]) Articolo 6, quinto e sesto comma, della legge sulle comunicazioni.
([52]) Articolo 6, sesto comma, della legge sulle comunicazioni.
([53]) Articolo 6, settimo comma, della legge sulle comunicazioni.
([54]) Articolo 6, settimo comma, della legge sulle comunicazioni.
([55]) Articolo 6, ottavo comma, della legge sulle comunicazioni.
([56]) Articolo 9, secondo comma, della legge sulle comunicazioni.
([57]) Articolo 15-2 della legge sulle comunicazioni e articolo 12 del decreto di applicazione di tale legge.
([58]) Articolo 9, quarto comma, della legge sulle comunicazioni.

Chiunque dia esecuzione alle misure di limitazione delle comunicazioni o sia invitato a cooperare deve tenere registri che specificano gli obiettivi delle misure, la loro esecuzione, la data in cui è stata fornita la cooperazione e l'oggetto ([59]). Anche le autorità di contrasto che attuano misure di limitazione delle comunicazioni devono tenere registri che definiscano i dettagli e gli esiti conseguiti ([60]). I funzionari della polizia giudiziaria devono fornire tali informazioni mediante una relazione al pubblico ministero quando chiudono un'indagine ([61]).

Quando emette un rinvio a giudizio in merito a un caso nel contesto del quale si è fatto ricorso a misure di limitazione delle comunicazioni oppure emette una disposizione attestante la decisione di non rinviare a giudizio o arrestare la persona fisica pertinente (ossia non si tratta soltanto di una sospensione del procedimento giudiziario), un pubblico ministero deve inviare una notifica alla persona fisica soggetta a misure di limitazione delle comunicazioni in merito all'avvenuta esecuzione di tali misure, all'agenzia che vi ha dato esecuzione e al periodo di esecuzione. Tale notifica deve essere fornita per iscritto entro 30 giorni dalla disposizione ([62]). Detta notifica può essere differita qualora sia suscettibile di mettere seriamente in pericolo la sicurezza nazionale o di perturbare la sicurezza e l'ordine pubblici oppure se è probabile che comporti danni materiali alla vita e all'incolumità di altri ([63]). Quando intende differire tale notifica, il pubblico ministero o il funzionario della polizia giudiziaria deve ottenere l'approvazione dal capo dell'ufficio distrettuale del pubblico ministero ([64]). Quando i motivi per tale differimento cessano di esistere, occorre effettuare la notifica entro 30 giorni a partire da tale momento ([65]).

La legge sulle comunicazioni stabilisce altresì una procedura specifica per la raccolta del contenuto di comunicazioni in situazioni di emergenza. In particolare le agenzie di contrasto possono raccogliere il contenuto di comunicazioni nel caso in cui la pianificazione o l'esecuzione di atti di criminalità organizzata o di un altro reato grave che possa causare direttamente il decesso o lesioni gravi sia imminente e vi sia un'emergenza che rende impossibile seguire la procedura normale (come illustrata sopra) ([66]). In tali emergenze, un funzionario di polizia o un pubblico ministero può adottare misure di limitazione delle comunicazioni senza l'autorizzazione preventiva di un organo giurisdizionale, ma subito dopo l'esecuzione deve presentare domanda di rilascio di tale autorizzazione a un organo giurisdizionale. Se l'agenzia di contrasto non riesce a ottenere l'autorizzazione dell'organo giurisdizionale entro 36 ore dal momento in cui sono state attuate le misure di emergenza, la raccolta deve essere interrotta immediatamente e in genere tale circostanza è seguita dalla distruzione delle informazioni raccolte ([67]). I funzionari di polizia che svolgono attività di sorveglianza di emergenza procedono in tal senso sotto il controllo di un pubblico ministero oppure, nel caso in cui la ricezione preventiva di istruzioni da parte del pubblico ministero sia impossibile in ragione della necessità di agire con urgenza, la polizia deve ottenere immediatamente l'approvazione di un pubblico ministero dopo l'avvio dell'esecuzione ([68]). Le norme sulla notifica alla persona fisica come descritto sopra si applicano anche alla raccolta del contenuto di comunicazioni in situazioni di emergenza.

La raccolta di informazioni in situazioni di emergenza deve sempre avvenire in conformità con una "*dichiarazione di censura/intercettazione di emergenza*" e l'autorità che effettua la raccolta deve tenere un registro di tutte le misure di emergenza ([69]). La richiesta presentata ad un organo giurisdizionale per la concessione dell'autorizzazione relativa alle misure di emergenza deve essere accompagnata da un documento scritto che indichi le misure di limitazione delle comunicazioni necessarie, l'obiettivo, l'oggetto, la portata, il periodo, il luogo di esecuzione, il metodo e una spiegazione del modo in cui le misure di limitazione delle comunicazioni soddisfano l'articolo 5, primo comma, della legge sulle comunicazioni ([70]), unitamente a documenti giustificativi.

Nei casi in cui le misure di emergenza vengono completate in breve tempo, escludendo quindi l'autorizzazione dell'organo giurisdizionale (ad esempio se il sospetto viene arrestato immediatamente dopo aver avviato l'intercettazione, che si arresta di conseguenza), il capo dell'ufficio del pubblico ministero competente notifica un avviso di misura di emergenza all'organo giurisdizionale competente ([71]). La notifica deve indicare l'obiettivo, l'oggetto, la portata, il periodo, il luogo di esecuzione e il metodo di raccolta nonché i motivi che giustificano la mancata presentazione di una richiesta di autorizzazione dell'organo giurisdizionale ([72]). Tale notifica consente all'organo giurisdizionale ricevente di esaminare la legalità della raccolta e deve essere inserito in un registro delle notifiche delle misure di emergenza.

([59]) Articolo 9, terzo comma, della legge sulle comunicazioni.
([60]) Articolo 18, primo comma, del decreto di applicazione della legge sulle comunicazioni.
([61]) Articolo 18, secondo comma, del decreto di applicazione della legge sulle comunicazioni.
([62]) Articolo 9-2, primo comma, della legge sulle comunicazioni.
([63]) Articolo 9-2, quarto comma, della legge sulle comunicazioni.
([64]) Articolo 9-2, quinto comma, della legge sulle comunicazioni.
([65]) Articolo 9-2, sesto comma, della legge sulle comunicazioni.
([66]) Articolo 8, primo comma, della legge sulle comunicazioni.
([67]) Articolo 8, secondo comma, della legge sulle comunicazioni.
([68]) Articolo 8, terzo comma, della legge sulle comunicazioni e articolo 16, terzo comma, del decreto di applicazione di tale legge.
([69]) Articolo 8, quarto comma, della legge sulle comunicazioni.
([70]) Ossia che attesti che vi è un motivo sostanziale per sospettare che si stia procedendo con la pianificazione o la commissione di determinati reati gravi reati oppure che questi ultimi siano già stati commessi, e sia impraticabile prevenire altrimenti la commissione di un reato, arrestare il criminale o raccogliere elementi di prova.
([71]) Articolo 8, quinto comma, della legge sulle comunicazioni.
([72]) Articolo 8, sesto e settimo comma, della legge sulle comunicazioni.

Come requisito generale, il contenuto di comunicazioni acquisito attraverso l'esecuzione di misure di limitazione delle comunicazioni ai sensi della legge sulle comunicazioni può essere utilizzato soltanto per indagare, perseguire o prevenire i reati specifici di cui sopra, nel contesto di procedimenti disciplinari relativi ai medesimi reati, una richiesta di risarcimento dei danni formulata da una parte coinvolta nelle comunicazioni o laddove ciò sia consentito da altre leggi ([73]).

Garanzie specifiche si applicano laddove vengano raccolte telecomunicazioni trasmesse via internet ([74]). Tali informazioni possono essere utilizzate soltanto per indagare in merito ai reati gravi elencati nell'articolo 5, primo comma, della legge sulle comunicazioni. Per conservare le informazioni occorre ottenere l'approvazione da parte dell'organo giurisdizionale che ha autorizzato le misure di limitazione delle comunicazioni ([75]). Una tale richiesta di conservazione deve contenere informazioni in merito alle misure di limitazione delle comunicazioni, una sintesi dei risultati delle misure, i motivi per la conservazione (unitamente a materiali a sostegno) e le telecomunicazioni da conservare ([76]). In assenza di tale richiesta, le telecomunicazioni acquisite devono essere cancellate entro 14 giorni dalla fine delle misure di limitazione delle comunicazioni ([77]). Se una richiesta viene respinta, le telecomunicazioni devono essere distrutte entro sette giorni ([78]). Laddove le telecomunicazioni vengano cancellate, entro sette giorni si deve presentare una relazione all'organo giurisdizionale che ha autorizzato le misure di limitazione delle comunicazioni, indicante i motivi della cancellazione, nonché i dettagli e le tempistiche.

Più in generale, se le informazioni sono state ottenute illecitamente mediante misure di limitazione delle comunicazioni, non saranno ammesse come elementi di prova nel contesto di procedimenti giudiziari o disciplinari ([79]). Inoltre la legge sulle comunicazioni vieta a qualsiasi persona che adotta misure di limitazione delle comunicazioni di divulgare informazioni riservate ottenute nel corso dell'attuazione di tali misure e di utilizzare le informazioni ottenute per danneggiare la reputazione di coloro che sono soggetti a dette misure ([80]).

2.2.2.3. Limitazioni e garanzie applicabili alla raccolta di informazioni di conferma di comunicazioni

Ai sensi della legge sulle comunicazioni le autorità di contrasto possono richiedere agli operatori di telecomunicazioni di fornire i dati di conferma di comunicazioni laddove ciò sia necessario per condurre un'indagine o dare esecuzione a una sentenza ([81]). A differenza della raccolta di dati relativi ai contenuti, la possibilità di raccogliere dati di conferma di comunicazioni non è limitata a determinati reati specifici. Tuttavia, come nel caso di dati relativi ai contenuti, la raccolta dei dati di conferma di comunicazioni richiede l'autorizzazione scritta preventiva da parte di un organo giurisdizionale, nel rispetto delle medesime condizioni descritte in precedenza ([82]). Quando motivi di urgenza rendono impossibile ottenere l'autorizzazione dell'organo giurisdizionale, i dati di conferma di comunicazioni possono essere raccolti in assenza di un mandato, nel qual caso l'autorizzazione deve essere ottenuta immediatamente dopo aver richiesto i dati e deve essere comunicata al fornitore di servizi di telecomunicazione ([83]). Qualora non si ottenga alcuna autorizzazione successiva, le informazioni raccolte devono essere distrutte ([84]).

I pubblici ministeri, i funzionari della polizia giudiziaria e gli organi giurisdizionali devono tenere registri delle richieste relative a dati di conferma di comunicazioni ([85]). Inoltre i fornitori di servizi di telecomunicazione devono riferire due volte l'anno al ministro della Scienza e delle tecnologie dell'informazione e della comunicazione (ministro della Scienza e delle TIC) in merito alla divulgazione dei dati di conferma di comunicazioni e devono tenere registri per sette anni dalla data in cui i dati sono stati divulgati ([86]).

In linea di massima le persone fisiche ricevono una notifica in merito al fatto che sono stati raccolti dati di conferma di comunicazioni ([87]). Le tempistiche per tale notifica dipendono dalle circostanze dell'indagine ([88]). Una volta presa una decisione di (non) procedere con l'azione giudiziaria, occorre inviarne notifica entro 30 giorni. Di contro, se il rinvio a giudizio viene sospeso, si deve effettuare la notifica di tale circostanza entro 30 giorni trascorso un anno dall'adozione di tale decisione. In ogni caso la notifica deve essere fornita entro 30 giorni trascorso un anno dal momento della raccolta delle informazioni.

Tale notifica può essere differita quando è probabile che: 1) comprometta la sicurezza nazionale, nonché la sicurezza e l'ordine pubblici; 2) causi un decesso o lesioni personali; 3) ostacoli procedimenti giudiziari equi (ad esempio

([73]) Articolo 12 della legge sulle comunicazioni.
([74]) Articolo 12-2 della legge sulle comunicazioni.
([75]) Il pubblico ministero o il funzionario di polizia che dà esecuzione alle misure di limitazione delle comunicazioni deve selezionare le telecomunicazioni da conservare entro 14 giorni dalla cessazione delle misure e richiedere l'approvazione da parte dell'organo giurisdizionale (nel caso di un funzionario di polizia, la domanda deve essere presentata a un pubblico ministero, il quale a sua volta presenta la richiesta all'organo giurisdizionale) (cfr. articolo 12-2, primo e secondo comma, della legge sulle comunicazioni).
([76]) Articolo 12-2, terzo comma, della legge sulle comunicazioni.
([77]) Articolo 12-2, quinto comma, della legge sulle comunicazioni.
([78]) Articolo 12-2, quinto comma, della legge sulle comunicazioni.
([79]) Articolo 4 della legge sulle comunicazioni.
([80]) Articolo 11, secondo comma, del decreto di applicazione della legge sulle comunicazioni.
([81]) Articolo 13, primo comma, della legge sulle comunicazioni.
([82]) Articoli 13 e 6 della legge sulle comunicazioni.
([83]) Articolo 13, secondo comma, della legge sulle comunicazioni. Come nel caso di urgenti misure di limitazione delle comunicazioni, occorre redigere un documento che riporti i dettagli del caso (il sospetto, le misure da adottare, il reato sospettato nonché l'urgenza). Cfr. articolo 37, quinto comma, del decreto di applicazione della legge sulle comunicazioni.
([84]) Articolo 13, terzo comma, della legge sulle comunicazioni.
([85]) Articolo 13, quinto e sesto comma, della legge sulle comunicazioni.
([86]) Articolo 13, settimo comma, della legge sulle comunicazioni.
([87]) Articolo 13-3, settimo comma, in combinato disposto con l'articolo 9-2, della legge sulle comunicazioni.
([88]) Articolo 13-3, primo comma, della legge sulle comunicazioni.

determinando la distruzione di elementi di prova o minacce ai testimoni); oppure 4) diffami l'indiziato, le vittime o altre persone collegate al caso oppure invada la loro vita privata ([89]). La notifica effettuata sulla base di uno dei motivi di cui sopra richiede l'autorizzazione dal direttore di un ufficio distrettuale del pubblico ministero competente ([90]). Quando i motivi per tale differimento cessano di esistere, occorre effettuare la notifica entro 30 giorni a partire da tale momento ([91]).

Le persone fisiche che ricevono la notifica possono presentare una richiesta scritta al pubblico ministero o al funzionario della polizia giudiziaria in merito ai motivi della raccolta dei dati di conferma di comunicazioni ([92]). In tal caso il pubblico ministero o il funzionario della polizia giudiziaria deve fornire tali motivi per iscritto entro 30 giorni dalla ricezione della richiesta, fatto salvo il caso in cui si applichi uno dei motivi di cui sopra (eccezioni per il differimento della notifica) ([93]).

2.2.3. *Divulgazione volontaria da parte di operatori economici di telecomunicazioni*

L'articolo 83, terzo comma, della legge sulle imprese di telecomunicazione consente agli operatori economici di telecomunicazioni di conformarsi volontariamente a una richiesta formulata (a sostegno di un processo penale, di un'indagine o dell'esecuzione di una sentenza) da un organo giurisdizionale, un pubblico ministero o il capo di un'agenzia investigativa, di divulgare "*dati relativi alle comunicazioni*". Nel contesto della legge sulle imprese di telecomunicazione la nozione di "*dati relativi alle comunicazioni*" concerne il nome, il numero di registrazione come residente, l'indirizzo e il numero di telefono di utenti, le date nelle quali gli utenti si abbonano o disdicono il loro abbonamento nonché i codici di identificazione utente (ossia i codici utilizzati per identificare l'utente legittimo di sistemi informatici o reti di comunicazione) ([94]). Ai fini della legge sulle imprese di telecomunicazione, soltanto le persone fisiche che acquistano direttamente servizi da un fornitore di servizi di telecomunicazione coreano sono considerati utenti ([95]). Di conseguenza è probabile che le circostanze nelle quali le persone fisiche dell'UE i cui dati vengono trasferiti verso la Repubblica della Corea siano considerati utenti ai sensi della legge sulle imprese di telecomunicazione siano molto limitate, dato che di norma tali persone fisiche non concludono un contratto diretto con un operatore di telecomunicazioni coreano.

Le richieste di ottenimento di dati relativi alle comunicazioni ai sensi della legge sulle imprese di telecomunicazione devono essere formulate per iscritto e indicare i motivi della richiesta, il legame con l'utente pertinente e la portata dei dati richiesti ([96]). Laddove sia impossibile fornire una richiesta scritta per motivi di urgenza, tale richiesta deve essere presentata non appena il motivo di urgenza cessa di applicarsi ([97]). Gli operatori economici di telecomunicazioni che soddisfano le richieste di divulgare dati relativi alle comunicazioni devono conservare registri contenenti registrazioni indicanti che i dati relativi alle comunicazioni sono stati forniti, nonché i materiali corrispondenti, quali la richiesta scritta ([98]). Inoltre gli operatori economici di telecomunicazioni devono riferire due volte l'anno in merito alla fornitura di dati relativi alle comunicazioni al ministro della Scienza e delle TIC ([99]).

Gli operatori economici di telecomunicazioni non sono tenuti in alcun modo a soddisfare le richieste di divulgare dati relativi alle comunicazioni sulla base della legge sulle imprese di telecomunicazione. Ogni richiesta deve quindi essere valutata dall'operatore in considerazione dei requisiti di protezione dei dati applicabili ai sensi della legge sulla protezione delle informazioni personali. In particolare un operatore economico di telecomunicazioni deve tenere conto degli interessi dell'interessato e non può divulgare informazioni qualora ciò sia suscettibile di violare ingiustamente l'interesse della persona fisica o di una terza parte ([100]). Inoltre, ai sensi della notifica n. 2021-1 sulle norme supplementari per l'interpretazione e l'applicazione della legge sulla protezione delle informazioni personali, la persona fisica interessata deve ricevere notifica della divulgazione. In situazioni eccezionali tale notifica può essere differita in particolare se e per tutto il tempo per il quale la notifica comprometterebbe un'indagine penale in corso o potrebbe minacciare la vita o ledere l'incolumità di un'altra persona, laddove tali diritti o interessi prevalgano manifestamente sui diritti dell'interessato ([101]).

Nel 2016 la Corte suprema ha confermato che la fornitura volontaria di dati relativi alle comunicazioni da parte di operatori economici di telecomunicazioni in assenza di un mandato ai sensi della legge sulle imprese di telecomunicazione non viola in quanto tale il diritto all'autodeterminazione informativa dell'utente del servizio di telecomunicazione. Allo stesso tempo la Corte ha chiarito una tale violazione si verificherebbe qualora fosse manifestamente evidente che l'agenzia richiedente abbia abusato della sua autorità per richiedere la divulgazione di dati relativi alle comunicazioni, violando in tal modo gli interessi della persona fisica in questione o di una terza parte ([102]). Più in generale, qualsiasi richiesta di divulgazione volontaria da parte di un'autorità di contrasto deve rispettare i principi di liceità, necessità e proporzionalità derivanti dalla costituzione coreana (articolo 12, primo comma, e articolo 37, secondo comma).

([89]) Articolo 13-3, secondo comma, della legge sulle comunicazioni.
([90]) Articolo 13-3, terzo comma, della legge sulle comunicazioni.
([91]) Articolo 13-3, quarto comma, della legge sulle comunicazioni.
([92]) Articolo 13-3, quinto comma, della legge sulle comunicazioni.
([93]) Articolo 13-3, sesto comma, della legge sulle comunicazioni.
([94]) Articolo 83, terzo comma, della legge sulle imprese di telecomunicazione.
([95]) Articolo 2, nono comma, della legge sulle imprese di telecomunicazione.
([96]) Articolo 83, quarto comma, della legge sulle imprese di telecomunicazione.
([97]) Articolo 83, quarto comma, della legge sulle imprese di telecomunicazione.
([98]) Articolo 83, quinto comma, della legge sulle imprese di telecomunicazione.
([99]) Articolo 83, sesto comma, della legge sulle imprese di telecomunicazione.
([100]) Articolo 18, secondo comma, della legge sulla protezione delle informazioni personali.
([101]) Notifica n. 2021-1 della PIPC sulle norme supplementari per l'interpretazione e l'applicazione della legge sulla protezione delle informazioni personali, sezione III, punto 2, sottopunto iii).
([102]) Decisione della Corte suprema n. 2012Da105482, 10 marzo 2016.

2.3. **Vigilanza**

La vigilanza da parte delle autorità di contrasto in materia penale viene attuata attraverso diversi meccanismi, tanto internamente quanto da organismi esterni.

2.3.1. *Controllo interno*

In conformità con l'*Act on Public Sector Audits* (legge sulle attività di revisione nel settore pubblico), le autorità pubbliche sono incoraggiate a istituire un organismo interno che svolga funzioni di controllo interno, incaricato tra l'altro di svolgere il controllo delle legalità ([103]). Ai capi di tali organismi di revisione deve essere garantita l'indipendenza nella misura massima possibile ([104]). Più specificamente, sono nominati dall'esterno dell'autorità competente (ad esempio ex giudici, professori) per un periodo da due a cinque anni e possono essere rimossi dal loro incarico esclusivamente per motivi giustificati (ad esempio quando non sono in grado di svolgere le loro funzioni in ragione di un disturbo mentale o fisico oppure se soggetti ad azioni disciplinari) ([105]). Analogamente i revisori sono nominati sulla base di condizioni specifiche stabilite in tale legge ([106]). Le relazioni di revisione possono comprendere raccomandazioni o richieste di risarcimento o rettifica, nonché ammonimenti e raccomandazioni o richieste di intraprendere un'azione disciplinare ([107]). Tali relazioni sono notificate al capo dell'autorità pubblica soggetto a revisione, nonché al *Board of Audit and Inspection* (BAI, consiglio di revisione e ispezione) (cfr. sezione 2.3.2) entro 60 giorni dal completamento della revisione ([108]). L'autorità interessata deve attuare le misure richieste e riferire i risultati al consiglio di revisione e ispezione ([109]). Inoltre, in genere, i risultati delle revisioni sono messi a disposizione del pubblico ([110]). Il rifiuto o l'ostruzione di controllo interno sono soggetti a sanzioni amministrative pecuniarie ([111]). Nel settore del contrasto penale, per conformarsi alla suddetta legislazione, l'agenzia di polizia nazionale mantiene operativo un sistema di ispettore generale per gestire gli audit interni, anche rispetto a possibili violazioni dei diritti umani ([112]).

2.3.2. *Il consiglio di revisione e ispezione*

Il consiglio di revisione e ispezione (in appresso "*BAI*") può ispezionare le attività delle autorità pubbliche e, sulla base di tali ispezioni, emettere raccomandazioni, richiedere l'adozione di azioni disciplinari o presentare una denuncia penale ([113]). Il BAI si colloca al di sotto del presidente della Repubblica di Corea, ma mantiene uno stato indipendente per quanto concerne i suoi doveri ([114]). Inoltre l'atto che istituisce il BAI impone che a tale consiglio sia concessa indipendenza nella misura massima possibile rispetto alla nomina, alla rimozione dall'incarico e all'organizzazione del suo personale, nonché alla compilazione del suo budget ([115]). Il presidente del BAI è nominato dal presidente della Repubblica di Corea, con il consenso dell'Assemblea nazionale ([116]). I sei commissari rimanenti sono nominati dal presidente della Repubblica di Corea, su raccomandazione del presidente del consiglio, per un termine di quattro anni ([117]). I commissari (compreso il presidente) devono soddisfare qualifiche specifiche stabilite dalla legge ([118]) e possono essere rimossi dall'incarico soltanto in caso di messa in stato di accusa, condanna a una pena detentiva o incapacità di adempiere le proprie funzioni in ragione di una debolezza mentale o fisica prolungata ([119]). Inoltre ai commissari è vietato partecipare alle attività politiche e detenere contemporaneamente incarichi in seno all'Assemblea nazionale, ad agenzie amministrative, a organizzazioni soggette a revisione e ispezione da parte del BAI oppure assumere qualsiasi altro incarico o qualsiasi altra posizione che comporti una remunerazione ([120]).

Il BAI conduce una revisione generale su base annuale, ma può altresì effettuare revisioni specifiche in merito a questioni di interesse speciale. Il BAI può richiedere la presentazione di documenti nel corso di un'ispezione e richiedere la partecipazione di persone fisiche ([121]). Nel contesto di una revisione, il BAI esamina le entrate e le spese dello Stato, ma vigila anche sul rispetto a livello generale dei doveri delle autorità pubbliche e dei funzionari pubblici al fine di

([103]) Articoli 3 e 5 della legge sulle attività di revisione nel settore pubblico.
([104]) Articolo 7 della legge sulle attività di revisione nel settore pubblico.
([105]) Articoli da 8 a 11 della legge sulle attività di revisione nel settore pubblico.
([106]) Articoli 16 e seguenti della legge sulle attività di revisione nel settore pubblico.
([107]) Articolo 23, secondo comma, della legge sulle attività di revisione nel settore pubblico.
([108]) Articolo 23, primo comma, della legge sulle attività di revisione nel settore pubblico.
([109]) Articolo 23, terzo comma, della legge sulle attività di revisione nel settore pubblico.
([110]) Articolo 26 della legge sulle attività di revisione nel settore pubblico.
([111]) Articolo 41 della legge sulle attività di revisione nel settore pubblico.
([112]) Cfr. in particolare le divisioni sotto il direttore generale per la revisione e l'ispezione: https://www.police.go.kr/eng/knpa/org/org01.jsp.
([113]) Articolo 24 e articoli da 31 a 35 della *Board of Audit and Inspection Act* (legge sul consiglio di revisione e ispezione, in appresso: "*legge sul BAI*").
([114]) Articolo 2, primo comma, della legge sul BAI.
([115]) Articolo 2, secondo comma, della legge sul BAI.
([116]) Articolo 4, primo comma, della legge sul BAI.
([117]) Articolo 5, primo comma, e articolo 6 della legge sul consiglio di revisione.
([118]) Ad esempio pubblico ministero o avvocato per almeno dieci anni, aver lavorato come funzionario pubblico o professore oppure aver occupato una posizione di livello superiore presso un'università per almeno otto anni, oppure aver lavorato per almeno dieci anni in una società quotata in borsa o un'istituzione a partecipazione statale (di cui almeno cinque anni in veste di alto dirigente) (cfr. articolo 7 della legge sul BAI).
([119]) Articolo 8 della legge sul BAI.
([120]) Articolo 9 della legge sul BAI.
([121]) Cfr. ad esempio articolo 27 della legge sul BAI.

migliorare il funzionamento della pubblica amministrazione ([122]). La sua vigilanza si estende pertanto oltre gli aspetti di bilancio e comprende anche un controllo della legalità.

2.3.3. *L'Assemblea nazionale*

L'Assemblea nazionale può indagare e ispezionare le autorità pubbliche ([123]). Nel corso di un'indagine o di un'ispezione, l'Assemblea nazionale può richiedere la divulgazione di documenti e imporre la comparizione di testimoni ([124]). Chiunque abbia commesso spergiuro durante un'inchiesta dell'Assemblea nazionale è soggetto a sanzioni penali (pena detentiva per un massimo di dieci anni) ([125]). Il processo e i risultati delle ispezioni possono essere resi pubblici ([126]). Qualora l'Assemblea nazionale rilevi un'attività illecita o impropria, può richiedere che l'autorità pubblica pertinente intraprenda misure correttive, compreso il riconoscimento di un risarcimento, l'adozione di azioni disciplinari e il miglioramento delle procedure interne di tale autorità ([127]). A seguito di tale richiesta, l'autorità deve agire senza indugio e riferire all'Assemblea nazionale in merito all'esito ([128]).

2.3.4. *La Commissione per la protezione delle informazioni personali*

La *Personal Information Protection Commission* (Commissione per la protezione delle informazioni personali, in appresso: "*PIPC*") esercita una vigilanza sul trattamento di informazioni personali da parte delle autorità di contrasto in materia penale in linea con la legge sulla protezione delle informazioni personali. Inoltre, ai sensi dell'articolo 7-8, terzo e quarto comma, dell'articolo 7-9, quinto comma, della legge sulla protezione delle informazioni personali, la vigilanza della PIPC copre anche possibili violazioni delle norme che definiscono limitazioni e garanzie rispetto alla raccolta di informazioni personali, comprese quelle contenute nelle leggi specifiche che disciplinano la raccolta di elementi di prova (elettronici) per finalità di contrasto penale (cfr. sezione 2.2). Dati i requisiti di cui all'articolo 3, primo comma, della legge sulla protezione delle informazioni personali per la raccolta lecita ed equa di tali informazioni, qualsiasi simile violazione costituisce anche una violazione di detta legge, una circostanza questa che consente alla PIPC di svolgere un'indagine e adottare misure correttive ([129]).

Nell'esercizio della propria vigilanza la PIPC ha accesso a tutte le informazioni pertinenti ([130]). La PIPC può fornire consulenza alle autorità di contrasto al fine di migliorare il livello della protezione delle informazioni personali delle loro attività di trattamento, imporre misure correttive (ad esempio sospensione del trattamento dei dati o adozione delle misure necessarie per proteggere le informazioni personali) o consigliare all'autorità di adottare azioni disciplinari ([131]). Infine per talune violazioni della legge sulla protezione delle informazioni personali, quali l'uso illecito o la divulgazione illeciti a terzi di informazioni personali oppure il trattamento illecito di informazioni sensibili, sono previste sanzioni penali ([132]). A tale riguardo, la PIPC può rinviare la questione all'agenzia investigativa competente (incluso un pubblico ministero) ([133]).

2.3.5. *La Commissione nazionale per i diritti umani*

La *National Human Rights Commission* (in appresso: *NHRC*, commissione nazionale per i diritti umani), un organismo indipendente incaricato di tutelare e promuovere i diritti fondamentali ([134]), ha il potere di indagare e porre rimedio a violazioni degli articoli da 10 a 22 della costituzione che comprendono i diritti alla tutela della vita privata e alla vita privata della corrispondenza. La NHRC è costituita da 11 commissari, nominati su proposta da parte dell'Assemblea nazionale (quattro), del presidente della Repubblica di Corea (quattro) e del giudice capo della Corte suprema (tre) ([135]). Per essere nominato un commissario deve: 1) aver prestato servizio per almeno dieci anni presso un'università o un istituto di ricerca autorizzato, quanto meno come professore associato; 2) aver prestato servizio come giudice, pubblico ministero o avvocato per almeno dieci anni; 3) essere stato impegnato in attività a tutela dei diritti umani per almeno dieci anni (ad esempio per un'organizzazione non governativa senza scopo di lucro o un'organizzazione internazionale); oppure 4) essere stato raccomandato da gruppi della società civile ([136]). Il presidente della commissione è nominato dal

([122]) Articoli 20 e 24 della legge sul BAI.
([123]) Articolo 128 della legge sull'assemblea nazionale e articoli 2, 3 e 15 della legge sull'ispezione e sull'indagine dell'amministrazione dello Stato. Rientrano in tale contesto ispezioni annuali di questioni governative nel loro complesso e indagini su questioni specifiche.
([124]) Articolo 10, primo comma, della legge sull'ispezione e sull'indagine dell'amministrazione dello Stato. Cfr. anche articoli 128 e 129 della legge sull'assemblea nazionale.
([125]) Articolo 14 della legge sulla testimonianza, sulla valutazione, ecc. dinanzi l'Assemblea nazionale.
([126]) Articolo 12-2 della legge sull'ispezione e sull'indagine dell'amministrazione dello Stato.
([127]) Articolo 16, secondo comma, della legge sull'ispezione e sull'indagine dell'amministrazione dello Stato.
([128]) Articolo 16, terzo comma, della legge sull'ispezione e sull'indagine dell'amministrazione dello Stato.
([129]) Cfr. notifica n. 2021-1 della PIPC sulle norme supplementari per l'interpretazione e l'applicazione della legge sulla protezione delle informazioni personali.
([130]) Articolo 63 della legge sulla protezione delle informazioni personali.
([131]) Articolo 61, secondo comma, articolo 65, primo e secondo comma e articolo 64, quarto comma, della legge sulla protezione delle informazioni personali.
([132]) Articoli da 70 a 74 della legge sulla protezione delle informazioni personali.
([133]) Articolo 65, primo comma, della legge sulla protezione delle informazioni personali.
([134]) Articolo 1 della legge sulla commissione per i diritti umani (di seguito "*legge sulla NHRC*").
([135]) Articolo 5, primo e secondo comma, della legge sulla NHRC.
([136]) Articolo 5, terzo comma, della legge sulla NHRC.

presidente della Repubblica di Corea tra i commissari e deve essere confermato dall'Assemblea nazionale ([137]). I commissari (compreso il presidente della commissione) sono nominati per un termine rinnovabile di tre anni e possono essere rimossi dall'incarico soltanto se vengono condannati a una pena detentiva o non sono più in grado di adempiere le loro funzioni in ragione di una debolezza fisica o mentale prolungata (nel qual caso due terzi dei commissari devono concordate con la rimozione dall'incarico) ([138]). Ai commissari della NHRC è vietato detenere un incarico simultaneo in seno all'Assemblea nazionale, a consigli locali, a qualsiasi amministrazione statale o governativa locale ([139]).

La NHRC può avviare un'indagine di propria iniziativa o sulla base di un'istanza presentata da una persona fisica. Nel contesto di una sua indagine, la NHRC può richiedere la presentazione di materiali pertinenti, condurre ispezioni e convocare persone fisiche affinché prestino testimonianza ([140]). A seguito di un'indagine, la NHRC può emettere raccomandazioni destinate a migliorare o rettificare politiche e prassi specifiche e può renderle pubbliche ([141]). Le autorità pubbliche devono notificare alla NHRC un piano per attuare tali raccomandazioni entro 90 giorni dal ricevimento ([142]). Inoltre, in caso di mancata attuazione delle raccomandazioni, l'autorità interessata deve informare la commissione ([143]). La NHRC può a sua volta rivelare tale incapacità all'Assemblea nazionale e/o renderla pubblica. In generale le autorità pubbliche si conformano alle raccomandazioni della NHRC e sono fortemente incentivate a procedere in tal senso dato che la loro attuazione viene presa in considerazione nel contesto della valutazione generale condotta dall'*Office for Government Policy Coordination* (Ufficio per il coordinamento delle politiche di governo), sotto l'egida dell'ufficio del primo ministro.

2.4. **Ricorso individuale**

2.4.1. *Meccanismi di ricorso a disposizione ai sensi della legge sulla protezione delle informazioni personali*

Le persone fisiche possono esercitare i loro diritti di accesso, rettifica, cancellazione e sospensione ai sensi della legge sulla protezione delle informazioni personali rispetto a tali informazioni trattate da autorità di contrasto in materia penale. L'accesso può essere richiesto direttamente dall'autorità pertinente oppure indirettamente tramite la PIPC ([144]). L'autorità competente può limitare o negare l'accesso soltanto se ciò è previsto dalla legge, qualora ciò possa costituire una minaccia per la vita o l'incolumità di una terza parte oppure possa risultare in una violazione ingiustificata di interessi patrimoniali o di altra natura di un'altra persona (ossia laddove gli interessi dell'altra persona prevalgano su quelli della persona fisica che effettua la richiesta) ([145]). Se viene negata una richiesta di accesso, la persona fisica deve essere informata dei motivi sottostanti e delle modalità di impugnazione ([146]). Analogamente una richiesta di correzione o cancellazione può essere negata laddove ciò sia previsto in altre leggi, nel qual caso la persona fisica deve essere informata delle ragioni sottostanti e della possibilità di impugnare la decisione ([147]).

Per quanto concerne il ricorso, le persone fisiche possono presentare un reclamo presso la PIPC, anche attraverso il call centre per la tutela della vita privata gestito dall'agenzia coreana per la sicurezza e internet ([148]). Inoltre una persona fisica può ottenere la mediazione attraverso il *Personal Information Dispute Mediation Committee* (comitato di mediazione per le controversie sulle informazioni personali) ([149]). Tali mezzi di ricorso sono disponibili in caso di possibili violazioni tanto delle norme contenute in leggi specifiche che definiscono limitazioni e garanzie rispetto alla raccolta di informazioni personali (sezione 2.2) quanto della legge sulla protezione delle informazioni personali. Inoltre le persone fisiche possono impugnare le decisioni o l'inazione della PIPC ai sensi della legge sui contenziosi amministrativi (cfr. sezione 2.4.3).

([137]) Articolo 5, quinto comma della legge sulla NHRC.
([138]) Articolo 7, primo comma, e articolo 8, della legge sulla NHRC.
([139]) Articolo 10 della legge sul NHRC.
([140]) Articolo 36 della legge sul NHRC. Conformemente all'articolo 36, settimo comma, di tale legge, la presentazione di materiali od oggetti può essere respinta qualora sia suscettibile di compromettere la riservatezza dello Stato, qualora possa avere un effetto sostanziale sulla sicurezza dello Stato o sulle relazioni diplomatiche oppure qualora costituisca un grave ostacolo a un'indagine penale o un procedimento in sospeso. In tali casi la commissione può richiedere ulteriori informazioni al capo dell'agenzia pertinente (che deve rispettare la buona fede) ove necessario per riesaminare l'eventualità o meno che il rifiuto di fornire le informazioni sia giustificato.
([141]) Articolo 25, primo comma, della legge sul NHRC.
([142]) Articolo 25, terzo comma, della legge sulla NHRC.
([143]) Articolo 25, quarto comma, della legge sulla NHRC.
([144]) Articolo 35, secondo comma, della legge sulla protezione delle informazioni personali.
([145]) Articolo 35, quarto comma, della legge sulla protezione delle informazioni personali.
([146]) Articolo 42, secondo comma, del decreto di applicazione della PIPA.
([147]) Articolo 36, primo e secondo comma, della legge sulla protezione delle informazioni personali e articolo 43, terzo comma, del decreto di applicazione di tale legge.
([148]) Articolo 62 della legge sulla protezione delle informazioni personali.
([149]) Articoli da 40 a 50 della legge sulla protezione delle informazioni personali e articoli da 48-2 a 57 del decreto di applicazione di tale legge.

2.4.2. *Ricorso dinanzi la commissione nazionale per i diritti umani*

La NHRC gestisce i reclami presentati da persone fisiche (cittadini coreani e stranieri) riguardanti violazioni dei diritti umani commesse da autorità pubbliche ([150]). Ai fini della presentazione di un reclamo alla NHRC le persone fisiche non devono soddisfare alcun requisito specifico ([151]). Di conseguenza un reclamo verrà gestito dalla NHRC anche se la persona fisica interessata non è in grado di dimostrare, nella fase di ammissibilità, a livello fattuale un pregiudizio subito. Nel contesto della raccolta di dati personali per finalità di contrasto penale, una persona fisica non sarebbe pertanto tenuta a dimostrare che le sue informazioni personali sono state effettivamente oggetto di accesso da parte delle autorità pubbliche coreane affinché un reclamo sia ammissibile dinanzi la NHRC. Una persona fisica può altresì richiedere di risolvere il reclamo attraverso una mediazione ([152]).

Per indagare in merito a un reclamo, la NHRC può avvalersi dei suoi poteri di indagine, anche richiedendo la presentazione di materiali pertinenti, conducendo ispezioni e citando persone fisiche a comparire in veste di testimoni ([153]). Laddove da un'indagine emerga che si è verificata una violazione delle leggi pertinenti, la NHRC può raccomandare l'attuazione di misure di riparazione o la rettifica o il miglioramento di qualsiasi statuto, istituzione, politica o prassi pertinente ([154]). Le misure di riparazione proposte possono comprendere la mediazione, la cessazione della violazione dei diritti umani, il risarcimento dei danni nonché misure per prevenire la reiterazione delle medesime violazioni o di violazioni analoghe ([155]). In caso di raccolta illecita di informazioni personali ai sensi delle norme vigenti, le misure di riparazione possono comprendere la cancellazione delle informazioni personali raccolte. Qualora si ritenga altamente probabile che la violazione sia in corso e si consideri probabile che, se non affrontata, la stessa possa determinare danni cui sarebbe difficile porre rimedio, la NHRC può adottare misure di riparazione urgenti ([156]).

Sebbene la NHRC non abbia il potere di imporre misure, le sue decisioni (ad esempio una decisione di non continuare l'indagine su un reclamo) ([157]) e le sue raccomandazioni possono essere impugnate dinanzi gli organi giurisdizionali coreani ai sensi della legge sui contenziosi amministrativi (cfr. sezione 2.4.3) ([158]). Inoltre se dalle constatazioni della NHRC emerge che i dati personali sono stati raccolti in maniera illecita da un'autorità pubblica, una persona fisica può cercare ulteriore riparazione promuovendo un'azione dinanzi gli organi giurisdizionali coreani contro tale autorità pubblica, ad esempio impugnando la raccolta ai sensi della legge sui contenziosi amministrativi, depositando un reclamo costituzionale ai sensi della legge sulla Corte costituzionale oppure richiedendo il risarcimento dei danni ai sensi della legge sul risarcimento da parte dello Stato (cfr. sezione 2.4.3).

2.4.3. *Ricorso giurisdizionale*

Le persone fisiche possono invocare le limitazioni e le garanzie descritte nelle sezioni che precedono per ottenere risarcimento dinanzi gli organi giurisdizionali coreani in diversi modi.

Innanzitutto, conformemente al codice di procedura penale, la persona fisica in questione e il suo legale possono essere presenti quando viene data esecuzione a un mandato di perquisizione o di sequestro e possono quindi sollevare un'obiezione nel momento in cui il mandato viene eseguito ([159]). Il codice di procedura penale prevede inoltre un cosiddetto meccanismo di "quasi-reclamo", che consente alle persone fisiche di presentare un'istanza all'organo giurisdizionale competente contenente una richiesta di annullamento o modifica di una disposizione resa da un pubblico ministero o un funzionario di polizia riguardante un sequestro ([160]). Ciò consente alle persone fisiche di impugnare le misure adottate per dare esecuzione a un mandato di sequestro.

([150]) Sebbene l'articolo 4 della legge sulla NHRC faccia riferimento ai cittadini e agli stranieri residenti nella Repubblica di Corea, il termine "residente" rispecchia un concetto di competenza giurisdizionale piuttosto che di territorio. Di conseguenza se i diritti fondamentali di uno straniero al di fuori della Corea sono violati dalle istituzioni nazionali in Corea, la persona fisica in questione può promuovere un reclamo presso la NHRC. Cfr. ad esempio la domanda corrispondente nella pagina delle domande frequenti della NHRC, disponibile all'indirizzo: https://www.humanrights.go.kr/site/program/board/basicboard/list?boardtypeid=7025&menuid=002004005001&pagesize=10&currentpage=2. Ciò si verificherebbe qualora le autorità pubbliche coreane avessero accesso in maniera illecita ai dati personali di uno straniero trasferiti in Corea.

([151]) In linea di massima un reclamo va depositato entro un anno dalla violazione, ma la NHRC può comunque decidere di indagare in merito a un reclamo che viene presentato trascorso tale termine fintantoché non sia scaduto il termine di prescrizione stabilito dal diritto penale o civile (articolo 32, primo comma, punto 4, della legge sulla NHRC).

([152]) Articoli 42 e seguenti della legge sulla NHRC.

([153]) Articoli 36 e 37 della legge sul NHRC.

([154]) Articolo 44 della legge sul NHRC.

([155]) Articolo 42, quarto comma, della legge sulla NHRC.

([156]) Articolo 48 della legge sul NHRC.

([157]) Ad esempio qualora eccezionalmente la NHRC non fosse in grado di ispezionare determinati materiali o strutture perché riguardano segreti di Stato passibili di avere un effetto sostanziale sulla sicurezza dello Stato o sulle relazioni diplomatiche, oppure qualora l'ispezione costituisse un grave ostacolo a un'indagine penale o un procedimento in sospeso (cfr. nota 166), e qualora ciò impedisse alla NHRC di svolgere l'indagine necessaria per valutare i meriti dell'istanza pervenuta, tale commissione informerà la persona fisica dei motivi per i quali la denuncia è stata respinta, in conformità con l'articolo 39 della legge sulla NHRC. In tal caso la persona fisica potrebbe impugnare la decisione della NHRC ai sensi della legge sui contenziosi amministrativi.

([158]) Cfr. ad esempio decisione dell'Alta Corte di Seoul 2007Nu27259, 18 aprile 2008, confermata dalla decisione della Corte suprema 2008Du7854 del 9 ottobre 2008; Decisione dell'Alta Corte di Seoul 2017Nu69382, 2 febbraio 2018.

([159]) Articoli 121 e 219 del codice di procedura penale.

([160]) Articolo 417 del codice di procedura penale, in combinato disposto con l'articolo 414, secondo comma, del codice di procedura penale. Cfr. anche decisione della Corte suprema n. 97Mo66, 29 settembre 1997.

Inoltre le persone fisiche possono ottenere un risarcimento per danni adendo gli organi giurisdizionali coreani. Ai sensi della legge sul risarcimento da parte dello Stato, le persone fisiche possono presentare domanda di risarcimento dei danni causati da funzionari pubblici nello svolgimento delle loro funzioni ufficiali in violazione della legge ([161]). Una tale richiesta può essere depositata presso un "consiglio per il risarcimento" specializzato oppure direttamente adendo gli organi giurisdizionali coreani ([162]). Se la vittima è un cittadino straniero, la legge sul risarcimento da parte dello Stato si applica nella misura in cui il paese di origine di tale cittadino garantisce allo stesso modo un risarcimento da parte dello Stato a favore di cittadini coreani ([163]). Secondo la giurisprudenza, tale condizione è soddisfatta se i requisiti per richiedere un risarcimento nell'altro paese "*non sono significativamente sbilanciati tra la Corea e l'altro paese*" e "*non sono in genere più severi rispetto a quelli determinati dalla Corea, senza alcuna differenza materiale e sostanziale*" ([164]). Il codice civile disciplina la responsabilità dello Stato in relazione al risarcimento e, di conseguenza, la responsabilità dello Stato copre anche i danni non materiali (ad esempio la sofferenza mentale) ([165]).

Per le violazioni delle norme sulla protezione dei dati, ai sensi della legge sulla protezione delle informazioni personali sono previsti mezzi di ricorso. Ai sensi dell'articolo 39 della legge sulla protezione delle informazioni personali, qualsiasi persona fisica che subisca un danno a causa di una violazione della legge sulla protezione delle informazioni personali o di perdita, furto, divulgazione, falsificazione, modifica o danneggiamento delle sue informazioni personali può ottenere un risarcimento dei danni adendo gli organi giurisdizionali. Non esiste alcun requisito analogo di reciprocità come nel quadro della legge sul risarcimento da parte dello Stato.

Oltre al risarcimento dei danni, si possono ottenere misure di riparazione amministrative nei confronti di azioni od omissioni di agenzie amministrative ai sensi della legge sui contenziosi amministrativi. Qualsiasi persona fisica può impugnare una disposizione (ossia l'esercizio o il rifiuto di esercizio di un potere pubblico in un caso specifico) oppure un'omissione (la prolungata mancata adozione da parte di un'agenzia amministrativa di una certa disposizione contraria a un obbligo giuridico a procedere in tale senso), che può portare alla revoca/modifica di una disposizione illegale, una constatazione di nullità (ossia una constatazione secondo la quale la disposizione non ha effetto giuridico o non esiste nell'ordinamento giuridico) oppure una constatazione del fatto che un'omissione è illegale ([166]). Per poter impugnare una disposizione amministrativa, quest'ultima deve avere un impatto diretto sui diritti e sugli obblighi civili ([167]). Ciò comprende misure per raccogliere dati personali, direttamente (ad esempio mediante intercettazione delle comunicazioni) oppure tramite una richiesta di divulgazione vincolante (ad esempio rivolta a un fornitore di servizi).

Le domande di cui sopra possono essere promosse innanzitutto dinanzi le commissioni di ricorso amministrativo istituite in seno a determinate autorità pubbliche (ad esempio il NIS o la NHRC) oppure dinanzi la *Central Administrative Appeals Commission* (commissione centrale per gli appelli amministrativi) istituita in seno alla commissione anticorruzione e per i diritti civili ([168]). Tale ricorso amministrativo mette a disposizione una procedura alternativa, più informale, per impugnare una disposizione o un'omissione di un'autorità pubblica. Tuttavia è possibile proporre reclamo anche direttamente presso gli organi giurisdizionali coreani ai sensi della legge sui contenziosi amministrativi.

Una richiesta di revoca/modifica di una disposizione ai sensi della legge sui contenziosi amministrativi può essere depositata da qualsiasi persona che abbia un interesse giuridico nel cercare di ottenere la revoca/modifica, oppure di ripristinare i suoi diritti mediante revoca/modifica nel caso in cui la disposizione non abbia più effetto ([169]). Analogamente il contenzioso per ottenere la constatazione di nullità può essere avviato da una persona che abbia un interesse giuridico a procedere in tal senso affermazione, mentre un contenzioso volto a ottenere la constatazione dell'illegittimità di un'omissione può essere avviato da qualsiasi persona che abbia effettuato una richiesta per una disposizione e abbia un interesse giuridico a cercare di ottenere la constatazione dell'illegalità dell'omissione ([170]). Secondo la giurisprudenza della Corte suprema, la nozione di "interesse giuridico" è interpretata come un "interesse protetto dalla legge", ossia un interesse diretto e specifico protetto da leggi e normative sulle quali si basano disposizioni amministrative (il che significa interessi non generali, indiretti e astratti di interessi del pubblico) ([171]). Le persone fisiche hanno pertanto un tale interesse giuridico in caso di violazione delle limitazioni e delle garanzie relative alla raccolta dei loro dati personali per finalità di contrasto penale (a norma di leggi specifiche o della legge sulla protezione delle informazioni personali). Una sentenza definitiva ai sensi della legge sui contenziosi amministrativi è vincolante sulle parti ([172]).

Una richiesta di revoca/modifica di una disposizione e una richiesta di constatazione dell'illegalità di un'omissione deve essere depositata entro 90 giorni dalla data in cui la persona fisica viene a conoscenza della disposizione/dell'omissione e in linea di

([161]) Articolo 2, primo comma, della legge sul risarcimento da parte dello Stato.
([162]) Articoli 9 e 12 della legge sul risarcimento da parte dello Stato. Tale legge istituisce i consigli distrettuali (presieduti dal vice pubblico ministero del corrispondente ufficio della procura), un consiglio centrale (presieduto dal vice ministro della Giustizia) e un consiglio speciale (presieduto dal vice ministro della Difesa nazionale e competente per le richieste di risarcimento di danni causati da personale militare o dipendenti civili delle forze armate). Le richieste di risarcimento sono in linea di principio gestite dai consigli distrettuali che, in determinate circostanze, devono rinviare i casi al consiglio centrale/speciale, ad esempio se il risarcimento supera un determinato importo o nel caso in cui una persona fisica presenti una domanda di nuova deliberazione. Tutti i consigli sono costituiti da membri nominati dal ministro della Giustizia (ad esempio tra i funzionari pubblici del ministero della Giustizia, degli ufficiali giudiziari, degli avvocati e delle persone che hanno esperienza in relazione al risarcimento da parte dello Stato) e sono soggetti a norme specifiche in materia di conflitti di interesse (cfr. articolo 7 del decreto di applicazione della legge sul risarcimento da parte dello Stato).
([163]) Articolo 7 della legge sul risarcimento da parte dello Stato.
([164]) Decisione della Corte suprema n. 2013Da208388, 11 giugno 2015.
([165]) Cfr. articolo 8 della legge sul risarcimento da parte dello Stato, nonché articolo 751 del codice civile.
([166]) Articoli 2 e 4 della legge sui contenziosi amministrativi.
([167]) Decisione della Corte suprema 98Du18435, 22 ottobre 1999, decisione della Corte suprema 99Du1113, 8 settembre 2000 e decisione della Corte suprema 2010Du3541 del 27 settembre 2012.
([168]) Articolo 6 della legge sui ricorsi amministrativi e articolo 18, primo comma, della legge sui contenziosi amministrativi.
([169]) Articolo 12 della legge sui contenziosi amministrativi.
([170]) Articoli 35 e 36 della legge sui contenziosi amministrativi.
([171]) Decisione della Corte suprema n. 2006Du330, 26 marzo 2006.
([172]) Articolo 30, primo comma, della legge sui contenziosi amministrativi.

principio, entro e non oltre un anno dalla data in cui viene emessa la disposizione o in cui si è verificata l'omissione, fatto salvo il caso in cui vi siano motivi giustificabili ([173]). Secondo la giurisprudenza della Corte suprema, la nozione di "motivi giustificabili" va interpretata in senso ampio e richiede di valutare se sia socialmente accettabile consentire un reclamo tardivo, in considerazione di tutte le circostanze del caso ([174]). Ad esempio ciò comprende (a titolo esemplificativo ma non esaustivo) motivi di ritardo non imputabili alla parte interessata (ossia imputabili a circostanze al di fuori del controllo della parte che presenta il reclamo, ad esempio, nel caso in cui tale parte non abbia ricevuto notifica della raccolta delle sue informazioni personali) oppure cause di forza maggiore (ad esempio un disastro naturale, una guerra).

Infine le persone fisiche possono altresì promuovere un reclamo costituzionale presso la Corte costituzionale ([175]). Ai sensi della legge sulla Corte costituzionale, qualsiasi persona i cui diritti fondamentali garantiti dalla costituzione siano violati dall'esercizio o dal mancato esercizio del potere governativo (escludendo le sentenze di organi giurisdizionali) possono richiedere l'esame di un reclamo costituzionale. Se sono disponibili altri mezzi di ricorso, occorre che vengano esperiti prima di adire la Corte costituzionale. Secondo la giurisprudenza della Corte costituzionale, i cittadini stranieri possono presentare un reclamo costituzionale nella misura in cui i loro diritti fondamentali siano riconosciuti nel contesto della costituzione coreana (cfr. spiegazioni di cui alla sezione 1.1) ([176]). I reclami costituzionali devono essere depositati entro 90 giorni dal momento in cui una persona fisica viene a conoscenza della violazione ed entro un anno dal verificarsi di quest'ultima. Dato che la procedura di cui alla legge sui contenziosi amministrativi si applica a un contenzioso ai sensi della legge sulla Corte costituzionale ([177]), un reclamo è comunque ricevibile qualora vi siano "motivi giustificabili", come interpretati in conformità con la giurisprudenza della Corte suprema di cui sopra.

Qualora sia necessario esperire prima altri mezzi di ricorso, un reclamo costituzionale deve essere depositato entro 30 giorni dalla decisione finale in merito a un tale mezzo di ricorso ([178]). La Corte costituzionale può invalidare l'esercizio del potere governativo che ha causato l'infrazione o confermare che una determinata inazione è incostituzionale ([179]). In tal caso, l'autorità competente è tenuta ad adottare misure per conformarsi alla decisione della Corte.

3. ACCESSO DA PARTE DELLE PUBBLICHE AMMINISTRAZIONI PER FINALITÀ DI SICUREZZA NAZIONALE

3.1. Autorità pubbliche competenti nel settore della sicurezza nazionale

La Repubblica di Corea dispone di due agenzie di intelligence dedicate: il NIS e il *Defense Security Support Command* (comando di sostegno alla protezione della difesa). Inoltre anche la polizia e i pubblici ministeri possono raccogliere informazioni personali per finalità di sicurezza nazionale.

Il NIS è istituito dalla legge sul servizio nazionale di intelligence (in appresso: "*legge sul NIS*") e opera direttamente nel contesto della competenza giurisdizionale e del controllo del presidente della Repubblica di Corea ([180]). In particolare il NIS raccoglie, compila e distribuisce informazioni in merito a paesi stranieri (e alla Corea del Nord) ([181]), intelligence relativa al compito di contrastare lo spionaggio (incluso lo spionaggio militare e industriale), il terrorismo e le attività della criminalità internazionale, l'intelligence su determinati tipi di reati rivolti contro la sicurezza pubblica e nazionale (ad esempio insurrezione interna, aggressione straniera) nonché intelligence relativa al compito di assicurare la cibersicurezza nonché prevenire o contrastare attacchi informatici e minacce ([182]). La legge sul NIS, che istituisce tale servizio e ne stabilisce i compiti, fissa altresì i principi generali che inquadrano tutte le sue attività. Come principio generale, il NIS deve mantenere la neutralità politica e proteggere la libertà e i diritti delle persone fisiche ([183]). Il presidente del NIS è competente per lo sviluppo di orientamenti generali che indicano i principi, la portata e le procedure per l'attuazione dei compiti del NIS in relazione alla raccolta e all'uso delle informazioni e deve riferirle all'Assemblea nazionale ([184]). L'Assemblea nazionale (attraverso il suo comitato per l'intelligence) può richiedere la rettifica o l'integrazione degli orientamenti laddove ritenga che siano illegali o ingiusti. Più in generale, nello svolgere le loro funzioni, il direttore e il personale del NIS non possono costringere alcuna istituzione, organizzazione o persona fisica a compiere alcuna azione che non sia tenuta a compiere, né a ostacolare l'esercizio dei diritti di qualsiasi persona, abusando della loro autorità ufficiale ([185]). Inoltre, qualsiasi censura di corrispondenza, intercettazione di telecomunicazioni, raccolta di informazioni

([173]) Articolo 20 della legge sui contenziosi amministrativi. Tale termine si applica anche a un reclamo volto ad ottenere la constatazione dell'illegalità di un'omissione (cfr. articolo 38, secondo comma, della legge sui contenziosi amministrativi).
([174]) Decisione della Corte suprema 90Nu6521, 28 giugno 1991.
([175]) Articolo 68, primo comma, della legge sulla Corte costituzionale.
([176]) Decisione della Corte costituzionale n. 99HeonMa194, 29 novembre 2001.
([177]) Articolo 40 della legge sulla Corte costituzionale.
([178]) Articolo 69 della legge sulla Corte costituzionale.
([179]) Articolo 75, terzo comma, della legge sulla Corte costituzionale.
([180]) Articolo 2 e articolo 4, secondo comma, della legge sul NIS.
([181]) Tale nozione non comprende le informazioni sulle persone fisiche, bensì informazioni di carattere generale sui paesi stranieri (tendenze, sviluppi) e sulle attività di attori statali di paesi terzi.
([182]) Articolo 3, primo comma, della legge sul NIS.
([183]) Articolo 3, primo comma, articolo 6, secondo comma, nonché articoli 11 e 21. Cfr. anche norme sui conflitti di interesse, in particolare gli articoli 10 e 12.
([184]) Articolo 4, secondo comma, della legge sul NIS.
([185]) Articolo 13 della legge sul NIS.

relative all'ubicazione, raccolta di dati di conferma di comunicazioni o registrazione o ascolto di comunicazioni private da parte del NIS deve rispettare la legge sulle comunicazioni, la legge sulle informazioni relative all'ubicazione o il codice di procedura penale ([186]). Qualsiasi abuso di potere o la raccolta di informazioni in violazione di tali leggi è soggetta a sanzioni penali ([187]).

Il comando di sostegno alla protezione della difesa è un'agenzia di intelligence militare, istituita in seno al ministero della Difesa. È competente per questioni di sicurezza nel contesto delle forze armate, per indagini penali militari (soggette alla legge sugli organi giurisdizionali militari) e per l'intelligence militare. In generale il comando di sostegno alla protezione della difesa non svolge attività di sorveglianza su civili, fatto salvo il caso in cui ciò sia necessario ai fini dell'adempimento delle sue funzioni militari. Le persone che possono essere oggetto di indagine sono il personale militare, dipendenti civili di forze armate, persone soggette a formazione militare, persone appartenenti alla riserva militare o attive nel servizio di reclutamento nonché prigionieri di guerra ([188]). Quando raccoglie informazioni sulle comunicazioni per finalità di sicurezza nazionale, il comando di sostegno alla protezione della difesa è soggetto alle limitazioni e alle garanzie stabilite dalla legge sulle comunicazioni e dal suo decreto di applicazione.

3.2. **Basi giuridiche e limitazioni**

La legge sulle comunicazioni, la legge antiterrorismo per la protezione dei cittadini e della sicurezza pubblica (in appresso: "*legge antiterrorismo*") e la legge sulle imprese di telecomunicazione forniscono le basi giuridiche per la raccolta di informazioni personali per finalità di sicurezza nazionale e stabiliscono le limitazioni e le garanzie applicabili ([189]). Tali limitazioni e garanzie, come descritte nelle sezioni che seguono, assicurano che la raccolta e il trattamento di informazioni siano limitati a quanto strettamente necessario ai fini del conseguimento di un obiettivo legittimo. Ciò esclude qualsiasi raccolta in modo massiccio e indiscriminato di informazioni personali per finalità di sicurezza nazionale.

3.2.1. *Raccolta di informazioni relative alle comunicazioni*

3.2.1.1. Raccolta di informazioni relative alle comunicazioni da parte di agenzie di intelligence

3.2.1.1.1. Base giuridica

La legge sulle comunicazioni consente alle agenzie di intelligence di raccogliere i dati relativi alle comunicazioni e impone ai fornitori di servizi di comunicazione di collaborare con le richieste formulate da tali agenzie ([190]). Come descritto nella sezione 2.2.2.1, la legge sulle comunicazioni distingue tra la raccolta del contenuto di comunicazioni (ad esempio "*misure di limitazione delle comunicazioni*" quali misure di "*intercettazione*" o "*censura*" ([191])) e la raccolta di "*dati di conferma di comunicazioni*" ([192]).

La soglia per la raccolta di tali due tipi di informazioni differisce, ma le procedure e le garanzie applicabili sono in larga misura identiche ([193]). La raccolta di dati di conferma di comunicazioni (o metadati) può avvenire con la finalità di prevenire minacce alla sicurezza nazionale ([194]). Una soglia più elevata si applica per l'esecuzione di misure di limitazione delle comunicazioni (ossia per la raccolta del contenuto di comunicazioni), che possono essere adottate soltanto quando si prevede che la sicurezza nazionale sia messa in grave pericolo e quando la raccolta di informazioni è necessaria per prevenire tale pericolo (ossia se esiste un rischio grave per la sicurezza nazionale e la raccolta è necessaria per prevenirlo) ([195]). Inoltre l'accesso al contenuto di comunicazioni può avvenire soltanto come misura di ultima istanza per garantire la sicurezza nazionale e devono essere compiuti sforzi per ridurre al minimo la violazione della vita privata delle comunicazioni ([196]). Anche qualora sia stata ottenuta l'approvazione/l'autorizzazione adeguata, tali misure devono essere cessate immediatamente non appena non sono più necessarie, garantendo così che qualsiasi violazione dei segreti di comunicazione delle persone fisiche sia limitata al minimo ([197]).

3.2.1.1.2. Limitazioni e garanzie che si applicano alla raccolta di informazioni relative alle comunicazioni che coinvolgono almeno un cittadino coreano

La raccolta di informazioni relative alle comunicazioni (contenuto e metadati) nel contesto delle quali una o entrambe le persone fisiche coinvolte nella comunicazione hanno cittadinanza coreana può avvenire soltanto previa autorizzazione

([186]) Articolo 14 della legge sul NIS.
([187]) Articoli 22 e 23 della legge sul NIS.
([188]) Articolo 1 della legge sugli organi giurisdizionali militari.
([189]) Nell'indagare in merito a reati relativi alla sicurezza nazionale, la polizia e il NIS agiscono ai sensi del codice di procedura penale, mentre il comando di sostegno alla protezione della difesa è soggetto alla legge sugli organi giurisdizionali militari.
([190]) Articolo 15-2 della legge sulle comunicazioni.
([191]) Articolo 2, sesto e settimo comma, della legge sulla tutela della vita privata nelle comunicazioni.
([192]) Articolo 2, undicesimo comma, della legge sulle comunicazioni.
([193]) Cfr. anche articolo 13-4, secondo comma, della legge sulle comunicazioni e articolo 37, quarto comma, del decreto di applicazione di tale legge, i quali stipulano che le procedure applicabili alla raccolta del contenuto di comunicazioni si applicano mutatis mutandis alla raccolta di dati di conferma di comunicazioni.
([194]) Articolo 13-4 della legge sulle comunicazioni.
([195]) Articolo 7, primo comma, della legge sulle comunicazioni.
([196]) Articolo 3, secondo comma, della legge sulle comunicazioni.
([197]) Articolo 2 del decreto di applicazione della legge sulle comunicazioni.

da parte di un giudice di alto livello dell'Alta Corte ([198]). La richiesta dell'agenzia di intelligence deve essere formulata per iscritto a un pubblico ministero o a un Ufficio dell'Alta Procura ([199]). Deve indicare i motivi della raccolta (ossia che si prevede che la sicurezza nazionale sia messa in grave pericolo o che la raccolta è necessaria per prevenire minacce alla sicurezza nazionale), unitamente ai materiali a sostegno di tali motivi, nonché stabilire un caso prima facie, così come i dettagli della richiesta (ossia gli obiettivi, le persone fisiche oggetto della misura, la portata, il periodo effettivo della raccolta, nonché le modalità della raccolta e dove si svolgerà) ([200]). Il pubblico ministero/l'Ufficio dell'Alta Procura richiede a sua volta l'autorizzazione a un giudice di alto livello dell'Alta Corte ([201]). Tale giudice può concedere l'autorizzazione scritta soltanto quando ritiene la domanda giustificata e respinge invece una richiesta che considera infondata ([202]). Il mandato specifica il tipo, l'obiettivo, l'oggetto, la portata e il periodo effettivo della raccolta, nonché dove e come potrebbe avvenire ([203]).

Norme specifiche si applicano nel caso in cui la misura miri ad indagare in merito a un atto di cospirazione che minaccia la sicurezza nazionale ed esista un'emergenza che rende impossibile l'espletamento delle procedure di cui sopra ([204]). Quando tali condizioni sono soddisfatte, le agenzie di intelligence possono attuare misure di sorveglianza in assenza dell'approvazione preventiva dell'organo giurisdizionale ([205]). Tuttavia, subito dopo l'esecuzione delle misure di emergenza, l'agenzia di intelligence deve richiedere l'autorizzazione dell'organo giurisdizionale. Laddove tale autorizzazione non venga ottenuta entro 36 ore dal momento in cui vengono adottate le misure, queste ultime devono essere interrotte immediatamente ([206]). La raccolta di informazioni in situazioni di emergenza deve sempre avvenire in conformità con una "dichiarazione di censura/intercettazione di emergenza" e l'agenzia di intelligence che effettua la raccolta deve tenere un registro di tutte le misure di emergenza ([207]).

Nei casi in cui la sorveglianza viene completata in breve tempo, escludendo l'autorizzazione dell'organo giurisdizionale, il capo dell'Ufficio dell'Alta Procura competente deve inviare una notifica di misura di emergenza predisposta dall'agenzia di intelligence al capo dell'organo giurisdizionale competente, che conserva il registro delle misure di emergenza ([208]). Ciò consente all'organo giurisdizionale di esaminare la legalità della raccolta.

3.2.1.1.3. Limitazioni e garanzie che si applicano alla raccolta di informazioni relative alle comunicazioni che coinvolgono soltanto cittadini non coreani

Al fine di raccogliere informazioni sulle comunicazioni che hanno luogo esclusivamente tra cittadini non coreani, le agenzie di intelligence devono ottenere un'approvazione scritta preventiva dal presidente della Repubblica di Corea ([209]). Tali comunicazioni saranno raccolte soltanto per finalità di sicurezza nazionale se rientrano in una delle diverse categorie menzionate, ossia se si tratta di comunicazioni tra funzionari governativi o altre persone fisiche di paesi ostili alla Repubblica di Corea, agenzie, gruppi o cittadini stranieri sospettati di impegnarsi in attività anti-coreane ([210]) o membri di gruppi all'interno della penisola coreana di fatto al di fuori della sovranità della Repubblica di Corea e dei loro gruppi ombrello aventi sede in paesi stranieri ([211]). Viceversa se una parte di una comunicazione è un cittadino coreano e l'altra un cittadino straniero, è necessaria l'approvazione dell'organo giurisdizionale in conformità con la procedura di cui alla sezione 3.2.1.1.1.2.

Il capo di un'agenzia di intelligence deve presentare al direttore del NIS un piano per le misure destinate ad essere adottate ([212]). Il direttore del NIS riesamina l'adeguatezza del piano e, in caso di esito favorevole, lo sottopone al presidente della Repubblica di Corea per approvazione ([213]). Le informazioni che devono essere incluse nel piano sono le stesse richieste per una domanda di autorizzazione da parte dell'organo giurisdizionale a raccogliere informazioni su cittadini coreani (come descritto sopra) ([214]). In particolare deve indicare i motivi della raccolta (ossia che si

([198]) Articolo 7, primo comma, punto 1, della legge sulle comunicazioni. L'organo giurisdizionale competente è l'Alta Corte che ha competenza giurisdizionale per il luogo del domicilio o della sede di una o di entrambe le parti soggette a sorveglianza.
([199]) Articolo 7, terzo comma, del decreto di applicazione della legge sulle comunicazioni.
([200]) Articolo 7, terzo comma, e articolo 6, quarto comma, della legge sulle comunicazioni.
([201]) Articolo 7, quarto comma, del decreto di applicazione della legge sulle comunicazioni. La richiesta del pubblico ministero all'organo giurisdizionale deve indicare i motivi principali di sospetto e, nella misura in cui sono richieste più autorizzazioni contemporaneamente, la loro giustificazione (cfr. articolo 4 del decreto di applicazione della legge sulle comunicazioni).
([202]) Articolo 7, terzo comma, e articolo 6, quinto e nono comma, della legge sulle comunicazioni.
([203]) Articolo 7, terzo comma, e articolo 6, sesto comma, della legge sulle comunicazioni.
([204]) Articolo 8 della legge sulle comunicazioni.
([205]) Articolo 8, primo comma, della legge sulle comunicazioni.
([206]) Articolo 8, secondo comma, della legge sulle comunicazioni.
([207]) Articolo 8, quarto comma, della legge sulle comunicazioni. Cfr. sezione 2.2.2.2 per le misure di emergenza nel contesto delle attività di contrasto.
([208]) Articolo 8, quinto e settimo comma, della legge sulle comunicazioni. Tale notifica deve indicare l'obiettivo, l'oggetto, la portata, il periodo, il luogo di esecuzione e il metodo di sorveglianza nonché i motivi che giustificano la mancata presentazione di una richiesta prima dell'adozione della misura (articolo 8, sesto comma, della legge sulle comunicazioni).
([209]) Articolo 7, primo comma, punto 2, della legge sulle comunicazioni.
([210]) Ciò si riferisce ad attività che minacciano l'esistenza e la sicurezza nazionali, l'ordine democratico o la sopravvivenza e la libertà della popolazione.
([211]) Inoltre, se una parte è una persona descritta all'articolo 7, primo comma, punto 2, della legge sulle comunicazioni e l'altra è sconosciuta o non può essere specificata, si applica la procedura prescritta dall'articolo 7, primo comma, punto 2.
([212]) Articolo 8, primo comma, del decreto di applicazione della legge sulle comunicazioni. Il direttore del NIS è nominato dal presidente della Repubblica di Corea in seguito a conferma da parte del parlamento (articolo 7 della legge sul NIS).
([213]) Articolo 8, secondo comma, del decreto di applicazione della legge sulle comunicazioni.
([214]) Articolo 8, terzo comma, del decreto di applicazione della legge sulle comunicazioni, in combinato disposto con l'articolo 6, quarto comma, di tale legge.

prevede che la sicurezza nazionale sia messa in grave pericolo o che la raccolta è necessaria per prevenire minacce alla sicurezza nazionale), i motivi principali per il sospetto nutrito, oltre ai materiali a sostegno di tali motivi, nonché stabilire un caso prima facie, così come i dettagli della richiesta (ossia gli obiettivi, le persone fisiche oggetto della misura, la portata, il periodo effettivo della raccolta, nonché le modalità della raccolta e dove si svolgerà). Laddove siano richieste più autorizzazioni contemporaneamente, il tenore e i motivi delle stesse ([215]).

In situazioni di emergenza ([216]) occorre ottenere l'approvazione preventiva da parte del ministro a cui fa capo l'agenzia di intelligence pertinente. Tuttavia in questo caso l'agenzia di intelligence deve richiedere l'approvazione del presidente della Repubblica di Corea immediatamente dopo che le misure di emergenza sono state adottate. Se un'agenzia di intelligence non riesce a ottenere l'approvazione entro 36 ore dal momento in cui viene presentata la domanda, la raccolta deve essere interrotta immediatamente ([217]). In tali casi le informazioni raccolte saranno sempre distrutte.

3.2.1.1.4. Limitazioni e garanzie generali

Quando richiedono la cooperazione di soggetti privati, le agenzie di intelligence devono fornire loro il mandato dell'organo giurisdizionale/l'autorizzazione presidenziale o una copia della copertina di una dichiarazione di censura di emergenza, che il soggetto tenuto a cooperare deve conservare nei suoi registri ([218]). I soggetti invitati a divulgare informazioni alle agenzie di intelligence ai sensi della legge sulle comunicazioni possono rifiutarsi di farlo laddove l'autorizzazione o la dichiarazione di censura di emergenza fa riferimento all'identificatore errato (ad esempio un numero di telefono appartenente a una persona fisica diversa da quella identificata). Inoltre le password utilizzate per le comunicazioni non possono essere divulgate in alcun caso ([219]).

Le agenzie di intelligence possono affidare l'attuazione delle misure di limitazione delle comunicazioni o della raccolta di informazioni di conferma di comunicazioni a un ufficio postale o un fornitore di servizi di telecomunicazione (come definito dalla legge sulle imprese di telecomunicazione) ([220]). Tanto l'agenzia di intelligence pertinente quanto il fornitore che riceve una richiesta di cooperazione devono tenere dei registri che indichino la finalità della richiesta di misure, la data di esecuzione o cooperazione, nonché l'oggetto delle misure (ad esempio corrispondenza postale, telefono, posta elettronica) per tre anni ([221]). I fornitori di servizi di telecomunicazioni che forniscono dati di conferma di comunicazioni devono conservare le informazioni sulla frequenza della raccolta nei loro archivi per sette anni e riferire in merito due volte l'anno al ministro della Scienza e delle TIC ([222]).

Le agenzie di intelligence devono riferire al direttore del NIS in merito alle informazioni che hanno raccolto e all'esito dell'attività di sorveglianza ([223]). Per quanto concerne la raccolta di dati di conferma di comunicazioni, si devono tenere registri attestanti la presentazione di una richiesta di tali dati, nonché la richiesta scritta stessa e l'istituzione che vi ha fatto affidamento ([224]).

La raccolta tanto del contenuto di comunicazioni quanto dei dati di conferma di comunicazioni può durare soltanto per un periodo massimo di quattro mesi e deve essere interrotta immediatamente qualora l'obiettivo perseguito venga conseguito nel frattempo ([225]). Se persistono le condizioni per il rilascio dell'autorizzazione, il termine può essere prorogato per un massimo di quattro mesi, con l'autorizzazione dell'organo giurisdizionale o l'approvazione del presidente della Repubblica di Corea. La domanda per l'ottenimento dell'approvazione della proroga delle misure di sorveglianza deve essere presentata per iscritto, indicando i motivi per cui si chiede la proroga e fornendo materiali a sostegno ([226]).

A seconda della base giuridica per la raccolta, le persone fisiche ricevono in genere una notifica quando le loro comunicazioni sono oggetto di raccolta. In particolare, indipendentemente dal fatto che le informazioni raccolte riguardino il contenuto di comunicazioni o dati di conferma di comunicazioni e indipendentemente dal fatto che le informazioni siano state ottenute attraverso la procedura ordinaria o in una situazione di emergenza, il capo dell'agenzia di intelligence deve notificare per iscritto la misura di sorveglianza alla persona fisica interessata entro 30 giorni dalla data in cui la sorveglianza si è conclusa ([227]). La notifica deve includere: 1) il fatto che le informazioni sono state

([215]) Articolo 8, terzo e quarto comma, del decreto di applicazione della legge sulle comunicazioni.
([216]) Ossia nei casi in cui la misura riguarda un atto di cospirazione che minaccia la sicurezza nazionale, in cui non vi è sufficiente tempo per ottenere l'approvazione del presidente della Repubblica di Corea e la mancata adozione di misure di emergenza può compromettere la sicurezza nazionale (articolo 8, ottavo comma, della legge sulle comunicazioni).
([217]) Articolo 8, nono comma, della legge sulle comunicazioni.
([218]) Articolo 9, secondo comma, della legge sulle comunicazioni e articolo 12 del decreto di applicazione della legge sulle comunicazioni.
([219]) Articolo 9, quarto comma, della legge sulle comunicazioni.
([220]) Articolo 13 del decreto di applicazione della legge sulle comunicazioni.
([221]) Articolo 9, terzo comma, della legge sulle comunicazioni e articolo 17, secondo comma, del decreto di applicazione della vita privata nelle comunicazioni. Tale termine non si applica ai dati di conferma di comunicazioni (cfr. articolo 39 del decreto di applicazione della legge sulle comunicazioni).
([222]) Articolo 13, settimo comma, della legge sulle comunicazioni e articolo 39 del decreto di applicazione di tale legge.
([223]) Articolo 18, terzo comma, del decreto di applicazione della legge sulle comunicazioni.
([224]) Articolo 13, quinto comma, e articolo 13-4, terzo comma, della legge sulle comunicazioni.
([225]) Articolo 7, secondo comma, della legge sulle comunicazioni.
([226]) Articolo 7, secondo comma, della legge sulle comunicazioni e articolo 5 del decreto di applicazione della legge sulle comunicazioni.
([227]) Articolo 9-2, terzo comma, della legge sulle comunicazioni. Conformemente all'articolo 13-4 della legge sulle comunicazioni, ciò si applica alla raccolta tanto del contenuto di comunicazioni quanto dei dati di conferma di comunicazioni.

raccolte; 2) l'agenzia che ha dato esecuzione alla misura; e 3) il periodo di esecuzione. Tuttavia qualora sia probabile che metta a rischio la sicurezza nazionale o la vita e la sicurezza fisica della popolazione, tale notifica può essere differita ([228]). La notifica deve essere fornita entro 30 giorni dal momento in cui i motivi per il differimento cessano di esistere ([229]).

Tale requisito di notifica si applica tuttavia soltanto alla raccolta di informazioni laddove almeno una delle parti sia un cittadino coreano. Di conseguenza i cittadini non coreani riceveranno una notifica soltanto nel caso in cui vengano raccolte loro comunicazioni con cittadini coreani. Non si applica quindi alcun requisito di notifica quando vengono raccolte comunicazioni esclusivamente tra cittadini non coreani.

Il contenuto di qualsiasi comunicazione e i dati di conferma di comunicazioni acquisiti attraverso la sorveglianza sulla base della legge sulle comunicazioni possono essere utilizzati soltanto: 1) per l'indagine, l'azione giudiziaria o la prevenzione di determinati reati; 2) per procedimenti disciplinari; 3) per procedimenti giudiziari nel contesto dei quali una parte che partecipa alla comunicazione fa affidamento su tali informazione per promuovere una richiesta di risarcimento dei danni; oppure 4) sulla base di altre leggi ([230]).

3.2.1.2. Raccolta di informazioni relative alle comunicazioni da parte della polizia/di pubblici ministeri per finalità di sicurezza nazionale

La polizia/un pubblico ministero può raccogliere informazioni relative alle comunicazioni (contenuto di comunicazioni e dati di conferma di comunicazioni) per finalità di sicurezza nazionale nel rispetto delle stesse condizioni di cui alla sezione 3.2.1.1. In caso di azione in situazioni di emergenza ([231]), la procedura applicabile è quella che è stata descritta in precedenza rispetto alla raccolta del contenuto di comunicazioni per finalità di contrasto in situazioni di emergenza (ossia articolo 8 della legge sulle comunicazioni).

3.2.2. *Raccolta di informazioni su sospetti terroristi*

3.2.2.1. Base giuridica

La legge antiterrorismo riconosce al direttore del NIS il potere di raccogliere informazioni su sospetti terroristi ([232]). Il concetto di "*sospetto terrorista*" è definito come membro di un gruppo terroristico ([233]), una persona che ha diffuso un gruppo terroristico (promuovendo e diffondendo idee o tattiche di un gruppo terroristico), ha raccolto fondi o fornito contributi al terrorismo ([234]) oppure è impegnato in altre attività di preparazione, cospirazione, propaganda del terrorismo o di istigazione al terrorismo, oppure una persona per la quale vi sono buoni motivi per sospettare che abbia svolto tali attività ([235]). Come norma generale, qualsiasi funzionario pubblico che dia esecuzione alla legge antiterrorismo deve rispettare i diritti fondamentali sanciti nella costituzione coreana ([236]).

La legge antiterrorismo non stabilisce di per sé poteri, limitazioni e garanzie specifici per la raccolta di informazioni su sospetti terroristi, ma fa piuttosto riferimento alle procedure previste da altre normative. Innanzitutto, ai sensi della legge antiterrorismo, il direttore del NIS può raccogliere: 1) informazioni sull'ingresso nella Repubblica di Corea e sull'uscita dal paese; 2) informazioni sulle operazioni finanziarie; e 3) informazioni sulle comunicazioni. A seconda del tipo di informazione ricercata, i requisiti procedurali pertinenti sono fissati rispettivamente nella legge sull'immigrazione e nella legge sulle dogane, nell'ARUSFTI o nella legge sulle comunicazioni ([237]). Per la raccolta di informazioni sull'ingresso in Corea e sull'uscita dal paese, la legge antiterrorismo fa riferimento alle procedure di cui alla legge sull'immigrazione e alla legge sulle dogane. Tuttavia, attualmente, tali atti legislativi non prevedono detti poteri. Per la raccolta di

([228]) Articolo 9-2, quarto comma, della legge sulle comunicazioni.
([229]) Articolo 13-4, secondo comma, e articolo 9-2, sesto comma, della legge sulle comunicazioni.
([230]) Articolo 5, primo e secondo comma, e articoli 12 e 13-5 della legge sulle comunicazioni.
([231]) Ossia nei casi in cui la misura è rivolta contro un atto di cospirazione che minaccia la sicurezza nazionale ed è presente un'emergenza che rende impossibile seguire la procedura di approvazione ordinaria (articolo 8, primo comma, della legge sulle comunicazioni).
([232]) Articolo 9 della legge antiterrorismo.
([233]) Il concetto di "*gruppo terroristico*" è definito come un gruppo di terroristi designato dalle Nazioni Unite (articolo 2, secondo comma, della legge antiterrorismo).
([234]) Il concetto di "*terrorismo*" è definito dall'articolo 2, primo comma, della legge antiterrorismo come una condotta attuata al fine di ostacolare l'esercizio dell'autorità dello Stato, di un'amministrazione locale o di un governo straniero (comprese le amministrazioni locali e le organizzazioni internazionali) oppure al fine di costringere tali soggetti ad assumere un determinato comportamento senza essere tenuti a farlo oppure al fine di minacciare il pubblico. Rientrano in tale contesto: a) l'uccisione di una persona o la messa a rischio della vita di una persona causandole lesioni personali oppure arrestandola, confinandola o rapendola oppure la presa in ostaggio di una persona; b) determinati tipi di condotta rivolti a un aeromobile (ad esempio schianto, dirottamento o danneggiamento di un aeromobile in volo); c) alcuni tipi di condotta relativi a una nave (ad esempio sequestro di una nave o di una struttura marittima in esercizio, distruzione di una nave o di una struttura marittima in esercizio oppure danneggiamento della stessa in misura tale da metterne in pericolo la sicurezza, compreso il danneggiamento del carico presente a bordo di una nave o di una struttura marina in esercizio); d) il collocamento, la detonazione, l'esplosione o l'utilizzo in qualsiasi altro modo di un'arma biochimica, esplosiva o incendiaria o di un dispositivo biochimico, esplosivo o incendiario con l'intenzione di causare decessi, lesioni gravi o danni materiali gravi oppure di ottenere tale effetto su determinati tipi di veicoli o strutture (ad esempio treni, tram, veicoli a motore, parchi pubblici e stazioni, impianti per la fornitura di energia elettrica, gas e telecomunicazioni, ecc.); e) determinati tipi di condotta relativi a materiali nucleari, materiali radioattivi o impianti nucleari (ad esempio lesivi nei confronti di vite umane, dell'incolumità o di interessi patrimoniali oppure la perturbazione della sicurezza pubblica distruggendo un reattore nucleare o manipolando illecitamente materiali radioattivi, ecc.).
([235]) Articolo 2, terzo comma, della legge antiterrorismo.
([236]) Articolo 3, terzo comma, della legge antiterrorismo.
([237]) Articolo 9, primo comma, della legge antiterrorismo.

informazioni relative alle comunicazioni e informazioni sulle operazioni finanziarie, la legge antiterrorismo fa riferimento alle limitazioni e alle garanzie di cui alla legge sulle comunicazioni (aspetto illustrato in maggiore dettaglio in appresso) e all'ARUSFTI (che, come spiegato nella sezione 2.1, non è pertinente al fine della valutazione per la decisione di adeguatezza).

Inoltre, l'articolo 9, terzo comma, della legge antiterrorismo specifica che il direttore del NIS può richiedere a un titolare del trattamento delle informazioni personali ([238]) o a un fornitore di informazioni relative all'ubicazione ([239]) di fornire informazioni personali o informazioni relative all'ubicazione di un sospetto terrorista. Tale possibilità è limitata alle richieste di divulgazione volontaria, a cui i titolari del trattamento delle informazioni personali e i fornitori di informazioni relative all'ubicazione non sono tenuti a rispondere e alle quali possono in ogni caso rispondere soltanto nel rispetto della legge sulla protezione delle informazioni personali e della legge sulle informazioni relative all'ubicazione (cfr. sezione 3.2.2.2).

3.2.2.2. Limitazioni e garanzie che si applicano alla divulgazione volontaria ai sensi della legge sulla protezione delle informazioni personali e della legge sulle informazioni relative all'ubicazione

Le richieste di cooperazione volontaria formulate ai sensi della legge antiterrorismo devono essere limitate a informazioni concernenti sospetti terroristi (cfr. 3.2.2.1). Qualsiasi richiesta del NIS deve rispettare i principi di liceità, necessità e proporzionalità derivanti dalla costituzione coreana (articolo 12, primo comma, e articolo 37, secondo comma) ([240]) nonché i requisiti di cui alla legge sulla protezione delle informazioni personali per la raccolta di tali informazioni (articolo 3, primo comma, della medesima legge; cfr. sezione 1.2). La legge sul NIS specifica inoltre che il servizio nazionale di intelligence non può costringere alcuna istituzione, organizzazione o persona fisica a compiere alcuna azione che non sia tenuta a compiere, né ostacolare l'esercizio dei diritti di qualsiasi persona, abusando della sua autorità ufficiale ([241]).Una violazione di tale divieto può essere soggetta a sanzioni penali ([242]).

I titolari del trattamento delle informazioni personali e i fornitori di informazioni relative all'ubicazione che ricevono richieste dal NIS ai sensi della legge antiterrorismo non sono tenuti a soddisfarle. Possono conformarvisi su base volontaria, ma sono autorizzati a farlo soltanto in conformità con la legge sulla protezione delle informazioni personali e la legge sulle informazioni relative all'ubicazione. Per quanto concerne il rispetto della legge sulla protezione delle informazioni personali, il titolare del trattamento deve tenere conto degli interessi dell'interessato e non può divulgare informazioni qualora ciò sia suscettibile di violare ingiustamente l'interesse della persona fisica o di una terza parte ([243]). Inoltre, ai sensi della notifica n. 2021-1 sulle norme supplementari per l'interpretazione e l'applicazione della legge sulla protezione delle informazioni personali, la persona fisica interessata deve ricevere notifica della divulgazione. In situazioni eccezionali tale notifica può essere differita in particolare se e per tutto il tempo per il quale la notifica comprometterebbe un'indagine penale in corso o potrebbe minacciare la vita o ledere l'incolumità di un'altra persona, laddove tali diritti o interessi prevalgano manifestamente sui diritti dell'interessato ([244]).

3.2.2.3. Limitazioni e garanzie ai sensi della legge sulle comunicazioni

Sulla base della legge antiterrorismo, le agenzie di intelligence possono raccogliere informazioni di comunicazione (contenuto di comunicazioni e dati di conferma di comunicazioni) soltanto se ciò è necessario per le attività di antiterrorismo, ossia per attività legate alla prevenzione e a contrastare il terrorismo. Le procedure della legge sulle comunicazioni di cui alla sezione 3.2.1 si applicano alla raccolta di informazioni relative alle comunicazioni per finalità antiterrorismo.

3.2.3. *Divulgazione volontaria da parte di operatori economici di telecomunicazioni*

Sulla base della legge sulle imprese di telecomunicazione, gli operatori economici di telecomunicazioni possono conformarsi a una richiesta di divulgazione di "dati relativi alle comunicazioni" formulata da un'agenzia di intelligence che intende raccogliere tali informazioni per prevenire una minaccia per la sicurezza nazionale ([245]). Qualsiasi richiesta di questo tipo deve rispettare i principi di liceità, necessità e proporzionalità derivanti dalla costituzione coreana (articolo 12, primo comma, e articolo 37, secondo comma) ([246]) nonché i requisiti di cui alla legge sulla protezione delle informazioni personali per la raccolta di tali informazioni (articolo 3, primo comma, della medesima legge; cfr. sezione 1.2). Inoltre si applicano le stesse limitazioni e garanzie rispetto alle divulgazioni volontarie per finalità di contrasto (cfr. sezione 2.2.3) ([247]).

([238]) Come definito all'articolo 2 della legge sulla protezione delle informazioni personali si tratta ad esempio di un ente pubblico, una persona giuridica, un'organizzazione, una persona fisica, ecc. che tratta informazioni personali direttamente o indirettamente per gestire fascicoli di informazioni personali per finalità commerciali.

([239]) Come definito all'articolo 5 della legge sulla protezione, sull'uso, ecc. delle informazioni relative all'ubicazione (in appresso: "legge sulle informazioni relative all'ubicazione") si tratta ad esempio di chiunque abbia ottenuto l'autorizzazione dalla commissione coreana per le comunicazioni ad esercitare un'attività aziendale incentrata sulle informazioni relative all'ubicazione.

([240]) Cfr. anche l'articolo 3, secondo e terzo comma, della legge antiterrorismo.

([241]) Articolo 11, primo comma, della legge sul NIS.

([242]) Articolo 19 della legge sul NIS.

([243]) Articolo 18, secondo comma, della legge sulla protezione delle informazioni personali.

([244]) Notifica n. 2021-1 della PIPC sulle norme supplementari per l'interpretazione e l'applicazione della legge sulla protezione delle informazioni personali, sezione III, punto 2, sottopunto iii).

([245]) Articolo 83, terzo comma, della legge sulle imprese di telecomunicazione.

([246]) Cfr. anche l'articolo 3, secondo e terzo comma, della legge antiterrorismo.

([247]) In particolare la richiesta deve essere formulata per iscritto e indicarne i motivi, nonché il legame con l'utente pertinente e la portata delle informazioni richieste e il fornitore aziendale di telecomunicazioni deve tenere registri e riferire due volte l'anno al ministro della Scienza e delle TIC.

Un operatore economico di telecomunicazioni non è tenuto a soddisfare tale richiesta, ma può farlo su base volontaria e soltanto in conformità con la legge sulla protezione delle informazioni personali. A tale riguardo agli operatori economici di telecomunicazioni si applicano i medesimi obblighi, anche per quanto concerne la notifica alla persona fisica, che si applicano loro quando ricevono richieste da autorità di contrasto in materia penale, come illustrato in modo più dettagliato nella sezione 2.2.3.

3.3. **Vigilanza**

Diversi organismi vigilano sulle attività delle agenzie di intelligence coreane. La vigilanza sul comando di sostegno alla protezione della difesa è effettuata dal ministero della Difesa nazionale ai sensi della direttiva del ministero sull'attuazione del controllo interno. Il NIS è soggetto a vigilanza da parte dell'esecutivo, dell'Assemblea nazionale e di altri organismi indipendenti, come spiegato in maggior dettaglio in appresso.

3.3.1. *Il responsabile della tutela dei diritti umani*

Quando le agenzie di intelligence raccolgono informazioni in merito a sospetti terroristi, la legge antiterrorismo prevede la vigilanza della commissione antiterrorismo e del responsabile della tutela dei diritti umani ([248]).

La commissione antiterrorismo sviluppa tra l'altro politiche relative ad attività antiterrorismo e vigila sull'attuazione di misure antiterrorismo nonché sulle attività di diverse autorità competenti nel settore del contrasto del terrorismo ([249]). La commissione è presieduta dal primo ministro e composta da diversi ministri e capi di agenzie governative, tra i quali il ministro degli Affari esteri, il ministro della Giustizia, il ministero della Difesa nazionale, il ministro degli Interni e della sicurezza, il direttore del NIS, il commissario generale dell'agenzia di polizia nazionale e il presidente della commissione per i servizi finanziari ([250]). Durante la conduzione di indagini di antiterrorismo e il tracciamento di sospetti terroristi al fine di raccogliere informazioni o materiali necessari per le attività antiterrorismo, il direttore del NIS deve riferire al presidente della commissione antiterrorismo (ossia al primo ministro) ([251]).

La legge antiterrorismo istituisce altresì la figura del responsabile della tutela dei diritti umani al fine di proteggere i diritti fondamentali delle persone contro violazioni causate da attività antiterrorismo ([252]). Il responsabile della tutela dei diritti umani è nominato dal presidente della commissione antiterrorismo tra le persone fisiche che soddisfano le qualifiche di cui al decreto di applicazione della legge antiterrorismo (ossia chiunque abbia la qualifica di avvocato con almeno dieci anni di esperienza lavorativa oppure con conoscenza a livello di esperto nel settore dei diritti umani e che stia prestando o abbia prestato servizio (quanto meno) come professore associato da/per almeno dieci anni oppure abbia prestato servizio in veste di funzionario pubblico di livello più alto in seno ad agenzie statali o in amministrazioni locali, oppure abbia almeno dieci anni di esperienza lavorativa nel settore dei diritti umani, ad esempio in seno ad un'organizzazione non governativa) ([253]). Il responsabile della tutela dei diritti umani è nominato per due anni (con possibilità di proroga del termine) e può essere rimosso dal suo incarico soltanto per motivi specifici e limitati e per giusta causa, ad esempio in caso di rinvio a giudizio nel contesto di un caso penale correlato ai suoi doveri, qualora divulghi informazioni riservate oppure in ragione di un'incapacità mentale o fisica prolungata ([254]).

In termini di poteri, il responsabile della tutela dei diritti umani può emettere raccomandazioni destinate a migliorare la protezione dei diritti umani da parte delle agenzie coinvolte nelle attività antiterrorismo ed elaborare istanze in sede civile (cfr. sezione 3.4.3) ([255]). Laddove si possa constatare ragionevolmente l'esistenza di una violazione dei diritti umani nello svolgimento di funzioni ufficiali, il responsabile della tutela dei diritti umani può raccomandare al capo dell'agenzia responsabile di porre rimedio a tale violazione ([256]). A sua volta l'agenzia responsabile deve notificare al responsabile della tutela dei diritti umani l'azione intrapresa per attuare tale raccomandazione ([257]). Qualora un'agenzia non attui una raccomandazione del responsabile della tutela dei diritti umani, la questione viene rinviata al livello superiore ossia alla commissione, compreso il suo presidente, ossia il primo ministro. Finora non vi sono stati casi in cui le raccomandazioni del responsabile della tutela dei diritti umani non siano state attuate.

3.3.2. *L'Assemblea nazionale*

Come descritto nella sezione 2.3.2, l'Assemblea nazionale può sottoporre a indagine e ispezione le autorità pubbliche e in tale contesto richiedere la divulgazione di documenti e imporre la comparizione di testimoni. Per quanto concerne questioni che rientrano nella competenza giurisdizionale del NIS, tale vigilanza parlamentare è svolta dal comitato per l'intelligence dell'Assemblea nazionale ([258]). Il direttore del NIS, che vigila sullo svolgimento dei compiti da parte

([248]) Articolo 7 della legge antiterrorismo.
([249]) Articolo 5, terzo comma, della legge antiterrorismo.
([250]) Articolo 3, primo comma, del decreto di applicazione della legge antiterrorismo.
([251]) Articolo 9, quarto comma, della legge antiterrorismo.
([252]) Articolo 7 della legge antiterrorismo.
([253]) Articolo 7, primo comma, del decreto di applicazione della legge antiterrorismo.
([254]) Articolo 7, terzo comma, del decreto di applicazione della legge antiterrorismo.
([255]) Articolo 8, primo comma, del decreto di applicazione della legge antiterrorismo.
([256]) Articolo 9, primo comma, del decreto di applicazione della legge antiterrorismo. Il responsabile della tutela dei diritti umani decide autonomamente in merito all'adozione di raccomandazioni, ma è tenuto a segnalarle al presidente della commissione antiterrorismo.
([257]) Articolo 9, secondo comma, del decreto di applicazione della legge antiterrorismo.
([258]) Articolo 36 e articolo 37, primo comma, punto 16, della legge sull'assemblea nazionale.

dell'agenzia, riferisce al comitato per l'intelligence (nonché al presidente della Repubblica di Corea) ([259]). Il comitato per l'intelligence stesso può altresì richiedere una relazione su una questione specifica e il direttore del NIS è tenuto a rispondere a tale richiesta senza indugio ([260]). Quest'ultimo può rifiutarsi di rispondere o testimoniare dinanzi il comitato per l'intelligence soltanto in relazione a segreti di Stato relativi a questioni militari, diplomatiche o concernenti la Corea del Nord che potrebbero avere un grave impatto sul destino nazionale qualora diventassero di dominio pubblico ([261]). In tal caso il comitato per l'intelligence può richiedere al primo ministro di fornire una spiegazione. Se tale spiegazione non viene presentata entro sette giorni dalla formulazione della richiesta, la risposta o la testimonianza non può più essere rifiutata.

Qualora l'Assemblea nazionale constati che è stata commessa un'attività illecita o impropria, può richiedere che l'autorità pubblica pertinente intraprenda misure correttive, compreso il riconoscimento di un risarcimento, l'adozione di azioni disciplinari e il miglioramento delle sue procedure interne ([262]). A seguito di tale richiesta, l'autorità deve agire senza indugio e riferire all'Assemblea nazionale in merito all'esito. Esistono norme specifiche relative alla vigilanza parlamentare rispetto al ricorso a misure di limitazione delle comunicazioni (ossia la raccolta del contenuto di comunicazioni) ai sensi della legge sulle comunicazioni ([263]). Per quanto concerne queste ultime, l'Assemblea nazionale può chiedere ai capi delle agenzie di intelligence di presentare una relazione in merito a qualsiasi misura specifica di limitazione delle comunicazioni. Inoltre può condurre ispezioni in loco su apparecchiature di intercettazione. Infine le agenzie di intelligence che hanno raccolto e gli operatori che hanno rivelato informazioni relative ai contenuti per finalità di sicurezza nazionale devono riferire in merito a tali divulgazioni su richiesta dell'Assemblea nazionale.

3.3.3. *Il consiglio di revisione e ispezione*

Il BAI svolge le stesse funzioni di vigilanza rispetto alle agenzie di intelligence illustrate per il settore delle attività di contrasto penale (cfr. sezione 2.3.2) ([264]).

3.3.4. *La Commissione per la protezione delle informazioni personali*

Per quanto concerne il trattamento di dati per finalità di sicurezza nazionale, compresa la fase di raccolta, una vigilanza aggiuntiva è attuata dalla PIPC. Come spiegato in modo più dettagliato nella sezione 1.2, rientrano in tale contesto i principi e gli obblighi generali di cui all'articoli 3 e all'articolo 58, quarto comma, della legge sulla protezione delle informazioni personali, nonché l'esercizio di diritti individuali garantiti dall'articolo 4 di quest'ultima legge. Inoltre, ai sensi dell'articolo 7-8, terzo e quarto comma, dell'articolo 7-9, quinto comma, della legge sulla protezione delle informazioni personali, la vigilanza della PIPC copre anche possibili violazioni delle norme contenute in leggi specifiche che definiscono limitazioni e garanzie rispetto alla raccolta di informazioni personali, quali la legge sulle comunicazioni, la legge antiterrorismo e la legge sulle imprese di telecomunicazione. Dati i requisiti di cui all'articolo 3, primo comma, della legge sulla protezione delle informazioni personali per la raccolta lecita e corretta di informazioni personali, qualsiasi violazione di tali leggi costituisce una violazione della legge sulla protezione delle informazioni personali. Di conseguenza la PIPC ha il potere di indagare ([265]) in merito a violazioni delle leggi che disciplinano l'accesso ai dati per finalità di sicurezza nazionale nonché delle norme di trattamento di cui alla legge sulla protezione delle informazioni personali, rilasciare pareri per il miglioramento, imporre misure correttive, raccomandare azioni disciplinari e segnalare potenziali reati alle autorità investigative pertinenti ([266]).

3.3.5. *La Commissione nazionale per i diritti umani*

La vigilanza da parte della NHRC si applica alle agenzie di intelligence allo stesso modo in cui si applica ad altre autorità governative (cfr. sezione 2.3.2).

3.4. **Ricorso individuale**

3.4.1. *Ricorso dinanzi il responsabile della tutela dei diritti umani*

Per quanto concerne la raccolta di informazioni personali nel contesto delle attività antiterrorismo, il responsabile della tutela dei diritti umani, istituito in seno alla commissione antiterrorismo, offre una procedura specifica di ricorso. Il responsabile della tutela dei diritti umani gestisce le istanze in sede civile relative alla violazione di diritti umani come conseguenza di attività antiterrorismo ([267]). Tale responsabile può raccomandare azioni correttive e l'agenzia pertinente deve riferire al funzionario qualsiasi misura adottata per attuare tale raccomandazione. Ai fini della presentazione di un reclamo le persone fisiche non devono soddisfare alcun requisito specifico. Di conseguenza un reclamo verrà gestito dal responsabile della tutela dei diritti umani anche se la persona fisica interessata non è in grado di dimostrare, nella fase di ammissibilità, a livello fattuale un pregiudizio subito.

([259]) Articolo 18 della legge sul NIS.
([260]) Articolo 15, secondo comma, della legge sul NIS.
([261]) Articolo 17, secondo comma, della legge sul NIS. I "segreti di Stato" sono definiti come "*fatti, beni o conoscenze classificati come segreti di Stato, l'accesso ai quali è consentito soltanto a un numero limitato di persone, e che non devono essere divulgati a nessun altro paese od organizzazione al fine di evitare un grave svantaggio per la sicurezza nazionale*" (cfr. articolo 13, quarto comma, della legge sul NIS).
([262]) Articolo 16, secondo comma, della legge sull'ispezione e sull'indagine dell'amministrazione dello Stato.
([263]) Articolo 15 della legge sulle comunicazioni.
([264]) Come nel caso in merito al comitato per l'intelligence dell'Assemblea nazionale, il direttore del NIS può rifiutarsi di rispondere al BAI soltanto in merito a questioni che costituiscono segreti di Stato e se l'accesso da parte del pubblico a tali informazioni inciderebbe gravemente sulla sicurezza nazionale (articolo 13, primo comma, della legge sul NIS).
([265]) Articolo 63 della legge sulla protezione delle informazioni personali.
([266]) Articolo 61, secondo comma, articolo 65, primo e secondo comma e articolo 64, quarto comma, della legge sulla protezione delle informazioni personali.
([267]) Articolo 8, primo comma, punto 2, del decreto di applicazione della legge antiterrorismo.

3.4.2. *Meccanismi di ricorso a disposizione ai sensi della legge sulla protezione delle informazioni personali*

Le persone fisiche possono esercitare i loro diritti di accesso, rettifica, cancellazione e sospensione ai sensi della legge sulla protezione delle informazioni personali rispetto a tali informazioni trattate per finalità di sicurezza nazionale ([268]). Le richieste di esercizio di tali diritti possono essere presentate direttamente all'agenzia di intelligence oppure indirettamente tramite la PIPC. L'agenzia di intelligence può ritardare, limitare o negare l'esercizio di un tale diritto nella misura e per il tempo necessari e proporzionati a proteggere un importante obiettivo di interesse pubblico (ad esempio nella misura in cui e per il tempo per il quale la concessione del diritto in questione comprometterebbe un'indagine in corso o costituirebbe una minaccia per la sicurezza nazionale) oppure qualora concedere il diritto in questione possa minacciare la vita o compromettere l'incolumità di una terza parte. Laddove la richiesta venga negata o limitata, la persona fisica deve ricevere una notifica dei motivi senza indugio.

Inoltre, conformemente all'articolo 58, quarto comma, della legge sulla protezione delle informazioni personali (requisito per garantire la gestione adeguata dei reclami individuali) e all'articolo 4, quinto comma, della medesima legge (diritto a un ricorso adeguato in relazione a qualsiasi danno derivante dal trattamento delle informazioni personali attraverso una procedura tempestiva ed equa), le persone fisiche hanno il diritto di ottenere un risarcimento. Ciò comprende il diritto di segnalare una presunta violazione al call centre per la tutela della vita privata gestito dall'agenzia coreana per la sicurezza e internet nonché di promuovere un reclamo presso la PIPC ([269]). Tali mezzi di ricorso sono disponibili in caso di possibili violazioni tanto delle norme contenute in leggi specifiche che definiscono limitazioni e garanzie rispetto alla raccolta di informazioni personali per finalità di sicurezza nazionale quanto della legge sulla protezione delle informazioni personali. Come spiegato nella notifica n. 2021-1, una persona fisica dell'UE può proporre reclamo alla PIPC attraverso la propria autorità nazionale di protezione dei dati. In tal caso la PIPC invierà una notifica alla persona fisica attraverso quest'ultima autorità una volta conclusa l'indagine (fornendo altresì, laddove applicabile, informazioni in merito a misure correttive imposte). Le decisioni o l'inazione da parte della PIPC possono essere ulteriormente impugnate adendo gli organi giurisdizionali coreani ai sensi della legge sui contenziosi amministrativi.

3.4.3. *Ricorso dinanzi la commissione nazionale per i diritti umani*

La possibilità di ottenere un ricorso individuale dinanzi la NHRC si applica alle agenzie di intelligence allo stesso modo in cui si applica ad altre autorità governative (cfr. sezione 2.4.2).

3.4.4. *Ricorso giurisdizionale*

Come nel caso in merito alle attività delle autorità di contrasto in materia penale, le persone fisiche possono ottenere un ricorso in sede giudiziaria nei confronti di agenzie di intelligence rispetto a violazioni delle limitazioni e delle garanzie di cui sopra in diversi modi.

Innanzitutto le persone fisiche possono ottenere un risarcimento dei danni ai sensi della legge sul risarcimento da parte dello Stato. Ad esempio, in un caso, il risarcimento è stato concesso in relazione ad attività di sorveglianza illecite attuate dal comando di sostegno alla difesa (l'ente predecessore del comando di sostegno alla protezione della difesa) ([270]).

In secondo luogo la legge sui contenziosi amministrativi consente alle persone fisiche di contestare le disposizioni e le omissioni da parte di agenzie amministrative, comprese le agenzie di intelligence ([271]).

Infine le persone fisiche possono proporre un reclamo costituzionale adendo la Corte costituzionale rispetto a misure adottate dalle agenzie di intelligence ai sensi della legge sulla Corte costituzionale.

([268]) Articolo 3, quinto comma e articolo 4, primo, terzo e quarto comma, della legge sulla protezione delle informazioni personali.
([269]) Articolo 62 e articolo 63, secondo comma, della legge sulla protezione delle informazioni personali.
([270]) Decisione della Corte suprema n. 96Da42789, 24 luglio 1998.
([271]) Articoli 3 e 4 della legge sui contenziosi amministrativi.