RELAZIONE ILLUSTRATIVA

Il presente schema di decreto legislativo è finalizzato a recepire nell'ordinamento interno la "*direttiva (UE) 2016/680 relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio*".

Il provvedimento, redatto nell'esercizio della delega conferita al Governo dagli articoli 1 e 11 della legge 25 ottobre 2017, n. 163, recante "*Delega al Governo per il recepimento delle direttive europee e l'attuazione di altri atti dell'Unione europea - Legge di delegazione europea 2016-2017*", ha ad oggetto la disciplina del trattamento interamente o parzialmente automatizzato di dati personali delle persone fisiche, nonché del trattamento non automatizzato di dati personali contenuti in un archivio, o ad esso destinati, nel settore penale.

Con riguardo alla tecnica redazionale, si è optato per la predisposizione di un unico corpo normativo, destinato a regolamentare il trattamento dei dati personali per finalità di prevenzione e repressione di reati, esecuzione di sanzioni penali, salvaguardia contro le minacce alla sicurezza pubblica e prevenzione delle stesse, da parte sia dell'autorità giudiziaria, sia delle forze di polizia.

In tal modo si propone di adottare un testo unitario, dedicato alla complessiva disciplina del trattamento di dati personali in ambito penale, con l'obiettivo di creare un vero e proprio statuto, contenente principi generali di regolamentazione della materia, rivolti anche al legislatore futuro, e disposizioni di dettaglio, nei vari settori in cui si può articolare il trattamento dei dati personali.

In sintonia con la direttiva che si va ad attuare nell'ordinamento interno, si è inteso anzitutto fornire una regolamentazione organica del trattamento dei dati personali delle persone fisiche per fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, la quale supera e sostituisce in gran parte quella attualmente contemplata nei titoli primo e secondo della parte seconda del Codice sul trattamento dei dati personali di cui al decreto legislativo 30 giugno 2003, n. 196, dedicate a specifici settori, in particolare quello giudiziario e quello dei trattamenti da parte delle forze di polizia.

La scelta è stata, dunque, di ridisegnare la regolamentazione del trattamento dei dati personali con riguardo alla sua finalità, piuttosto che in relazione all'autorità competente al trattamento, in ogni caso assicurando le distinzioni rese necessarie dalle diverse caratteristiche e dalla differente natura delle autorità interessate, giudiziaria e di polizia.

Con specifico riferimento all'ambito giudiziario, attualmente trovano applicazione gli articoli da 46 a 52 del codice della privacy, dedicate ai trattamenti svolti nell'esercizio delle funzioni sia civili che penali, ivi compresi i trattamenti in materia di status giuridico ed economico del personale della magistratura che, seppure non direttamente correlati alla trattazione giudiziaria di affari e di controversie, abbiano una diretta incidenza sulla funzione giurisdizionale, nonché quelli svolti nell'ambito di attività ispettiva su uffici giudiziari.

Per quanto concerne, invece, i trattamenti effettuati dall'autorità di pubblica sicurezza per fini di prevenzione, accertamento o repressione dei reati o di tutela della sicurezza pubblica, la disciplina dettata dalla direttiva assorbe totalmente quella oggi prevista dagli articoli da 53 a 57 del codice della privacy, che vengono conseguentemente abrogati.

Rimane, invece, del tutto compatibile con i principi enunciati nella direttiva 2016/680 quanto stabilito dall'articolo 7, comma 3, del decreto legge 18 febbraio 2015, n. 7, circa l'individuazione,

con decreto adottato dal Ministro dell'interno, dei trattamenti non occasionali effettuati per fini di polizia, previsti da norme legislative o regolamentari. Tale elencazione, infatti, insieme al registro delle operazioni di trattamento, è volta a garantire una maggiore conoscibilità, prima di tutto ai cittadini, dei trattamenti eseguiti per fini di polizia, oggi previsti da una molteplicità di disposizioni, spesso anche risalenti nel tempo.

Al fine di conferire alla disciplina la necessaria organicità e sistematicità, lo schema di decreto è stato suddiviso in otto Capi, dedicati a specifici aspetti della materia, che rinviano al regolamento (UE) 2016/679 nelle parti il cui contenuto risulta coincidente con la direttiva.

Il **Capo I** indica i principi di carattere generale, i presupposti e le condizioni di liceità del trattamento.
Particolarmente significativa risulta, in tale ambito, la disposizione in tema di conservazione, la quale prescrive che i dati siano conservati per il tempo necessario al conseguimento delle finalità per le quali sono trattati, sottoposti a esame periodico per verificarne la persistente necessità di conservazione e cancellati o anonimizzati una volta decorso tale termine. L'individuazione dei termini di conservazione per i trattamenti non occasionali, ove non già stabiliti da disposizioni di legge o di regolamento, viene demandata a un decreto del Presidente della Repubblica, ai sensi dell'articolo 17, comma 1, della legge 23 agosto 1988, n. 400.
Merita inoltre di essere segnalata la disposizione in tema di differenziazione tra categorie di dati (fondati su fatti ovvero su valutazioni) e di interessati, in ragione della loro specifica posizione processuale, atteso il differenziato regime applicabile agli interessati anche in ragione di tali specifici elementi.
In ordine ai presupposti di liceità del trattamento, conformemente al considerando n. 33 della direttiva, si è indicata quale fonte normativa, oltre a quella legislativa, anche quella regolamentare, più adatta a prevedere specifici trattamenti, pure di dati sensibili. Si è riservata, invece, alla sola fonte legislativa la disciplina dei processi decisionali automatizzati, compresa la profilazione, considerati i rischi insiti in tale tipologia di trattamenti per le libertà e i diritti dell'interessato.

Il **Capo II**, intitolato ai diritti dell'interessato, recepisce le norme di cui al capo terzo della direttiva, prevedendo che di dati personali contenuti in una decisione giudiziaria, in atti o documenti oggetto di trattamento nel corso di accertamenti o indagini, nel casellario giudiziale o in un fascicolo oggetto di trattamento nel corso di un procedimento penale o in fase di esecuzione penale, l'esercizio di tali diritti (ricezione di informazioni, accesso, rettifica, cancellazione, limitazione del trattamento) è regolato dalle disposizioni normative che disciplinano tali atti e procedimenti.
In ambito giudiziario, la tutela degli interessati è quindi assicurata, per le parti, dall'ampia gamma di garanzie che riconoscono i diritti di difesa all'interno del procedimento penale, anche con riguardo ai dati personali necessariamente oggetto di trattamento; analoghe garanzie vengono assicurate ai terzi attraverso la previsione del comma 3 dell'articolo 14 dello schema, che a sua volta richiama l'articolo 116 c.p.p., in punto di accesso, e la disciplina sulla correzione dell'errore materiale di cui all'articolo 130 c.p.p.
In tal modo si assicura la possibilità di limitare l'esercizio dei diritti dell'interessato, conformemente alle esigenze di prevenzione, di indagine e processuali.

Il **Capo III** ha ad oggetto i profili generali riguardanti il titolare e il responsabile del trattamento, nonché la descrizione di alcuni dei principali obblighi, articolati con riferimento agli adempimenti funzionali alla sicurezza e alla nomina del responsabile della protezione dati.
Vengono poi disciplinati obblighi in materia di sicurezza del trattamento, con particolare riguardo alla notifica della violazione dei dati personali e al responsabile della protezione dati, la cui nomina è stata prevista come obbligatoria anche per l'autorità giudiziaria, in ragione dell'ausilio che tale figura può fornire nella gestione di trattamenti complessi e spesso inerenti dati sensibili, quali appunto quelli svolti in sede giurisdizionale.

Il **Capo IV** si occupa dei trasferimenti di dati personali verso Paesi terzi o organizzazioni internazionali, mentre il quinto reca, oltre alle abrogazioni, alcune norme particolarmente significative, tra cui l'esclusione del potere di controllo del Garante in ordine al trattamento svolto dall'autorità giudiziaria nell'esercizio delle funzioni giurisdizionali, comprese quelle del pubblico ministero, nel rispetto di quanto disposto dall'articolo 45, paragrafo 2 della direttiva.

Il **Capo V** è dedicato alla tutela e alle sanzioni amministrative, mentre il **Capo VI** individua le condotte costituenti illecito penale, selezionate in relazione alla gravità e capacità offensiva dei diritti dell'interessato.

Il **Capo VII** trasferisce nello schema di decreto alcune disposizioni già presenti nel codice della privacy in materia di dati di polizia.

Il **Capo VIII** contiene le disposizioni di coordinamento e le abrogazioni.

Quanto al contenuto dello schema di decreto legislativo, esso si compone di cinquantuno articoli, che di seguito si illustrano.

Il **Capo I** contiene le «*Disposizioni generali* » e, in otto articoli, recepisce le disposizioni dei primi due Capi della Direttiva, dedicate alle disposizioni generali e ai principi.

L'**articolo 1**, rubricato «*Oggetto e ambito di applicazione*», individua i contenuti e l'ambito di applicazione del decreto legislativo. L'atto normativo attua nell'ordinamento interno le disposizioni della direttiva 27 aprile 2016, n. 2016/680/UE del Parlamento europeo e del Consiglio, in materia di trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati. Al comma 2 l'ambito di applicazione viene circoscritto, in aderenza alle disposizioni di cui agli articoli 1 e 2 della direttiva, al trattamento interamente o parzialmente automatizzato di dati personali delle persone fisiche e al trattamento non automatizzato di dati personali delle persone fisiche contenuti in un archivio o ad esso destinati, svolti dalle autorità competenti per finalità sopra descritte. Restano pertanto esclusi dall'applicazione del decreto, come reso chiaro dalla definizione di «archivio» contenuta nel successivo art. 2 e dal considerando n. 18 della direttiva, i trattamenti di dati delle persone giuridiche e quelli di dati non contenuti in archivi, tra i quali i fascicoli o le serie di fascicoli non strutturati secondo criteri specifici, con le rispettive copertine. Sono infine estranei all'ambito applicativo del decreto, come specificato al comma 3, i trattamenti effettuati nello svolgimento di attività concernenti la sicurezza nazionale o rientranti

nell'ambito di applicazione del titolo V capo 2 del trattato sull'Unione europea (in materia di politica estera e sicurezza comune), nonché tutte le attività non rientranti nell'ambito di applicazione del diritto dell'Unione europea. Il richiamo, tra le esclusioni oggettive, ai trattamenti effettuati nello svolgimento di attività concernenti la sicurezza nazionale o rientranti nell'ambito di applicazione del titolo V capo 2 del trattato sull'Unione europea riproduce il considerando n. 14, maggiormente esplicativo, rispetto alla formulazione dell'articolo 2 della direttiva, dell'ambito di applicazione della direttiva.

L'**articolo 2**, rubricato «*Definizioni*» contiene l'esplicazione del lessico utilizzato nel testo. Alcune definizioni si segnalano per la loro rilevanza ai fini dell'individuazione dell'oggetto e delle condizioni di liceità del trattamento, nonché della portata dei diritti e degli obblighi descritti ai capi II e III. In particolare, si evidenziano le nozioni di «*trattamento*» (inteso quale operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati, applicate a dati personali o insiemi di dati personali), «*autorità competente*» (caratterizzata funzionalmente dall'esercizio di pubblici poteri in materia di prevenzione e repressione di reati, di esecuzione di sanzioni penali o di salvaguardia contro le minacce alla sicurezza pubblica), «*profilazione*» (forma di trattamento automatizzato di dati personali oggetto di peculiari cautele, considerate le sue potenzialità discriminatorie) «*titolare del trattamento*» (l'autorità competente che determina le finalità e i mezzi del trattamento di dati personali). Per la centralità che ancora rivestono, in relazione al controllo dei trattamenti e alla tutela amministrativa avverso i trattamenti effettuati dalle autorità di pubblica sicurezza e dalle forze di polizia, si sono definiti in questa sede anche «il Garante» (quale il Garante di cui all'articolo 153 del decreto legislativo 30 giugno 2003, n. 196, identificato quale autorità di controllo indipendente, ai sensi dell'articolo 41 della Direttiva) e il «Codice» (con riferimento al Codice in materia di protezione dei dati personali, adottato con il decreto legislativo 30 giugno 2003, n. 196).

L'**articolo 3** enuncia i «*Principi applicabili al trattamento di dati personali* ». Il comma 1 riproduce i criteri di trattamento analiticamente previsti dall'art. 4 della Direttiva, imponendo liceità, correttezza e trasparenza del trattamento (lett. a); effettuazione della raccolta dei dati per finalità determinate, espresse e legittime e compatibilità del trattamento con le stesse (lett. b); adeguatezza, pertinenza e continenza dei trattamenti in rapporto alle finalità predette (lett. c); esattezza e aggiornamento dei dati (lett. d); temporaneità della conservazione dei dati o della identificabilità dell'interessato (lett. e); sicurezza e protezione dei dati (lett. f). Il senso e la portata dei principi sono chiariti nei considerando nn. 26 e 29 della Direttiva, in cui si spiega che qualsiasi trattamento di dati personali dovrebbe essere lecito, corretto e trasparente nei confronti della persona fisica interessata e perseguire unicamente fini specifici previsti dalla legge; che le finalità del trattamento dovrebbero essere esplicite, legittime e precisate al momento della raccolta; che i dati personali dovrebbero essere adeguati e pertinenti alle finalità del trattamento; che la raccolta dei dati personali non dovrebbe essere eccessiva e che i dati dovrebbero essere conservati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati; che il trattamento di dati personali dovrebbe ammettersi solo quando la sua finalità non è ragionevolmente conseguibile con altri mezzi e che, onde garantire che i dati non siano conservati più a lungo del necessario, il titolare del trattamento dovrebbe stabilire un termine per la cancellazione o per la verifica periodica. Utili indicazioni si rinvengono anche a chiarimento del requisito della esattezza, da considerare in relazione alla natura e alle finalità del trattamento (si che, come esemplificato nel considerando 30, nel caso di una "dichiarazione" resa in un procedimento giudiziario, basata su percezione

soggettiva, tale requisito non può essere riferito al contenuto della dichiarazione, ma al semplice fatto che è stata rilasciata), e della liceità (considerando n. 35, secondo cui, per essere lecito, il trattamento dei dati personali dovrebbe essere necessario per l'esecuzione di un compito svolto nell'interesse pubblico da un'autorità competente ai fini di prevenzione e repressione dei reati, esecuzione di sanzioni penali, salvaguardia contro e prevenzione di minacce alla sicurezza pubblica). Il comma 2 contempla la possibilità di trattamento dei dati per finalità diverse da quelle per cui sono stati raccolti, pur sempre rientranti fra quelle dell'art. 1 comma 2 e lo consente solo se autorizzato dalle norme dell'ordinamento interno o dell'Unione europea e se necessario e proporzionato alla diversa finalità. Al comma 3 viene precisato che il trattamento per le finalità di cui all'art. 1 comma 2 può comprendere anche l'archiviazione nel pubblico interesse o per finalità scientifiche, storiche o statistiche, nel rispetto dei diritti e delle libertà degli interessati. Infine, al comma 4, il titolare del trattamento viene reso espressamente responsabile del rispetto dei principi indicati ai commi 1, 2 e 3. Si è ritenuto superfluo riprodurre la previsione ulteriore contenuta nella corrispondente norma della direttiva (art. 5 comma 4), secondo cui il titolare del trattamento non solo è "*competente*" per il rispetto dei principi applicabili al trattamento, ma è altresì "*in grado di provarlo*", poiché nell'ordinamento interno tale onere è implicito nell'attribuzione stessa della responsabilità.

L'articolo 4, sotto la rubrica «*Conservazione e verifica della qualità dei dati, distinzione tra categorie di interessati e di dati*», detta prescrizioni in tema di catalogazione, conservazione e trasmissione dei dati. Il comma 1 dispone che il titolare del trattamento effettui, se del caso e per quanto possibile, una chiara distinzione tra i dati personali relativi a diverse categorie di interessati. Per consentire catalogazioni omogenee, si è deciso di circoscrivere la distinzione alle categorie di interessati "*previste dalla legge*", facendo riferimento, cioè, alle diverse vesti e alle diverse denominazioni che, nell'ordinamento interno, le persone fisiche assumono nell'ambito di una attività di indagine o di un procedimento penale o di prevenzione. L'utilità della disposizione è spiegata nel considerando 31 della Direttiva, con riferimento al trattamento dei dati personali nel settore della cooperazione giudiziaria in materia penale e della cooperazione di polizia, nel caso in cui siano trattati dati personali relativi a diverse categorie di interessati (quali indiziati, condannati, persone offese, testimoni, persone informate dei fatti, persone in contatto o collegate a indiziati o condannati). I commi 2 e 3 pongono a carico dell'autorità competente alcuni doveri per il caso di trasmissione di dati personali. Il comma 2 dispone che i dati personali inesatti, incompleti o non più aggiornati non siano trasmessi o resi disponibili. Al fine di garantire la protezione delle persone fisiche, l'esattezza, la completezza dei dati personali o la misura in cui essi sono aggiornati e l'affidabilità dei dati personali trasmessi o resi disponibili, è previsto che le autorità competenti, nella misura del possibile, verifichino la qualità dei dati prima della trasmissione o della messa a disposizione e aggiungano le informazioni necessarie in tutte le trasmissioni di dati personali. Nel caso di trasmissione illecita di dati o di inesattezza dei dati trasmessi, il comma 3 dispone che il destinatario deve esserne informato senza ritardo. In tal caso, i dati personali devono essere rettificati o cancellati o il trattamento deve essere limitato a norma dell'articolo 12.

L'articolo 5 pone le condizioni di «*Liceità del trattamento*», individuate con riferimento alle finalità (che debbono essere quelle di cui all'articolo 1, comma 2) e al fondamento giuridico del trattamento stesso. Il comma 1 prevede, a questo riguardo, che i dati personali da trattare e le finalità del trattamento debbano essere previsti da norme dell'Unione europea o dell'ordinamento interno, di natura legislativa o regolamentare. Particolarmente rilevante è la norma di cui al comma

2, con cui sono demandati a un decreto regolamentare, ai sensi dell'art. 17, comma 1, della legge 23 agosto 1988, n. 400, l'individuazione dei trattamenti o le categorie di trattamenti di cui al comma 1, i termini e le modalità di conservazione dei dati, i soggetti legittimati ad accedervi, le condizioni di accesso, le modalità di consultazione, nonché le modalità e le condizioni per l'esercizio dei diritti dell'interessato previsti ai successivi articoli 9, 10, 11 e 13. La norma fa salvi i casi in cui detti elementi siano già stabiliti da disposizioni di legge o di regolamento.

L'articolo 6 detta «*Condizioni di trattamento specifiche*», per il caso in cui il diritto dell'Unione europea o la legge consentano il trattamento per finalità diverse da quelle di cui all'articolo 1 comma 2 per le quali i dati siano stati raccolti. Tali trattamenti restano assoggettati al Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016 (regolamento generale sulla protezione dei dati), salvo che siano effettuati nell'ambito di attività alle quali non si applica il diritto dell'Unione europea o nei casi di cui all'articolo 58 del Codice (ossia nell'ambito di attività dei servizi di informazione e di sicurezza o avente ad oggetto dati coperti dal segreto di Stato o nell'ambito di attività svolta da soggetti pubblici per finalità di difesa o sicurezza dello Stato). Il comma 2 della norma prevede che il Regolamento si applica, con le stesse esclusioni di cui all'articolo 58 del Codice, anche ai trattamenti eseguiti per finalità diverse da quelle di cui all'articolo 1, comma 2, comprese le attività di archiviazione nel pubblico interesse, di ricerca scientifica o storica o per finalità statistiche. Il comma 3 dispone che, nel caso di trasmissione dei dati, l'autorità competente informi il destinatario dell'eventuale esistenza di condizioni specifiche di trattamento e dell'obbligo di rispettarle. Al comma 4, infine, è previsto che le condizioni applicate ai destinatari dall'autorità competente che trasmette i dati ai destinatari di altri Stati membri o ad agenzie, uffici e organi istituiti a norma del titolo V, capi 4 e 5, TFUE siano le stesse condizioni applicabili alle trasmissioni di dati all'interno dello Stato.

L'articolo 7, sotto la rubrica «*Trattamento di categorie particolari di dati personali*», appronta una speciale protezione ai dati personali di cui all'articolo 9 del Regolamento. Tali dati, come spiegato nel considerando n. 37, "*per loro natura, sono particolarmente sensibili sotto il profilo dei diritti e delle libertà fondamentali, dal momento che il contesto del loro trattamento potrebbe creare rischi significativi per i diritti e le libertà fondamentali*". Per tale ragione, il trattamento è consentito solo se assistito da garanzie adeguate per i diritti e le libertà dell'interessato e solo se specificamente previsto dal diritto dell'Unione europea o da legge o regolamento, ovvero, ferme le garanzie dei diritti e delle libertà, se necessario per salvaguardare un interesse vitale dell'interessato o di un'altra persona fisica o se ha ad oggetto dati resi manifestamente pubblici dall'interessato. A migliore esplicazione delle cautele che devono assistere il trattamento in questi casi, il considerando n. 37 aggiunge che "*garanzie adeguate per i diritti e le libertà dell'interessato potrebbero comprendere la possibilità di raccogliere tali dati unicamente in connessione con altri dati relativi alla persona fisica interessata, la possibilità di provvedere adeguatamente alla sicurezza dei dati raccolti, norme più severe riguardo all'accesso ai dati da parte del personale dell'autorità competente e il divieto di trasmissione di tali dati*".

L'articolo 8, rubricato «*Processo decisionale automatizzato relativo alle persone fisiche*», vieta le decisioni basate unicamente su un trattamento automatizzato, compresa la profilazione, che producano effetti negativi nei confronti sull'interessato, salvo che siano autorizzate dal diritto dell'Unione europea o da specifiche disposizioni di legge. In ogni caso, a norma del comma 2, tale trattamento deve essere subordinato per legge a garanzie adeguate e deve essere assicurato all'interessato il diritto di ottenere l'intervento umano. Nel considerando 38 si precisa che tra le

garanzie adeguate dovrebbe essere compreso "*il rilascio di specifiche informazioni all'interessato e il diritto di ottenere l'intervento umano, in particolare di esprimere la propria opinione, di ottenere una spiegazione della decisione raggiunta dopo tale valutazione e di impugnare la decisione*". Nel comma 3 è ulteriormente innalzato il livello di tutela per il caso di decisioni automatizzate basate su dati sensibili, ammesse esclusivamente se sono in vigore misure adeguate a salvaguardia dei diritti, delle libertà e dei legittimi interessi dell'interessato. Viene infine vietata, al comma 4, la profilazione finalizzata alla discriminazione di persone fisiche sulla base di dati personali sensibili, fermo il divieto di cui all'articolo 21 della Carta dei diritti fondamentali dell'Unione europea.

Il **Capo II** - intitolato ai diritti dell'interessato- recepisce le norme di cui al Capo III della direttiva riconoscendo all'interessato taluni specifici diritti in relazione ai trattamenti in esame e disciplinandone condizioni, modalità di esercizio e limiti, a fronte di precisi obblighi (in particolare informativi) del titolare.

In particolare, **l'articolo 9** sancisce, in capo al titolare del trattamento, l'obbligo di adottare misure adeguate a fornire all'interessato le informazioni necessarie sul trattamento (specificamente disciplinate all'articolo 10), ad agevolare l'esercizio dei diritti riconosciuti all'interessato medesimo, nonché a fornire riscontro alla richiesta pervenuta per iscritto e senza ingiustificato ritardo.
Il comma 5 dell'articolo 9 demanda, infine, a un decreto di natura non regolamentare (adottato dal Ministro competente) l'individuazione - ove necessario anche per categorie - dei trattamenti non occasionali effettuati per fini di prevenzione e repressione, sulla base di previsioni legislative e regolamentari, con l'indicazione del relativo titolare. Tale decreto, dal contenuto essenzialmente ricognitivo, mira a garantire, soprattutto ai cittadini, maggiore certezza in ordine alle tipologie di trattamenti ai quali i propri dati personali possano essere soggetti e ai titolari ai quali rivolgersi per l'esercizio dei diritti. Si tratta di una previsione particolarmente importante, soprattutto con riferimento a settori (si pensi, in particolare, a quello della pubblica sicurezza), nei quali la numerosità dei trattamenti e la molteplicità di fonti normative stratificatesi nel tempo rischiano di ostacolare l'esercizio dei diritti da parte dell'interessato.
L'articolo 10 disciplina il contenuto delle informazioni che il titolare del trattamento è tenuto a rendere all'interessato. Al primo comma sono previsti i contenuti informativi minimi, riguardanti l'identificazione del titolare e le finalità del trattamento, i diritti azionabili e le modalità di reclamo. Tali informazioni possono essere messe a disposizione anche attraverso il sito internet del titolare del trattamento. Al secondo comma sono invece elencate una serie di informazioni ulteriori che il titolare del trattamento deve fornire quando previsto da disposizioni di legge di regolamento. La distinzione rileva poiché solo per questa seconda categoria di informazioni è possibile una limitazione dei diritti dell'interessato, nei casi indicati dall'articolo 14, comma 2.
L'articolo 11 disciplina il diritto di accesso dell'interessato ai dati che lo riguardano, nonché a specifiche informazioni caratterizzanti il trattamento (finalità, titolo giuridico, categorie di dati trattati, destinatari, periodo di conservazione). Si precisa peraltro che ogni diniego o limitazione dell'accesso, alle condizioni previste dall'articolo 14, deve essere motivato e comunicato per iscritto all'interessato, il quale deve altresì informato del diritto di proporre reclamo dinanzi Garante o di proporre ricorso giurisdizionale.

L'articolo 12 riconosce all'interessato il diritto di ottenere la rettifica dei dati inesatti che lo riguardano, l'integrazione dei dati incompleti, la cancellazione di quelli trattati illegittimamente, nonché la limitazione del trattamento rispetto a dati la cui esattezza, contestata dall'interessato, non possa essere accertata o comunque nei casi nei quali non possa disporsi la cancellazione per esigenze probatorie. Anche in questo caso, sono riconosciuti all'interessato il diritto di informazione per iscritto in ordine ai motivi della decisione che limita i suoi diritti e alle modalità di tutela mediante reclamo o ricorso giurisdizionale.

L'articolo 13 consente all'interessato, al di fuori del caso di trattamento effettuato dell'autorità giudiziaria, di esercitare i suoi diritti tramite il Garante.

L'articolo 14 disciplina le limitazioni dell'esercizio dei diritti dell'interessato con riguardo a due fattispecie peculiari.

La prima, delineata dal comma 1, prevede che relativamente ai dati personali contenuti in una decisione giudiziaria, in atti o documenti oggetto di trattamento nel corso di accertamenti o indagini, nel casellario giudiziale o in un fascicolo oggetto di trattamento nel corso di un procedimento penale o in fase di esecuzione penale, i diritti dell'interessato di cui agli articoli 10, 11 e 12 siano esercitati conformemente alle norme di legge o di regolamento che disciplinano tali atti o procedimenti. La norma si avvale della specifica possibilità riconosciuta, in tal senso, agli Stati membri dall'articolo 18 della direttiva, al fine di modulare le esigenze di tutela dei diritti dell'interessato sulla base delle peculiarità proprie dell'attività di prevenzione e repressione dei reati.

Al fine consentire il pieno esercizio dei predetti diritti in ambito giudiziario, si prevede che qualunque interessato, durante il procedimento penale o dopo la sua definizione, possa chiedere, con le modalità di cui all'articolo 116 del codice di procedura penale, la rettifica, la cancellazione o la limitazione dei dati personali che lo riguardano. Il giudice in tal caso procede alle correzioni necessarie con le forme dell'articolo 130 del codice di procedura penale.

Il comma 2 dell'articolo 14 prevede la possibilità di ritardare, limitare o escludere l'esercizio dei diritti di informazione, accesso, rettifica o cancellazione o limitazione del trattamento, ovvero l'adempimento dell'obbligo del titolare del trattamento di fornire le informazioni aggiuntive di cui all'articolo 10 comma 2, nella misura e per il tempo necessari a salvaguardare il buon esito dell'attività di prevenzione e repressione dei reati, ovvero le esigenze di tutela della sicurezza pubblica, della sicurezza nazionale, dei diritti delle libertà altrui. In ogni caso la limitazione deve tenere conto dei diritti fondamentali e dei legittimi interessi della persona i cui dati sono trattati.

Il Capo III – intitolato al titolare e al responsabile del trattamento – contiene le disposizioni sugli adempimenti ai quali tali figure sono tenute e si suddivide al suo interno- come nella direttiva- in tre sezioni: la prima concernente gli obblighi generali (artt. 15-24), la seconda la sicurezza dei dati personali (artt.25-27), la terza il responsabile della protezione dati (artt. 28-30).

L'articolo 15 sancisce, in capo al titolare del trattamento, l'obbligo generale di adozione (nonché di riesame ed aggiornamento, ove necessario) di misure tecniche e organizzative adeguate per garantire la conformità del trattamento alla disciplina dettata dal decreto stesso.

L'articolo 16 sancisce, in capo al titolare del trattamento, l'obbligo generale di adozione di misure per la protezione dei dati fin dalla progettazione e per impostazione predefinita, volte a integrare nel trattamento le necessarie garanzie a tutela dei diritti degli interessati.

L'articolo 17 disciplina la contitolarità del trattamento, imponendo ai contitolari di concordare con modalità trasparenti gli ambiti delle rispettive responsabilità e di designare il punto di contatto cui possano rivolgersi gli interessati, i quali possono tuttavia, indipendentemente da tale accordo, esercitare i propri diritti nei confronti di ciascun titolare.

L'articolo 18 concerne il responsabile del trattamento, che come nel Regolamento generale per la protezione dei dati personali assume una connotazione per molti aspetti diversa da quella oggi prevista dal d.lgs. 30 giugno 2003, n. 196. In particolare, l'effettuazione, per conto del titolare, di un trattamento è affidata al responsabile (che garantisca misure tecniche e organizzative adeguate) da un contratto o altro atto giuridico, redatto in forma scritta, che disciplini le caratteristiche essenziali del trattamento e gli obblighi generali del responsabile. Si precisa peraltro che qualora il responsabile, in violazione della disciplina dettata dal decreto, determini *motu proprio* finalità e mezzi del trattamento, se ne considera titolare, con tutto ciò che ne consegue in termini di obblighi e responsabilità.

L'articolo 19 disciplina l'ipotesi in cui il trattamento sia svolto sotto l'autorità del titolare o del responsabile, prevedendo che in tal caso l'agente possa trattare i dati ai quali abbia accesso solo conformemente alle istruzioni ricevute, salvo diversa previsione normativa.

L'articolo 20 sancisce, in capo al titolare del trattamento, l'obbligo di tenere, in forma scritta, un registro delle categorie delle attività di trattamento effettuate sotto la propria responsabilità, dal contenuto specificamente disciplinato secondo quanto previsto dal comma 1. Analogo obbligo (sia pure con contenuti del registro diversi) è sancito, al comma 2, in capo al responsabile del trattamento, relativamente alle categorie di attività di trattamento svolte per conto del titolare.

L'articolo 21 impone l'obbligo di tracciabilità (con registrazione in appositi file di log) delle operazioni essenziali svolte sui dati personali in sistemi di trattamento automatizzati, in modo tale da poter consentire la verifica della liceità del trattamento nell'ambito di controlli interni o di procedimenti penali.

L'articolo 22 sancisce, in capo al titolare e al responsabile del trattamento, l'obbligo di cooperazione, su richiesta, con il Garante, nell'esercizio delle sue funzioni.

L'articolo 23 impone al titolare di effettuare una valutazione d'impatto sulla protezione dei dati (con il contenuto disciplinato al comma 2), prima di procedere al trattamento, qualora esso – in ragione della sua natura, delle nuove tecnologie utilizzate, dell'ambito di applicazione, del contesto o delle finalità – presenti un rischio elevato per i diritti e le libertà (non solo, dunque, per il diritto alla protezione dei dati) delle persone.

L'articolo 24 prevede l'obbligo di consultazione preventiva del Garante se, all'esito della valutazione d'impatto, il trattamento presenterebbe comunque un rischio elevato in assenza di misure idonee ad attenuarlo, ovvero qualora il trattamento presenti comunque tale rischio, in particolare in ragione dell'utilizzo di tecnologie o procedure nuove ovvero di dati genetici o biometrici. Si prevede anche la facoltà per il Garante di stabilire un elenco di trattamenti soggetti a consultazione preventiva. In ogni caso, qualora ritenga che il trattamento non sia conforme alla disciplina di riferimento, il Garante fornisce un parere scritto entro sei settimane (termine suscettibile di proroga nella misura di un mese nel caso di trattamento complesso).

Al comma 2, si prevede altresì l'obbligo di consultazione del Garante in ordine a progetti di atti normativi di rango primario e secondario, nonché di decreti non aventi natura regolamentare, secondo una procedura che nel nostro ordinamento era peraltro già invalsa.

L' **articolo 25** che apre la sezione intitolata alla sicurezza dei dati personali - sancisce, in capo al titolare e al responsabile del trattamento, l'obbligo generale di adozione di misure tecniche e organizzative tali da garantire un livello di sicurezza adeguato al rischio di violazione dei dati personali trattati e finalizzate ad obiettivi specificamente indicati al comma 2.

L'articolo 26 sancisce, in capo al titolare del trattamento, l'obbligo di notifica del *data breach* eventualmente occorso, con le modalità previste dall'articolo 33 del Regolamento. Qualora, poi, la violazione di dati personali sia suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone, il titolare è tenuto a effettuare una specifica comunicazione all'interessato senza ingiustificato ritardo.

L'articolo 28 che apre la sezione intitolata al responsabile della protezione dei dati – disciplina la designazione e i requisiti di tale figura, la cui nomina è stata prevista come necessaria anche per l'autorità giudiziaria, in ragione dell'ausilio che tale figura professionale può fornire nella gestione di trattamenti complessi e spesso inerenti dati sensibili, quali appunto quelli svolti in sede giudiziaria.

L'articolo 29 sancisce, in capo al titolare, l'obbligo di coinvolgere adeguatamente e tempestivamente il responsabile della protezione dati in tutte le questioni riguardanti la protezione dati, fornendogli anche le risorse necessarie per assolvere i suoi compiti.

L'articolo 30 indica dettagliatamente tali compiti, di natura non soltanto consultiva ma anche di controllo in ordine alla conformità del trattamento alla relativa disciplina e di cooperazione con il Garante.

Il **Capo IV**, dedicato alla materia relativa al trasferimento dei dati personali verso paesi terzi o verso organizzazioni internazionali, differenzia presupposti, condizioni, modalità e garanzie nella trasmissione, a seconda delle situazioni concrete in cui essa avviene e delle specifiche finalità che si intendono realizzare.

In particolare, **l'articolo 31** individua i principi generali in tale materia, stabilendo che il trasferimento di dati personali oggetto di trattamento, o destinati ad esserlo a seguito del trasferimento verso un paese terzo o un'organizzazione internazionale, inclusi i trasferimenti successivi verso un ulteriore altro paese terzo o organizzazione internazionale, è consentito solo in presenza di specifiche condizioni, segnatamente: il trasferimento è necessario per le finalità di cui all'articolo 1, comma 2, dello schema di decreto; i dati personali sono trasferiti al titolare del trattamento in un paese terzo o a un'organizzazione internazionale che risulti essere un'autorità competente per le finalità di cui all'articolo 1, comma 2; nel caso in cui i dati siano trasmessi o resi disponibili da uno Stato membro, lo stesso abbia fornito la preliminare autorizzazione al trasferimento conformemente al diritto interno; la Commissione dell'Unione Europea abbia adottato una decisione di adeguatezza, a norma dell'articolo 32 (di cui si dirà) o, in mancanza, vi siano garanzie adeguate ai sensi dell'articolo 33, nonché, in assenza di una decisione di adeguatezza e di garanzie adeguate, trovino applicazione deroghe per situazioni specifiche di cui all'articolo 34, nonché, in caso di trasferimento successivo a un altro paese terzo o a un'altra organizzazione internazionale, l'autorità competente che ha effettuato il trasferimento originario o un'altra autorità competente dello stesso Stato membro, autorizzi il trasferimento successivo dopo avere valutato tutti i fattori pertinenti.

Nei casi più gravi, cioè quando il trasferimento di dati personali si renda necessario per prevenire una minaccia grave e immediata alla sicurezza pubblica di uno Stato membro o di un paese terzo o agli interessi vitali di uno Stato membro, si prevede che il trasferimento è eseguito anche senza autorizzazione preliminare se non può essere ottenuta con la tempestività richiesta dalla concreta situazione di emergenza.

L'**articolo 32** riguarda il trasferimento di dati personali effettuato sulla base di una decisione di adeguatezza, che esclude la necessità di autorizzazioni specifiche. La decisione è emessa dalla Commissione dell'Unione europea la quale valuta che il paese terzo, un territorio o uno o più settori specifici all'interno del paese terzo, o l'organizzazione internazionale, garantiscono un livello di protezione adeguato.

All'**articolo 33** sono indicate le garanzie adeguate che devono sussistere in mancanza di una decisione di adeguatezza Commissione dell'Unione europea di cui all'articolo 32, segnatamente: debbono essere fornite garanzie adeguate per la protezione dei dati personali oppure il titolare del trattamento deve ritenere che sussistano garanzie adeguate per la protezione dei dati personali.

In quest'ultimo caso grava sul titolare del trattamento un obbligo di informativa all'autorità di controllo dei trasferimenti effettuati.

L'**articolo 34** prevede, invece, le deroghe in situazioni specifiche, quando manchi una decisione di adeguatezza ai sensi dell'articolo 32 o garanzie adeguate di cui all'articolo 33. In dette ipotesi il trasferimento o una categoria di trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale sono consentiti solo se necessari: a) per tutelare un interesse vitale dell'interessato o di un'altra persona; b) per salvaguardare i legittimi interessi dell'interessato quando lo preveda il diritto dello Stato membro che trasferisce i dati personali; c) per prevenire una minaccia grave e immediata alla sicurezza pubblica di uno Stato membro o di un paese terzo; d) nei casi specifici, per le finalità di cui all'articolo 1, comma 2, oppure e) nel caso specifico, per accertare, esercitare o difendere un diritto in sede giudiziaria in relazione alle finalità di cui all'articolo 1, comma 2.

L'**articolo 35** detta una deroga al principio secondo il quale i dati personali sono trasferiti al titolare del trattamento in un Paese terzo solo se quest'ultima è un'autorità competente per le finalità di cui all'articolo 1, comma 2, consentendo in singoli e specifici casi previsti da norme di legge o dal diritto dell'Unione europea di trasferire i dati direttamente a destinatari stabiliti in Paesi terzi, fatti salvi eventuali accordi internazionali.

Tale eccezione è prevista nei casi in cui il trasferimento è strettamente necessario per l'assolvimento di un compito previsto dal diritto dell'Unione o dall'ordinamento interno, per le finalità di cui all'articolo 1, comma 2; b) l'autorità competente che effettua il trasferimento valuta che i diritti e le libertà fondamentali dell'interessato non prevalgono sull'interesse pubblico che rende necessario il trasferimento; c) l'autorità competente che effettua il trasferimento ritiene che il trasferimento a un'autorità per le finalità di cui all'articolo 1, comma 2, nel Paese terzo sia inefficace o inidoneo, soprattutto in considerazione della tempestività con cui deve essere eseguito; d) l'autorità competente ai fini di cui all'articolo 1, comma 2, nel Paese terzo è informata senza ingiustificato ritardo, sempre se ciò non pregiudichi la finalità per cui il trasferimento è effettuato; e) l'autorità competente che effettua il trasferimento informa il destinatario della finalità specifica o delle finalità specifiche per le quali i dati personali devono essere trattati, a condizione che tale trattamento sia necessario.

Infine all'articolo 36 si stabilisce che restano in vigore, fino alla loro modifica, sostituzione o revoca, gli accordi internazionali relativi al trasferimento di dati personali verso Paesi, terzi o organizzazioni internazionali conclusi anteriormente alla data del 6 maggio 2016, sempre che siano conformi al diritto dell'Unione applicabile a tale data.

Il Capo V dello schema di decreto è intitolato alla tutela e alle sanzioni.

L'articolo 37, in apertura del capo in esame individua nel Garante nazionale, l'autorità deputata a vigilare sul rispetto delle norme attuative della direttiva in funzione della tutela dei diritti e delle libertà fondamentali delle persone fisiche, coinvolti dalle attività di trattamento di dati personali. Si tratta di opzione discendente direttamente dall'articolo 41 della direttiva.
Al Garante - già istituito per legge - le disposizioni in esame attribuiscono "*i poteri e le funzioni di cui all'articolo 154 del Codice*". Si tratta cioè dei compiti già riconosciuti e disciplinati dal vigente Codice in materia di protezione dei dati personali. Sempre al Garante competono i poteri di cui agli articoli da 46 a 49 della Direttiva, esplicitati nel comma 2. Le ulteriori attribuzioni sono modulate su quelle già tipiche del Garante e funzionali al controllo del rispetto delle norme in materia di protezione dei dati personali e alla conseguente tutela dei soggetti lesi da trattamenti illegittimi, mediante la possibilità di reclamo, oltre che di vigilanza e indagine sui titolari del trattamento. Sono infine tipici del Garante i poteri consultivi e le attribuzioni in tema di sensibilizzazione e informazione in materia di trattamento dei dati personali.
Il comma 6 dell'articolo in esame è volto espressamente ad escludere la competenza del Garante "*in ordine al controllo del rispetto delle norme del presente decreto, limitatamente ai trattamenti effettuati dall'autorità giudiziaria nell'esercizio delle funzioni giurisdizionali, nonché di quelle giudiziarie del pubblico ministero*". La disposizione trova la sua fonte nell'articolo 45, paragrafo 2, della direttiva: "Ogni Stato membro dispone che ciascuna autorità di controllo non sia preposta a controllare i trattamenti effettuati dalle autorità giurisdizionali nell'esercizio delle loro funzioni giurisdizionali. Gli Stati membri possono disporre che le rispettive autorità di controllo non siano competenti per il controllo dei trattamenti effettuati da altre autorità giurisdizionali indipendenti nell'esercizio delle loro funzioni giurisdizionali". Agevole spiegazione della esclusione in parola si rinviene nell'esigenza di evitare ogni interferenza con le attribuzioni proprie degli organi giurisdizionali e a tutela delle loro prerogative di indipendenza. Secondo il considerando 80) della direttiva, infatti, "sebbene la presente direttiva si applichi anche alle attività delle autorità giurisdizionali nazionali e di altre autorità giudiziarie, non è opportuno che rientri nella competenza delle autorità di controllo il trattamento di dati personali effettuato dalle autorità giurisdizionali nell'esercizio delle loro funzioni giurisdizionali, al fine di salvaguardare l'indipendenza dei giudici nell'adempimento dei loro compiti giurisdizionali. Tale esenzione dovrebbe essere limitata all'attività giurisdizionale e non applicarsi ad altre attività a cui i giudici potrebbero partecipare in forza del diritto dello Stato membro. Gli Stati membri dovrebbero inoltre poter disporre che nella competenza delle autorità di controllo non rientri il trattamento di dati personali effettuato da altre autorità giudiziarie indipendenti nell'esercizio delle loro funzioni giurisdizionali, ad esempio le procure. In ogni caso, il rispetto delle norme della presente direttiva da parte di autorità giurisdizionali e altre autorità giudiziarie indipendenti è sempre soggetto a un controllo indipendente conformemente all'articolo 8, paragrafo 3, della Carta".

L'articolo 38 dello schema di decreto disciplina le attribuzioni del Garante in tema di cooperazione con le omologhe autorità europee secondo quanto previsto dall'articolo 50 della direttiva.
La norma si ispira ai principi di leale collaborazione ed è funzionale a garantire in via generale l'applicazione e l'attuazione conforme sul territorio dell'Unione della direttiva. Tuttavia l'articolo reca disposizioni specifiche ai fini dello scambio di informazioni di indagine e di esecuzione delle richieste delle autorità straniere ai medesimi fini. In particolare, mediante rinvio alle corrispondenti disposizioni dell'articolo 61 del regolamento (UE) 2016/679, sono stabiliti i termini entro i quali l'assistenza è prestata, nonché le modalità, ispirate a principi di massima semplificazione, anche con riguardo alla possibilità di attività ispettive e di sorveglianza congiunte. La norma fa tuttavia salva la facoltà di rifiutare la richiesta di collaborazione quando essa sia contraria al diritto dell'Unione ovvero a specifiche norme di diritto interno. Si tratta così di salvaguardare i principi fondamentali dell'ordinamento interno laddove le forme di assistenza richiesta siano tali pregiudicare gravemente diritti delle persone coinvolte. Si pensi ai limiti posti all'autorità amministrativa in materia di perquisizione domiciliare collegata ad attività ispettiva.
L'**articolo 39** è dedicato alla disciplina del reclamo al Garante, nonché del ricorso giurisdizionale riconosciuti ai soggetti che lamentino un trattamento, in senso lato, dei propri dati personali in maniera difforme da quanto stabilito in direttiva. È ribadito che dalla disciplina in punto di reclamo sono esclusi i dati trattati nell'ambito di un procedimento giurisdizionale, mediante la formula per cui resta fermo quanto previsto dall'articolo 37, comma 6.
Al di fuori dell'eccezione richiamata, la norma rinvia alle disposizioni vigenti del Codice, con riguardo alla procedura di reclamo. Il Garante avrà cura di prestare l'assistenza necessaria, anche di ufficio, in favore dell'interessato (cfr. articolo 52 della direttiva).
La norma assicura comunque la tutela giurisdizionale attraverso il procedimento per ricorso già disciplinato dagli articoli 152 e ss. del Codice della privacy, pure espressamente richiamati. La previsione discende dalla direttiva secondo la quale "ciascun interessato dovrebbe avere il diritto di proporre reclamo a un'unica autorità di controllo e a un ricorso giurisdizionale effettivo a norma dell'articolo 47 della Carta qualora ritenga che siano stati violati i diritti di cui gode ai sensi delle disposizioni adottate a norma della presente direttiva o se l'autorità di controllo non dà seguito a un reclamo, lo respinge in tutto o in parte o lo archivia o non agisce quando è necessario intervenire per proteggere i diritti dell'interessato". Sotto questo profilo la legislazione vigente già contempla la possibilità che i diritti riconosciuti dalla direttiva "possono essere fatti valere dinanzi all'autorità giudiziaria o con ricorso al Garante" e prevede, altresì, la possibilità di ricorrere contro le decisioni del Garante.
L'**articolo 40** costituisce attuazione dell'articolo 55 della direttiva. Le disposizioni in esame riconoscono la tutela dei diritti contemplati dalla direttiva anche mediante l'esercizio attraverso associazioni ed enti collettivi: "*L'interessato può dare mandato a un ente del terzo settore soggetto alla disciplina del decreto legislativo 3 luglio 2017, n. 117, che sia attivo nel settore della tutela dei diritti e delle libertà degli interessati con riguardo alla protezione dei dati personali, al fine di esercitare per suo conto i diritti di cui all'articolo 39, ferme le disposizioni in materia di patrocinio previste dal codice di procedura civile.*" A questo riguardo si è ritenuto opportuno chiarire che gli enti in parola sono quelli del terzo settore, già soggetti alla disciplina del decreto legislativo 3 luglio 2017, n. 117, a condizione che tali enti siano attivi nello specifico "*settore della tutela dei diritti e delle libertà degli interessati con riguardo alla protezione dei dati personali*". Resta naturalmente ferma la disciplina processuale interna circa i rapporti tra l'azione instaurata singolarmente e l'intervento processuale dell'ente, in ciò risolvendosi la clausola: "*ferme le disposizioni in materia di patrocinio previste dal codice di procedura civile*".

L'**articolo 41** stabilisce che "*il titolare o il responsabile del trattamento sono tenuti, a norma dell'articolo 82 del regolamento, al risarcimento del danno patrimoniale o non patrimoniale cagionato da un trattamento o da qualsiasi altro atto compiuti in violazione delle disposizioni del presente decreto*". Si tratta di norma ricognitiva, dal momento che ribadisce l'obbligo di risarcimento del danno laddove il trattamento sia ritenuto civilmente illecito. La previsione discende da quanto stabilito dall'articolo 56 della direttiva.

L'**articolo 42**, predispone l'apparato di sanzioni amministrative per la violazione delle singole disposizioni del decreto. In mancanza di criteri e principi direttivi contenuti nell'articolo 11 della legge n.163 del 2017, che mantiene ferme le sanzioni penali vigenti, occorre far riferimento ai principi richiamati all'articolo 1 delle medesima legge, che espressamente rinvia all'articolo 32 della legge quadro n. 234 del 2012. I limiti edittali delle sanzioni pecuniarie amministrative pertanto non possono superare nel massimo 150.000 euro. E al riguardo non è invocabile il disallineamento con analoghe previsioni sanzionatorie del regolamento: la predisposizione in ipotesi di sanzioni pecuniarie amministrative più elevate si scontrerebbe con i limiti della delega legislativa.

Si è inteso pertanto punire con le sanzioni più elevate (da 50.000 a 150.000 euro) le violazioni inerenti le modalità del trattamento, al fine di assicurare la piena corrispondenza al principio di legalità sul piano del vincolo finalistico determinato per legge dell'attività di trattamento, nonché agli ulteriori principi di correttezza, esattezza, aggiornamento, temporaneità e sicurezza previsti dall'art. 3 lettere a) b), d), e) e f). È fatta salva naturalmente l'attività che deroga ai predetti principi sempre per espressa previsione di legge. Con le medesime sanzioni sono punite le violazioni in tema di predisposizione delle misure che garantiscono l'esattezza e la completezza dei dati destinati alla trasmissione o comunicazione (art. 4 commi 2 e 3), nonché quelle relative al trattamento in casi specifici (art. 6, commi 3 e 4) . Analoga gravità rivestono le violazioni delle norme dedicate al trattamento di dati sensibili (art. 7) e alla gestione automatizzata dei dati, anche sotto il profilo del divieto di profilazione, alle condizioni indicate dall'art. 8, e alla garanzia dell'intervento correttivo umano a richiesta dell'interessato. È prevista la medesima sanzione anche per le attività di trasferimento dei dati verso paesi terzi in mancanza delle condizioni di legge, vale a dire laddove manchi la decisione di adeguatezza, unica che autorizza il trasferimento, o non ricorrano le ulteriori condizioni che comunque lo consentirebbero, come disciplinate dagli articoli 33 e 34 del decreto.

Il comma 2 è dedicato alle violazioni ritenute meno gravi, inerenti l'esercizio dei diritti di informazione, accesso, rettifica o cancellazione dei dati personali e limitazione del trattamento, nonché le limitazioni all'esercizio di detti diritti. La sanzione indicata nel massimo di 80.000 euro si applica anche alle violazioni formali dei doveri facenti capo al titolare del trattamento, come indicati dai singoli articoli del decreto richiamati.

Nell'applicazione delle sanzioni il Garante si atterrà ai criteri direttivi specificamente indicati dal Regolamento all'articolo 83, paragrafo 2, al fine di adeguare la sanzione alle specificità del caso concreto.

Infine il comma 4 rinvia per il procedimento di applicazione alle vigenti norme del Codice.

Il **Capo VI** è intitolato agli illeciti penali. Il criterio direttivo è, quindi, quello ricavabile dall'articolo 11 delle legge di delega, che stabilisce espressamente che resta ferma la disciplina vigente per le fattispecie penali già oggetto di previsione. Ne discende che non si è intervenuti sui reati già contemplati dal codice penale (articoli 615 bis e ss. c.p., posti a tutela del domicilio informatico e dell'integrità dei sistemi). Si è, in contrario, reso necessario intervenire sugli illeciti

contemplati dal Codice della privacy al fine di garantire continuità normativa alle norme penali ivi stabilite, limitatamente ai dati trattati per finalità di prevenzione, repressione e accertamento dei reati. Accanto alle fattispecie penali già esistenti, si sono poi introdotti due nuovi reati, per le violazioni di maggiore offensività.

L'**articolo 43, comma 1**, punisce il trattamento illecito di dati personali per violazione dell'art. 5, comma 1, perché effettuato al di fuori dei casi consentiti dal diritto dell'Unione o da disposizione di legge o di regolamento o per finalità estranee a quelle dell'articolo 1, comma 2. La norma si pone in continuità con quanto previsto dall'art. 167 del Codice della privacy, quale delitto caratterizzato, sul piano soggettivo, dal fine di profitto o di danno e, sul piano oggettivo, dalla circostanza che dal fatto derivi nocumento.

L'**articolo 43 comma 1** contiene altresì la nuova fattispecie incriminatrice del trattamento di dati in violazione dell'art. 8, comma 4, ossia la profilazione finalizzata alla discriminazione.

L'**articolo 43, comma 2**, prevede, come nuova fattispecie incriminatrice, il trattamento illecito dei dati sensibili (quelli cioè che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona, oggi disciplinati dall'articolo 9 del regolamento, cui rinvia l'art. 7 del presente schema di decreto).

L'**articolo 44** riproduce sostanzialmente il contenuto dell'art.168 del Codice, punendo le attività di falsificazione, volte a ostacolare quindi il controllo del Garante, già punite dalla norma citata.

Analogamente gli **articoli 45** e **46** riproducono il contenuto dei vigenti articoli 170 e 172 del Codice, in tema di inosservanza dei provvedimenti del garante e di pene accessorie.

L'**articolo 47** riproduce nello schema di decreto le norme attualmente vigenti e contenute nel Codice della privacy relative alla particolari modalità di trattamento dei dati da parte delle forze di polizia, nonché al centro elaborazione dati, in uso alle medesime, istituito con legge n. 121 del 1981. Norme che, pertanto, vengono meramente trasferite nel presente testo, senza alcuna innovazione, per ragioni di ordine sistematico e per completezza della disciplina in materia.

Analogamente per quanto concerne l'**articolo 48**, dedicato alla tutela dell'interessato rispetto a tale tipo di trattamento.

L'**articolo 49** dispone le abrogazioni delle norme del Codice concernenti il trattamento dei dati da parte delle Forze di polizia, ormai confluite nel presente testo o superate dalle nuove norme e fa salve, sino all'eventuale adozione di nuova disciplina ai sensi degli articoli 5, comma 2, e 9, comma 5, le disposizioni recate dal recente decreto del Ministro dell'Interno in data 24 maggio 2017, nonché dai decreti del Presidente della Repubblica di attuazione dell'articolo 57 del decreto legislativo 30 giugno 2003, n. 196.

L'**articolo 50** reca la clausola di invarianza finanziaria.

SCHEMA DI DECRETO LEGISLATIVO RECANTE ATTUAZIONE DELLA DIRETTIVA (UE) 2016/680/UE, DEL PARLAMENTO EUROPEO E DEL CONSIGLIO DEL 27 APRILE 2016, RELATIVA ALLA PROTEZIONE DELLE PERSONE FISICHE CON RIGUARDO AL TRATTAMENTO DEI DATI PERSONALI DA PARTE DELLE AUTORITÀ COMPETENTI A FINI DI PREVENZIONE, INDAGINE, ACCERTAMENTO E PERSEGUIMENTO DI REATI O ESECUZIONE DI SANZIONI PENALI, NONCHÉ ALLA LIBERA CIRCOLAZIONE DI TALI DATI E CHE ABROGA LA DECISIONE QUADRO 2008/977/GAI DEL CONSIGLIO.

Tabella di concordanza

Direttiva n. 2016/680/UE	Norme di recepimento	Legislazione nazionale e commenti
CAPO I ***Disposizioni generali*** *Articolo 1* **Oggetto e obiettivi**	CAPO I DISPOSIZIONI GENERALI ART. 1 (*Oggetto e ambito di applicazione*)	Gli articoli 1 e 2 della direttiva sono stati integralmente recepiti nell'articolo 1 dello schema di decreto.
1. La presente direttiva stabilisce le norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia e la prevenzione di minacce alla sicurezza pubblica. 2. Ai sensi della presente direttiva gli Stati membri: a)tutelano i diritti e le libertà fondamentali delle persone fisiche, in particolare il diritto	1. Il presente decreto attua nell'ordinamento interno le disposizioni della direttiva 27 aprile 2016, n. (UE)2016/680/UE del Parlamento europeo e del Consiglio del 27 aprile 2016 relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di tutela della sicurezza e dell'ordine pubblico, di prevenzione, e repressione dei reati indagine, accertamento e perseguimento di reati o di esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati, e che abroga la	

alla protezione dei dati personali; e b) garantiscono che lo scambio dei dati personali da parte delle autorità competenti all'interno dell'Unione, qualora tale scambio sia richiesto dal diritto dell'Unione o da quello dello Stato membro, non sia limitato né vietato per motivi attinenti alla protezione delle persone fisiche con riguardo al trattamento dei dati personali. 3. La presente direttiva non pregiudica la facoltà degli Stati membri di prevedere garanzie più elevate di quelle in essa stabilite per la tutela dei diritti e delle libertà dell'interessato con riguardo al trattamento dei dati personali da parte delle autorità competenti.	decisione quadro 2008/977/GAI del Consiglio. 2. Il presente decreto si applica al trattamento interamente o parzialmente automatizzato di dati personali delle persone fisiche e al trattamento non automatizzato di dati personali delle persone fisiche contenuti in un archivio o ad esso destinati, svolti dalle autorità competenti per finalità di tutela della sicurezza e dell'ordine pubblico, a fini di prevenzione, indagine, accertamento e repressione perseguimento di reati, o di esecuzione di sanzioni penali, incluse la salvaguardia contro e la prevenzione di minacce alla sicurezza pubblica. 3. Il presente decreto non si applica ai trattamenti di dati personali: a) effettuati nello svolgimento di attività concernenti la sicurezza nazionale o rientranti nell'ambito di applicazione del titolo V capo 2 del trattato sull'Unione europea e per tutte le attività che non rientrano nell'ambito di applicazione del diritto dell'Unione europea; b) effettuati da istituzioni, organi, uffici e agenzie dell'Unione europea.	
Articolo 2 **Ambito di applicazione** 1. La presente direttiva si applica al trattamento dei dati personali da parte delle autorità competenti per le finalità di cui all'articolo 1, paragrafo 1. 2. La presente direttiva 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. 3. La presente direttiva non si applica ai trattamenti di dati personali:		

a) effettuati per attività che non rientrano nell'ambito di applicazione del diritto dell'Unione; b) effettuati da istituzioni, organi, uffici e agenzie dell'Unione.		
Articolo 3 **Definizioni** Ai fini della presente direttiva si intende per: 1) **«dati personali»**: qualsiasi informazione riguardante una persona fisica identificata o identificabile, (l'«interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, in particolare con riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici dell'identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale di tale persona fisica; 2) **«trattamento»**: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi	ART. 2 (*Definizioni*) 1. Ai fini del presente decreto, si applicano le seguenti definizioni: a) dati personali: qualsiasi informazione riguardante una persona fisica; b) l'interessato: la persona fisica, identificata o identificabile, alla quale si riferiscono i dati personali. Si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, in particolare con riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici dell'identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale di tale persona fisica; c) trattamento: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati, applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a	La disposizione della direttiva è stata integralmente recepita dallo schema di decreto.

altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione; 3) **«limitazione di trattamento»**: il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro; 4) **«profilazione»**: qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica; 5) **«pseudonimizzazione»**: il 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 i dati personali non siano attribuiti a una persona fisica identificata o identificabile; 6) **«archivio»**: qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico;	disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione; d) limitazione di trattamento: il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro; e) pseudonimizzazione: il 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 i dati personali non siano attribuiti a una persona fisica identificata o identificabile f) profilazione: qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica; g) archivio: qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico; h) autorità competente: 1) qualsiasi autorità pubblica dello Stato, di uno Stato membro dell'Unione europea o di	

7) «**autorità competente**»: a) qualsiasi autorità pubblica competente in materia di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia contro e la prevenzione di minacce alla sicurezza pubblica; o b) qualsiasi altro organismo o entità incaricati dal diritto dello Stato membro di esercitare l'autorità pubblica e i poteri pubblici a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia e la prevenzione di minacce alla sicurezza pubblica; 8) «**titolare del trattamento**»: l'autorità competente che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o dello Stato membro, il titolare del trattamento o i criteri specifici applicabili alla sua nomina possono essere previsti dal diritto dell'Unione o dello Stato membro; 9) «**responsabile del trattamento**»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento; 10) «**destinatario**»: la persona fisica o	uno Stato terzo competente in materia di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia contro e la prevenzione di minacce alla sicurezza pubblica; 2) qualsiasi altro organismo o entità incaricato dagli ordinamenti interni di esercitare l'autorità pubblica e i poteri pubblici a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia e la prevenzione di minacce alla sicurezza pubblica; i) titolare del trattamento: l'autorità competente che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione europea o dello Stato, i criteri specifici applicabili alla sua nomina possono essere previsti dal diritto dell'Unione europea o dello Stato; l) responsabile del trattamento: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento; m) destinatario: la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione europea o dello Stato non	

giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o dello Stato membro non sono considerate destinatari; il trattamento di tali dati da parte di tali autorità pubbliche è conforme alle norme in materia di protezione dei dati applicabili secondo le finalità del trattamento; 11) **«violazione dei dati personali»**: la violazione della sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati; 12) **«dati genetici»**: i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica, che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione; 13) **«dati biometrici»**: i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici;	sono considerate destinatari; il trattamento di tali dati da parte di tali autorità pubbliche è conforme alle norme in materia di protezione dei dati applicabili secondo le finalità del trattamento; n) violazione dei dati personali: la violazione della sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati; o) dati genetici: i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica, che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione; p) dati biometrici: i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici; q) dati relativi alla salute: i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute; r) file di log: registro degli accessi e delle operazioni; s) autorità di controllo: l'autorità pubblica indipendente istituita negli Stati membri ai	

14) «**dati relativi alla salute**»: i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute; 15) «**autorità di controllo**»: l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 41; 16) «**organizzazione internazionale**»: un'organizzazione e gli organismi di diritto internazionale pubblico a essa subordinati o qualsiasi altro organismo istituito da o sulla base di un accordo tra due o più Stati.	sensi dell'articolo 41 della direttiva; t) il Garante: autorità di controllo nell'ordinamento interno, individuata nel Garante per la protezione dei dati personali, istituito dal decreto legislativo 30 giugno 2003, n. 196; u) organizzazione internazionale: un'organizzazione e gli organismi di diritto internazionale pubblico a essa subordinati o qualsiasi altro organismo istituito da o sulla base di un accordo tra due o più Stati; v) Codice: Codice in materia di protezione dei dati personali, adottato con il decreto legislativo 30 giugno 2003, n. 196; z) Stato membro: Stato membro dell'Unione europea; aa) Paese terzo: Stato non membro dell'Unione europea; bb) direttiva: la direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio (se non già compresa nelle definizioni generali) del 27 aprile 2016; cc) regolamento: il regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016; dd) Forze di polizia: le Forze di polizia di cui all'articolo 16 della legge 1° aprile 1981, n. 121	
CAPO II ***Principi***	ART. 3 (*Principi applicabili al trattamento di dati personali*)	La disposizione della direttiva è stata integralmente recepita dallo schema di decreto.

Articolo 4 **Principi applicabili al trattamento di dati personali** 1. Gli Stati membri dispongono che i dati personali siano: a) trattati in modo lecito e corretto; b)raccolti per finalità determinate, esplicite e legittime e trattati in modo non incompatibile con tali finalità; c)adeguati, pertinenti e non eccedenti rispetto alle finalità per le quali sono trattati; d)esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati; e)conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati; f)trattati in modo da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non	1. I dati personali di cui all'articolo 1, comma 2, sono: a) trattati in modo lecito e corretto; b) raccolti per finalità determinate, espresse e legittime e trattati in modo compatibile con tali finalità; c) adeguati, pertinenti e non eccedenti rispetto alle finalità per le quali sono trattati; d) esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati; e) conservati con modalità che consentano l'identificazione degli interessati per il tempo necessario al conseguimento delle finalità per le quali sono trattati, sottoposti a esame periodico per verificarne la persistente necessità di conservazione, cancellati o anonimizzati una volta decorso tale termine; f) trattati in modo da garantire un'adeguata sicurezza e protezione da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali, mediante l'adozione di misure tecniche e organizzative adeguate. 2. Il trattamento per una delle finalità di cui all'articolo 1, comma 2, diversa da quella per cui sono raccolti, è consentito se il titolare del trattamento, anche se diverso da quello che ha raccolto i dati, è autorizzato a trattarli per detta finalità, conformemente al diritto dell'Unione europea o dell'ordinamento interno e se il trattamento è necessario e proporzionato a tale	

autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali. 2. Il trattamento da parte dello stesso o di un altro titolare del trattamento per una qualsiasi delle finalità di cui all'articolo 1, paragrafo 1, diversa da quella per cui sono raccolti i dati personali, è consentito nella misura in cui: a) il titolare del trattamento è autorizzato a trattare tali dati personali per detta finalità conformemente al diritto dell'Unione o dello Stato membro; e b) il trattamento è necessario e proporzionato a tale altra finalità conformemente al diritto dell'Unione o dello Stato membro. 3. Il trattamento da parte dello stesso o di un altro titolare del trattamento può comprendere l'archiviazione nel pubblico interesse, l'utilizzo scientifico, storico o statistico per le finalità di cui all'articolo 1, paragrafo 1, fatte salve le garanzie adeguate per i diritti e le libertà degli interessati. 4. Il titolare del trattamento è competente per il rispetto dei paragrafi 1, 2 e 3 e in grado di comprovarlo.	diversa finalità, conformemente al diritto dell'Unione europea o dell'ordinamento interno. 3. Il trattamento per le finalità di cui all'articolo 1, comma 2, può comprendere l'archiviazione nel pubblico interesse, l'utilizzo scientifico, storico o statistico, fatte salve le garanzie adeguate per i diritti e le libertà degli interessati. 4. Il titolare del trattamento è responsabile del rispetto dei principi di cui ai commi 1, 2 e 3.	
Articolo 5 **Termini per conservazione ed esame** Gli Stati membri dispongono che siano fissati adeguati termini per la cancellazione dei dati personali o per un esame periodico della	ART. 5 (*Liceità del trattamento*) 1. [..] 2. Con decreto del Presidente della Repubblica, adottato ai sensi dell'articolo 17, comma 1, della legge 23 agosto 1988, n. 400,	Per il recepimento dell'art. 5 della direttiva si prevede l'adozione di norme regolamentari che disciplinino, ove già non stabiliti da disposizioni di legge o di regolamento, i termini e le modalità di conservazione dei dati. Si segnala che nell'ordinamento interno i

necessità della conservazione dei dati personali. Misure procedurali garantiscono che tali termini siano rispettati.	sono individuati, per i trattamenti o le categorie di trattamenti non occasionali di cui al comma 1, i termini, ove non già stabiliti da disposizioni di legge o di regolamento, e le modalità di conservazione dei dati, i soggetti legittimati ad accedervi, le condizioni di accesso, le modalità di consultazione, nonché le modalità e le condizioni per l'esercizio dei diritti di cui agli articoli 9, 10, 11 e 13.	termini e le modalità di conservazione sono già disciplinati con riferimento ad alcune categorie di dati trattati nel settore penale. Di seguito, si richiamano le disposizioni di maggior rilievo: **D.M. 27 marzo 2000, n. 264 Regolamento recante norme per la tenuta dei registri presso gli uffici giudiziari** Art. 12. *Obblighi di conservazione e di custodia* 1. I registri e gli atti tenuti in modo informatico sono conservati per il tempo previsto dal decreto legislativo 29 ottobre 1999, n. 490. 2. I soggetti di cui all'articolo 7, comma 1, curano la conservazione dei registri e degli atti di cui al precedente comma 1, mediante l'utilizzo di supporti non riscrivibili, rinnovati a scadenze prestabilite e secondo le regole tecniche emanate dall'Autorità per l'informatica nella pubblica amministrazione a norma dell'articolo 2, comma 15, della legge 24 dicembre 1993, n. 537. 3. I soggetti di cui al comma 2 procedono, almeno ogni tre anni, alla formazione di una copia storica dell'archivio e ne dispongono la conservazione nei modi di cui al comma 2. Eseguita tale operazione dal registro in uso possono essere eliminati gli atti relativi agli affari esauriti da almeno due anni. **D.P.R. 7 aprile 2016, n. 87** **(Regolamento recante disposizioni di attuazione della legge 30 giugno 2009, n. 85,**

concernente l'istituzione della banca dati nazionale del DNA e del laboratorio centrale per la banca dati nazionale del DNA, ai sensi dell'articolo 16 della legge n. 85 del 2009).

Art. 25. *Tempi di conservazione dei profili del DNA*

1. I profili del DNA ottenuti dai soggetti di cui all'articolo 9 della legge sono conservati per trenta anni dalla data dell'ultima registrazione di cui all'articolo 5, comma 1.

2. Quando il profilo del DNA si riferisce a persone condannate con sentenza irrevocabile per uno o più dei reati per i quali la legge prevede l'arresto obbligatorio in flagranza, o per taluno dei reati di cui all'articolo 407, comma 2, lettera a), del codice di procedura penale, il periodo di conservazione è elevato a quaranta anni dalla data dell'ultima registrazione di cui all'articolo 5.

3. Il profilo del DNA ottenuto da un soggetto di cui all'articolo 9 della legge nei cui confronti, in sede di emissione di sentenza di condanna irrevocabile, sia stata ritenuta la recidiva, è conservato per quaranta anni.

4. In caso di concordanza del profilo del DNA ottenuto da un reperto con quello ottenuto da un campione, nella Banca dati è conservato il solo profilo del DNA acquisito dal campione biologico di cui ai commi 1, 2 e 3 per la durata massima ivi prevista.

D.LGS. 30 giugno 2003, n. 196 (Codice in materia di protezione dei dati personali).

		Art. 132 *Conservazione di dati di traffico per altre finalità* 1. Fermo restando quanto previsto dall'articolo 123, comma 2, i dati relativi al traffico telefonico sono conservati dal fornitore per ventiquattro mesi dalla data della comunicazione, per finalità di accertamento e repressione di reati, mentre, per le medesime finalità, i dati relativi al traffico telematico, esclusi comunque i contenuti delle comunicazioni, sono conservati dal fornitore per dodici mesi dalla data della comunicazione. 1-bis. I dati relativi alle chiamate senza risposta, trattati temporaneamente da parte dei fornitori di servizi di comunicazione elettronica accessibili al pubblico oppure di una rete pubblica di comunicazione, sono conservati per trenta giorni. [2. Decorso il termine di cui al comma 1, i dati relativi al traffico telefonico, inclusi quelli concernenti le chiamate senza risposta, sono conservati dal fornitore per ulteriori ventiquattro mesi e quelli relativi al traffico telematico, esclusi comunque i contenuti delle comunicazioni, sono conservati per ulteriori sei mesi per esclusive finalità di accertamento e repressione dei delitti di cui all'articolo 407, comma 2, lettera a) del codice di procedura penale, nonché dei delitti in danno di sistemi informatici o telematici.] 3. Entro il termine di cui al comma 1, i dati sono acquisiti presso il fornitore con decreto motivato del pubblico ministero anche su

		istanza del difensore dell'imputato, della persona sottoposta alle indagini, della persona offesa e delle altre parti private. Il difensore dell'imputato o della persona sottoposta alle indagini può richiedere, direttamente al fornitore i dati relativi alle utenze intestate al proprio assistito con le modalità indicate dall'articolo 391-quater del codice di procedura penale, ferme restando le condizioni di cui all'articolo 8, comma 2, lettera f), per il traffico entrante. [4. Dopo la scadenza del termine indicato al comma 1, il giudice autorizza l'acquisizione dei dati, con decreto motivato, se ritiene che sussistano sufficienti indizi dei delitti di cui all'articolo 407, comma 2, lettera a), del codice di procedura penale, nonché dei delitti in danno di sistemi informatici o telematici.] [4-bis. Nei casi di urgenza, quando vi è fondato motivo di ritenere che dal ritardo possa derivare grave pregiudizio alle indagini, il pubblico ministero dispone la acquisizione dei dati relativi al traffico telefonico con decreto motivato che è comunicato immediatamente, e comunque non oltre ventiquattro ore, al giudice competente per il rilascio dell'autorizzazione in via ordinaria. Il giudice, entro quarantotto ore dal provvedimento, decide sulla convalida con decreto motivato. Se il decreto del pubblico ministero non è convalidato nel termine stabilito, i dati acquisiti non possono essere utilizzati.] 4-ter. Il Ministro dell'interno o, su sua delega, i responsabili degli uffici centrali specialistici in

		materia informatica o telematica della Polizia di Stato, dell'Arma dei carabinieri e del Corpo della guardia di finanza, nonché gli altri soggetti indicati nel comma 1 dell'articolo 226 delle norme di attuazione, di coordinamento e transitorie del codice di procedura penale, di cui al decreto legislativo 28 luglio 1989, n. 271, possono ordinare, anche in relazione alle eventuali richieste avanzate da autorità investigative straniere, ai fornitori e agli operatori di servizi informatici o telematici di conservare e proteggere, secondo le modalità indicate e per un periodo non superiore a novanta giorni, i dati relativi al traffico telematico, esclusi comunque i contenuti delle comunicazioni, ai fini dello svolgimento delle investigazioni preventive previste dal citato articolo 226 delle norme di cui al decreto legislativo n. 271 del 1989, ovvero per finalità di accertamento e repressione di specifici reati. Il provvedimento, prorogabile, per motivate esigenze, per una durata complessiva non superiore a sei mesi, può prevedere particolari modalità di custodia dei dati e l'eventuale indisponibilità dei dati stessi da parte dei fornitori e degli operatori di servizi informatici o telematici ovvero di terzi. 4-quater. Il fornitore o l'operatore di servizi informatici o telematici cui è rivolto l'ordine previsto dal comma 4-ter deve ottemperarvi senza ritardo, fornendo immediatamente all'autorità richiedente l'assicurazione dell'adempimento. Il fornitore o l'operatore di servizi informatici o telematici è tenuto a

		mantenere il segreto relativamente all'ordine ricevuto e alle attività conseguentemente svolte per il periodo indicato dall'autorità. In caso di violazione dell'obbligo si applicano, salvo che il fatto costituisca più grave reato, le disposizioni dell'articolo 326 del codice penale. 4-quinquies. I provvedimenti adottati ai sensi del comma 4-ter sono comunicati per iscritto, senza ritardo e comunque entro quarantotto ore dalla notifica al destinatario, al pubblico ministero del luogo di esecuzione il quale, se ne ricorrono i presupposti, li convalida. In caso di mancata convalida, i provvedimenti assunti perdono efficacia. 5. Il trattamento dei dati per le finalità di cui al comma 1 è effettuato nel rispetto delle misure e degli accorgimenti a garanzia dell'interessato prescritti ai sensi dell'articolo 17, volti a garantire che i dati conservati possiedano i medesimi requisiti di qualità, sicurezza e protezione dei dati in rete, nonché a: a) prevedere in ogni caso specifici sistemi di autenticazione informatica e di autorizzazione degli incaricati del trattamento di cui all'allegato b); [b) disciplinare le modalità di conservazione separata dei dati una volta decorso il termine di cui al comma 1;] [c) individuare le modalità di trattamento dei dati da parte di specifici incaricati del trattamento in modo tale che, decorso il termine di cui al comma 1, l'utilizzazione dei dati sia consentita solo nei casi di cui al

		comma 4 e all'articolo 7;] d) indicare le modalità tecniche per la periodica distruzione dei dati, decorsi i termini di cui al comma 1. **LEGGE 20 novembre 2017, n. 167.** **(Disposizioni per l'adempimento degli obblighi derivanti dall'appartenenza dell'Italia all'Unione europea - Legge europea 2017)** Art. 24. *Termini di conservazione dei dati di traffico telefonico e telematico* 1. In attuazione dell'articolo 20 della direttiva (UE) 2017/541 del Parlamento europeo e del Consiglio, del 15 marzo 2017, sulla lotta contro il terrorismo e che sostituisce la decisione quadro 2002/475/GAI del Consiglio, al fine di garantire strumenti di indagine efficace in considerazione delle straordinarie esigenze di contrasto del terrorismo, anche internazionale, per le finalità dell'accertamento e della repressione dei reati di cui agli articoli 51, comma 3-quater, e 407, comma 2, lettera a), del codice di procedura penale il termine di conservazione dei dati di traffico telefonico e telematico nonché dei dati relativi alle chiamate senza risposta, di cui all'articolo 4-bis, commi 1 e 2, del decreto-legge 18 febbraio 2015, n. 7, convertito, con modificazioni, dalla legge 17 aprile 2015, n. 43, è stabilito in settantadue mesi, in deroga a quanto previsto dall'articolo 132, commi 1 e 1-bis, del codice in materia di protezione dei dati personali, di cui al decreto legislativo 30 giugno 2003, n.

196.

Codice di procedura penale

art. 269. *Conservazione della documentazione.*

1. I verbali e le registrazioni, e ogni altro atto ad esse relativo, sono conservati integralmente in apposito archivio riservato presso l'ufficio del pubblico ministero che ha richiesto ed eseguito le intercettazioni, e sono coperti da segreto. Al giudice per le indagini preliminari e ai difensori dell'imputato per l'esercizio dei loro diritti e facoltà è in ogni caso consentito l'accesso all'archivio e l'ascolto delle conversazioni o comunicazioni registrate.

1-bis. Non sono coperti da segreto i verbali e le registrazioni delle comunicazioni e conversazioni acquisite al fascicolo di cui all'articolo 373, comma 5.

2. Salvo quanto previsto dall'articolo 271 comma 3, le registrazioni sono conservate fino alla sentenza non più soggetta a impugnazione. Tuttavia gli interessati, a tutela della riservatezza, possono chiedere la distruzione delle registrazioni non acquisite al giudice che ha autorizzato o convalidato l'intercettazione. Il giudice decide in camera di consiglio a norma dell'articolo 127.

3. La distruzione, nei casi in cui è prevista, viene eseguita sotto controllo del giudice. Dell'operazione è redatto verbale.

Art. 271. *Divieti di utilizzazione.*

1. I risultati delle intercettazioni non possono essere utilizzati qualora le stesse siano state

		eseguite fuori dei casi consentiti dalla legge o qualora non siano state osservate le disposizioni previste dagli articoli 267 e 268 commi 1 e 3. 1-bis. Non sono in ogni caso utilizzabili i dati acquisiti nel corso delle operazioni preliminari all'inserimento del captatore informatico sul dispositivo elettronico portatile e i dati acquisiti al di fuori dei limiti di tempo e di luogo indicati nel decreto autorizzativo. 2. Non possono essere utilizzate le intercettazioni relative a conversazioni o comunicazioni delle persone indicate nell'articolo 200 comma 1, quando hanno a oggetto fatti conosciuti per ragione del loro ministero, ufficio o professione, salvo che le stesse persone abbiano deposto sugli stessi fatti o li abbiano in altro modo divulgati. 3. In ogni stato e grado del processo il giudice dispone che la documentazione delle intercettazioni previste dai commi 1, 1-bis e 2 sia distrutta, salvo che costituisca corpo del reato . **D.P.R. 14 novembre 2002, n. 313** **(Testo unico delle disposizioni legislative e regolamentari in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti).** Art. 5 *Eliminazione delle iscrizioni* 1. Le iscrizioni nel casellario giudiziale sono eliminate al compimento dell'ottantesimo anno di età o per morte della persona alla quale si

		riferiscono. 2. Sono, inoltre, eliminate le iscrizioni relative: a) ai provvedimenti giudiziari revocati a seguito di revisione, o a norma dell'articolo 673, del codice di procedura penale; b) ai provvedimenti giudiziari dichiarati mancanti o non esecutivi o dei quali è stata sospesa l'esecuzione o disposta la restituzione nel termine, ai sensi dell'articolo 670, del codice di procedura penale; c) ai provvedimenti giudiziari di proscioglimento o di non luogo a procedere per difetto di imputabilità, trascorsi dieci anni in caso di delitto o tre anni in caso di contravvenzione dal giorno in cui il provvedimento è divenuto irrevocabile o, nel caso di non luogo a procedere, dal giorno in cui è scaduto il termine per l'impugnazione; d) ai provvedimenti giudiziari di condanna per contravvenzioni per le quali è stata inflitta la pena dell'ammenda, salvo che sia stato concesso alcuno dei benefici di cui agli articoli 163 e 175 del codice penale, trascorsi dieci anni dal giorno in cui la pena è stata eseguita ovvero si è in altro modo estinta; d-bis) ai provvedimenti giudiziari che hanno dichiarato la non punibilità ai sensi dell'articolo 131-bis del codice penale, trascorsi dieci anni dalla pronuncia; e) ai provvedimenti giudiziari di proscioglimento per difetto di imputabilità emessi dal giudice di pace, trascorsi tre anni dal giorno in cui il provvedimento è divenuto irrevocabile;

		f) ai provvedimenti giudiziari di proscioglimento per difetto di imputabilità relativi ai reati di competenza del giudice di pace, emessi da un giudice diverso, limitatamente alle iscrizioni concernenti questi reati, trascorsi tre anni dal giorno in cui il provvedimento è divenuto irrevocabile; g) ai provvedimenti giudiziari di condanna emessi dal giudice di pace, trascorsi cinque anni dal giorno in cui la sanzione è stata eseguita se è stata inflitta la pena pecuniaria, o dieci anni se è stata inflitta una pena diversa, se nei periodi indicati non è stato commesso un ulteriore reato; h) ai provvedimenti giudiziari di condanna relativi ai reati di competenza del giudice di pace emessi da un giudice diverso, limitatamente alle iscrizioni concernenti questi reati, trascorsi cinque anni dal giorno in cui la sanzione è stata eseguita se è stata inflitta la pena pecuniaria, o dieci anni se è stata inflitta una pena diversa, se nei periodi indicati non è stato commesso un ulteriore reato; [i) ai provvedimenti giudiziari con i quali l'imprenditore è stato dichiarato fallito ed è stato chiuso il fallimento, quando il fallimento è revocato con provvedimento definitivo;] l) ai provvedimenti amministrativi di espulsione, quando sono annullati con provvedimento giudiziario o amministrativo definitivo; l-bis) ai provvedimenti con cui il giudice dispone la sospensione del procedimento ai sensi dell'articolo 420-quater del codice di

		procedura penale, quando il provvedimento è revocato. 3. Se sono state applicate misure di sicurezza, i termini previsti dal comma 2 decorrono dalla data della revoca della misura di sicurezza e, se questa è stata applicata o sostituita con provvedimento giudiziario di esecuzione, è eliminata anche l'iscrizione relativa a quest'ultimo. 4. Le iscrizioni di provvedimenti giudiziari relativi a minori di età sono eliminate al compimento del diciottesimo anno di età della persona cui si riferiscono, eccetto quelle relative al perdono giudiziale, che sono eliminate al compimento del ventunesimo anno, ed eccetto quelle relative ai provvedimenti di condanna a pena detentiva, anche se condizionalmente sospesa. Art. 5-quater *Eliminazione delle iscrizioni* 1. Le iscrizioni nel casellario giudiziale europeo sono eliminate a seguito di identica eliminazione comunicata dall'autorità centrale di altro Stato membro di condanna. Art. 8 *Eliminazioni delle iscrizioni* 1.Le iscrizioni nel casellario dei carichi pendenti sono eliminate: a) al compimento dell'ottantesimo anno di età o per morte della persona alla quale si riferiscono; b) alla cessazione della qualità di imputato ai sensi dell'articolo 60, comma 2, del codice di procedura penale.

		Art. 11 *Eliminazione delle iscrizioni* 1. Le iscrizioni nell'anagrafe delle sanzioni amministrative sono eliminate trascorsi cinque anni dal giorno in cui è stata eseguita la sanzione pecuniaria, o trascorsi dieci anni dal giorno in cui è cessata l'esecuzione di qualunque altra diversa sanzione, se negli stessi periodi non è stato commesso un ulteriore illecito amministrativo. Art. 14 *Eliminazione delle iscrizioni* 1. Le iscrizioni dell'anagrafe dei carichi pendenti delle sanzioni amministrative sono eliminate alla cessazione della qualità di ente sottoposto al procedimento di accertamento relativo agli illeciti amministrativi dipendenti da reato.
Articolo 6 **Distinzione tra diverse categorie di interessati** Gli Stati membri dispongono che il titolare del trattamento, se del caso e nella misura del possibile, operi una chiara distinzione tra i dati personali delle diverse categorie di interessati, quali: a)le persone per le quali vi sono fondati motivi di ritenere che abbiano commesso o stiano per commettere un reato; b) le persone condannate per un reato;	ART. 4 *(Conservazione e verifica della qualità dei dati, distinzione tra categorie di interessati e di dati)* 1. Il titolare del trattamento, se necessario rispetto alla finalità di trattamento e per quanto possibile, distingue i dati personali in relazione alle diverse categorie di interessati previste dalla legge, i dati fondati su fatti da quelli fondati su valutazioni. 2. [...] 3. [...]	La disposizione della direttiva si ritiene adeguatamente recepita dallo schema di decreto mediante la previsione di una distinzione dei dati personali effettuata sulla base delle categorie di interessati previste dalla legge. Quanto alla normativa interna già in vigore, che in larga misura contiene prescrizioni conformi alla direttiva, si fa rinvio al D.M. 27 marzo 2000, n. 264, Regolamento recante norme per la tenuta dei registri presso gli uffici giudiziari e correlate regole procedurali, adottate con decreto ministeriale 27 aprile 2009 (cfr. quanto esposto sub art. 20 dello schema di decreto)

c)le vittime di reato o le persone che alcuni fatti autorizzano a considerare potenziali vittime di reato, e d)altre parti rispetto a un reato, quali le persone che potrebbero essere chiamate a testimoniare nel corso di indagini su reati o di procedimenti penali conseguenti, le persone che possono fornire informazioni su reati o le persone in contatto o collegate alle persone di cui alle lettere a) e b).		
Articolo 7 **Distinzione tra i dati personali e verifica della qualità dei dati personali** 1. Gli Stati membri dispongono che i dati personali fondati su fatti siano differenziati, nella misura del possibile, da quelli fondati su valutazioni personali. 2. Gli Stati membri dispongono che le autorità competenti adottino tutte le misure ragionevoli per garantire che i dati personali inesatti, incompleti o non più aggiornati non siano trasmessi o resi disponibili. A tal fine, ciascuna autorità competente verifica, per quanto possibile, la qualità dei dati personali prima che questi siano trasmessi o resi disponibili. Per quanto possibile, tutte le trasmissioni di dati personali sono corredate delle informazioni necessarie che consentono all'autorità competente ricevente di valutare il	ART. 4 (*Conservazione e verifica della qualità dei dati, distinzione tra categorie di interessati e di dati*) 1. Il titolare del trattamento, se necessario rispetto alla finalità di trattamento e per quanto possibile, distingue i dati personali in relazione alle diverse categorie di interessati previste dalla legge, i dati fondati su fatti da quelli fondati su valutazioni. 2. Le autorità competenti adottano misure adeguate a garantire che i dati personali inesatti, incompleti o non aggiornati non siano trasmessi o resi disponibili. A tal fine ciascuna autorità competente, per quanto possibile, verifica la qualità dei dati personali prima che questi siano trasmessi o resi disponibili e correda la loro trasmissione delle informazioni che consentono all'autorità ricevente di valutarne il grado di esattezza, completezza,	La disposizione della direttiva è stata integralmente recepita dallo schema di decreto.

grado di esattezza, completezza e affidabilità dei dati personali, e la misura in cui essi sono aggiornati. 3. Qualora risulti che sono stati trasmessi dati personali inesatti o che sono stati trasmessi dati personali illecitamente, il destinatario deve esserne informato quanto prima. In tal caso, i dati personali devono essere rettificati o cancellati o il trattamento deve essere limitato a norma dell'articolo 16.	aggiornamento e affidabilità. 3. Quando risulta che i dati personali sono stati trasmessi illecitamente o sono inesatti, il destinatario ne è tempestivamente informato. In tal caso, i dati personali devono essere rettificati o cancellati o il trattamento deve essere limitato a norma dell'articolo 12.	
Articolo 8 **Liceità del trattamento** 1. Gli Stati membri dispongono che il trattamento sia lecito solo se e nella misura in cui è necessario per l'esecuzione di un compito di un'autorità competente, per le finalità di cui all'articolo 1, paragrafo 1, e si basa sul diritto dell'Unione o dello Stato membro. 2. Il diritto dello Stato membro che disciplina il trattamento nell'ambito di applicazione della presente direttiva specifica quanto meno gli obiettivi del trattamento, i dati personali da trattare e le finalità del trattamento.	ART. 5 (*Liceità del trattamento*) 1. Il trattamento è lecito se è necessario per l'esecuzione di un compito di un'autorità competente per le finalità di cui all'articolo 1, comma 2, e si basa sul diritto dell'Unione europea o su disposizioni di legge o di regolamento che individuano i dati personali e le finalità del trattamento. 2. Con decreto del Presidente della Repubblica, adottato ai sensi dell'articolo 17, comma 1, della legge 23 agosto 1988, n. 400, sono individuati, per i trattamenti o le categorie di trattamenti non occasionali di cui al comma 1, i termini, ove non già stabiliti da disposizioni di legge o di regolamento, e le modalità di conservazione dei dati, i soggetti legittimati ad accedervi, le condizioni di accesso, le modalità di consultazione, nonché le modalità e le condizioni per l'esercizio dei diritti di cui agli articoli 9, 10, 11 e 13.	La disposizione della direttiva è stata integralmente recepita dallo schema di decreto. Quanto alla normativa interna già in vigore, si fa rinvio al D.M. 27 marzo 2000, n. 264, Regolamento recante norme per la tenuta dei registri presso gli uffici giudiziari e correlate regole procedurali, adottate con decreto ministeriale 27 aprile 2009 (cfr. quanto esposto *sub* art. 20 dello schema di decreto)

Articolo 9 **Condizioni di trattamento specifiche** 1. I dati personali raccolti dalle autorità competenti per le finalità di cui all'articolo 1, paragrafo 1, non possono essere trattati per finalità diverse da quelle di cui all'articolo 1, paragrafo 1, a meno che tale trattamento non sia autorizzato dal diritto dell'Unione o dello Stato membro. Qualora i dati personali siano trattati per tali finalità diverse, si applica il regolamento (UE) 2016/679, a meno che il trattamento non sia effettuato nell'ambito di un'attività che non rientra nell'ambito di applicazione del diritto dell'Unione. 2. Qualora il diritto dello Stato membro affidi alle autorità competenti l'esecuzione di compiti diversi da quelli eseguiti per le finalità di cui all'articolo 1, paragrafo 1, il regolamento (UE) 2016/679 si applica al trattamento per tali finalità, comprese quelle di archiviazione nel pubblico interesse, di ricerca scientifica o storica o per finalità statistiche, a meno che il trattamento non sia effettuato nel contesto di un'attività che non rientra nell'ambito di applicazione del diritto dell'Unione. 3. Gli Stati membri dispongono che, nei casi in cui il diritto dell'Unione o dello Stato membro applicabile all'autorità competente che trasmette i dati preveda condizioni specifiche per il trattamento, l'autorità competente che	ART. 6 (*Condizioni di trattamento specifiche*) 1. I dati personali raccolti per le finalità di cui all'articolo 1, comma 2, non possono essere trattati per finalità diverse, salvo che tale trattamento sia consentito dal diritto dell'Unione europea o dalla legge. 2. Ai trattamenti eseguiti per finalità diverse da quelle di cui all'articolo 1, comma 2, comprese le attività di archiviazione nel pubblico interesse, di ricerca scientifica o storica o per finalità statistiche, si applica il Regolamento, salve le disposizioni di cui all'articolo 58 del Codice. 3. Se il diritto dell'Unione europea o le disposizioni legislative o regolamentari prevedono condizioni specifiche per il trattamento dei dati personali, l'autorità competente che trasmette tali dati informa il destinatario delle condizioni e dell'obbligo di rispettarle. 4. L'autorità competente che trasmette i dati applica le stesse condizioni previste per le trasmissioni di dati all'interno dello Stato ai destinatari di altri Stati membri o ad agenzie, uffici e organi istituiti a norma del titolo V, capi 4 e 5, del Trattato sul funzionamento dell'Unione europea.	La disposizione della direttiva è stata integralmente recepita dallo schema di decreto.

trasmette i dati informi il destinatario di tali dati personali di tali condizioni e dell'obbligo di rispettarle. 4. Gli Stati membri dispongono che l'autorità competente che trasmette i dati non applichi a destinatari di altri Stati membri o a agenzie, uffici e organi istituiti a norma del titolo V, capi 4 e 5, TFUE condizioni ai sensi del paragrafo 3 diverse da quelle applicabili a trasmissioni di dati analoghe all'interno dello Stato membro dell'autorità competente che trasmette i dati.		
Articolo 10 **Trattamento di categorie particolari di dati personali** Il trattamento di dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche o l'appartenenza sindacale, e il trattamento di dati genetici, di dati biometrici intesi a identificare in modo univoco una persona fisica o di dati relativi alla salute o di dati relativi alla vita sessuale della persona fisica o all'orientamento sessuale è autorizzato solo se strettamente necessario, soggetto a garanzie adeguate per i diritti e le libertà dell'interessato e soltanto: a)se autorizzato dal diritto dell'Unione o dello Stato membro; b)per salvaguardare un interesse vitale	ART. 7 (*Trattamento di categorie particolari di dati personali*) 1. Il trattamento di dati di cui all'articolo 9 del regolamento è autorizzato solo se assistito da garanzie adeguate per i diritti e le libertà dell'interessato e specificamente previsto dal diritto dell'Unione europea o da legge o regolamento, ovvero, ferme le garanzie dei diritti e delle libertà, se necessario per salvaguardare un interesse vitale dell'interessato o di un'altra persona fisica o se ha ad oggetto dati resi manifestamente pubblici dall'interessato.	La disposizione della direttiva è stata integralmente recepita dallo schema di decreto.

dell'interessato o di un'altra persona fisica; o c)se il suddetto trattamento riguarda dati resi manifestamente pubblici dall'interessato.		
Articolo 11 **Processo decisionale automatizzato relativo alle persone fisiche** 1. Gli Stati membri dispongono che una decisione basata unicamente su un trattamento automatizzato, compresa la profilazione, che produca effetti giuridici negativi o incida significativamente sull'interessato sia vietata salvo che sia autorizzata dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento e che preveda garanzie adeguate per i diritti e le libertà dell'interessato, almeno il diritto di ottenere l'intervento umano da parte del titolare del trattamento. 2. Le decisioni di cui al paragrafo 1 del presente articolo non si basano sulle categorie particolari di dati personali di cui all'articolo 10, a meno che non siano in vigore misure adeguate a salvaguardia dei diritti, delle libertà e dei legittimi interessi dell'interessato. 3. La profilazione che porta alla discriminazione di persone fisiche sulla base di categorie particolari di dati personali di cui all'articolo 10 è vietata, conformemente al diritto dell'Unione.	ART. 8 (*Processo decisionale automatizzato relativo alle persone fisiche*) 1. Sono vietate le decisioni basate unicamente su un trattamento automatizzato, compresa la profilazione, che producono effetti negativi nei confronti dell'interessato, salvo che siano autorizzate dal diritto dell'Unione europea o da specifiche disposizioni di legge. 2. Le disposizioni di legge devono prevedere garanzie adeguate per i diritti e le libertà dell'interessato. In ogni caso è garantito il diritto di ottenere l'intervento umano da parte del titolare del trattamento. 3. Le decisioni di cui al comma 1 non possono basarsi sulle categorie particolari di dati personali di cui all'articolo 9 del regolamento, salvo che siano in vigore misure adeguate a salvaguardia dei diritti, delle libertà e dei legittimi interessi dell'interessato. 4. Fermo il divieto di cui agli articoli 21 della Carta dei diritti fondamentali dell'Unione europea, è vietata la profilazione finalizzata alla discriminazione di persone fisiche sulla base di categorie particolari di dati personali di cui all'articolo 9 del regolamento.	La disposizione della direttiva è stata integralmente recepita dallo schema di decreto.

CAPO III ***Diritti dell'interessato*** *Articolo 12* **Comunicazioni e modalità per l'esercizio dei diritti dell'interessato** 1. Gli Stati membri dispongono che il titolare del trattamento adotti misure ragionevoli per fornire all'interessato tutte le informazioni di cui all'articolo 13 e faccia le comunicazioni con riferimento agli articoli 11, da 14 a 18 e 31, relative al trattamento, in forma concisa, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro. Le informazioni sono fornite con qualsiasi mezzo adeguato, anche per via elettronica. Come regola generale il titolare del trattamento fornisce le informazioni nella stessa forma della richiesta. 2. Gli Stati membri dispongono che il titolare del trattamento faciliti l'esercizio dei diritti di cui agli articoli 11 e da 14 a 18 da parte dell'interessato. 3. Gli Stati membri dispongono che il titolare del trattamento informi senza ingiustificato ritardo l'interessato per iscritto del seguito alla sua richiesta. 4. Gli Stati membri dispongono che le informazioni fornite ai sensi dell'articolo 13 ed eventuali comunicazioni effettuate o azioni intraprese ai sensi degli articoli 11, da 14 a 18	CAPO II DIRITTI DELL'INTERESSATO ART. 9 *(Comunicazioni e modalità per l'esercizio dei diritti dell'interessato)* 1. Il titolare del trattamento adotta misure adeguate a fornire all'interessato tutte le informazioni di cui all'articolo 10 ed effettua le comunicazioni relative al trattamento di cui agli articoli 8, 11, 12, 13, 14 e 27, in forma concisa, intellegibile e facilmente accessibile, con un linguaggio semplice e chiaro. Le informazioni sono fornite con qualsiasi mezzo adeguato, anche per via elettronica, se possibile con le stesse modalità della richiesta. 2. Il titolare del trattamento facilita l'esercizio dei diritti di cui agli articoli 8, 11, 12, 13, 14 da parte dell'interessato. 3. Il titolare del trattamento informa l'interessato senza ingiustificato ritardo e per iscritto dell'esito della sua richiesta. 4. E' assicurata la gratuità del rilascio di informazioni ai sensi dell'articolo 10 e dell'esercizio dei diritti previsti dagli articoli 8, 11, 12, 13, 14 e 27. Si applicano le disposizioni di cui all'articolo 12, paragrafo 5, secondo periodo, del regolamento. 5. Fermo quanto previsto dall'articolo 5 comma 1, con decreto adottato dal Ministro competente sono individuati, ove necessario anche per categorie, i trattamenti non	La disposizione della direttiva è stata integralmente recepita dallo schema di decreto, anche mediante il rinvio a disposizioni di contenuto equivalente previste dal regolamento.

e 31 siano gratuite. Se le richieste dell'interessato sono manifestamente infondate o eccessive, in particolare per il loro carattere ripetitivo, il titolare del trattamento può: a) addebitare un contributo spese ragionevole tenendo conto dei costi amministrativi per fornire le informazioni o la comunicazione o intraprendere l'azione richiesta, oppure b) rifiutare di soddisfare la richiesta. Incombe al titolare del trattamento dimostrare il carattere manifestamente infondato o eccessivo della richiesta. 5. Qualora il titolare del trattamento nutra ragionevoli dubbi circa l'identità della persona fisica che presenta una richiesta di cui agli articoli 14 o 16, può richiedere ulteriori informazioni necessarie per confermare l'identità dell'interessato.	occasionali effettuati con strumenti elettronici per le finalità di cui all'articolo 1, comma 2, previsti da disposizioni di legge o di regolamento, nonché i relativi titolari.	
Articolo 13 **Informazioni da rendere disponibili o da fornire all'interessato** 1. Gli Stati membri dispongono che il titolare del trattamento metta a disposizione dell'interessato almeno le seguenti informazioni: a) l'identità e i dati di contatto del titolare del trattamento;	ART. 10 (*Informazioni da rendere disponibili o da fornire all'interessato*) 1. Il titolare del trattamento mette a disposizione dell'interessato, anche sul proprio sito internet, le seguenti informazioni: a) l'identità e i dati di contatto del titolare del trattamento; b) i dati di contatto del responsabile della protezione dei dati, se previsto; c) le finalità del trattamento cui sono destinati i	La disposizione della direttiva è stata integralmente recepita dallo schema di decreto. La disciplina delle limitazioni alle informazioni da rendere disponibili all'interessato è contenuta nell'art. 14, con una norma di carattere generale riguardante l'esercizio di tutti i diritti di cui agli art. 10, comma 2, 11, comma 1 e 2, e 12, comma 5.

b)i dati di contatto del responsabile della protezione dei dati, se del caso; c)le finalità del trattamento cui sono destinati i dati personali; d)il diritto di proporre reclamo a un'autorità di controllo e i dati di contatto di detta autorità; e)l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento l'accesso ai dati e la rettifica o la cancellazione dei dati personali e la limitazione del trattamento dei dati personali che lo riguardano. 2. In aggiunta alle informazioni di cui al paragrafo 1, gli Stati membri dispongono per legge che il titolare del trattamento fornisca all'interessato, in casi specifici, le seguenti ulteriori informazioni per consentire l'esercizio dei diritti dell'interessato: a) la base giuridica per il trattamento; b)il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo; c)se del caso, le categorie di destinatari dei dati personali, anche in paesi terzi o in seno a organizzazioni internazionali;	dati personali; d) la sussistenza del diritto di proporre reclamo al Garante e i relativi dati di contatto; e) la sussistenza del diritto di chiedere al titolare del trattamento l'accesso ai dati e la rettifica o la cancellazione dei dati personali e la limitazione del trattamento dei dati personali che lo riguardano. 2. In aggiunta alle informazioni di cui al comma 1, il titolare del trattamento, quando previsto da disposizioni di legge o di regolamento, fornisce all'interessato le seguenti ulteriori informazioni, funzionali all'esercizio dei propri diritti: a) il titolo giuridico del trattamento; b) il periodo di conservazione dei dati personali o i criteri per determinare tale periodo; c) le categorie di destinatari dei dati personali, anche in Paesi terzi o in seno a organizzazioni internazionali; d) le ulteriori informazioni ritenute utili all'esercizio dei diritti. Vedi art. 14.	

d)se necessario, ulteriori informazioni, in particolare nel caso in cui i dati personali siano raccolti all'insaputa dell'interessato. 3. Gli Stati membri possono adottare misure legislative intese a ritardare, limitare o escludere la comunicazione di informazioni all'interessato ai sensi del paragrafo 2 nella misura e per il tempo in cui ciò costituisca una misura necessaria e proporzionata in una società democratica, tenuto debito conto dei diritti fondamentali e dei legittimi interessi della persona fisica interessata al fine di: a)non compromettere indagini, inchieste o procedimenti ufficiali o giudiziari; b)non compromettere la prevenzione, l'indagine, l'accertamento e il perseguimento di reati o l'esecuzione di sanzioni penali; c) proteggere la sicurezza pubblica; d) proteggere la sicurezza nazionale; e) proteggere i diritti e le libertà altrui. 4. Gli Stati membri possono adottare misure legislative al fine di determinare le categorie di trattamenti cui può applicarsi, in tutto o in parte, una delle lettere del paragrafo 3.		
Articolo 14	ART. 11 *(Diritto di accesso dell'interessato)*	La disposizione della direttiva è stata integralmente recepita dallo schema di decreto.

Diritto di accesso dell'interessato Fatto salvo l'articolo 15, gli Stati membri dispongono che l'interessato abbia il diritto di ottenere dal titolare del trattamento la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e, in tal caso, di ottenere l'accesso ai dati personali e alle seguenti informazioni: a) le finalità e la base giuridica del trattamento; b) le categorie di dati personali trattati; c) i destinatari o le categorie di destinatari a cui i dati personali sono stati comunicati, in particolare se destinatari di paesi terzi o organizzazioni internazionali; d) quando possibile, il periodo di conservazione dei dati personali previsto oppure, se non è possibile, i criteri utilizzati per determinare tale periodo; e) l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento la rettifica o cancellazione dei dati personali o la limitazione del trattamento dei dati personali che lo riguardano; f) il diritto di proporre reclamo all'autorità di controllo e le coordinate di contatto di detta autorità;	1. L'interessato ha il diritto di ottenere dal titolare del trattamento conferma dell'esistenza di un trattamento in corso di dati personali che lo riguardano e, in tal caso, l'accesso ai dati e alle seguenti informazioni: a) le finalità e il titolo giuridico del trattamento; b) le categorie di dati personali trattati; c) i destinatari o le categorie di destinatari a cui i dati personali sono stati comunicati; d) il periodo di conservazione dei dati personali o i criteri per determinare tale periodo; e) il diritto di chiedere al titolare del trattamento la rettifica o la cancellazione dei dati personali o la limitazione del trattamento dei dati personali che lo riguardano; f) il diritto di proporre reclamo al Garante, con i relativi dati di contatto; g) la comunicazione dei dati personali oggetto del trattamento e di tutte le informazioni disponibili sulla loro origine. 2. Nei casi di cui all'articolo 14, comma 2, il titolare del trattamento informa l'interessato, senza ingiustificato ritardo e per iscritto, di ogni rifiuto o limitazione dell'accesso e dei relativi motivi, nonché del diritto di proporre reclamo dinanzi al Garante o di proporre ricorso giurisdizionale. 3. Il titolare del trattamento documenta i motivi di fatto o di diritto su cui si basa la decisione di cui al comma 2. Tali informazioni sono rese disponibili al Garante.	La disciplina delle limitazioni al diritto di accesso dell'interessato è contenuta nell'art. 14, con una norma di carattere generale riguardante l'esercizio di tutti i diritti di cui agli art. 10, comma 2, 11, comma 1 e 2, e 12, comma 5.

g)la comunicazione dei dati personali oggetto del trattamento e di tutte le informazioni disponibili sulla loro origine.	Vedi art. 14.	
Articolo 15 **Limitazioni del diritto di accesso** 1. Gli Stati membri possono adottare misure legislative volte a limitare, in tutto o in parte, il diritto di accesso dell'interessato nella misura e per il tempo in cui tale limitazione totale o parziale costituisca una misura necessaria e proporzionata in una società democratica, tenuto debito conto dei diritti fondamentali e dei legittimi interessi della persona fisica interessata al fine di: a)non compromettere indagini, inchieste o procedimenti ufficiali o giudiziari; b)non compromettere la prevenzione, l'indagine, l'accertamento e il perseguimento di reati o l'esecuzione di sanzioni penali; c) proteggere la sicurezza pubblica; d) proteggere la sicurezza nazionale; e) proteggere i diritti e le libertà altrui. 2. Gli Stati membri possono adottare misure legislative al fine di determinare le categorie di	ART. 14 (*Limitazioni dell'esercizio dei diritti dell'interessato*) 1. I diritti di cui agli articoli 10, 11 e 12, relativamente ai dati personali contenuti in una decisione giudiziaria, in atti o documenti oggetto di trattamento nel corso di accertamenti o indagini, nel casellario giudiziale o in un fascicolo oggetto di trattamento nel corso di un procedimento penale o in fase di esecuzione penale, sono esercitati conformemente a quanto previsto dalle disposizioni di legge o di regolamento che disciplinano tali atti e procedimenti. Chiunque vi abbia interesse, durante il procedimento penale o dopo la sua definizione, può chiedere, con le modalità di cui all'articolo 116 del codice di procedura penale, la rettifica, la cancellazione o la limitazione dei dati personali che lo riguardano. Il giudice provvede con le forme dell'articolo 130 del codice di procedura penale. 2. Fermo quanto previsto dal comma 1, l'esercizio dei diritti di cui agli articoli 11, commi 1 e 2, e 12 comma 5, nonché l'adempimento dell'obbligo di cui all'articolo 10, comma 2, possono essere ritardati, limitati o esclusi nella misura e per il tempo in cui ciò	La disposizione della direttiva è stata integralmente recepita dallo schema di decreto, con una norma di carattere generale riguardante le limitazioni all'esercizio di tutti i diritti di cui agli art. 10, comma 2, 11, comma 1 e 2, e 12, comma 5.

trattamenti cui possono applicarsi, in tutto o in parte, le lettere da a) a e) del paragrafo 1. 3. Nei casi di cui ai paragrafi 1 e 2, gli Stati membri dispongono che il titolare del trattamento informi l'interessato, senza ingiustificato ritardo e per iscritto, di ogni rifiuto o limitazione dell'accesso e dei motivi del rifiuto o della limitazione. Detta comunicazione può essere omessa qualora il suo rilascio rischi di compromettere una delle finalità di cui al paragrafo 1. Gli Stati membri dispongono che il titolare del trattamento informi l'interessato della possibilità di proporre reclamo dinanzi a un'autorità di controllo o di proporre ricorso giurisdizionale. 4. Gli Stati membri dispongono che il titolare del trattamento documenti i motivi di fatto o di diritto su cui si basa la decisione. Tali informazioni sono rese disponibili alle autorità di controllo.	costituisca una misura necessaria e proporzionata, tenuto conto dei diritti fondamentali e dei legittimi interessi della persona fisica interessata al fine di: a) non compromettere il buon esito dell'attività di prevenzione, indagine, accertamento e perseguimento di reati o l'esecuzione di sanzioni penali, nonché l'applicazione delle misure di prevenzione personali e patrimoniali e delle misure di sicurezza; b) tutelare la sicurezza pubblica; c) tutelare la sicurezza nazionale; d) tutelare i diritti e le libertà altrui.	
Articolo 16 **Diritto di rettifica o cancellazione di dati personali e limitazione di trattamento** 1. Gli Stati membri dispongono che l'interessato abbia il diritto di ottenere dal titolare del trattamento la rettifica dei dati personali inesatti che lo riguardano senza ingiustificato ritardo. Tenuto conto delle finalità del trattamento, gli Stati membri dispongono che l'interessato abbia il diritto di ottenere l'integrazione dei dati personali	ART. 12 (*Diritto di rettifica o cancellazione di dati personali e limitazione di trattamento*) 1. L'interessato ha il diritto di ottenere dal titolare del trattamento, senza ingiustificato ritardo, la rettifica dei dati personali inesatti che lo riguardano. Tenuto conto delle finalità del trattamento, l'interessato ha il diritto di ottenere l'integrazione dei dati personali incompleti, anche fornendo una dichiarazione integrativa.	La disposizione della direttiva è stata integralmente recepita dallo schema di decreto. La disciplina delle limitazioni al diritto di rettifica è contenuta nell'art. 14, con una norma di carattere generale riguardante l'esercizio di tutti i diritti di cui agli art. 10, comma 2, 11, comma 1 e 2, e 12, comma 5.

incompleti, anche fornendo una dichiarazione integrativa. Gli Stati membri impongono al titolare del trattamento di cancellare i dati personali senza ingiustificato ritardo e stabiliscono il diritto dell'interessato di ottenere dal titolare del trattamento la cancellazione di dati personali che lo riguardano senza ingiustificato ritardo qualora il trattamento violi le disposizioni adottate a norma degli articoli 4, 8 o 10 o qualora i dati personali debbano essere cancellati per conformarsi a un obbligo legale al quale è soggetto il titolare del trattamento. 3. Anziché cancellare, il titolare del trattamento limita il trattamento quando: a)l'esattezza dei dati personali è contestata dall'interessato e la loro esattezza o inesattezza non può essere accertata; o b)i dati personali devono essere conservati a fini probatori. Quando il trattamento è limitato a norma della lettera a), primo comma, il titolare del trattamento informa l'interessato prima di revocare la limitazione del trattamento. 4. Gli Stati membri dispongono che il titolare del trattamento informi l'interessato per iscritto di ogni rifiuto di rettifica o cancellazione dei dati personali o limitazione del trattamento e dei motivi del rifiuto. Gli Stati membri possono adottare misure legislative volte a	2. Fermo quanto previsto dall'articolo 14, comma 1 e 2, il titolare del trattamento cancella senza ingiustificato ritardo i dati personali, quando il trattamento si pone in contrasto con le disposizioni di cui agli articoli 3, 5 o 7 o e in ogni altro caso previsto dalla legge. 3. In luogo della cancellazione, il titolare del trattamento limita il trattamento quando l'esattezza dei dati, contestata dall'interessato, non può essere accertata o se i dati devono essere conservati a fini probatori. 4. Quando il trattamento è limitato per l'impossibilità di accertare l'esattezza dei dati, il titolare del trattamento informa l'interessato prima di revocare la limitazione. 5. L'interessato ha diritto di essere informato per iscritto dal titolare del trattamento del rifiuto di rettifica, di cancellazione o di limitazione del trattamento e dei relativi motivi, nonché del diritto di proporre reclamo dinanzi al Garante o di proporre ricorso giurisdizionale. 7. Il titolare del trattamento comunica le rettifiche dei dati personali inesatti all'autorità competente da cui provengono. 8. Qualora i dati personali siano stati rettificati o cancellati o il trattamento sia stato limitato ai sensi dei commi 1, 2 e 3, il titolare del trattamento ne informa i destinatari e questi provvedono, sotto la propria responsabilità, alla rettifica o cancellazione dei dati personali ovvero alla limitazione del trattamento.	

limitare, in tutto o in parte, l'obbligo di fornire tali informazioni nella misura in cui tale limitazione costituisca una misura necessaria e proporzionata in una società democratica, tenuto debito conto dei diritti fondamentali e dei legittimi interessi della persona fisica interessata per: a)non compromettere indagini, inchieste o procedimenti ufficiali o giudiziari; b)non compromettere la prevenzione, l'indagine, l'accertamento e il perseguimento di reati o l'esecuzione di sanzioni penali; c) proteggere la sicurezza pubblica; d) proteggere la sicurezza nazionale; e) proteggere i diritti e le libertà altrui. Gli Stati membri dispongono che il titolare del trattamento informi l'interessato delle possibilità di proporre reclamo dinanzi a un'autorità di controllo o di proporre ricorso giurisdizionale. 5. Gli Stati membri dispongono che il titolare del trattamento comunichi le rettifiche dei dati personali inesatti all'autorità competente da cui i dati personali inesatti provengono. 6. Gli Stati membri dispongono che, qualora i dati personali siano stati rettificati o cancellati o il trattamento sia stato limitato a norma dei	Vedi Art. 14.	

paragrafi 1, 2 e 3, il titolare del trattamento ne informi i destinatari e che i destinatari rettifichino o cancellino i dati personali o limitino il trattamento dei dati personali sotto la propria responsabilità.		
Articolo 17 **Esercizio dei diritti dell'interessato e verifica da parte dell'autorità di controllo** 1. Nei casi di cui all'articolo 13, paragrafo 3, all'articolo 15, paragrafo 3, e all'articolo 16, paragrafo 4, gli Stati membri adottano misure che dispongano che i diritti dell'interessato possano essere esercitati anche tramite l'autorità di controllo competente. 2. Gli Stati membri dispongono che il titolare del trattamento informi l'interessato della possibilità di esercitare i suoi diritti tramite l'autorità di controllo ai sensi del paragrafo 1. 3. Qualora sia esercitato il diritto di cui al paragrafo 1, l'autorità di controllo informa l'interessato, perlomeno, di aver eseguito tutte le verifiche necessarie o un riesame. L'autorità di controllo informa inoltre l'interessato del diritto di quest'ultimo di proporre ricorso giurisdizionale.	ART. 13 *(Esercizio dei diritti dell'interessato e verifica da parte del Garante)* 1. Al di fuori dei casi di trattamento effettuato dall'autorità giudiziaria per le finalità di cui all'articolo 1, comma 2, i diritti dell'interessato possono essere esercitati anche tramite Garante con le modalità di cui all'articolo 160 del codice. 2. Il titolare del trattamento informa l'interessato della facoltà di cui al comma 1. 3. Nei casi di cui al comma 1, il Garante informa l'interessato di aver eseguito tutte le verifiche necessarie o di aver svolto un riesame, nonché del diritto dell'interessato di proporre ricorso giurisdizionale.	La disposizione della direttiva è stata integralmente recepita dallo schema di decreto.
Articolo 18 **Diritti dell'interessato nel corso di indagini e procedimenti penali** Gli Stati membri possono disporre che i diritti	ART. 14 *(Limitazioni dell'esercizio dei diritti dell'interessato)* 1. I diritti di cui agli articoli 10, 11 e 12,	Con l'art. 14 si esercita la facoltà concessa dalla direttiva di rimettere alla normativa interna la disciplina dell'esercizio dei diritti di informazione, di accesso, di rettifica o cancellazione, nonché di limitazione del

di cui agli articoli 13, 14 e 16 siano esercitati conformemente al diritto dello Stato membro qualora i dati personali figurino in una decisione giudiziaria, in un casellario o in un fascicolo giudiziario oggetto di trattamento nel corso di un'indagine e di un procedimento penale.	relativamente ai dati personali contenuti in una decisione giudiziaria, in atti o documenti oggetto di trattamento nel corso di accertamenti o indagini, nel casellario giudiziale o in un fascicolo oggetto di trattamento nel corso di un procedimento penale o in fase di esecuzione penale, sono esercitati conformemente a quanto previsto dalle disposizioni di legge o di regolamento che disciplinano tali atti e procedimenti. Chiunque vi abbia interesse, durante il procedimento penale o dopo la sua definizione, può chiedere, con le modalità di cui all'articolo 116 del codice di procedura penale, la rettifica, la cancellazione o la limitazione dei dati personali che lo riguardano. Il giudice provvede con le forme dell'articolo 130 del codice di procedura penale. 2. [...]	trattamento, allorché si tratti di dati personali contenuti in una decisione giudiziaria, in atti o documenti oggetto di trattamento nel corso di accertamenti o indagini, nel casellario giudiziale o in un fascicolo oggetto di trattamento nel corso di un procedimento penale o in fase di esecuzione penale. Con riferimento agli atti del procedimento penale, si osserva che, fermo il principio generale dell'obbligo del segreto nella fase delle indagini preliminari di cui all'art. 329 c.p.p., l'ordinamento interno contiene un'ampia gamma di disposizioni che disciplinano il diritto degli interessati (persona sottoposta a indagini/imputato, persona offesa/parte civile e difensori) di essere informati delle attività processuali, di avere accesso agli atti e di estrarne copia, nonché di formulare richieste all'autorità giudiziaria di rettifica di dati errati. A seguito dell'esercizio dell'azione penale, con il deposito della documentazione relativa alle indagini espletate e la conseguente discovery degli atti, è garantita alle parti la piena conoscenza degli atti processuali, compresi i dati personali oggetto di trattamento. Si segnalano, in particolare, le disposizioni del **codice di procedura penale** di cui agli articoli 66, comma 3, 90, 90 *bis*, 121, 130, 268, 270, 293, comma 1, 294, comma 1 bis, 309, comma 8, 310, comma 2, 335, comma 3, 335, comma 3 bis, 335, comma 3 ter, 360, 375, 386, comma 1, 391, comma 2, 398, comma 3 bis, art. 116,

		415 bis, 406, comma 3, 408, comma 2, 3, 3 bis, 419, 456, 482, 552. Come norma di chiusura, ad integrazione delle disposizioni già esistenti, si è prevista una specifica procedura per garantire a chiunque abbia un interesse, nel corso del procedimento penale o dopo la sua definizione, l'esercizio dei diritti di rettifica, cancellazione o limitazione dei dati che lo riguardano. Al di fuori del codice di procedura penale, i diritti sopra menzionati trovano tutela anche nelle seguenti norme, contenute nel **D.P.R. 14 novembre 2002, n. 313 (Testo unico delle disposizioni legislative e regolamentari in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti)**: Art. 22 *Certificato del casellario giudiziale, del casellario giudiziale europeo e del casellario dei carichi pendenti richiesto dal difensore*) 1. Previa autorizzazione del giudice procedente, il difensore ha diritto di ottenere il certificato di tutte le iscrizioni esistenti riferite ad un determinato soggetto, avente la qualità di persona offesa dal reato o di testimone, per le finalità riconosciute dal codice di procedura penale. Art. 23 *Certificati del casellario giudiziale richiesti dall'interessato.* 1. L'interessato ha il diritto di ottenere il

		certificato generale, il certificato penale, il certificato civile, di cui agli articoli 24, 25 e 26, senza motivare la richiesta. Art. 25-ter *Certificato del casellario giudiziale europeo richiesto dall'interessato*. 1. Il cittadino italiano ha diritto di ottenere, senza motivare la richiesta, il rilascio del certificato contenente le iscrizioni esistenti nel casellario giudiziale europeo, nella misura in cui il diritto dello Stato membro di condanna ne preveda la menzione. 2. Il cittadino di altro Stato membro dell'Unione europea che rivolge richiesta di informazioni all'Ufficio centrale acquisisce da esso le informazioni relative alle condanne pronunciate nello Stato membro di cittadinanza e a quelle dallo stesso ricevute e conservate, nella misura in cui il diritto dello Stato membro di condanna ne preveda la menzione. Art. 27 *Certificato del casellario dei carichi pendenti richiesto dall'interessato.* 1. L'interessato ha il diritto di ottenere il certificato senza motivare la richiesta. 2. Nel certificato sono riportate le iscrizioni esistenti nel casellario dei carichi pendenti ad eccezione di quelle relative: a) alle condanne delle quali è stato ordinato che non si faccia menzione nel certificato a norma dell'articolo 175, del codice penale, purché il beneficio non sia stato revocato; b) alle condanne per contravvenzioni punibili con la sola ammenda;

		c) alle condanne per i reati per i quali si è verificata la causa speciale di estinzione prevista dall'articolo 556 del codice penale; d) ai provvedimenti previsti dall'articolo 445 del codice di procedura penale e ai decreti penali; e) ai provvedimenti giudiziari emessi dal giudice di pace; f) ai provvedimenti giudiziari relativi ai reati di competenza del giudice di pace emessi da un giudice diverso, limitatamente alle iscrizioni concernenti questi reati. Art. 40 *Questioni concernenti le iscrizioni e i certificati* 1. Sulle questioni concernenti le iscrizioni e i certificati del casellario giudiziale e dei carichi pendenti decide, in composizione monocratica e con le forme stabilite dall'articolo 666 del codice di procedura penale, il tribunale del luogo dove ha sede l'ufficio locale nel cui ambito territoriale è nata la persona cui è riferita l'iscrizione o il certificato, o il Tribunale di Roma, per le persone nate all'estero, o delle quali non è stato accertato il luogo di nascita nel territorio dello Stato. 2. Sulle questioni concernenti le iscrizioni e i certificati dell'anagrafe delle sanzioni amministrative dipendenti da reato e dell'anagrafe dei carichi pendenti degli illeciti amministrativi dipendenti da reato decide il Tribunale di Roma, in composizione monocratica e con le forme stabilite dall'articolo 666 del codice di procedura

		penale, in quanto applicabili.
CAPO IV ***Titolare del trattamento e responsabile del trattamento*** **Sezione 1** **Obblighi generali** *Articolo 19* **Obblighi del titolare del trattamento** 1. Gli Stati membri dispongono che il titolare del trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, metta in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato ai sensi della presente direttiva. Tali misure sono riesaminate e aggiornate qualora necessario. 2. Se ciò è proporzionato rispetto alle attività di trattamento, le misure di cui al paragrafo 1 includono l'attuazione di politiche adeguate in materia di protezione dei dati da parte del titolare del trattamento.	CAPO III TITOLARE DEL TRATTAMENTO E RESPONSABILE DEL TRATTAMENTO SEZIONE I *OBBLIGHI GENERALI* ART. 15 (*Obblighi del titolare del trattamento*) 1. Il titolare del trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi per i diritti e le libertà delle persone fisiche, mette in atto misure tecniche e organizzative adeguate per garantire che il trattamento sia effettuato in conformità alle norme del presente decreto. 2. Le misure di cui al comma 1 sono riesaminate e aggiornate qualora necessario e, ove proporzionato rispetto all'attività di trattamento, includono l'attuazione di politiche adeguate in materia di protezione dei dati da parte del titolare del trattamento.	La disposizione della direttiva è stata integralmente recepita dallo schema di decreto.
Articolo 20 **Protezione dei dati fin dalla progettazione e**	ART. 16 (*Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita*)	La disposizione della direttiva è stata integralmente recepita dallo schema di decreto.

protezione per impostazione predefinita 1. Gli Stati membri dispongono che il titolare del trattamento, tenuto conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento, sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso, mettà in atto misure tecniche e organizzative adeguate, quali la pseudonimizzazione, volte ad attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione, e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti della presente direttiva e tutelare i diritti degli interessati. 2. Gli Stati membri dispongono che il titolare del trattamento metta in atto misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento. Tale obbligo vale per la quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità. In particolare, tali misure garantiscono che, per impostazione predefinita, non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica.	1. Il titolare del trattamento, tenuto conto delle cognizioni tecniche disponibili e dei costi di attuazione, della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi per i diritti e le libertà delle persone fisiche, mette in atto misure tecniche e organizzative adeguate, quale la pseudonimizzazione, per garantire la protezione dei dati e per tutelare i diritti degli interessati, in conformità alle norme del presente decreto. 2. Il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento. Tale obbligo vale per la quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità. In particolare, tali misure garantiscono che, per impostazione predefinita, non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica.	

Articolo 21 **Contitolari del trattamento** 1. Gli Stati membri dispongono che, allorché due o più titolari del trattamento determinano congiuntamente le finalità e i mezzi del trattamento, essi siano contitolari del trattamento. Essi determinano in modo trasparente, mediante un accordo interno, le rispettive responsabilità in merito all'osservanza della presente direttiva, con particolare riguardo all'esercizio dei diritti dell'interessato, e le rispettive funzioni di comunicazione delle informazioni di cui all'articolo 13, a meno che e nella misura in cui le rispettive responsabilità siano determinate dal diritto dell'Unione o dello Stato membro cui i titolari del trattamento sono soggetti. Tale accordo designa il punto di contatto per gli interessati. Gli Stati membri possono designare quale dei contitolari del trattamento possa fungere da punto di contatto unico ai fini dell'esercizio da parte degli interessati dei loro diritti. 2. Indipendentemente dalle disposizioni dell'accordo di cui al paragrafo 1, gli Stati membri possono disporre che l'interessato possa esercitare i propri diritti a norma delle disposizioni adottate ai sensi della presente direttiva nei confronti di e contro ciascun titolare del trattamento.	ART. 17 *(Contitolari del trattamento)* 1. Due o più titolari del trattamento che determinano congiuntamente le finalità e i mezzi del trattamento sono contitolari del trattamento. 2. I contitolari del trattamento concordano con modalità trasparenti gli ambiti delle rispettive responsabilità per l'osservanza delle norme di cui al presente decreto, salvo che detti ambiti siano determinati dal diritto dell'Unione europea o da disposizioni legislative o regolamentari. 3. Con l'accordo di cui al comma 2 è designato il punto di contatto per gli interessati. Indipendentemente dalle disposizioni di tale accordo, l'interessato può esercitare i diritti nei confronti di e contro ciascun titolare del trattamento.	La disposizione della direttiva è stata integralmente recepita dallo schema di decreto.

Articolo 22 **Responsabile del trattamento** 1. Gli Stati membri dispongono che, qualora un trattamento debba essere effettuato per conto del titolare del trattamento, quest'ultimo ricorra unicamente a responsabili del trattamento che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti della presente direttiva e garantisca la tutela dei diritti dell'interessato. 2. Gli Stati membri dispongono che il responsabile del trattamento non ricorra a un altro responsabile senza previa autorizzazione scritta, specifica o generale, del titolare del trattamento. Nel caso di autorizzazione scritta generale, il responsabile del trattamento informa il titolare del trattamento di eventuali modifiche previste riguardanti l'aggiunta o la sostituzione di altri responsabili del trattamento, dando così al titolare del trattamento l'opportunità di obiettare a tali modifiche. 3. Gli Stati membri dispongono che l'esecuzione dei trattamenti da parte di un responsabile del trattamento sia disciplinata da un contratto o da altro atto giuridico a norma del diritto dell'Unione o dello Stato membro, che vincoli il responsabile del trattamento al titolare del trattamento e che stipuli la materia	ART. 18 (*Responsabile del trattamento*) 1. Qualora un trattamento debba essere effettuato per conto del titolare del trattamento, quest'ultimo ricorre a responsabili del trattamento che garantiscono misure tecniche e organizzative adeguate ad assicurare la protezione dei dati personali e la tutela dei diritti dell'interessato. 2. Il responsabile del trattamento non può ricorrere a un altro responsabile senza preventiva autorizzazione scritta del titolare del trattamento. 3. L'esecuzione dei trattamenti da parte di un responsabile del trattamento è disciplinata da un contratto o da altro atto giuridico che preveda l'oggetto, la durata, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del titolare del trattamento. Tale contratto o diverso atto giuridico debbono anche prevedere che il responsabile del trattamento: a) agisca soltanto su istruzione del titolare del trattamento; b) garantisca che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza; c) assista il titolare del trattamento con ogni mezzo adeguato per garantire il rispetto delle disposizioni relative ai diritti dell'interessato;	La disposizione della direttiva è stata integralmente recepita dallo schema di decreto.

disciplinata e la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del titolare del trattamento. Tale contratto o altro atto giuridico deve prevedere in particolare che il responsabile del trattamento: a)agisca soltanto su istruzione del titolare del trattamento; b)garantisca che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza; c)assista il titolare del trattamento con ogni mezzo adeguato per garantire la conformità con le disposizioni relative ai diritti dell'interessato; d)su scelta del titolare del trattamento, cancelli o gli restituisca tutti i dati personali dopo che è terminata la prestazione dei servizi di trattamento di dati e cancelli le copie esistenti, salvo che il diritto dell'Unione o dello Stato membro preveda la conservazione dei dati personali; e)metta a disposizione del titolare del trattamento tutte le informazioni necessarie per dimostrare la conformità con il presente articolo;	d) su scelta del titolare del trattamento, cancelli o gli restituisca tutti i dati personali dopo che è terminata la prestazione dei servizi di trattamento di dati e cancelli le copie esistenti, salvo che il diritto dell'Unione europea o la legge preveda la conservazione dei dati personali; e) metta a disposizione del titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto delle condizioni di cui al presente articolo; f) rispetti le condizioni di cui ai paragrafi 2 e 3 nel caso di ricorso ad altro responsabile del trattamento. 4. Il contratto o il diverso atto di cui al comma 3 è stipulato per iscritto, anche in formato elettronico. 5. Se un responsabile del trattamento determina, in violazione del presente decreto, le finalità e i mezzi del trattamento, è considerato titolare del trattamento.	

f)soddisfi le condizioni di cui ai paragrafi 2 e 3 per ricorrere a un altro responsabile del trattamento. 4. Il contratto o l'altro atto giuridico di cui al paragrafo 3 è stipulato per iscritto, anche in formato elettronico. 5. Se un responsabile del trattamento determina, in violazione della presente direttiva, le finalità e i mezzi del trattamento, è considerato un titolare del trattamento relativamente al trattamento in questione.		
Articolo 23 **Trattamento sotto l'autorità del titolare del trattamento o del responsabile del trattamento** Gli Stati membri dispongono che il responsabile del trattamento, o chiunque agisca sotto la sua autorità o sotto quella del titolare del trattamento, che abbia accesso a dati personali non tratti tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o dello Stato membro.	ART. 19 (*Trattamento sotto l'autorità del titolare del trattamento o del responsabile del trattamento*) 1. Il responsabile del trattamento o chiunque agisca sotto la sua autorità o sotto quella del titolare del trattamento possono trattare i dati personali cui hanno accesso solo in conformità alle istruzioni del titolare del trattamento, salvo che sia diversamente previsto dal diritto dell'Unione europea o da disposizioni di legge o regolamento.	La disposizione della direttiva è stata integralmente recepita dallo schema di decreto.
Articolo 24 **Registri delle attività di trattamento** 1. Gli Stati membri dispongono che i titolari del trattamento tengano un registro di tutte le categorie di attività di trattamento sotto la	ART. 20 (*Registri delle attività di trattamento*) 1. I titolari del trattamento tengono un registro di tutte le categorie di attività di trattamento sotto la propria responsabilità. Tale registro	La disposizione della direttiva è stata integralmente recepita dallo schema di decreto. Si segnala che la normativa nazionale in materia di registri informatizzati dell'amministrazione della giustizia e, in

propria responsabilità. Tale registro contiene tutte le seguenti informazioni:

a)il nome e i dati di contatto del titolare del trattamento e, se del caso, di ogni contitolare del trattamento e del responsabile della protezione dei dati;

b) le finalità del trattamento;

c)le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi od organizzazioni internazionali;

d)una descrizione delle categorie di interessati e delle categorie di dati personali;

e) se del caso, il ricorso alla profilazione;

f)se del caso, le categorie di trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale;

g)un'indicazione della base giuridica del trattamento, compresi i trasferimenti, al quale sono destinati i dati personali;

h)ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati personali;

contiene le seguenti informazioni:
a) il nome e i dati di contatto del titolare del trattamento e, se previsti, di ogni contitolare del trattamento e del responsabile della protezione dei dati;
b) le finalità del trattamento;
c) le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi o presso organizzazioni internazionali;
d) una descrizione delle categorie di interessati e delle categorie di dati personali;
e) se previsto, il ricorso alla profilazione;
f) se previste, le categorie di trasferimenti di dati personali verso un Paese terzo o verso organizzazioni internazionali;
g) un'indicazione del titolo giuridico del trattamento cui sono destinati i dati personali, anche in caso di trasferimento;
h) ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati personali;
i) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 25 comma 1.
2. I responsabili del trattamento tengono un registro di tutte le categorie di attività di trattamento svolte per conto di un titolare del trattamento, contenente le seguenti informazioni:
a) il nome e i dati di contatto del responsabile o dei responsabili del trattamento, di ogni titolare del trattamento per conto del quale agiscono e, se esistente, del responsabile della

particolare, la normativa che disciplina la tenuta informatizzata dei registri nel settore della cognizione penale di 1° e 2° grado e nelle indagini preliminari (Sistema Informativo della Cognizione Penale, S.I.C.P.) disciplina la tenuta dei registri di trattamento con modalità in gran parte conformi alle indicazioni della direttiva. Si fa rinvio, al riguardo, al **D.M. 27 marzo 2000, n. 264**, Regolamento recante norme per la tenuta dei registri presso gli uffici giudiziari e correlate regole procedurali, adottate con **D.M. 27 aprile 2009** (Nuove regole procedurali relative alla tenuta dei registri informarizzati dell'amministrazione della giustizia), nonché alle Circolari del Dipartimento per gli affari di giustizia, Direzione generale della giustizia penale, Dipartimento dell'organizzazione giudiziaria, del personale e dei servizi - Direzione generale per i sistemi informativi automatizzati in data 11 giugno 2013 e 9 dicembre 2014, sulla Tenuta informatizzata dei registri penali - S.I.C.P.
La tenuta informatizzata dei registri secondo le regole tecniche e le regole procedurali di attuazione garantisce la integrità, la disponibilità e la riservatezza dei dati e consente l'identificazione del soggetto che accede al registro (art. 4 D.M. 264/2000). È infatti tracciata e conservata qualsiasi operazione di accesso, creazione, modifica e cancellazione delle informazioni riguardanti i dati personali trattati. Più specificamente, ai sensi del combinato disposto degli artt. 28, 29

i)ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 29, paragrafo 1.

2. Gli Stati membri dispongono che tutti i responsabili del trattamento tengano un registro di tutte le categorie di attività di trattamento svolte per conto di un titolare del trattamento, contenente:

a)il nome e i dati di contatto del responsabile o dei responsabili del trattamento, di ogni titolare del trattamento per conto del quale agisce e, se del caso, del responsabile della protezione dei dati;

b)le categorie dei trattamenti effettuati per conto di ogni titolare del trattamento;

c)se del caso, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale ove esplicitamente istruito in tal senso dal titolare del trattamento, compresa l'identificazione del paese terzo o dell'organizzazione internazionale;

d)ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 29, paragrafo 1.

3. I registri di cui ai paragrafi 1 e 2 sono tenuti in forma scritta, anche in formato elettronico.

Su richiesta, il titolare del trattamento e il

protezione dei dati;

b) le categorie dei trattamenti effettuati per conto di ogni titolare del trattamento;

c) i trasferimenti di dati personali effettuati su istruzione del titolare del trattamento verso un Paese terzo o verso un'organizzazione internazionale;

d) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 25, paragrafo 1.

3. I registri di cui ai paragrafi 1 e 2 sono tenuti in forma scritta, anche in formato elettronico. Su richiesta, il titolare del trattamento e il responsabile del trattamento mettono tali registri a disposizinne del Garante.

e 46 del D.lgs. 196/2003 ed alla luce dell'art. 13 co. 3 del D.M. 27 aprile 2009, il dirigente o responsabile dell'Ufficio, quale "responsabile della qualità dei dati" può designare, con formale provvedimento, le persone autorizzate alle operazioni di immissione, cancellazione, variazione ed esibizione dei dati nel sistema informatico, nonché ad ogni altro trattamento previsto dall'art. 4 co. 1 lett. a) d.lgs.vo 196/2003. L'identificazione di colui che effettua dette operazioni, nonché della relativa data ed ora, è conservata nel sistema informatico, ai sensi del D.M. 27/4/2009.

In considerazione dell'integrazione delle registrazioni dei dati tra i vari Uffici di primo e di secondo grado e dei collegamenti con il Casellario, per la creazione della Banca dati nazionale dei carichi pendenti, con la Banca dati nazionale delle misure cautelari personali e con Equitalia Giustizia, è prescritto che siano inserite, in modo completo ed esaustivo, una serie dettagliate di informazioni, tra le quali le indicazioni anagrafiche di tutti i soggetti interessati da ogni singola annotazione (indagato, persona offesa, ricorrente, proprietario di un bene sequestrato etc.).

E' altresì previsto che il collegamento ai registri non possa essere attivato per l'estrazione o l'aggregazione di dati sensibili.

responsabile del trattamento mettono tali registri a disposizione dell'autorità di controllo.		
Articolo 25 **Registrazione** 1. Gli Stati membri dispongono che siano registrati in sistemi di trattamento automatizzato almeno i seguenti trattamenti: raccolta, modifica, consultazione, comunicazione, inclusi i trasferimenti, interconnessione e cancellazione. Le registrazioni delle consultazioni e delle comunicazioni consentono di stabilire la motivazione, la data e l'ora di tali operazioni e, nella misura del possibile, di identificare la persona che ha consultato o comunicato i dati personali, nonché di stabilire l'identità dei destinatari di tali dati personali. 2. Le registrazioni sono usate ai soli fini della verifica della liceità del trattamento, dell'autocontrollo, per garantire l'integrità e la sicurezza dei dati personali e nell'ambito di procedimenti penali. 3. Su richiesta, il titolare del trattamento e il responsabile del trattamento mettono le registrazioni a disposizione dell'autorità di controllo.	ART. 21 *(Registrazione)* 1. Le operazioni di raccolta, modifica, consultazione, comunicazione, trasferimento, interconnessione e cancellazione di dati, eseguite in sistemi di trattamento automatizzati, sono registrate in appositi file di log. 2. Le registrazioni delle operazioni di cui al comma 1 debbono consentire di conoscere i motivi, la data e l'ora di tali operazioni e, se possibile, di identificare la persona che ha eseguito le operazioni e i destinatari. 2. Le registrazioni sono usate ai soli fini della verifica della liceità del trattamento, per finalità di controllo interno, per garantire l'integrità e la sicurezza dei dati personali e nell'ambito di procedimenti penali. 3. Su richiesta e fatto salvo quanto previsto dall'articolo 37 comma 3, il titolare del trattamento e il responsabile del trattamento mettono le registrazioni a disposizione del Garante.	La disposizione della direttiva è stata integralmente recepita dallo schema di decreto. Si rinvia a quanto esposto *sub* art. 20 dello schema, quanto alla normativa nazionale che regolamenta le modalità di tenuta dei registri informatizzati dell'amministrazione della giustizia.
Articolo 26 **Cooperazione con l'autorità di controllo** Gli Stati membri dispongono che il titolare del	ART. 22 *(Cooperazione con il Garante)* 1. Salvo quanto previsto dall'articolo 37	La disposizione della direttiva è stata integralmente recepita dallo schema di decreto.

trattamento e il responsabile del trattamento cooperino, su richiesta, con l'autorità di controllo nell'esecuzione dei suoi compiti.	comma 3, il titolare del trattamento e il responsabile del trattamento cooperano, su richiesta, con il Garante.	
Articolo 27 **Valutazione d'impatto sulla protezione dei dati** 1. Quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'ambito di applicazione, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, gli Stati membri dispongono che il titolare del trattamento effettui, prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali. 2. La valutazione di cui al paragrafo 1 contiene almeno una descrizione generale dei trattamenti previsti, una valutazione dei rischi per i diritti e le libertà degli interessati, le misure previste per affrontare tali rischi, le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità alla presente direttiva, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.	ART. 23 (*Valutazione d'impatto sulla protezione dei dati*) 1. Se il trattamento, per l'uso di nuove tecnologie e per la sua natura, per l'ambito di applicazione, per il contesto e per le finalità, presenta un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento, prima di procedere al trattamento, effettua una valutazione del suo impatto sulla protezione dei dati personali. 2. La valutazione di cui al comma 1 contiene una descrizione generale dei trattamenti previsti, una valutazione dei rischi per i diritti e le libertà degli interessati, le misure previste per affrontare tali rischi, le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e il rispetto delle norme del presente decreto.	La disposizione della direttiva è stata integralmente recepita dallo schema di decreto.
Articolo 28	ART. 24 (*Consultazione preventiva del Garante*)	La disposizione della direttiva è stata integralmente recepita dallo schema di decreto.

Consultazione preventiva dell'autorità di controllo 1. Gli Stati membri dispongono che il titolare del trattamento o il responsabile del trattamento consulti l'autorità di controllo prima del trattamento di dati personali che figureranno in un nuovo archivio di prossima creazione se: a) una valutazione d'impatto sulla protezione dei dati di cui all'articolo 27 indica che il trattamento presenterebbe un rischio elevato in assenza di misure adottate dal titolare del trattamento per attenuare il rischio; oppure b) il tipo di trattamento, in particolare se utilizza tecnologie, procedure o meccanismi nuovi, presenta un rischio elevato per i diritti e le libertà degli interessati. 2. Gli Stati membri dispongono che l'autorità di controllo sia consultata durante l'elaborazione di una proposta di atto legislativo che deve essere adottato dai parlamenti nazionali o di misura regolamentare basata su tale atto legislativo relativamente al trattamento. 3. Gli Stati membri dispongono che l'autorità di controllo possa stabilire un elenco di trattamenti soggetti a consultazione preventiva ai sensi del paragrafo 1. 4. Gli Stati membri dispongono che il titolare del trattamento trasmetta all'autorità di	1. Salvo quanto previsto dall'articolo 37, comma 6, il titolare del trattamento o il responsabile del trattamento consultano il Garante prima del trattamento di dati personali che figureranno in un nuovo archivio di prossima creazione se: a) una valutazione d'impatto sulla protezione dei dati di cui all'articolo 23 indica che il trattamento presenterebbe un rischio elevato in assenza di misure adottate dal titolare del trattamento per attenuare il rischio; oppure b) il tipo di trattamento presenta un rischio elevato per i diritti e le libertà degli interessati anche in regione dell'utilizzo di tecnologie, procedure o meccanismi nuovi ovvero di dati genetici o biometrici. 2. Il Garante è consultato nel corso dell'esame di un progetto di legge o di uno schema di decreto legislativo ovvero di uno schema di regolamento o decreto non avente carattere regolamentare, suscettibile di rilevare ai fini della garanzia del diritto alla protezione dei dati personali. 3. Il Garante può stabilire un elenco di trattamenti soggetti a consultazione preventiva ai sensi del comma 1. 4. Il titolare del trattamento trasmette al Garante la valutazione d'impatto sulla protezione dei dati di cui all'articolo 23 e, su richiesta, ogni altra informazione, al fine di consentire a detta autorità di effettuare una valutazione della conformità del trattamento, dei rischi per la protezione dei dati personali	

controllo la valutazione d'impatto sulla protezione dei dati di cui all'articolo 27 e, su richiesta, ogni altra informazione, al fine di consentire all'autorità di controllo di effettuare una valutazione della conformità del trattamento, in particolare dei rischi per la protezione dei dati personali dell'interessato e delle relative garanzie. 5. Gli Stati membri dispongono che, se ritiene che il trattamento previsto di cui al paragrafo 1 del presente articolo violi le disposizioni adottate a norma della presente direttiva, in particolare qualora il titolare del trattamento non abbia identificato o attenuato sufficientemente il rischio, l'autorità di controllo fornisca, entro un termine di sei settimane dal ricevimento della richiesta di consultazione, un parere per iscritto al titolare del trattamento e, ove applicabile, al responsabile del trattamento e possa avvalersi dei poteri di cui all'articolo 47. Tale periodo può essere prorogato di un mese, tenendo conto della complessità del trattamento previsto. L'autorità di controllo informa il titolare del trattamento e, ove applicabile, il responsabile del trattamento di tale proroga, unitamente ai motivi del ritardo, entro un mese dal ricevimento della richiesta di consultazione.	dell'interessato e delle relative garanzie. 5. Ove ritenga che il trattamento di cui al comma 1 violi le disposizioni del presente decreto, il Garante fornisce, entro un termine di sei settimane dal ricevimento della richiesta di consultazione, un parere per iscritto al titolare del trattamento e, se esistente, al responsabile del trattamento. Il Garante si avvale dei poteri di cui all'articolo 37 comma 3. 6. Il termine di cui al comma 5 può essere prorogato di un mese nel caso di trattamento complesso. Il Garante informa della proroga e dei motivi del ritardo il titolare del trattamento e, se esistente, il responsabile del trattamento, entro un mese dal ricevimento della richiesta di consultazione.	
Sezione 2 **Sicurezza dei dati personali**	SEZIONE II *SICUREZZA DEI DATI PERSONALI* ART. 25	La disposizione della direttiva è stata integralmente recepita dallo schema di decreto. Si segnala, peraltro, che l'ordinamento interno già contiene un apparato normativo che

Articolo 29 **Sicurezza del trattamento** 1. Gli Stati membri dispongono che il titolare del trattamento e il responsabile del trattamento, tenuto conto dello stato dell'arte, dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, mettano in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, in particolare riguardo al trattamento di categorie particolari di dati personali di cui all'articolo 10. 2. Ciascuno Stato membro dispone che per il trattamento automatizzato il titolare del trattamento o il responsabile del trattamento, previa valutazione dei rischi, metta in atto misure volte a: a) vietare alle persone non autorizzate l'accesso alle attrezzature utilizzate per il trattamento («controllo dell'accesso alle attrezzature»); b) impedire che supporti di dati possano essere letti, copiati, modificati o asportati da persone non autorizzate («controllo dei supporti di dati»); c) impedire che i dati personali siano inseriti	*(Sicurezza del trattamento)* 1. Il titolare del trattamento e il responsabile del trattamento, tenuto conto delle cognizioni tecniche disponibili, dei costi di attuazione, della natura, dell'oggetto, del contesto e delle finalità del trattamento, nonché del grado di rischio per i diritti e le libertà delle persone fisiche, mettono in atto misure tecniche e organizzative che garantiscano un livello di sicurezza adeguato al rischio di violazione dei dati. 2. Per il trattamento automatizzato il titolare o il responsabile del trattamento, previa valutazione dei rischi, adottano misure volte a: a) vietare alle persone non autorizzate l'accesso alle attrezzature utilizzate per il trattamento («controllo dell'accesso alle attrezzature»); b) impedire che supporti di dati possano essere letti, copiati, modificati o asportati da persone non autorizzate («controllo dei supporti di dati»); c) impedire che i dati personali siano inseriti senza autorizzazione e che i dati personali conservati siano visionati, modificati o cancellati senza autorizzazione («controllo della conservazione»); d) impedire che persone non autorizzate utilizzino sistemi di trattamento automatizzato mediante attrezzature per la trasmissione di dati («controllo dell'utente»); e) garantire che le persone autorizzate a usare un sistema di trattamento automatizzato abbiano accesso solo ai dati personali cui si	approntà una serie di misure di sicurezza, divieti, limitazioni e controlli per l'accesso ai dati personali trattati in ambito giudiziario, già satisfattivi, in larga misura, degli obblighi derivanti dalla direttiva. L'efficacia delle prescrizioni è corroborata dalla previsione di sanzioni penali, per il caso di violazione della integrità dei dati e dei sistemi informatici e della riservatezza dei dati e delle comunicazioni informatiche. Quanto alla normativa interna già in vigore, in ambito giudiziario, si fa rinvio, in particolare, al D.M. 27 marzo 2000, n. 264, Regolamento recante norme per la tenuta dei registri presso gli uffici giudiziari e correlate regole procedurali, adottate con decreto ministeriale 27 aprile 2009 (cfr. quanto esposto *sub* art. 20 dello schema di decreto). Si richiamano, altresì, le seguenti disposizioni di rilievo. **Codice di procedura penale.** Art. 114. *Divieto di pubblicazione di atti e di immagini* 1. E' vietata la pubblicazione, anche parziale o per riassunto, con il mezzo della stampa o con altro mezzo di diffusione, degli atti coperti dal segreto o anche solo del loro contenuto. 2. E' vietata la pubblicazione, anche parziale, degli atti non più coperti dal segreto fino a che non siano concluse le indagini preliminari ovvero fino al termine dell'udienza preliminare, fatta eccezione per l'ordinanza indicata dall'articolo 292.

senza autorizzazione e che i dati personali conservati siano visionati, modificati o cancellati senza autorizzazione («controllo della conservazione»); d) impedire che persone non autorizzate utilizzino sistemi di trattamento automatizzato mediante attrezzature per la trasmissione di dati («controllo dell'utente»); e) garantire che le persone autorizzate a usare un sistema di trattamento automatizzato abbiano accesso solo ai dati personali cui si riferisce la loro autorizzazione d'accesso («controllo dell'accesso ai dati»); f) garantire la possibilità di verificare e accertare gli organismi ai quali siano stati o possano essere trasmessi o resi disponibili i dati personali utilizzando attrezzature per la trasmissione di dati («controllo della trasmissione»); g) garantire la possibilità di verificare e accertare a posteriori quali dati personali sono stati introdotti nei sistemi di trattamento automatizzato, il momento della loro introduzione e la persona che l'ha effettuata («controllo dell'introduzione»); h) impedire che i dati personali possano essere letti, copiati, modificati o cancellati in modo	riferisce la loro autorizzazione d'accesso («controllo dell'accesso ai dati»); f) garantire la possibilità di individuare i soggetti ai quali siano stati o possano essere trasmessi o resi disponibili i dati personali utilizzando attrezzature per la trasmissione di dati («controllo della trasmissione»); g) garantire la possibilità di verificare e accertare a posteriori quali dati personali sono stati introdotti nei sistemi di trattamento automatizzato, il momento della loro introduzione e la persona che l'ha effettuata («controllo dell'introduzione»); h) impedire che i dati personali possano essere letti, copiati, modificati o cancellati in modo non autorizzato durante i trasferimenti di dati personali o il trasporto di supporti di dati («controllo del trasporto»); i) garantire che, in caso di interruzione, i sistemi utilizzati possano essere ripristinati («recupero»); l) garantire che le funzioni del sistema siano operative, che eventuali errori di funzionamento siano segnalati («affidabilità») e che i dati personali conservati non possano essere falsati da un errore di funzionamento del sistema («integrità»).	3. Se si procede al dibattimento, non è consentita la pubblicazione, anche parziale, degli atti del fascicolo per il dibattimento, se non dopo la pronuncia della sentenza di primo grado, e di quelli del fascicolo del pubblico ministero, se non dopo la pronuncia della sentenza in grado di appello. E' sempre consentita la pubblicazione degli atti utilizzati per le contestazioni. 4. E' vietata la pubblicazione, anche parziale, degli atti del dibattimento celebrato a porte chiuse nei casi previsti dall'articolo 472 commi 1 e 2. In tali casi il giudice, sentite le parti, può disporre il divieto di pubblicazione anche degli atti o di parte degli atti utilizzati per le contestazioni. Il divieto di pubblicazione cessa comunque quando sono trascorsi i termini stabiliti dalla legge sugli archivi di Stato ovvero è trascorso il termine di dieci anni dalla sentenza irrevocabile e la pubblicazione è autorizzata dal ministro di grazia e giustizia. 5. Se non si procede al dibattimento, il giudice, sentite le parti, può disporre il divieto di pubblicazione di atti o di parte di atti quando la pubblicazione di essi può offendere il buon costume o comportare la diffusione di notizie sulle quali la legge prescrive di mantenere il segreto nell'interesse dello Stato ovvero causare pregiudizio alla riservatezza dei testimoni o delle parti private. Si applica la disposizione dell'ultimo periodo del comma 4. 6. E' vietata la pubblicazione delle generalità e dell'immagine dei minorenni testimoni, persone offese o danneggiati dal reato fino a

non autorizzato durante i trasferimenti di dati personali o il trasporto di supporti di dati («controllo del trasporto»); i)garantire che, in caso di interruzione, i sistemi utilizzati possano essere ripristinati («recupero»); j)garantire che le funzioni del sistema siano operative, che eventuali errori di funzionamento siano segnalati («affidabilità») e che i dati personali conservati non possano essere falsati da un errore di funzionamento del sistema («integrità»).		quando non sono divenuti maggiorenni. E altresì vietata la pubblicazione di elementi che anche indirettamente possano comunque portare alla identificazione dei suddetti minorenni. Il tribunale per i minorenni, nell'interesse esclusivo del minorenne, o il minorenne che ha compiuto i sedici anni, può consentire la pubblicazione. 6-bis. E' vietata la pubblicazione dell'immagine di persona privata della libertà personale ripresa mentre la stessa si trova sottoposta all'uso di manette ai polsi ovvero ad altro mezzo di coercizione fisica, salvo che la persona vi consenta. 7. E' sempre consentita la pubblicazione del contenuto di atti non coperti dal segreto. Art. 115. *Violazione del divieto di pubblicazione*. 1. Salve le sanzioni previste dalla legge penale, la violazione del divieto di pubblicazione previsto dagli articoli 114 e 329 comma 3 lettera b) costituisce illecito disciplinare quando il fatto è commesso da impiegati dello Stato o di altri enti pubblici ovvero da persone esercenti una professione per la quale è richiesta una speciale abilitazione dello Stato. 2. Di ogni violazione del divieto di pubblicazione commessa dalle persone indicate nel comma 1 il pubblico ministero informa l'organo titolare del potere disciplinare. Art. 329. *Obbligo del segreto.*

		1. Gli atti d'indagine compiuti dal pubblico ministero e dalla polizia giudiziaria, le richieste del pubblico ministero di autorizzazione al compimento di atti di indagine e gli atti del giudice che provvedono su tali richieste sono coperti dal segreto fino a quando l'imputato non ne possa avere conoscenza e, comunque, non oltre la chiusura delle indagini preliminari. 2. Quando è necessario per la prosecuzione delle indagini, il pubblico ministero può, in deroga a quanto previsto dall'articolo 114, consentire, con decreto motivato, la pubblicazione di singoli atti o di parti di essi. In tal caso, gli atti pubblicati sono depositati presso la segreteria del pubblico ministero. 3. Anche quando gli atti non sono più coperti dal segreto a norma del comma 1, il pubblico ministero, in caso di necessità per la prosecuzione delle indagini, può disporre con decreto motivato: a) l'obbligo del segreto per singoli atti, quando l'imputato lo consente o quando la conoscenza dell'atto può ostacolare le indagini riguardanti altre persone; b) il divieto di pubblicare il contenuto di singoli atti o notizie specifiche relative a determinate operazioni. Art. 226. *Conferimento dell'incarico.* 1. Il giudice, accertate le generalità del perito, gli chiede se si trova in una delle condizioni previste dagli articoli 222 e 223, lo avverte degli obblighi e delle responsabilità previste

dalla legge penale e lo invita a rendere la seguente dichiarazione: «consapevole della responsabilità morale e giuridica che assumo nello svolgimento dell'incarico, mi impegno ad adempiere al mio ufficio senza altro scopo che quello di far conoscere la verità e a mantenere il segreto su tutte le operazioni peritali».
2. [...]

Codice penale.
Art. 326. *Rivelazione ed utilizzazione di segreti di ufficio.*
Il pubblico ufficiale o la persona incaricata di un pubblico servizio, che, violando i doveri inerenti alle funzioni o al servizio, o comunque abusando della sua qualità, rivela notizie d'ufficio, le quali debbano rimanere segrete, o ne agevola in qualsiasi modo la conoscenza, è punito con la reclusione da sei mesi a tre anni.
Se l'agevolazione è soltanto colposa, si applica la reclusione fino a un anno.
Il pubblico ufficiale o la persona incaricata di un pubblico servizio, che, per procurare a sé o ad altri un indebito profitto patrimoniale, si avvale illegittimamente di notizie d'ufficio, le quali debbano rimanere segrete, è punito con la reclusione da due a cinque anni. Se il fatto è commesso al fine di procurare a sé o ad altri un ingiusto profitto non patrimoniale o di cagionare ad altri un danno ingiusto, si applica la pena della reclusione fino a due anni.

Art. 379 bis. *Rivelazione di segreti inerenti a un procedimento penale.*

Salvo che il fatto costituisca più grave reato, chiunque rivela indebitamente notizie segrete concernenti un procedimento penale, da lui apprese per avere partecipato o assistito ad un atto del procedimento stesso, è punito con la reclusione fino a un anno. La stessa pena si applica alla persona che, dopo avere rilasciato dichiarazioni nel corso delle indagini preliminari, non osserva il divieto imposto dal pubblico ministero ai sensi dell'articolo 391-quinquies del codice di procedura penale.

art. 621. *Rivelazione del contenuto di documenti segreti.*
Chiunque, essendo venuto abusivamente a cognizione del contenuto, che debba rimanere segreto, di altrui atti o documenti, pubblici o privati, non costituenti corrispondenza, lo rivela, senza giusta causa, ovvero lo impiega a proprio o altrui profitto, è punito, se dal fatto deriva nocumento, con la reclusione fino a tre anni o con la multa da euro 103 a euro 1.032.
Agli effetti della disposizione di cui al primo comma è considerato documento anche qualunque supporto informatico contenente dati, informazioni o programmi.
Il delitto è punibile a querela della persona offesa

Art. 622. *Rivelazione di segreto professionale.*
Chiunque, avendo notizia, per ragione del proprio stato o ufficio, o della propria professione o arte, di un segreto, lo rivela, senza giusta causa, ovvero lo impiega a

proprio o altrui profitto, è punito, se dal fatto può derivare nocumento, con la reclusione fino a un anno o con la multa da euro 30 a euro 516.
La pena è aggravata se il fatto è commesso da amministratori, direttori generali, dirigenti preposti alla redazione dei documenti contabili societari (1), sindaci o liquidatori o se è commesso da chi svolge la revisione contabile della società.
Il delitto è punibile a querela della persona offesa.

Art. 684. *Pubblicazione arbitraria di atti di un procedimento penale.*
Chiunque pubblica, in tutto o in parte, anche per riassunto o a guisa d'informazione, atti o documenti di un procedimento penale, di cui sia vietata per legge la pubblicazione è punito con l'arresto fino a trenta giorni o con l'ammenda da euro 51 a euro 258.

Sempre all'interno del codice penale, è poi previsto un ampio spettro di sanzioni penali per la violazione della integrità dei dati e dei sistemi informatici e della riservatezza dei dati e delle comunicazioni informatiche, mediante la previsione di fattispecie incriminatrici in tema di: falsa dichiarazione o attestazione al certificatore sull'identità o su qualità personali proprie o di altri (art. 495 bis); frodi informatiche (art. 640 ter); falsificazioni in documenti informatici (art. 491 ter); danneggiamento di sistemi informatici e

		telematici (art. 635 bis); danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità (art. 635 ter); danneggiamento di sistemi informatici o telematici (art. 635 quater); attentato a impianti di pubblica utilità (art. 420); accesso abusivo ad un sistema informatico o telematico (art. 615 ter); detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (art. 615 quater); diffusione di programmi diretti a danneggiare o interrompere un sistema informatico (art. 615 quinquies); intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617 quater); installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche (art. 617 quinquies); falsificazione, alterazione o soppressione del contenuto di comunicazioni informatiche o telematiche (art. 617 sexies). **D.P.R. 14 novembre 2002, n. 313** **(Testo unico delle disposizioni legislative e regolamentari in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti).** Art. 41 (*Principi e funzioni*) 1. Il sistema consente lo svolgimento, con tecnologie informatiche, delle attività degli uffici e tra essi concernenti l'iscrizione, l'eliminazione, lo scambio, la trasmissione e

conservazione dei dati, e delle attività concernenti i servizi certificativi, anche nei rapporti con l'utenza, nel rispetto di rigorosi criteri di completezza, aggiornamento, esattezza e sicurezza delle notizie e delle informazioni raccolte.

2. Il sistema consente, altresì, attraverso l'utilizzo di appositi strumenti di controllo, il costante monitoraggio dei soggetti che compiono le attività, della data e della tipologia delle stesse, nonché delle attività di acquisizione, certificazione e visura dei dati.

3. Il sistema opera in modo tale da assicurare il rispetto del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, e delle regole tecniche emanate in attuazione dello stesso, nonché delle disposizioni sulla tutela della riservatezza dei dati personali.

Art. 42 (*Regole tecniche del sistema*)

1. Le regole tecniche di funzionamento del sistema, attinenti alle procedure degli uffici e tra gli uffici interessati, alle procedure concernenti l'utilizzazione del codice identificativo e il numero identificativo, ai relativi tempi, e ai servizi certificativi, sono stabilite con decreto dirigenziale del Ministero della Giustizia, nel contesto della disciplina generale di cui all'articolo 41, comma 3, sentiti la Presidenza del Consiglio dei ministri - Dipartimento per l'innovazione e le tecnologie e il Garante per la protezione dei dati personali.

1-bis. Le regole procedurali di carattere

		tecnico-operativo relative agli scambi tra i casellari giudiziali europei sono stabilite con decreto del Ministero della giustizia, da emanarsi entro sei mesi dalla data di entrata in vigore della presente disposizione, nell'ambito della disciplina generale di cui all'articolo 41, comma 3, sentiti l'Agenzia per l'Italia digitale e il Garante per la protezione dei dati personali. 2. Per le procedure concernenti l'utilizzazione del codice identificativo di cui all'articolo 43, il decreto dirigenziale è adottato sentito altresì il Ministero dell'interno. Per le procedure concernenti l'utilizzazione del codice fiscale, fatte salve la disciplina in materia di anagrafe tributaria e codice fiscale e le relative competenze del Ministero dell'economia e delle finanze e delle agenzie fiscali, il decreto è adottato altresì sulla base delle prescrizioni tecniche stabilite con decreto dirigenziale del Ministero dell'economia e delle finanze. 3. Le tecnologie informatiche sono finalizzate a prevenire e correggere eventuali errori nella immissione, scambio, trasmissione e conservazione dei dati, anche in collegamento con il sistema informatizzato dei registri.
Articolo 30 **Notifica di una violazione dei dati personali all'autorità di controllo** 1. Gli Stati membri dispongono che, in caso di violazione dei dati personali, il titolare del	ART. 26 (*Notifica al Garante di una violazione di dati personali*) 1. Salvo quanto previsto dall'articolo 37 comma 3, in caso di violazione di dati	La disposizione della direttiva è stata integralmente recepita dallo schema di decreto.

trattamento notifichi la violazione all'autorità di controllo senza ingiustificato ritardo, ove possibile entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, è corredata dei motivi del ritardo. 2. Il responsabile del trattamento informa il titolare del trattamento senza ingiustificato ritardo dopo essere venuto a conoscenza della violazione. 3. La notifica di cui al paragrafo 1 deve almeno: a) descrivere la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione; b) comunicare il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni; c) descrivere le probabili conseguenze della violazione dei dati personali;	personali, il titolare del trattamento notifica la violazione al Garante con le modalità di cui all'articolo 33 del Regolamento. 2. Se la violazione dei dati personali riguarda dati personali che sono stati trasmessi dal o al titolare del trattamento di un altro Stato membro, le informazioni previste dal citato articolo 33 sono comunicate, senza ingiustificato ritardo, al titolare del trattamento di tale Stato membro.	

d)descrivere le misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, misure per attenuarne i possibili effetti negativi. 4. Qualora e nella misura in cui non sia possibile fornire le informazioni contestualmente, le informazioni possono essere fornite in fasi successive senza ulteriore ingiustificato ritardo. 5. Gli Stati membri dispongono che il titolare del trattamento documenti qualsiasi violazione dei dati personali di cui al paragrafo 1, comprese le circostanze in cui si è verificata la violazione dei dati personali, le sue conseguenze e i provvedimenti adottati per porvi rimedio. Tale documentazione consente all'autorità di controllo di verificare il rispetto del presente articolo. 6. Gli Stati membri dispongono che, se la violazione dei dati personali riguarda dati personali che sono stati trasmessi dal o al titolare del trattamento di un altro Stato membro, le informazioni di cui al paragrafo 3 siano comunicate al titolare del trattamento di tale Stato membro senza ingiustificato ritardo.		
Articolo 31 **Comunicazione di una violazione dei dati personali all'interessato**	ART. 27 (*Comunicazione di una violazione di dati personali all'interessato*) 1. Quando la violazione di dati personali è	La disposizione della direttiva è stata integralmente recepita dallo schema di decreto.

1. Gli Stati membri dispongono che, quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento comunichi la violazione all'interessato senza ingiustificato ritardo. 2. La comunicazione all'interessato di cui al paragrafo 1 del presente articolo descrive con un linguaggio semplice e chiaro la natura della violazione dei dati personali e contiene almeno le informazioni e le misure di cui all'articolo 30, paragrafo 3, lettere b), c) e d). 3. Non è richiesta la comunicazione all'interessato di cui al paragrafo 1 se è soddisfatta una delle seguenti condizioni: a)il titolare del trattamento ha messo in atto le misure tecnologiche e organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura; b)il titolare del trattamento ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati di cui al paragrafo 1; c)detta comunicazione richiederebbe sforzi	suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, si osservano le disposizioni in tema di comunicazioni di cui all'articolo 34 del regolamento. 2. La comunicazione all'interessato di cui al comma 1 può essere ritardata, limitata od omessa alle condizioni e per i motivi di cui all'articolo 14, comma 2.	

sproporzionati. In tal caso, si procede invece a una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia. 4. Nel caso in cui il titolare del trattamento non abbia ancora comunicato all'interessato la violazione dei dati personali, l'autorità di controllo può richiedere, dopo aver valutato la probabilità che la violazione dei dati personali presenti un rischio elevato, che vi provveda o può decidere che una delle condizioni di cui al paragrafo 3 è soddisfatta. 5. La comunicazione all'interessato di cui al paragrafo 1 del presente articolo può essere ritardata, limitata od omessa alle condizioni e per i motivi di cui all'articolo 13, paragrafo 3.		
Sezione 3 **Responsabile della protezione dei dati** *Articolo 32* **Designazione del responsabile della protezione dei dati** 1. Gli Stati membri dispongono che il titolare del trattamento designi un responsabile della protezione dei dati. Gli Stati membri possono esentare le autorità giurisdizionali e le altre autorità giudiziarie indipendenti quando esercitano le loro funzioni giurisdizionali da tale obbligo. 2. Il responsabile della protezione dei dati è	SEZIONE III *RESPONSABILE DELLA PROTEZIONE DEI DATI* ART. 28 (*Designazione del responsabile della protezione dei dati*) 1. Il titolare del trattamento designa un responsabile della protezione dei dati. 2. Il responsabile della protezione dei dati è designato in funzione delle qualità professionali, in particolare della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, e della capacità di assolvere i compiti di cui all'articolo 30.	La disposizione della direttiva è stata integralmente recepita dallo schema di decreto.

designato in funzione delle qualità professionali, in particolare della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, e della capacità di assolvere i compiti di cui all'articolo 34. 3. Può essere designato un unico responsabile della protezione dei dati per più autorità competenti, tenuto conto della loro struttura organizzativa e dimensione. 4. Gli Stati membri dispongono che il titolare del trattamento pubblichi i dati di contatto del responsabile della protezione dei dati e le comunichi all'autorità di controllo.	3. Può essere designato un unico responsabile della protezione dei dati per più autorità competenti, tenuto conto della loro struttura organizzativa e dimensione. 4. Il titolare del trattamento pubblica i dati di contatto del responsabile della protezione dei dati e, salvo quanto previsto dall'articolo 37, comma 6, li comunica al Garante.	
Articolo 33 **Posizione del responsabile della protezione dei dati** 1. Gli Stati membri dispongono che il titolare del trattamento si assicuri che il responsabile della protezione dei dati sia coinvolto adeguatamente e tempestivamente in tutte le questioni riguardanti la protezione dei dati personali. 2. Il titolare del trattamento sostiene il responsabile della protezione dei dati nell'esecuzione dei compiti di cui all'articolo 34 fornendogli le risorse necessarie per assolvere tali compiti e accedere ai dati personali e ai trattamenti e per mantenere la propria conoscenza specialistica.	ART. 29 (*Posizione del responsabile della protezione dei dati*) 1. Il titolare del trattamento si assicura che il responsabile della protezione dei dati sia coinvolto adeguatamente e tempestivamente in tutte le questioni riguardanti la protezione dei dati personali. 2. Il titolare del trattamento coadiuva il responsabile della protezione dei dati nell'esecuzione dei compiti di cui all'articolo 29 fornendogli le risorse necessarie per assolvere tali compiti, per accedere ai dati personali e ai trattamenti e per mantenere la propria conoscenza specialistica.	La disposizione della direttiva è stata integralmente recepita dallo schema di decreto.

Articolo 34 **Compiti del responsabile della protezione dei dati** Gli Stati membri dispongono che il titolare del trattamento conferisca al responsabile della protezione dei dati almeno i seguenti compiti: a) informare e consigliare il titolare del trattamento e i dipendenti che effettuano il trattamento in merito ai loro obblighi derivanti dalla presente direttiva nonché da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati; b) sorvegliare l'osservanza della presente direttiva, di altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati nonché delle politiche del titolare del trattamento in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo; c) fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'articolo 27; d) cooperare con l'autorità di controllo;	ART. 30 *(Compiti del responsabile della protezione dei dati)* 1. Il titolare del trattamento conferisce al responsabile della protezione dei dati almeno i seguenti compiti: a) informare il titolare del trattamento e i dipendenti che effettuano il trattamento degli obblighi derivanti dal presente decreto nonché da altre disposizioni dell'Unione europea o dello Stato relative alla protezione dei dati; b) vigilare sull'osservanza del presente decreto e di altre disposizioni dell'Unione europea o dello Stato relative alla protezione dei dati nonché delle previsioni di programma del titolare del trattamento in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo; c) fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'articolo 23; d) cooperare con il Garante; e) fungere da punto di contatto per il Garante per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'articolo 24, ed effettuare, ove necessario, consultazioni relativamente a qualunque altra questione.	La disposizione della direttiva è stata integralmente recepita dallo schema di decreto.

e)fungere da punto di contatto per l'autorità di controllo per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'articolo 28, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione.		
CAPO V. ***Trasferimenti di dati personali verso paesi terzi o organizzazioni internazionali*** *Articolo 35* **Principi generali per il trasferimento di dati personali** 1. Gli Stati membri dispongono che qualunque trasferimento, a cura delle autorità competenti, di dati personali oggetto di un trattamento o destinati a essere oggetto di un trattamento dopo il trasferimento verso un paese terzo o un'organizzazione internazionale, compresi trasferimenti successivi verso un altro paese terzo o un'altra organizzazione internazionale, abbia luogo, fatta salva la conformità alle disposizioni nazionali adottate a norma delle altre disposizioni della presente direttiva, soltanto se sono soddisfatte le condizioni di cui al presente capo, vale a dire: a)il trasferimento è necessario per le finalità di cui all'articolo 1, paragrafo 1;	CAPO IV TRASFERIMENTO DI DATI PERSONALI VERSO PAESI TERZI O ORGANIZZAZIONI INTERNAZIONALI ART. 31 (*Principi generali in materia di trasferimento di dati personali*) 1. Il trasferimento di dati personali oggetto di un trattamento o destinati a essere oggetto di un trattamento dopo il trasferimento verso un Paese terzo o un'organizzazione internazionale, compresi trasferimenti successivi verso un altro Paese terzo o un'altra organizzazione internazionale è consentito se: a)il trasferimento è necessario per le finalità di cui all'articolo 1, comma 2; b) i dati personali sono trasferiti al titolare del trattamento in un Paese terzo o a un'organizzazione internazionale che sia un'autorità competente per le finalità di cui all'articolo 1, comma 2;	La disposizione della direttiva è stata integralmente recepita dallo schema di decreto.

b) i dati personali sono trasferiti al titolare del trattamento in un paese terzo o un'organizzazione internazionale che sia un'autorità competente per le finalità di cui all'articolo 1, paragrafo 1;

c) qualora i dati personali siano trasmessi o resi disponibili da un altro Stato membro, tale Stato membro ha fornito la propria autorizzazione preliminare al trasferimento conformemente al proprio diritto nazionale;

d) la Commissione ha adottato una decisione di adeguatezza, a norma dell'articolo 36, oppure, in mancanza di detta decisione, sono state fornite o esistono garanzie adeguate ai sensi dell'articolo 37, oppure, in mancanza di una decisione di adeguatezza ai sensi dell'articolo 36 e di garanzie adeguate ai sensi dell'articolo 37, si applicano deroghe per situazioni specifiche a norma dell'articolo 38; e

e) in caso di trasferimento successivo a un altro paese terzo o a un'altra organizzazione internazionale, l'autorità competente che ha effettuato il trasferimento originario o un'altra autorità competente dello stesso Stato membro autorizza il trasferimento successivo, dopo aver tenuto debitamente conto di tutti i fattori pertinenti, tra cui la gravità del reato, la finalità per la quale i dati

c) qualora i dati personali siano trasmessi o resi disponibili da uno Stato membro, tale Stato ha fornito la propria autorizzazione preliminare al trasferimento conformemente al proprio diritto nazionale;

d) la Commissione europea ha adottato una decisione di adeguatezza, a norma dell'articolo 32 o, in mancanza, sono state fornite o esistono garanzie adeguate ai sensi dell'articolo 33; in assenza di una decisione di adeguatezza e di garanzie adeguate, si applicano deroghe per situazioni specifiche ai sensi dell'articolo 34; e

e) in caso di trasferimento successivo a un altro Paese terzo o a un'altra organizzazione internazionale, l'autorità competente che ha effettuato il trasferimento originario o un'altra autorità competente dello stesso Stato membro autorizza il trasferimento successivo dopo avere valutato tutti i fattori pertinenti, tra cui la gravità del reato, la finalità per la quale i dati personali sono stati trasferiti e il livello di protezione dei dati personali previsto nel Paese terzo o nell'organizzazione internazionale verso i quali i dati personali sono successivamente trasferiti.

2. In assenza dell'autorizzazione preventiva di un altro Stato membro di cui al comma 1, lettera c), il trasferimento di dati personali è consentito solo se necessario per prevenire una minaccia grave e immediata alla sicurezza

personali sono stati originariamente trasferiti e il livello di protezione dei dati personali nel paese terzo o nell'organizzazione internazionale verso i quali i dati personali sono successivamente trasferiti. 2. Gli Stati membri dispongono che i trasferimenti senza l'autorizzazione preventiva di un altro Stato membro conformemente al paragrafo 1, lettera c), siano consentiti soltanto se il trasferimento di dati personali è necessario per prevenire una minaccia grave e immediata alla sicurezza pubblica di uno Stato membro o di un paese terzo o agli interessi vitali di uno Stato membro e l'autorizzazione preliminare non può essere ottenuta tempestivamente. L'autorità competente a rilasciare l'autorizzazione preliminare è informata senza indugio. 3. Tutte le disposizioni del presente capo sono applicate al fine di assicurare che il livello di protezione delle persone fisiche assicurato dalla presente direttiva non sia pregiudicato.	pubblica di uno Stato membro o di un Paese terzo o agli interessi vitali di uno Stato membro e l'autorizzazione preliminare non può essere ottenuta tempestivamente. L'autorità competente a rilasciare l'autorizzazione preliminare è informata senza ritardo.	
Articolo 36 **Trasferimento sulla base di una decisione di adeguatezza** 1. Gli Stati membri dispongono che il trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale sia ammesso se la Commissione ha deciso che il	ART. 32 (*Trasferimento sulla base di una decisione di adeguatezza*) 1 Il trasferimento di dati personali verso un Paese terzo o un'organizzazione internazionale è consentito se la Commissione dell'Unione europea ha deciso che il Paese terzo, un	La disposizione della direttiva è stata integralmente recepita dallo schema di decreto.

paese terzo, un territorio o uno o più settori specifici all'interno del paese terzo, o l'organizzazione internazionale in questione garantiscano un livello di protezione adeguato. In tal caso il trasferimento non necessita di autorizzazioni specifiche. 2. Nel valutare l'adeguatezza del livello di protezione la Commissione prende in considerazione in particolare i seguenti elementi: a) lo stato di diritto, il rispetto dei diritti umani e delle libertà fondamentali, la pertinente legislazione generale e settoriale (anche in materia di sicurezza pubblica, difesa, sicurezza nazionale, diritto penale e accesso delle autorità pubbliche ai dati personali), come anche l'attuazione di tale legislazione, le norme in materia di protezione dei dati, le regole professionali e le misure di sicurezza, comprese le regole per il trasferimento successivo dei dati personali verso un altro paese terzo o un'altra organizzazione internazionale osservate nel paese o dall'organizzazione internazionale in questione, la giurisprudenza, nonché i diritti effettivi e azionabili degli interessati e un ricorso effettivo in sede amministrativa e giudiziaria per gli interessati i cui dati personali sono trasferiti; b) l'esistenza e l'effettivo funzionamento di una o più autorità di controllo indipendenti nel paese terzo o cui è soggetta	territorio o uno o più settori specifici all'interno del Paese terzo, o l'organizzazione internazionale garantiscono un livello di protezione adeguato. In tal caso non sono necessarie autorizzazioni specifiche.	

un'organizzazione internazionale, con competenza per garantire e controllare il rispetto delle norme in materia di protezione dei dati, comprensiva di adeguati poteri esecutivi, per assistere e consigliare gli interessati in merito all'esercizio dei loro diritti e cooperare con le autorità di controllo degli Stati membri; e c) gli impegni internazionali assunti dal paese terzo o dall'organizzazione internazionale in questione o altri obblighi derivanti da convenzioni o strumenti giuridicamente vincolanti come pure dalla loro partecipazione a sistemi multilaterali o regionali, in particolare in relazione alla protezione dei dati personali. 3. La Commissione, previa valutazione dell'adeguatezza del livello di protezione, può decidere, mediante un atto 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 ai sensi del paragrafo 2 del presente articolo. L'atto di esecuzione prevede un meccanismo di riesame periodico, almeno ogni quattro anni, che tenga conto di tutti gli sviluppi pertinenti nel paese terzo o nell'organizzazione internazionale. L'atto di esecuzione specifica il proprio ambito di applicazione geografico e settoriale e, se del caso, identifica la o le autorità di controllo di cui al paragrafo 2, lettera b), del presente		

articolo. L'atto di esecuzione è adottato secondo la procedura d'esame di cui all'articolo 58, paragrafo 2. 4. La Commissione controlla su base continuativa gli sviluppi nei paesi terzi e nelle organizzazioni internazionali che potrebbero incidere sul funzionamento delle decisioni adottate a norma del paragrafo 3. 5. Se risulta dalle informazioni disponibili, in particolare in seguito al riesame di cui al paragrafo 3 del presente articolo, che un paese terzo, un territorio o uno o più settori specifici all'interno di un paese terzo, o un'organizzazione internazionale non garantiscono più un livello di protezione adeguato ai sensi del paragrafo 2 del presente articolo, la Commissione revoca, modifica o sospende nella misura necessaria la decisione di cui al paragrafo 3 del presente articolo mediante atti di esecuzione senza effetto retroattivo. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 58, paragrafo 2. Per imperativi motivi di urgenza debitamente giustificati, la Commissione adotta atti di esecuzione immediatamente applicabili secondo la procedura di cui all'articolo 58, paragrafo 3. 6. La Commissione avvia consultazioni con il paese terzo o l'organizzazione internazionale per porre rimedio alla situazione che ha motivato la decisione di cui al paragrafo 5.		

7. Gli Stati membri dispongono che una decisione ai sensi del paragrafo 5 lasci impregiudicato il trasferimento di dati personali verso il paese terzo, il territorio o uno o più settori specifici all'interno del paese terzo, o verso l'organizzazione internazionale in questione, a norma degli articoli 37 e 38. 8. La Commissione pubblica nella *Gazzetta ufficiale dell'Unione europea* e sul suo sito web l'elenco dei paesi terzi, dei territori e settori specifici all'interno di un paese terzo, e delle organizzazioni internazionali per i quali ha deciso che è o non è più garantito un livello di protezione adeguato.		
Articolo 37 **Trasferimenti soggetti a garanzie adeguate** 1. In mancanza di una decisione ai sensi dell'articolo 36, paragrafo 3, gli Stati membri dispongono che sia ammesso un trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale se: a) sono fornite garanzie adeguate per la protezione dei dati personali in uno strumento giuridicamente vincolante; oppure b) il titolare del trattamento ha valutato tutte le circostanze relative al trasferimento dei dati personali e ritiene che sussistano garanzie adeguate per la protezione dei dati personali.	ART. 33 *(Trasferimenti soggetti a garanzie adeguate)* 1. In mancanza o in caso di revoca, modifica o sospensione di una decisione di adeguatezza di cui all'articolo 32, il trasferimento di dati personali verso un Paese terzo o un'organizzazione internazionale è consentito se: a) sono fornite garanzie adeguate per la protezione dei dati personali; o b) il titolare del trattamento ritiene che sussistano garanzie adeguate per la protezione dei dati personali. 2. Il titolare del trattamento informa il Garante dei trasferimenti effettuati ai sensi del	La disposizione della direttiva è stata integralmente recepita dallo schema di decreto.

2. Il titolare del trattamento informa l'autorità di controllo in merito alle categorie di trasferimenti di cui al paragrafo 1, lettera b). 3. Qualora sia basato sul paragrafo 1, lettera b), un tale trasferimento deve essere documentato e, su richiesta, la documentazione deve essere messa a disposizione dell'autorità di controllo con l'indicazione della data e dell'ora del trasferimento, delle informazioni sull'autorità competente ricevente, della motivazione del trasferimento e dei dati personali trasferiti.	comma 1, lettera b), con l'indicazione, se richiesta, della data e dell'ora del trasferimento, dell'autorità competente ricevente, della motivazione del trasferimento e dei dati personali trasferiti.	
Articolo 38 **Deroghe in specifiche situazioni** 1. In mancanza di una decisione di adeguatezza ai sensi dell'articolo 36 o di garanzie adeguate ai sensi dell'articolo 37, gli Stati membri provvedono affinché un trasferimento o una categoria di trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale possano aver luogo soltanto a condizione che il trasferimento sia necessario: a) per tutelare un interesse vitale dell'interessato o di un'altra persona; b) per salvaguardare i legittimi interessi dell'interessato qualora lo preveda il diritto dello Stato membro che trasferisce i dati	ART. 34 (*Deroghe in situazioni specifiche*) 1. In mancanza o in caso di revoca, modifica o sospensione di una decisione di adeguatezza ai sensi dell'articolo 32 o di garanzie adeguate di cui all'articolo 33, il trasferimento o una categoria di trasferimenti di dati personali verso un Paese terzo o un'organizzazione internazionale sono consentiti se necessari per una delle seguenti finalità: a) per tutelare un interesse vitale dell'interessato o di un'altra persona; b) per salvaguardare i legittimi interessi dell'interessato quando lo preveda il diritto dello Stato membro che trasferisce i dati personali;	La disposizione della direttiva è stata integralmente recepita dallo schema di decreto.

personali; c) per prevenire una minaccia grave e immediata alla sicurezza pubblica di uno Stato membro o di un paese terzo; d) nei singoli casi, per le finalità di cui all'articolo 1, paragrafo 1; oppure e) nel singolo caso, per accertare, esercitare o difendere un diritto in sede giudiziaria in relazione alle finalità di cui all'articolo 1, paragrafo 1. 2. I dati personali non sono trasferiti se l'autorità competente che opera il trasferimento determina che i diritti e le libertà fondamentali dell'interessato prevalgono sull'interesse pubblico al trasferimento di cui al paragrafo 1, lettere d) ed e). 3. Qualora sia basato sul paragrafo 1, un tale trasferimento deve essere documentato e, su richiesta, la documentazione deve essere messa a disposizione dell'autorità di controllo con l'indicazione della data e dell'ora del trasferimento, delle informazioni sull'autorità competente ricevente, della motivazione del trasferimento e dei dati personali trasferiti.	c) per prevenire una minaccia grave e immediata alla sicurezza pubblica di uno Stato membro o di un Paese terzo; d) per le finalità di cui all'articolo 1, comma 2; e) per accertare, esercitare o difendere un diritto in sede giudiziaria in relazione alle finalità di cui all'articolo 1, comma 2. 2. Nei casi di cui al comma 1, lettere d) ed e), i dati personali non sono trasferiti se l'autorità competente che effettua il trasferimento valuta i diritti e le libertà fondamentali dell'interessato prevalenti rispetto all'interesse pubblico al trasferimento. 3. Il trasferimento effettuato ai sensi del comma 1 deve essere documentato e, su richiesta, la documentazione deve essere messa a disposizione del Garante con l'indicazione della data e dell'ora del trasferimento, dell'autorità competente ricevente, della motivazione del trasferimento e dei dati personali trasferiti.	
Articolo 39 **Trasferimenti di dati personali a destinatari**	ART. 35 *(Trasferimenti di dati personali a destinatari stabiliti in Paesi terzi)*	La disposizione della direttiva è stata integralmente recepita dallo schema di decreto.

stabiliti in paesi terzi 1. In deroga all'articolo 35, paragrafo 1, lettera b), e fatti salvi eventuali accordi internazionali di cui al paragrafo 2 del presente articolo, il diritto dell'Unione o dello Stato membro può disporre che le autorità competenti di cui all'articolo 3, punto 7), lettera a), possano, in casi singoli e specifici, trasferire dati personali direttamente a destinatari stabiliti in paesi terzi soltanto se le altre disposizioni della presente direttiva sono rispettate e se sono soddisfatte tutte le seguenti condizioni: a) il trasferimento è strettamente necessario per l'assolvimento di un compito dell'autorità competente che opera il trasferimento ai sensi del diritto dell'Unione o dello Stato membro per le finalità di cui all'articolo 1, paragrafo 1; b) l'autorità competente che opera il trasferimento determina che i diritti e le libertà fondamentali dell'interessato non prevalgono sull'interesse pubblico che rende necessario il trasferimento nel caso in questione; c) l'autorità competente che opera il trasferimento ritiene che il trasferimento a un'autorità competente per le finalità di cui all'articolo 1, paragrafo 1, nel paese terzo sia inefficace o inadatto, in particolare in quanto	1. In deroga a quanto previsto dall'articolo 31, comma 1, lettera b), e fatti salvi eventuali accordi internazionali di cui al comma 2, le autorità competenti di cui all'articolo 2, comma 1, lettera h) numero 1), possono, in singoli e specifici casi previsti da norme di legge o di regolamento o dal diritto dell'Unione europea, trasferire dati personali direttamente a destinatari stabiliti in Paesi terzi se: a) il trasferimento è strettamente necessario per l'assolvimento di un compito previsto dal diritto dell'Unione europea o dall'ordinamento interno, per le finalità di cui all'articolo 1, comma 2; b) l'autorità competente che effettua il trasferimento valuta che i diritti e le libertà fondamentali dell'interessato non prevalgono sull'interesse pubblico che rende necessario il trasferimento; c) l'autorità competente che effettua il trasferimento ritiene che il trasferimento a un'autorità per le finalità di cui all'articolo 1, comma 2, nel Paese terzo sia inefficace o inidoneo, in particolare in quanto non può essere effettuato tempestivamente; d) l'autorità competente ai fini di cui all'articolo 1, comma 2, nel Paese terzo è informata senza ingiustificato ritardo, salvo che ciò pregiudichi la finalità per cui il	

il trasferimento non può essere effettuato tempestivamente; d) l'autorità competente ai fini di cui all'articolo 1, paragrafo 1, nel paese terzo è informata senza ingiustificato ritardo, a meno che ciò sia inefficace o inadatto; e) l'autorità competente che opera il trasferimento informa il destinatario della finalità specifica o delle finalità specifiche per le quali i dati personali devono essere trattati da quest'ultimo soltanto a condizione che tale trattamento sia necessario. 2. Per accordo internazionale di cui al paragrafo 1 si intende qualsiasi accordo internazionale bilaterale o multilaterale in vigore tra gli Stati membri e paesi terzi nel settore della cooperazione giudiziaria in materia penale e della cooperazione di polizia. 3. L'autorità competente del trasferimento informa l'autorità di controllo in merito ai trasferimenti a norma del presente articolo. 4. Qualora sia basato sul paragrafo 1, un tale trasferimento è documentato.	trasferimento è effettuato; e) l'autorità competente che effettua il trasferimento informa il destinatario della finalità specifica o delle finalità specifiche per le quali i dati personali devono essere trattati, a condizione che tale trattamento sia necessario. 2. Per accordo internazionale di cui al comma 1 si intende qualsiasi accordo internazionale bilaterale o multilaterale in vigore tra gli Stati membri e Paesi terzi nel settore della cooperazione giudiziaria in materia penale e della cooperazione di polizia. 3. L'autorità competente informa il Garante dei trasferimenti previsti dal presente articolo. 4. Il trasferimento effettuato ai sensi del comma 1 è documentato.	
Articolo 40 **Cooperazione internazionale per la protezione dei dati personali** In relazione ai paesi terzi e alle organizzazioni	ART. 36 *(Cooperazione internazionale per la protezione dei dati personali e accordi internazionali precedentemente conclusi)*	La disposizione della direttiva è stata integralmente recepita dallo schema di decreto.

internazionali, la Commissione e gli Stati membri adottano misure appropriate per: a)sviluppare meccanismi di cooperazione internazionale per facilitare l'applicazione efficace della legislazione sulla protezione dei dati personali; b)prestare assistenza reciproca a livello internazionale nell'applicazione della legislazione sulla protezione dei dati personali, in particolare mediante notificazione, deferimento dei reclami, assistenza alle indagini e scambio di informazioni, fatte salve garanzie adeguate per la protezione dei dati personali e gli altri diritti e libertà fondamentali; c)coinvolgere le parti interessate pertinenti in discussioni e attività dirette a promuovere la cooperazione internazionale nell'applicazione della legislazione sulla protezione dei dati personali; d)promuovere lo scambio e la documentazione delle legislazioni e prassi in materia di protezione dei dati personali, compresi i conflitti di giurisdizione con paesi terzi.	1. In relazione ai Paesi terzi e alle organizzazioni internazionali, sono adottate misure appropriate per le finalità di cui all'articolo 50 del regolamento. 2. Restano in vigore, fino alla loro modifica, sostituzione o revoca, gli accordi internazionali relativi al trasferimento di dati personali verso Paesi terzi o organizzazioni internazionali conclusi anteriormente al 6 maggio 2016 e che sono conformi al diritto dell'Unione europea applicabile a tale data.	
CAPO VI ***Autorità di controllo indipendenti***	CAPO V TUTELA E SANZIONI AMMINISTRATIVE ART. 37	La disposizione della direttiva è stata recepita dallo schema di decreto.

Sezione 1 **Indipendenza** *Articolo 41* **Autorità di controllo** 1. Ogni Stato membro dispone che una o più autorità pubbliche indipendenti siano incaricate di sorvegliare l'applicazione della presente direttiva al fine di tutelare i diritti e le libertà fondamentali delle persone fisiche con riguardo al trattamento e di agevolare la libera circolazione dei dati personali all'interno dell'Unione («autorità di controllo»). 2. Ogni autorità di controllo contribuisce alla coerente applicazione della presente direttiva in tutta l'Unione. A tale scopo, le autorità di controllo cooperano tra loro e con la Commissione, a norma del capo VII. 3. Gli Stati membri possono disporre che un'autorità di controllo istituita ai sensi del regolamento (UE) 2016/679 sia l'autorità di controllo di cui alla presente direttiva e assolva i compiti dell'autorità di controllo da istituirsi ai sensi del paragrafo 1 del presente articolo. 4. Qualora in uno Stato membro siano istituite più autorità di controllo, tale Stato membro designa l'autorità di controllo che rappresenta tali autorità nel comitato di cui all'articolo 51.	(*Autorità di controllo*) 1. Il Garante è l'autorità di controllo incaricata di vigilare sull'applicazione delle norme di cui al presente decreto, al fine di tutelare i diritti e le libertà fondamentali delle persone fisiche con riguardo al trattamento di dati personali e di agevolare la libera circolazione dei dati all'interno dell'Unione europea. 2. [...] 3. [...] 4. [...] 5. [...] 6. [...] ART. 38 (*Assistenza reciproca*) 1. Il Garante scambia con le autorità di controllo degli altri Stati membri le informazioni utili e presta assistenza reciproca al fine di attuare e applicare il presente decreto in maniera coerente, e di cooperare efficacemente con loro. L'assistenza reciproca comprende le richieste di informazioni e le misure di controllo, quali le richieste di effettuare consultazioni, ispezioni e indagini. [...]	La normativa interna che disciplina i compiti del Garante, peraltro, già contempla la cooperazione tra diverse autorità di controllo. **D.LGS. 30 giugno 2003, n. 196 (Codice in materia di protezione dei dati personali).** Art. 154 (*Compiti*) [...] 3. Il Garante coopera con altre autorità amministrative indipendenti nello svolgimento dei rispettivi compiti. A tale fine, il Garante può anche invitare rappresentanti di un'altra autorità a partecipare alle proprie riunioni, o essere invitato alle riunioni di altra autorità, prendendo parte alla discussione di argomenti di comune interesse; può richiedere, altresì, la collaborazione di personale specializzato addetto ad altra autorità.

Articolo 42

Indipendenza

1. Ogni Stato membro dispone che ciascuna autorità di controllo agisca in piena indipendenza nell'adempimento dei propri compiti e nell'esercizio dei propri poteri previsti dalla presente direttiva.

2. Gli Stati membri dispongono che, nell'adempimento dei rispettivi compiti e nell'esercizio dei rispettivi poteri previsti dalla presente direttiva, il membro o i membri delle rispettive autorità di controllo non subiscano pressioni esterne, né dirette, né indirette, e non sollecitino né accettino istruzioni da alcuno.

3. I membri delle autorità di controllo degli Stati membri si astengono da qualunque azione incompatibile con le loro funzioni e per tutta la durata del mandato non possono esercitare alcuna altra attività incompatibile, remunerata o meno.

4. Ogni Stato membro provvede affinché ciascuna autorità di controllo sia dotata delle risorse umane, tecniche e finanziarie, dei locali e delle infrastrutture necessari per l'effettivo adempimento dei propri compiti e l'esercizio dei propri poteri, compresi quelli nell'ambito dell'assistenza reciproca, della cooperazione e della partecipazione al comitato.

5. Ogni Stato membro provvede affinché ciascuna autorità di controllo selezioni e

Non si è resa necessaria una specifica norma di recepimento, in quanto la normativa interna già soddisfa le indicazioni della direttiva:

D.LGS. 30 giugno 2003, n. 196 (Codice in materia di protezione dei dati personali).

Art. 153 (*Il Garante*)

1. Il Garante opera in piena autonomia e con indipendenza di giudizio e di valutazione.

2. Il Garante è organo collegiale costituito da quattro componenti, eletti due dalla Camera dei deputati e due dal Senato della Repubblica con voto limitato. I componenti sono scelti tra persone che assicurano indipendenza e che sono esperti di riconosciuta competenza delle materie del diritto o dell'informatica, garantendo la presenza di entrambe le qualificazioni.

3. I componenti eleggono nel loro ambito un presidente, il cui voto prevale in caso di parità. Eleggono altresì un vice presidente, che assume le funzioni del presidente in caso di sua assenza o impedimento.

4. Il presidente e i componenti durano in carica quattro anni e non possono essere confermati per più di una volta; per tutta la durata dell'incarico il presidente e i componenti non possono esercitare, a pena di decadenza, alcuna attività professionale o di consulenza, né essere amministratori o dipendenti di enti pubblici o privati, né ricoprire cariche elettive. (146)

disponga di personale proprio, soggetto alla direzione esclusiva del membro o dei membri dell'autorità di controllo in questione. 6. Ogni Stato membro garantisce che ciascuna autorità di controllo sia soggetta a un controllo finanziario che non ne pregiudichi l'indipendenza e disponga di bilanci annuali, separati e pubblici, che possono far parte del bilancio generale statale o nazionale.		5. All'atto dell'accettazione della nomina il presidente e i componenti sono collocati fuori ruolo se dipendenti di pubbliche amministrazioni o magistrati in attività di servizio; se professori universitari di ruolo, sono collocati in aspettativa senza assegni ai sensi dell'articolo 13 del decreto del Presidente della Repubblica 11 luglio 1980, n. 382, e successive modificazioni. Il personale collocato fuori ruolo o in aspettativa non può essere sostituito. 6. Al presidente compete una indennità di funzione non eccedente, nel massimo, la retribuzione spettante al primo presidente della Corte di cassazione. Ai componenti compete un'indennità non eccedente nel massimo, i due terzi di quella spettante al presidente. Le predette indennità di funzione sono determinate dall'articolo 6 del decreto del Presidente della Repubblica 31 marzo 1998, n. 501, in misura tale da poter essere corrisposte a carico degli ordinari stanziamenti. 7. Alle dipendenze del Garante è posto l'Ufficio di cui all'articolo 156. Art. 155. (*Principi applicabili*) 1. All'Ufficio del Garante, al fine di garantire la responsabilità e l'autonomia ai sensi della legge 7 agosto 1990, n. 241, e successive modificazioni, e del decreto legislativo 30 marzo 2001, n. 165, e successive modificazioni, si applicano i principi riguardanti l'individuazione e le funzioni del

		responsabile del procedimento, nonché quelli relativi alla distinzione fra le funzioni di indirizzo e di controllo, attribuite agli organi di vertice, e le funzioni di gestione attribuite ai dirigenti. Si applicano altresì le disposizioni del medesimo decreto legislativo n. 165 del 2001 espressamente richiamate dal presente codice. Art. 156 (*Ruolo organico e personale*) 1. All'Ufficio del Garante è preposto un segretario generale scelto anche tra magistrati ordinari o amministrativi. 2. Il ruolo organico del personale dipendente è stabilito nel limite di cento unità. 3. Con propri regolamenti pubblicati nella Gazzetta ufficiale della Repubblica italiana, il Garante definisce: a) l'organizzazione e il funzionamento dell'Ufficio anche ai fini dello svolgimento dei compiti di cui all'articolo 154; b) l'ordinamento delle carriere e le modalità di reclutamento del personale secondo le procedure previste dall'articolo 35 del decreto legislativo n. 165 del 2001; c) la ripartizione dell'organico tra le diverse aree e qualifiche; d) il trattamento giuridico ed economico del personale, secondo i criteri previsti dalla legge 31 luglio 1997, n. 249 e successive modificazioni e, per gli incarichi dirigenziali, dagli articoli 19, comma 6, e 23-bis del decreto legislativo 30 marzo 2001, n. 165, tenuto conto delle specifiche esigenze funzionali e

		organizzative. Nelle more della più generale razionalizzazione del trattamento economico delle autorità amministrative indipendenti, al personale è attribuito l'ottanta per cento del trattamento economico del personale dell'Autorità per le garanzie nelle comunicazioni; e) la gestione amministrativa e la contabilità, anche in deroga alle norme sulla contabilità generale dello Stato, l'utilizzo dell'avanzo di amministrazione nel quale sono iscritte le somme già versate nella contabilità speciale, nonché l'individuazione dei casi di riscossione e utilizzazione dei diritti di segreteria o di corrispettivi per servizi resi in base a disposizioni di legge secondo le modalità di cui all'articolo 6, comma 2, della legge 31 luglio 1997, n. 249. 4. L'Ufficio può avvalersi, per motivate esigenze, di dipendenti dello Stato o di altre amministrazioni pubbliche o di enti pubblici collocati in posizione di fuori ruolo o equiparati nelle forme previste dai rispettivi ordinamenti, ovvero in aspettativa ai sensi dell'articolo 13 del decreto del Presidente della Repubblica 11 luglio 1980, n. 382, e successive modificazioni, in numero non superiore, complessivamente, a venti unità e per non oltre il venti per cento delle qualifiche dirigenziali, lasciando non coperto un corrispondente numero di posti di ruolo. Al personale di cui al presente comma è corrisposta un'indennità pari all'eventuale differenza tra il trattamento erogato

dall'amministrazione o dall'ente di provenienza e quello spettante al personale di ruolo, sulla base di apposita tabella di corrispondenza adottata dal Garante, e comunque non inferiore al cinquanta per cento della retribuzione in godimento, con esclusione dell'indennità integrativa speciale.

5. In aggiunta al personale di ruolo, l'Ufficio può assumere direttamente dipendenti con contratto a tempo determinato, in numero non superiore a venti unità ivi compresi i consulenti assunti con contratto a tempo determinato ai sensi del comma.

6. Si applicano le disposizioni di cui all'articolo 30 del decreto legislativo n. 165 del 2001.

7. Nei casi in cui la natura tecnica o la delicatezza dei problemi lo richiedono, il Garante può avvalersi dell'opera di consulenti, i quali sono remunerati in base alle vigenti tariffe professionali ovvero sono assunti con contratti a tempo determinato, di durata non superiore a due anni, che possono essere rinnovati per non più di due volte.

8. Il personale addetto all'Ufficio del Garante ed i consulenti sono tenuti al segreto su ciò di cui sono venuti a conoscenza, nell'esercizio delle proprie funzioni, in ordine a notizie che devono rimanere segrete.

9. Il personale dell'Ufficio del Garante addetto agli accertamenti di cui all'articolo 158 riveste, in numero non superiore a cinque unità, nei limiti del servizio cui è destinato e secondo le rispettive attribuzioni, la qualifica di ufficiale o

		agente di polizia giudiziaria. 10. Le spese di funzionamento del Garante sono poste a carico di un fondo stanziato a tale scopo nel bilancio dello Stato e iscritto in apposito capitolo dello stato di previsione del Ministero dell'economia e delle finanze. Il rendiconto della gestione finanziaria è soggetto al controllo della Corte dei conti.
Articolo 43 **Condizioni generali per i membri dell'autorità di controllo** 1. Gli Stati membri dispongono che ciascun membro delle rispettive autorità di controllo sia nominato attraverso una procedura trasparente: — dal rispettivo parlamento; — dal rispettivo governo; — dal rispettivo capo di Stato; o — da un organismo indipendente incaricato della nomina ai sensi del diritto dello Stato membro. 2. Ogni membro possiede le qualifiche, l'esperienza e le competenze, in particolare nel settore della protezione dei dati personali, richieste per l'esercizio delle sue funzioni e dei suoi poteri.		Non si è resa necessaria una specifica norma di recepimento, in quanto la normativa interna già soddisfa le indicazioni della direttiva: si rinvia agli articoli 153, 155 e 156 D.Lgs. 30 giugno 2003, n. 196 (Codice in materia di protezione dei dati personali).

3. Il mandato dei membri cessa alla scadenza del termine o in caso di dimissioni o di provvedimento d'ufficio, a norma del diritto dello Stato membro interessato. 4. Un membro è rimosso solo in casi di colpa grave o se non soddisfa più le condizioni richieste per l'esercizio delle sue funzioni.		
Articolo 44 **Norme sull'istituzione dell'autorità di controllo** 1. Ogni Stato membro prevede con legge tutte le condizioni seguenti: a)l'istituzione di ciascuna autorità di controllo; b)le qualifiche e le condizioni di idoneità richieste per essere nominato membro di ciascuna autorità di controllo; c)le norme e le procedure per la nomina del membro o dei membri di ciascuna autorità di controllo; d)la durata del mandato del membro o dei membri di ciascuna autorità di controllo non inferiore a quattro anni, salvo per le prime nomine dopo il 6 maggio 2016, alcune delle quali possono avere una durata inferiore qualora ciò sia necessario per tutelare		Non si è resa necessaria una specifica norma di recepimento, in quanto la normativa interna già soddisfa le indicazioni della direttiva: si rinvia agli articoli 153, 155 e 156 D.Lgs. 30 giugno 2003, n. 196 (Codice in materia di protezione dei dati personali).

l'indipendenza dell'autorità di controllo mediante una procedura di nomina scaglionata; e)l'eventuale rinnovabilità e, in caso positivo, il numero di rinnovi del mandato del membro o dei membri di ciascuna autorità di controllo; f)le condizioni che disciplinano gli obblighi del membro o dei membri e del personale di ciascuna autorità di controllo, i divieti relativi ad attività, professioni e benefici incompatibili con tali obblighi durante e dopo il mandato e le regole che disciplinano la cessazione del rapporto di lavoro. 2. Il membro o i membri e il personale di ogni autorità di controllo sono tenuti, in virtù del diritto dell'Unione o degli Stati membri, al segreto professionale in merito alle informazioni riservate cui hanno avuto accesso nell'esecuzione dei loro compiti o nell'esercizio dei loro poteri, sia durante che dopo il mandato. Per tutta la durata del loro mandato, tale obbligo del segreto professionale si applica in particolare alle segnalazioni da parte di persone fisiche di violazioni della presente direttiva.		
Sezione 2 **Competenza, compiti e poteri**	ART. 37 (*Autorità di controllo*) 1. [...]	L'articolo 37 recepisce integralmente le disposizioni di cui agli articoli da 45 a 49 della direttiva, riproducendone i contenuti non previsti nell'ordinamento interno e, per il resto,

Articolo 45 **Competenza** 1. Ogni Stato membro dispone che ciascuna autorità di controllo sia competente a eseguire i compiti assegnati e a esercitare i poteri a essa conferiti, ai sensi della presente direttiva nel territorio del rispettivo Stato membro. 2. Ogni Stato membro dispone che ciascuna autorità di controllo non sia preposta a controllare i trattamenti effettuati dalle autorità giurisdizionali nell'esercizio delle loro funzioni giurisdizionali. Gli Stati membri possono disporre che le rispettive autorità di controllo non siano competenti per il controllo dei trattamenti effettuati da altre autorità giurisdizionali indipendenti nell'esercizio delle loro funzioni giurisdizionali.	2. Ai fini di cui al comma 1 sono attribuiti al Garante le funzioni di cui all'articolo 154 del Codice, nonché le seguenti: a) promozione di una diffusa conoscenza e della consapevolezza circa i rischi, le norme, le garanzie e i diritti in relazione al trattamento; b) promozione della consapevolezza in capo ai titolari e responsabili del trattamento dell'importanza degli obblighi previsti dal presente decreto; c) espressione di pareri nei casi previsti dalla legge; d) rilascio, su richiesta dell'interessato, di informazioni in merito all'esercizio dei diritti previsti dal presente decreto e, se del caso, cooperazione, a tal fine, con le autorità di controllo di altri Stati membri; e) trattazione dei reclami proposti da un interessato, da un organismo, un'organizzazione o un'associazione ai sensi dell'articolo 40 e compimento delle indagini sull'oggetto del reclamo, informando il reclamante dello stato e dell'esito delle indagini entro un termine ragionevole, in particolare ove siano necessarie ulteriori indagini o un coordinamento con un'altra autorità di controllo; f) supporto agli interessati nella proposizione dei reclami; g) accertamento della liceità del trattamento ai sensi dell'articolo 13 e informazione all'interessato entro un termine ragionevole dell'esito della verifica ai sensi del comma 3 di detto articolo, o dei motivi per cui non è stata	facendo rinvio all'art. 154 del Codice della privacy, che già attribuisce al Garante i rimanenti compiti e poteri previsti dalla direttiva. Si trascrive di seguito il testo della norma richiamata. **D.Lgs. 30 giugno 2003, n. 196 (Codice in materia di protezione dei dati personali),** Art. 154 (*Compiti*) 1. Oltre a quanto previsto da specifiche disposizioni, il Garante, anche avvalendosi dell'Ufficio e in conformità al presente codice, ha il compito di: a) controllare se i trattamenti sono effettuati nel rispetto della disciplina applicabile e in conformità alla notificazione, anche in caso di loro cessazione e con riferimento alla conservazione dei dati di traffico; b) esaminare i reclami e le segnalazioni e provvedere sui ricorsi presentati dagli interessati o dalle associazioni che li rappresentano; c) prescrivere anche d'ufficio ai titolari del trattamento le misure necessarie o opportune al fine di rendere il trattamento conforme alle disposizioni vigenti, ai sensi dell'articolo 143; (d) vietare anche d'ufficio, in tutto o in parte, il trattamento illecito o non corretto dei dati o disporne il blocco ai sensi dell'articolo 143, e di adottare gli altri provvedimenti previsti dalla disciplina applicabile al trattamento dei dati personali;

	effettuata; h) collaborazione, anche tramite scambi di informazioni, con le altre autorità di controllo e attività di assistenza reciproca, al fine di garantire l'applicazione e l'attuazione del presente decreto; i) verifica degli sviluppi tecnologici e sociali che presentano un interesse, se ed in quanto incidenti sulla protezione dei dati personali, in particolare l'evoluzione delle tecnologie dell'informazione e della comunicazione; l) prestazione di consulenza in merito ai trattamenti di cui all'articolo 24; m) contribuzione alle attività del comitato di cui all'art. 68 del Regolamento; 3. Ai fini di cui al comma 1 sono attribuiti al Garante i seguenti poteri: a) svolgere indagini sull'applicazione del presente decreto, anche sulla base di informazioni ricevute da un'altra autorità di controllo o da un'altra autorità pubblica. Lo svolgimento delle indagini è disciplinato dalle disposizioni del Codice; b) ottenere, dal titolare del trattamento e dal responsabile del trattamento, l'accesso a tutti i dati personali oggetto del trattamento e a tutte le informazioni necessarie per l'adempimento dei suoi compiti; c) rivolgere avvertimenti al titolare del trattamento o al responsabile del trattamento in ordine alle possibili violazioni delle norme del presente decreto; d) ingiungere al titolare del trattamento o al responsabile del trattamento di conformare i	e) promuovere la sottoscrizione di codici ai sensi dell'articolo 12 e dell'articolo 139; f) segnalare al Parlamento e al Governo l'opportunità di interventi normativi richiesti dalla necessità di tutelare i diritti di cui all'articolo 2 anche a seguito dell'evoluzione del settore; g) esprimere pareri nei casi previsti; h) curare la conoscenza tra il pubblico della disciplina rilevante in materia di trattamento dei dati personali e delle relative finalità, nonché delle misure di sicurezza dei dati; i) denunciare i fatti configurabili come reati perseguibili d'ufficio, dei quali viene a conoscenza nell'esercizio o a causa delle funzioni; l) tenere il registro dei trattamenti formato sulla base delle notificazioni di cui all'articolo 37; m) predisporre annualmente una relazione sull'attività svolta e sullo stato di attuazione del presente codice, che è trasmessa al Parlamento e al Governo entro il 30 aprile dell'anno successivo a quello cui si riferisce. 2. Il Garante svolge altresì, ai sensi del comma 1, la funzione di controllo o assistenza in materia di trattamento dei dati personali prevista da leggi di ratifica di accordi o convenzioni internazionali o da regolamenti comunitari e, in particolare: a) dalla legge 30 settembre 1993, n. 388, e successive modificazioni, di ratifica ed esecuzione dei protocolli e degli accordi di adesione all'accordo di Schengen e alla relativa

	trattamenti alle disposizioni del presente decreto, se del caso, con specifiche modalità ed entro un determinato termine, ordinando in particolare la rettifica o la cancellazione di dati personali o la limitazione del trattamento ai sensi dell'articolo 12; e) imporre un limitazione provvisoria o definitiva al trattamento, incluso il divieto e il blocco dello stesso; f) promuovere la segnalazione riservata di violazioni del presente decreto; g) denunciare i reati dei quali viene a conoscenza nell'esercizio o a causa delle funzioni; h) predisporre annualmente una relazione sull'attività svolta, da trasmettere al Parlamento e al Governo, anche ai sensi dell'articolo 154, comma 1, lettera m), del Codice e da mettere a disposizione del pubblico, della Commissione e del comitato, in cui può figurare un elenco delle tipologie di violazioni notificate e di sanzioni imposte. 4. I poteri di cui al comma 3 sono esercitati nei modi, nelle forme e con le garanzie previste dalla legge. 5. Le funzioni e i poteri di cui ai commi 2 e 3 sono esercitati senza spese per l'interessato o per il responsabile della protezione dati. Il Garante non provvede in ordine alle richieste manifestamente infondate o inammissibili in quanto ripropongono, senza nuovi elementi, richieste già rigettate. 6. Il Garante non è competente in ordine al controllo del rispetto delle norme del presente	convenzione di applicazione; b) dalla legge 23 marzo 1998, n. 93, e successive modificazioni, di ratifica ed esecuzione della convenzione istitutiva dell'Ufficio europeo di polizia (Europol); c) dal regolamento (Ce) n. 515/97 del Consiglio, del 13 marzo 1997, e dalla legge 30 luglio 1998, n. 291, e successive modificazioni, di ratifica ed esecuzione della convenzione sull'uso dell'informatica nel settore doganale; d) dal regolamento (Ce) n. 2725/2000 del Consiglio, dell'11 dicembre 2000, che istituisce l'"Eurodac" per il confronto delle impronte digitali e per l'efficace applicazione della convenzione di Dublino; e) nel capitolo IV della convenzione n. 108 sulla protezione delle persone rispetto al trattamento automatizzato di dati di carattere personale, adottata a Strasburgo il 28 gennaio 1981 e resa esecutiva con legge 21 febbraio 1989, n. 98, quale autorità designata ai fini della cooperazione tra Stati ai sensi dell'articolo 13 della convenzione medesima. 3. Il Garante coopera con altre autorità amministrative indipendenti nello svolgimento dei rispettivi compiti. A tale fine, il Garante può anche invitare rappresentanti di un'altra autorità a partecipare alle proprie riunioni, o essere invitato alle riunioni di altra autorità, prendendo parte alla discussione di argomenti di comune interesse; può richiedere, altresì, la collaborazione di personale specializzato addetto ad altra autorità.

	decreto, limitatamente ai trattamenti effettuati dall'autorità giudiziaria nell'esercizio delle funzioni giurisdizionali, nonché di quelle giudiziarie del pubblico ministero.	4. Il Presidente del Consiglio dei ministri e ciascun ministro consultano il Garante all'atto della predisposizione delle norme regolamentari e degli atti amministrativi suscettibili di incidere sulle materie disciplinate dal presente codice. 5. Fatti salvi i termini più brevi previsti per legge, il parere del Garante è reso nei casi previsti nel termine di quarantacinque giorni dal ricevimento della richiesta. Decorso il termine, l'amministrazione può procedere indipendentemente dall'acquisizione del parere. Quando, per esigenze istruttorie, non può essere rispettato il termine di cui al presente comma, tale termine può essere interrotto per una sola volta e il parere deve essere reso definitivamente entro venti giorni dal ricevimento degli elementi istruttori da parte delle amministrazioni interessate. 6. Copia dei provvedimenti emessi dall'autorità giudiziaria in relazione a quanto previsto dal presente codice o in materia di criminalità informatica è trasmessa, a cura della cancelleria, al Garante.
Articolo 46 **Compiti** 1. Ogni Stato membro dispone che sul proprio territorio ciascuna autorità di controllo: a)sorvegli e assicuri l'applicazione delle disposizioni adottate a norma della presente direttiva e delle relative misure di esecuzione;	V. art. 37.	Si rinvia a quanto esposto *sub* art. 37 dello schema di decreto.

b)promuova la sensibilizzazione e favorisca la comprensione del pubblico riguardo ai rischi, alle norme, alle garanzie e ai diritti in relazione al trattamento;		
c)fornisca consulenza, a norma del diritto dello Stato membro, al parlamento nazionale, al governo e ad altri organismi e istituzioni in merito alle misure legislative e amministrative relative alla tutela dei diritti e delle libertà delle persone fisiche con riguardo al trattamento;		
d)promuova la consapevolezza dei titolari del trattamento e dei responsabili del trattamento degli obblighi imposti loro dalla presente direttiva;		
e)su richiesta, fornisca informazioni all'interessato in merito all'esercizio dei propri diritti derivanti dalla presente direttiva e, se del caso, cooperi a tal fine con le autorità di controllo di altri Stati membri;		
f)tratti i reclami proposti da un interessato, o da un organismo, un'organizzazione o un'associazione ai sensi dell'articolo 55, e svolga le indagini opportune sull'oggetto del reclamo e informi il reclamante dello stato e dell'esito delle indagini entro un termine ragionevole, in particolare ove siano		

necessarie ulteriori indagini o un coordinamento con un'altra autorità di controllo; g)verifichi la liceità del trattamento ai sensi dell'articolo 17 e informi l'interessato entro un termine ragionevole dell'esito della verifica ai sensi del paragrafo 3 di tale articolo, o dei motivi per cui non è stata effettuata; h)collabori, anche tramite scambi di informazioni, con le altre autorità di controllo e presti assistenza reciproca al fine di garantire l'applicazione e l'attuazione coerente della presente direttiva; i)svolga indagini sull'applicazione della presente direttiva, anche sulla base di informazioni ricevute da un'altra autorità di controllo o da un'altra autorità pubblica; j)sorvegli gli sviluppi che presentano un interesse, se ed in quanto incidenti sulla protezione dei dati personali, in particolare l'evoluzione delle tecnologie dell'informazione e della comunicazione; k)fornisca consulenza in merito ai trattamenti di cui all'articolo 28; e		

l) contribuisca alle attività del comitato. 2. Ogni autorità di controllo agevola la proposizione di reclami di cui al paragrafo 1, lettera f), tramite provvedimenti quali, ad esempio, la messa a disposizione di un modulo per la proposizione dei reclami compilabile anche elettronicamente, senza escludere altri mezzi di comunicazione. 3. Ogni autorità di controllo svolge i propri compiti senza spese né per l'interessato né per il titolare della protezione dei dati. 4. Qualora una richiesta sia manifestamente infondata o eccessiva, in particolare in quanto ripetitiva, l'autorità di controllo può addebitare un contributo spese ragionevole basato sui propri costi amministrativi o può rifiutare di soddisfare la richiesta. Incombe all'autorità di controllo dimostrare che la richiesta è manifestamente infondata o eccessiva.		
Articolo 47 **Poteri** 1. Ogni Stato membro dispone per legge che ciascuna autorità di controllo abbia poteri d'indagine effettivi. Tali poteri comprendono almeno il potere di ottenere, dal titolare del trattamento e dal responsabile del trattamento, l'accesso a tutti i dati personali oggetto del trattamento e a tutte le informazioni necessarie per l'adempimento dei suoi compiti.	V. art. 37	Si rinvia a quanto esposto *sub* art. 37 dello schema di decreto.

2. Ogni Stato membro dispone per legge che ciascuna autorità di controllo abbia poteri correttivi effettivi, come ad esempio: a)rivolgere avvertimenti al titolare del trattamento o al responsabile del trattamento sul fatto che i trattamenti previsti possono verosimilmente violare le disposizioni adottate a norma della presente direttiva; b)ingiungere al titolare del trattamento o al responsabile del trattamento di conformare i trattamenti alle disposizioni adottate a norma della presente direttiva, se del caso, in una determinata maniera ed entro un determinato termine, ordinando in particolare la rettifica o la cancellazione di dati personali o la limitazione del trattamento ai sensi dell'articolo 16; c)imporre un limitazione provvisoria o definitiva al trattamento, incluso il divieto di trattamento. 3. Ogni Stato membro dispone per legge che ciascuna autorità di controllo abbia poteri consultivi effettivi per fornire consulenza al titolare del trattamento, secondo la procedura di consultazione preventiva di cui all'articolo 28, e per formulare, di propria iniziativa o su richiesta, pareri destinati al proprio parlamento nazionale e al proprio governo dello Stato membro, oppure, conformemente al proprio diritto nazionale, ad altri istituzioni e		

organismi nonché al pubblico su questioni riguardanti la protezione dei dati personali. 4. L'esercizio da parte di un'autorità di controllo dei poteri attribuitile dal presente articolo è soggetto a garanzie adeguate, inclusi il ricorso giurisdizionale effettivo e il giusto processo, previste dal diritto dell'Unione e dello Stato membro conformemente alla Carta. 5. Ogni Stato membro dispone per legge che ciascuna autorità di controllo abbia il potere di sottoporre all'attenzione di autorità giudiziarie violazioni delle disposizioni adottate a norma della presente direttiva e, se del caso, di intentare un'azione o di agire in sede giudiziale, per far rispettare le disposizioni adottate a norma della presente direttiva.		
Articolo 48 **Segnalazione di violazioni** Gli Stati membri dispongono che le autorità competenti pongano in essere meccanismi efficaci per incoraggiare la segnalazione riservata di violazioni della presente direttiva.	V. art. 37 comma 3 lett. f)	Si rinvia a quanto esposto *sub* art. 37 dello schema di decreto.
Articolo 49 **Relazioni di attività** Ogni autorità di controllo elabora una relazione annuale sulla propria attività, in cui può figurare un elenco delle tipologie di	V. art. 37 comma 3 lett. h)	Si rinvia a quanto esposto *sub* art. 37 dello schema di decreto.

violazioni notificate e di sanzioni imposte. Tali relazioni sono trasmesse al parlamento nazionale, al governo e alle altre autorità designate dal diritto dello Stato membro. Esse sono messe a disposizione del pubblico, della Commissione e del comitato.		
CAPO VII *Cooperazione* *Articolo 50* Assistenza reciproca 1. Ogni Stato membro dispone che le rispettive autorità di controllo si scambino le informazioni utili e si prestino assistenza reciproca al fine di attuare e applicare la presente direttiva in maniera coerente, e mettano in atto misure per cooperare efficacemente tra loro. L'assistenza reciproca comprende, in particolare, le richieste di informazioni e le misure di controllo, quali le richieste di effettuare consultazioni, ispezioni e indagini. 2. Ogni Stato membro dispone che ciascuna autorità di controllo adotti tutte le misure opportune necessarie per dare seguito a una richiesta di un'altra autorità di controllo senza ingiustificato ritardo e comunque entro un mese dal ricevimento della richiesta. Tali misure possono consistere, in particolare, nella trasmissione di informazioni utili sullo	ART. 38 (*Assistenza reciproca*) 1. Il Garante scambia con le autorità di controllo degli altri Stati membri le informazioni utili e presta assistenza reciproca al fine di attuare e applicare il presente decreto in maniera coerente, e di cooperare efficacemente con loro. L'assistenza reciproca comprende le richieste di informazioni e le misure di controllo, quali le richieste di effettuare consultazioni, ispezioni e indagini. 2. Il Garante adotta, con proprio provvedimento, le misure di cui all'articolo 61, paragrafo 2, del regolamento. 3. Le richieste di assistenza sono conformi alle modalità di cui all'articolo 61, paragrafo 3, del Regolamento. 4. Il Garante non può rifiutare di dare seguito alla richiesta, salvo che sia incompetente o l'intervento richiesto violi il diritto interno o dell'Unione europea. 5. Il Garante osserva le disposizioni di cui all'articolo 61, paragrafi 5, 6 e 7, del regolamento.	La disposizione della direttiva è stata recepita dallo schema di decreto, anche mediante il rinvio alle disposizioni del Regolamento (UE) 216/679 di contenuto equivalente.

svolgimento di un'indagine. 3. Le richieste di assistenza contengono tutte le informazioni necessarie, compresi lo scopo e i motivi della richiesta. Le informazioni scambiate sono utilizzate ai soli fini per cui sono state richieste. 4. L'autorità di controllo cui è presentata la richiesta non deve rifiutare di darvi seguito, salvo che: a)non sia competente per trattare l'oggetto della richiesta o per le misure cui deve dare esecuzione; o b)l'intervento richiesto violerebbe la presente direttiva o il diritto dell'Unione o dello Stato membro cui è soggetta l'autorità di controllo che riceve la richiesta. 5. L'autorità di controllo che riceve la richiesta informa l'autorità di controllo richiedente dell'esito o, se del caso, dei progressi delle misure adottate per rispondere alla richiesta. L'autorità di controllo che riceve la richiesta fornisce le motivazioni del rifiuto di darvi seguito ai sensi del paragrafo 4. 6. Di norma, le autorità di controllo che ricevono le richieste forniscono, con mezzi elettronici, usando un modulo standard, le informazioni richieste da altre autorità di controllo. 7. Le autorità di controllo che ricevono le richieste non addebitano un contributo spese		

per le misure da loro adottate a seguito di una richiesta di assistenza reciproca. Le autorità di controllo possono concordare di concedersi gli indennizzi per spese specifiche risultanti dalla prestazione di assistenza reciproca in circostanze eccezionali. 8. La Commissione può, mediante atti di esecuzione, specificare il formato e le procedure per l'assistenza reciproca di cui al presente articolo e le modalità per lo scambio di informazioni con mezzi elettronici tra autorità di controllo e tra le autorità di controllo e il comitato. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 58, paragrafo 2.		
Articolo 51 **Compiti del comitato** 1. Il comitato istituito dal regolamento (UE) 2016/679 adempie tutti i seguenti compiti in relazione ai trattamenti rientranti nell'ambito di applicazione della presente direttiva: a) consiglia la Commissione in merito a qualsiasi questione relativa alla protezione dei dati personali nell'Unione, comprese eventuali proposte di modifica della presente direttiva; b) esamina, di propria iniziativa, su richiesta di uno dei suoi membri o della Commissione, qualsiasi questione relativa all'applicazione		Non è necessaria alcuna norma di attuazione, considerata la diretta applicabilità del Regolamento (UE) 216/679.

della presente direttiva e pubblica linee guida, raccomandazioni e migliori prassi al fine di promuovere l'applicazione coerente della presente direttiva; c)elabora linee guida per le autorità di controllo concernenti l'applicazione delle misure di cui all'articolo 47, paragrafi 1 e 3; d)pubblica linee guida, raccomandazioni e migliori prassi conformemente alla lettera b) del presente comma, per accertare la violazione di dati personali e determinare l'ingiustificato ritardo di cui all'articolo 30, paragrafi 1 e 2, e le circostanze particolari in cui il titolare del trattamento o il responsabile del trattamento è tenuto a notificare la violazione dei dati personali; e)pubblica linee guida, raccomandazioni e migliori prassi conformemente alla lettera b) del presente comma relative alle circostanze in cui una violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche di cui all'articolo 31, paragrafo 1; f)valuta l'applicazione pratica delle linee guida, raccomandazioni e migliori prassi di cui alle lettere b) e c); g)trasmette alla Commissione un parere per		

valutare l'adeguatezza del livello di protezione in un paese terzo, un territorio o uno o più settori specifici all'interno di un paese terzo o in un'organizzazione internazionale, come pure per valutare se tale paese terzo, territorio, settore specifico o organizzazione internazionale non garantiscano più un livello adeguato di protezione; h)promuove la cooperazione e l'effettivo scambio di informazioni e migliori prassi tra le autorità di controllo a livello bilaterale e multilaterale; i)promuove programmi comuni di formazione e facilita lo scambio di personale tra le autorità di controllo e, se del caso, con le autorità di controllo di paesi terzi o con organizzazioni internazionali; j)promuove lo scambio di conoscenze e documentazione sul diritto e sulle prassi in materia di protezione dei dati tra autorità di controllo di tutto il mondo. Con riguardo alla lettera g), primo comma, la Commissione fornisce al comitato tutta la documentazione necessaria, inclusa la corrispondenza con il governo del paese terzo, con il territorio o il settore specifico all'interno di tale paese terzo o con l'organizzazione internazionale.		

2. Qualora chieda consulenza al comitato, la Commissione può indicare un termine, tenuto conto dell'urgenza della questione. 3. Il comitato trasmette pareri, linee guida, raccomandazioni e migliori prassi alla Commissione e al comitato di cui all'articolo 58, paragrafo 1, e li pubblica. 4. La Commissione informa il comitato del seguito dato ai suoi pareri, linee guida, raccomandazioni e migliori prassi.		
CAPO VIII ***Ricorsi, responsabilità e sanzioni*** *Articolo 52* **Diritto di proporre reclamo all'autorità di controllo** 1. Gli Stati membri dispongono che, fatto salvo ogni altro ricorso amministrativo o giurisdizionale, l'interessato che ritenga che il trattamento dei dati personali che lo riguardano violi le disposizioni adottate a norma della presente direttiva abbia il diritto di proporre reclamo a un'unica autorità di controllo. 2. Gli Stati membri dispongono che l'autorità di controllo a cui è stato proposto il reclamo lo trasmetta senza ingiustificato ritardo all'autorità di controllo competente qualora il reclamo non sia proposto a quest'ultima ai	ART. 39 (*Reclamo al Garante e ricorso giurisdizionale*) 1. Fermo quanto previsto dall'articolo 37, comma 6, l'interessato, se ritiene che il trattamento dei dati personali che lo riguardano violi le disposizioni del presente decreto, può proporre reclamo al Garante, con le modalità di cui agli articoli 142 e 143 del Codice. 2. Il Garante informa l'interessato dello stato o dell'esito del reclamo, compresa la possibilità del ricorso giurisdizionale. 3. [...]	La disposizione della direttiva è stata recepita dallo schema di decreto, anche mediante il rinvio alle disposizioni del Codice della privacy. Si trascrivono di seguito le norme richiamate, che disciplinano il reclamo con modalità satisfattive delle indicazioni della direttiva. **D.Lgs. 30 giugno 2003, n. 196 (Codice in materia di protezione dei dati personali).** Art. 142 (*Proposizione dei reclami*) 1. Il reclamo contiene un'indicazione per quanto possibile dettagliata dei fatti e delle circostanze su cui si fonda, delle disposizioni che si presumono violate e delle misure richieste, nonché gli estremi identificativi del titolare, del responsabile, ove conosciuto, e dell'istante. 2. Il reclamo è sottoscritto dagli interessati, o da associazioni che li rappresentano anche ai

sensi dell'articolo 45, paragrafo 1. L'interessato è informato della trasmissione. 3. Gli Stati membri dispongono che l'autorità di controllo a cui sia stato proposto il reclamo fornisca ulteriore assistenza su richiesta dell'interessato. 4. L'autorità di controllo competente informa l'interessato dello stato o dell'esito del reclamo, compresa la possibilità di un ricorso giurisdizionale ai sensi dell'articolo 53.		sensi dell'articolo 9, comma 2, ed è presentato al Garante senza particolari formalità. Il reclamo reca in allegato la documentazione utile ai fini della sua valutazione e l'eventuale procura, e indica un recapito per l'invio di comunicazioni anche tramite posta elettronica, telefax o telefono. 3. Il Garante può predisporre un modello per il reclamo da pubblicare nel Bollettino e di cui favorisce la disponibilità con strumenti elettronici. Art. 143 (*Procedimento per i reclami*) 1. Esaurita l'istruttoria preliminare, se il reclamo non è manifestamente infondato e sussistono i presupposti per adottare un provvedimento, il Garante, anche prima della definizione del procedimento: a) prima di prescrivere le misure di cui alla lettera b), ovvero il divieto o il blocco ai sensi della lettera c), può invitare il titolare, anche in contraddittorio con l'interessato, ad effettuare il blocco spontaneamente; b) prescrive al titolare le misure opportune o necessarie per rendere il trattamento conforme alle disposizioni vigenti; c) dispone il blocco o vieta, in tutto o in parte, il trattamento che risulta illecito o non corretto anche per effetto della mancata adozione delle misure necessarie di cui alla lettera b), oppure quando, in considerazione della natura dei dati o, comunque, delle modalità del trattamento o degli effetti che esso può determinare, vi è il concreto rischio del verificarsi di un

		pregiudizio rilevante per uno o più interessati; d) può vietare in tutto o in parte il trattamento di dati relativi a singoli soggetti o a categorie di soggetti che si pone in contrasto con rilevanti interessi della collettività. 2. I provvedimenti di cui al comma 1 sono pubblicati nella Gazzetta Ufficiale della Repubblica italiana se i relativi destinatari non sono facilmente identificabili per il numero o per la complessità degli accertamenti.
Articolo 53 **Diritto a un ricorso giurisdizionale effettivo nei confronti dell'autorità di controllo** 1. Fatto salvo ogni altro ricorso amministrativo o extragiudiziale, gli Stati membri prevedono il diritto di una persona fisica o giuridica a un ricorso giurisdizionale effettivo avverso una decisione giuridicamente vincolante dell'autorità di controllo che la riguarda. 2. Fatto salvo ogni altro ricorso amministrativo o extragiudiziale, ciascun interessato ha il diritto di proporre un ricorso giurisdizionale effettivo qualora l'autorità di controllo che sia competente ai sensi dell'articolo 45, paragrafo 1, non tratti un reclamo o non lo informi entro tre mesi dello stato o dell'esito del reclamo proposto ai sensi dell'articolo 52. 3. Gli Stati membri dispongono che le azioni nei confronti dell'autorità di controllo siano	ART. 39 (*Reclamo al Garante e ricorso giurisdizionale*) 1. [...] 2. Il Garante informa l'interessato dello stato o dell'esito del reclamo, compresa la possibilità del ricorso giurisdizionale. [...]	Non è necessario recepire espressamente le norme sul diritto dell'interessato al ricorso giurisdizionale avverso la decisione dell'autorità di controllo, in quanto già assicurato dall'ordinamento interno. Si trascrive, di seguito, la disposizione del Codice della privacy sul punto. **D.Lgs. 30 giugno 2003, n. 196 (Codice in materia di protezione dei dati personali).** Art. 152 (*Autorità giudiziaria ordinaria*) 1. Tutte le controversie che riguardano, comunque, l'applicazione delle disposizioni del presente codice, comprese quelle inerenti ai provvedimenti del Garante in materia di protezione dei dati personali o alla loro mancata adozione, nonché le controversie previste dall'articolo 10, comma 5, della legge 1° aprile 1981, n. 121, e successive modificazioni, sono attribuite all'autorità giudiziaria ordinaria. 1-bis. Le controversie di cui al comma 1 sono disciplinate dall'articolo 10 del decreto

promosse dinanzi alle autorità giurisdizionali dello Stato membro in cui l'autorità di controllo è stabilita		legislativo 1° settembre 2011, n. 150.
Articolo 54 **Diritto a un ricorso giurisdizionale effettivo nei confronti del titolare del trattamento o del responsabile del trattamento** Gli Stati membri dispongono che, fatto salvo ogni altro ricorso amministrativo o extragiudiziale disponibile, compreso il diritto di proporre reclamo a un'autorità di controllo ai sensi dell'articolo 52, l'interessato abbia il diritto a un ricorso giurisdizionale effettivo qualora ritenga che i diritti di cui gode ai sensi delle disposizioni adottate a norma della presente direttiva siano stati violati a seguito del trattamento dei propri dati personali in violazione di tali disposizioni.	ART. 39 (*Reclamo al Garante e ricorso giurisdizionale*) 1. [...] 2. [...] 3. Per l'inosservanza delle disposizioni del presente decreto in violazione dei suoi diritti, l'interessato può proporre ricorso giurisdizionale secondo quanto previsto e regolato dalla disciplina contenuta nella parte terza, titolo primo, capo secondo del Codice.	La disposizione della direttiva è stata recepita integralmente dallo schema di decreto.
Articolo 55 **Rappresentanza degli interessati** Gli Stati membri dispongono che, conformemente al diritto processuale dello Stato membro, l'interessato abbia il diritto di dare mandato a un organismo, un'organizzazione o un'associazione senza scopo di lucro, che siano debitamente costituiti secondo il diritto dello Stato membro, abbiano obiettivi statutari che siano di pubblico	ART. 40 (*Rappresentanza degli interessati*) 1. L'interessato può dare mandato a un ente del terzo settore soggetto alla disciplina del decreto legislativo 3 luglio 2017, n. 117, che sia attivo nel settore della tutela dei diritti e delle libertà degli interessati con riguardo alla protezione dei dati personali, al fine di esercitare per suo conto i diritti di cui all'articolo 39, ferme le disposizioni in materia	La disposizione della direttiva è stata recepita integralmente dallo schema di decreto.

interesse e siano attivi nel settore della tutela dei diritti e delle libertà degli interessati con riguardo alla protezione dei dati personali, di proporre il reclamo per suo conto e di esercitare per suo conto i diritti di cui agli articoli 52, 53 e 54.	di patrocinio previste dal codice di procedura civile.	
Articolo 56 **Diritto al risarcimento** Gli Stati membri dispongono che chiunque subisca un danno materiale o immateriale cagionato da un trattamento illecito o da qualsiasi altro atto che violi le disposizioni adottate a norma della presente direttiva abbia il diritto di ottenere il risarcimento del danno dal titolare del trattamento o da altra autorità competente in base al diritto dello Stato membro.	ART. 41 (*Diritto al risarcimento*) 1.Il titolare o il responsabile del trattamento sono tenuti, a norma dell'articolo 82 del regolamento, al risarcimento del danno patrimoniale o non patrimoniale cagionato da un trattamento o da qualsiasi altro atto compiuti in violazione delle disposizioni del presente decreto.	La disposizione della direttiva è stata recepita integralmente dallo schema di decreto, anche mediante rinvio al Regolamento (UE) 2016/679.
Articolo 57 **Sanzioni** Gli Stati membri stabiliscono le norme relative alle sanzioni applicabili in caso di violazione delle disposizioni adottate a norma della presente direttiva e adottano tutti i provvedimenti necessari per assicurarne l'applicazione. Le sanzioni previste devono essere effettive, proporzionate e dissuasive.	ART. 42 (*Sanzioni amministrative*) 1. Salvo che il fatto costituisca reato e ad esclusione dei trattamenti svolti in ambito giudiziario, la violazione delle disposizioni di cui all'articolo 3, comma 1, lettere a),b), d), e) ed f), all'articolo 4, commi 2 e 3, all'articolo 6, commi 3 e 4, all'articolo 7, all'articolo 8, è punita con la sanzione amministrativa del pagamento di una somma da 50.000 euro a 150.000 euro. La medesima sanzione	La direttiva rimette agli Stati membri la scelta delle sanzioni da applicare, purché siano effettive, proporzionate e dissuasive. Si è optato per una graduazione delle sanzioni, amministrative e penali, in relazione alla gravità e offensività delle condotte, comunque attenendosi ai limiti imposti dall'articolo 11 della legge n. 163 del 2017 e ai principi richiamati all'articolo 1 della medesima legge, che espressamente rinvia all'articolo 32 della legge quadro n. 234 del 2012.

amministrativa si applica al trasferimento dei dati personali verso un Paese terzo o un'organizzazione internazionale in assenza della decisione di adeguatezza della Commissione dell'Unione europea, salvo quanto previsto dagli articoli 33 e 34.

2. Salvo che il fatto costituisca reato e ad esclusione dei trattamenti svolti in ambito giudiziario, è punita con la sanzione amministrativa del pagamento di una somma da 20.000 euro a 80.000 euro la violazione delle disposizioni di cui all'articolo 14 comma 2. Con la medesima sanzione è punita la violazione delle disposizioni di cui all'articolo 17, comma 2, all'articolo 18, commi 1, 2, 3 e 4, all'articolo 19, all'articolo 20, all'articolo 21, all'articolo 22, all'articolo 23, all'articolo 24, commi 1 e 4, all'articolo 26, all'articolo 27, all'articolo 28, commi 1 e 4, all'articolo 29, comma 2.

3. Nella determinazione della sanzione amministrativa da applicare secondo quanto previsto dai commi precedenti si tiene conto dei criteri di cui all'articolo 83, paragrafo 2, lettere a), b), c), d) e), f), g), h), i), k) del regolamento.

4. Il procedimento per l'applicazione delle sanzioni è regolato dall'articolo 166 del Codice. Si applica altresì l'articolo 165 del Codice.

CAPO VI
ILLECITI PENALI

ART. 43

(Trattamento illecito di dati)

1. Salvo che il fatto costituisca più grave reato, chiunque, al fine di trarne per sé o per altri profitto o di recare ad altri un danno, procede al trattamento di dati personali in violazione di quanto disposto dagli articoli 5, comma 1, e 8, comma 4, è punito, se dal fatto deriva nocumento, con la reclusione da sei a diciotto mesi o, se la condotta comporta comunicazione o diffusione dei dati, con la reclusione da sei a ventiquattro mesi.

2. Salvo che il fatto costituisca più grave reato, chiunque, al fine di trarne per sé o per altri profitto o di recare ad altri un danno, procede al trattamento di dati personali in violazione di quanto disposto dall'articolo 7 è punito, se dal fatto deriva nocumento, con la reclusione da uno a tre anni.

ART. 44

(Falsità nelle dichiarazioni e notificazioni al Garante)

1. Chiunque in comunicazioni, atti, documenti o dichiarazioni resi o esibiti in un procedimento dinanzi al Garante o nel corso di accertamenti, dichiara o attesta falsamente notizie o circostanze o produce atti o documenti falsi, è punito, salvo che il fatto costituisca più grave reato, con la reclusione da sei mesi a tre anni.

	ART. 45 (*Inosservanza di provvedimenti del Garante*) 1. Chiunque, essendovi tenuto, non osserva il provvedimento adottato dal Garante ai sensi dell'articolo 143, comma 1, lettera c), del Codice è punito con la reclusione da tre mesi a due anni. ART. 46 (*Pene accessorie*) 1. La condanna per uno dei delitti previsti dal presente decreto importa la pubblicazione della sentenza, ai sensi dell'articolo 36, commi 2 e 3, del codice penale.	
CAPO IX ***Atti di esecuzione*** *Articolo 58* **Procedura di comitato** 1. La Commissione è assistita dal comitato istituito dall'articolo 93 del regolamento (UE) 2016/679. Esso è un comitato ai sensi del regolamento (UE) n. 182/2011. 2. Nei casi in cui è fatto riferimento al presente paragrafo, si applica l'articolo 5 del		La disposizione non necessita di recepimento.

regolamento (UE) n. 182/2011. 3. Nei casi in cui è fatto riferimento al presente paragrafo, si applica l'articolo 8 del regolamento (UE) n. 182/2011 in combinato disposto con il suo articolo 5.		
CAPO X ***Disposizioni finali*** *Articolo 59* **Abrogazione della decisione quadro 2008/977/GAI** 1. La decisione quadro 2008/977/GAI è abrogata a decorrere dal 6 maggio 2018. 2. I riferimenti alla decisione abrogata di cui al paragrafo 1 si intendono fatti alla presente direttiva.		La disposizione non necessita di recepimento.
Articolo 60 **Atti giuridici dell'Unione già in vigore** Rimangono impregiudicate le disposizioni specifiche per la protezione dei dati personali contenute in atti giuridici dell'Unione che sono entrati in vigore il o anteriormente al 6 maggio 2016 nel settore della cooperazione giudiziaria in materia penale e della cooperazione di polizia, che disciplinano il trattamento tra Stati membri e l'accesso delle autorità nazionali		La disposizione non necessita di recepimento.

designate ai sistemi d'informazione istituiti ai sensi dei trattati, nell'ambito di applicazione della presente direttiva.		
Articolo 61 **Rapporto con gli accordi internazionali precedentemente conclusi nel settore della cooperazione giudiziaria in materia penale e della cooperazione di polizia** Restano in vigore, fino alla loro modifica, sostituzione o revoca, gli accordi internazionali relativi al trasferimento di dati personali verso paesi terzi o organizzazioni internazionali che sono stati conclusi dagli Stati membri anteriormente al 6 maggio 2016 e che sono conformi al diritto dell'Unione applicabile anteriormente a tale data.	ART. 36 *(Cooperazione internazionale per la protezione dei dati personali e accordi internazionali precedentemente conclusi)* 1. [...] 2. Restano in vigore, fino alla loro modifica, sostituzione o revoca, gli accordi internazionali relativi al trasferimento di dati personali verso Paesi terzi o organizzazioni internazionali conclusi anteriormente al 6 maggio 2016 e che sono conformi al diritto dell'Unione europea applicabile a tale data.	La disposizione della direttiva è stata integralmente recepita.
Articolo 62 **Relazioni della Commissione** 1. Entro il 6 maggio 2022 e, successivamente, ogni quattro anni, la Commissione trasmette al Parlamento europeo e al Consiglio una relazione di valutazione e sul riesame della presente direttiva. Tale relazione è pubblicata. 2. Nel contesto delle valutazioni e dei riesami di cui al paragrafo 1 la Commissione esamina, in particolare, l'applicazione e il funzionamento del capo V sul trasferimento di dati personali verso paesi terzi o		La disposizione non necessita di recepimento.

organizzazioni internazionali, con particolare riguardo alle decisioni adottate ai sensi dell'articolo 36, paragrafo 3, e dell'articolo 39. 3. Ai fini dei paragrafi 1 e 2 la Commissione può richiedere informazioni agli Stati membri e alle autorità di controllo. 4. Nello svolgere le valutazioni e i riesami di cui ai paragrafi 1 e 2, la Commissione tiene conto delle posizioni e delle conclusioni del Parlamento europeo, del Consiglio, nonché di altri organismi o fonti pertinenti. 5. Se del caso, la Commissione presenta opportune proposte di modifica della presente direttiva tenuto conto, in particolare, degli sviluppi delle tecnologie dell'informazione e dei progressi della società dell'informazione. 6. Entro il 6 maggio 2019, la Commissione riesamina gli altri atti giuridici adottati dall'Unione che disciplinano il trattamento da parte delle autorità competenti per le finalità di cui all'articolo 1, paragrafo 1, in particolare quelli di cui all'articolo 60, al fine di valutare la necessità di allinearli alla presente direttiva e formulare, ove opportuno, le proposte necessarie per modificarli in modo da garantire un approccio coerente alla protezione dei dati personali nell'ambito della presente direttiva.		
Articolo 63 **Recepimento**		I criteri di recepimento della direttiva sono stati individuati dalla legge 25 ottobre 2017, n. 163, recante delega al Governo per il

1. Gli Stati membri adottano e pubblicano, entro il 6 maggio 2018, le disposizioni legislative, regolamentari e amministrative necessarie per conformarsi alla presente direttiva. Essi comunicano immediatamente alla Commissione il testo di tali disposizioni. Essi applicano tali disposizioni a decorrere dal 6 maggio 2018. Le disposizioni adottate dagli Stati membri contengono un riferimento alla presente direttiva o sono corredate di tale riferimento all'atto della pubblicazione ufficiale. Le modalità del riferimento sono stabilite dagli Stati membri. 2. In deroga al paragrafo 1, uno Stato membro può disporre che, in via eccezionale, qualora ciò comporti sforzi sproporzionati, i sistemi di trattamento automatizzato istituiti anteriormente al 6 maggio 2016 siano resi conformi all'articolo 25, paragrafo 1, entro il 6 maggio 2023. 3. In deroga ai paragrafi 1 e 2 del presente articolo, uno Stato membro può, in circostanze eccezionali, rendere un sistema di trattamento automatizzato di cui al paragrafo 2 del presente articolo conforme all'articolo 25, paragrafo 1, entro un termine specificato dopo il termine di cui al paragrafo 2 del presente articolo, qualora ciò causi altrimenti gravi difficoltà per il funzionamento di tale particolare sistema di trattamento automatizzato. Lo Stato membro in questione comunica alla Commissione i motivi		recepimento delle direttive europee e l'attuazione di altri atti dell'Unione europea - Legge di delegazione europea 2016-2017 e, in particolare, dagli articoli 1 e 11.

di tali gravi difficoltà e i motivi del termine specificato entro il quale rende tale particolare sistema di trattamento automatizzato conforme all'articolo 25, paragrafo 1. Il termine specificato non supera in ogni caso il 6 maggio 2026. 4. Gli Stati membri comunicano alla Commissione il testo delle disposizioni fondamentali di diritto interno che adottano nel settore disciplinato dalla presente direttiva.		
Articolo 64 **Entrata in vigore** La presente direttiva entra in vigore il giorno successivo alla pubblicazione nella *Gazzetta ufficiale dell'Unione europea*.		La disposizione non necessita di recepimento.
Articolo 65 **Destinatari** Gli Stati membri sono destinatari della presente direttiva.		La disposizione non necessita di recepimento.

RELAZIONE TECNICA

Lo schema di decreto legislativo in esame è teso a recepire nell'ordinamento interno la direttiva (UE) 2016/680/UE del Parlamento europeo e del Consiglio inerente alla protezione delle persone fisiche da parte delle autorità competenti, per quanto riguarda il trattamento dei dati personali ai fini di prevenzione, indagine, accertamento e perseguimento di reati, esecuzione di sanzioni penali, nonché alla libera circolazione dei medesimi in conformità all'esercizio della delega di cui all'articolo 11 della legge 25 ottobre 2017, n. 163.

Il provvedimento si occupa, altresì, di disciplinare l'acquisizione e le modalità di trattamento dei dati da parte delle citate autorità, non solo per i fini penali sopra descritti, ma anche per altre finalità e in settori di materie diverse, incluse la salvaguardia contro e la prevenzione di minacce alla sicurezza pubblica, sia in via automatizzata che in via non automatizzata.

Lo schema di decreto è anche diretto ad individuare nel Garante per la protezione dei dati personali l'autorità di controllo incaricata di vigilare sull'applicazione delle norme attuative, al fine di tutelare i diritti e le libertà fondamentali delle persone fisiche con riguardo al trattamento di dati personali e di agevolare la libera circolazione dei dati all'interno dell'Unione europea.

In premessa, comunque, preme evidenziare gli effetti di neutralità per la finanza pubblica recati dal provvedimento stesso, trattandosi precipuamente di modifiche normative volte a dare luogo ad interventi di carattere meramente ordinamentale e/o procedimentale.

Al fine dare organicità e sistematicità all'intera disciplina del trattamento dei dati, lo schema di decreto è stato suddiviso in otto capi, ciascuno dei quali è diretto a regolamentare un aspetto determinato della materia per complessivi cinquanta articoli.

In particolare, il ***Capo I,*** contiene le *"Disposizioni generali" (articoli 1-8)* nelle quali è contemplato l'oggetto e l'ambito di applicazione della normativa ed i profili generali, fornendo le definizioni e precisazioni a livello terminologico e concettuale riguardo ai soggetti, ai dati trattati, alle attività e modalità di svolgimento delle stesse, ai destinatari e titolari del trattamento, all'autorità di controllo - individuata nel Garante per la protezione dei dati personali istituito dal D.lgs 196/2003 - e relativi riferimenti giuridici. Vengono, poi, elencati i principi applicabili, la conservazione e qualità dei dati, i presupposti e le condizioni di legittimità del trattamento. *In particolare, in relazione al trattamento ed alla conservazione dei dati si evidenzia che le attività descritte negli articoli 3 e 4 del presente provvedimento sono già contemplate dal vigente codice in materia di protezione dei dati personali di cui al decreto legislativo 30 giugno 2003, n. 196, che qui vengono puntualizzate e specificate ai fini di assicurare un maggior grado di affidabilità anche in*

relazione al loro eventuale aggiornamento. Pertanto, si garantisce che gli adempimenti connessi a tali attività vengono svolti dal personale in servizio e con strumentazioni adeguate già a disposizione delle autorità competenti al predetto trattamento. Le disposizioni di cui al presente capo non sono suscettibili di determinare oneri aggiuntivi per la finanza pubblica potendo essere fronteggiate con le risorse umane, strumentali e finanziarie disponibili a legislazione vigente.

Il Capo II concerne i *"Diritti dell'interessato" (articoli 9-14)* e si occupa del riconoscimento di alcuni specifici diritti dell'interessato al trattamento dei dati, individuati nella ricezione di informazioni, accesso, rettifica, cancellazione, limitazione del trattamento, disciplinandone condizioni e modalità di esercizio. L'esercizio di tali diritti deve sempre essere garantito, anche per quanto riguarda i dati contenuti in una decisione giudiziaria, in atti o documenti oggetto di trattamento nel corso di indagini, nel casellario giudiziale o contenuti in un fascicolo nel corso di un procedimento penale o in fase di esecuzione penale, conformemente a quanto previsto da disposizioni di legge o di regolamento. L'esercizio dei diritti sopra menzionati può essere ritardato, limitato o escluso nella misura e per il tempo in cui ciò costituisca uno strumento necessario e proporzionato nei casi in cui possano essere compromesse le attività di indagine connesse a procedimenti giudiziari ovvero le attività collegate all'applicazione di misure di sicurezza e prevenzione oppure per salvaguardare la sicurezza pubblica e nazionale o non ledere prioritari diritti e libertà altrui.

Alla tutela dei diritti ed al loro legittimo esercizio è deputata la figura del Garante attraverso il quale l'interessato ed il titolare del trattamento possono accedere per ottenere qualsiasi informazione per ottenere il riesame del caso e contro il rifiuto o limitazione dell'accesso o per altri motivi: lo stesso Garante fornisce a costoro le necessarie comunicazioni riguardo alla possibilità di proporre reclamo o ricorso giurisdizionale.

Come già evidenziato per il capo I, si conferma che le attività previste per il capo secondo sono contemplate dalle disposizioni del vigente codice sulla privacy (D.lgvo. 196/2003). Gli adempimenti connessi a tali attività vengono svolti dal personale in servizio e con strumentazioni adeguate già a disposizione delle autorità competenti al predetto trattamento anche ai fini di fornire le adeguate comunicazioni ed informazioni agli interessati per via telematica e in forma gratuita, con particolare riferimento alle informazioni relative all'esercizio dei diritti di cui agli articoli 8, 11, 12, 13, 14 e 27 del presente decreto. Le informazioni, comunicazioni e rettifiche in esame riguardano direttamente i dati personali dell'interessato dei quali il medesimo può richiedere la variazione anche in forma orale o attraverso delega ad enti, associazioni o altri organismi che svolgano un servizio di assistenza al pubblico. Pertanto, già attualmente, ai sensi

della normativa vigente, le attività di cui sopra vengono svolte in forma gratuita e le comunicazioni di riferimento avvengono in forma orale direttamente all'interessato o ai predetti enti o associazioni tramite sistemi telematici senza alcuna formalità e senza comportare effetti negativi a carico dell'erario. Solo nel caso in cui la richiesta di rettifica, cancellazione o limitazione dei dati personali avvenga nel corso di un procedimento penale, l'interessato è tenuto ad attenersi alle modalità di cui all'articolo 116 c.p.p. con rilascio a proprie spese di copie, estratti o certificati di singoli atti.

Si tratta, quindi, di attività che non comportano oneri aggiuntivi per la finanza pubblica potendosi espletare attraverso le risorse umane, strumentali e finanziarie disponibili a legislazione vigente, potendosi provvedere ai relativi adempimenti con le ordinarie risorse umane, strumentali e finanziarie disponibili a legislazione vigente, iscritte nel bilancio del Ministero della Giustizia, U.d.V. 1.2 - Giustizia civile e penale – CDR "Dipartimento dell'organizzazione giudiziaria, del personale e dei servizi" - Azione "Sviluppo degli strumenti di innovazione tecnologica in materia informatica e telematica per l'erogazione dei servizi di giustizia" – capitolo 1501, che reca uno stanziamento di euro 49.932.429 per l'anno 2018 e di euro 47.993.808 per ciascun anno del biennio 2019-2020.

Per quanto riguarda l'attività di supervisione ed informazione circa il legittimo trattamento dei dati personali, si assicura che le stesse saranno assicurate dal Garante attraverso le risorse iscritte nel bilancio del Ministero dell'economia e delle finanze U.d.V. 14.1 – Protezione sociale per particolari categorie - CDR "Dipartimento del Tesoro" – Azione "Tutela della privacy" – capitolo 1733, che reca uno stanziamento di euro 22.548.494 per l'anno 2018 e di euro 26.665.523 per ciascun anno del biennio 2019-2020.

Il Capo III, che è intitolato *"Titolare del trattamento e responsabile del trattamento" (articoli 15-30)*, definisce le figure del titolare e del responsabile del trattamento dei dati e gli obblighi sugli stessi incombenti - tra i quali sicuramente rientra la responsabilità della tenuta di registri relativi a tutte le categorie di attività di trattamento prevista all'art. 20 del presente provvedimento e che definisce meglio l'attività di conservazione e registrazione dei dati e degli adempimenti agli stessi connessi già prevista dalla normativa vigente - indica le misure di sicurezza adottabili per assicurare un corretto trattamento e si occupa di elencare in maniera precisa le procedure di registrazione in appositi file di log, precisando che le stesse vengono eseguite in sistemi di trattamento automatizzati.

Prima di procedere al trattamento dei dati personali, il titolare del trattamento ha l'obbligo di effettuare una valutazione dell'impatto sulla protezione dei dati personali, quando un tipo di

trattamento che prevede l'uso di nuove tecnologie, nuove procedure o meccanismi nuovi, può presentare un elevato rischio per i diritti e le libertà delle persone fisiche.

Viene inoltre prevista la consultazione preventiva del trattamento dei dati da parte del Garante, quando lo richiedono il titolare o il responsabile del trattamento oppure nell'ipotesi in cui il trattamento presenti un rischio elevato a causa dell'utilizzo delle nuove tecnologie, procedure e meccanismi ovvero di dati genetici o biometrici.

Si disciplinano anche gli obblighi in materia di sicurezza del trattamento, con particolare riguardo alla notifica da parte del titolare del trattamento al Garante, della violazione dei dati personali e alla designazione obbligatoria del responsabile della protezione dei dati da parte del titolare del trattamento, comunicata anche al predetto Garante.

In riferimento al profilo della sicurezza del trattamento, la norma prevede che il titolare e il responsabile del trattamento pongano in essere misure tecniche e organizzative idonee a garantire un livello di sicurezza adeguato al rischio di violazione dei dati.

Tali misure possono consistere nel vietare l'accesso alle attrezzature utilizzate per il trattamento dei dati a persone non autorizzate, nell'impedire che supporti di dati possano essere letti, modificati o asportati da persone non autorizzate, nell'esercitare un controllo sull'utente oppure nel garantire alle persone autorizzate di usare un sistema di trattamento automatizzato dei soli dati personali cui si riferisce la loro autorizzazione d'accesso (c.d. controllo dell'accesso ai dati) e nell'assicurare che in caso di interruzione i sistemi utilizzati possano essere ripristinati e che eventuali errori nel sistema vengano segnalati.

La prevenzione di comportamenti illeciti e la protezione ed il trattamento in sicurezza dei dati personali, saranno assicurati dal Garante attraverso le risorse iscritte nel bilancio del Ministero dell'economia e delle finanze U.d.V. 14.1 – Protezione sociale per particolari categorie – CDR "Dipartimento del Tesoro" – Azione "Tutela della privacy" – capitolo 1733, che reca uno stanziamento di euro 22.548.494 per l'anno 2018 e di euro 26.665.523 per ciascun anno del biennio 2019-2020.

Il Capo IV che è rubricato come *"Trasferimento di dati personali verso Paesi Terzi o organizzazioni internazionali" (articoli 31-36)* si preoccupa di disciplinare i trasferimenti di dati personali verso Paesi Terzi o organizzazioni internazionali, con i rinvii alle disposizioni del Regolamento europeo 2016/679 sulla protezione dei dati, solo quando vi sia coincidenza con le previsioni della direttiva.

Il Capo V che disciplina *"Tutela e sanzioni amministrative" (articoli 37-42)* individua nel Garante per la protezione dei dati personali l'autorità di controllo incaricata di vigilare che la Direttiva e le norme del presente decreto siano rispettate, al fine di tutelare i diritti e le libertà fondamentali delle persone fisiche con riferimento ai dati personali e di agevolare la libera circolazione dei dati all'interno dell'Unione europea, con esclusione del potere di controllo per i trattamenti effettuati dall'autorità giudiziaria nell'esercizio delle funzioni giurisdizionali nonché di quelle giudiziarie del pubblico ministero. Per le suddette finalità sono dettagliatamente precisate le funzioni ed i compiti attribuiti alla predetta Authority quali ad esempio: promozione sulla conoscenza e consapevolezza dei rischi e delle norme, espressione di pareri, rilascio informazioni, trattazione e supporto per la proposizione di reclami, prestazione di consulenze etc. Vengono, altresì, definiti a poteri attribuiti allo stesso Garante quali: rivolgere avvertimenti riguardo possibili violazioni, imporre limitazioni , promuovere segnalazioni, denunciare reati etc.

Sono state, inoltre, previste sanzioni amministrative per la violazione delle norme di recepimento della direttiva, secondo lo schema generale previsto dal succitato Regolamento, con i criteri e le garanzie ivi previsti, tenendo presente che tali sanzioni sono inflitte in relazione alle circostanze di ogni singolo caso e comunque in aggiunta alle misure già previste nel Regolamento e con previsione di limiti più elevati per le sanzioni, qualora la violazione concerna la violazione dei principi fondamentali e le condizioni di liceità del trattamento di cui agli artt. 3 e 5, i divieti e le condizioni particolari di trattamento di cui agli artt. 6, 7 e 8, nonché le norme sul trasferimento dei dati all'estero.

Ai poteri di controllo assegnati al Garante tramite il presente provvedimento nonché ai compiti di vigilanza e supervisione attribuiti all'Authority potrà darsi attuazione attraverso le risorse iscritte nel bilancio del Ministero dell'economia e delle finanze U.d.V. 14.1 – Protezione sociale per particolari categorie – CDR "Dipartimento del Tesoro" – Azione "Tutela della privacy" – capitolo 1733, che reca uno stanziamento di euro 22.548.494 per l'anno 2018 e di euro 26.665.523 per ciascun anno del biennio 2019-2020.

Il Capo VI invece è deputato ad inquadrare gli *"Illeciti penali" (articoli 43-46)* relativi alla materia e, pur mantenendo le previsioni già contemplate dal codice penale per alcune tipologie di violazioni, ha rafforzato ed integrato la tutela codicistica attraverso un'ulteriore catalogazione di fattispecie ritenute giuridicamente rilevanti, con particolare riguardo trattamento illecito per difetto di titolo giuridico o per finalità diverse da quelle consentite, alla profilazione discriminatoria, alla falsità delle dichiarazioni rese al Garante ed alle notificazioni al medesimo nonché riguardo alla inosservanza dei provvedimenti della citata Authority.

Le attività e gli adempimenti connessi all' indagine, accertamento e perseguimento di reati già sanzionati dalle disposizioni del codice privacy in vigore nonché per i residui reati introdotti dal presente provvedimento sono già correntemente espletati dagli organi a ciò preposti con il proprio personale e le proprie dotazioni materiali e finanziarie e, pertanto, non sono suscettibili di determinare effetti onerosi per la finanza dello Stato in quanto potranno essere fronteggiati attraverso le risorse umane, strumentali e finanziarie disponibili a legislazione vigente con particolare riguardo agli stanziamenti iscritti nel bilancio del Ministero della giustizia U.d.V. 1.4 – Servizi di gestione amministrativa per l'attività giudiziaria - CDR "Dipartimento per gli Affari di Giustizia" – Azione "Supporto allo svolgimento dei procedimenti giudiziari attraverso le spese di giustizia" – capitolo 1360, che reca uno stanziamento di euro 472.701.564 per l'anno 2018 e di euro 466.616.730 per ciascun anno del biennio 2019-2020.

Il Capo VII tratta le "Disposizioni integrative sui trattamenti delle Forze di Polizia" *(articoli 47-48)* e si occupa del flusso e delle modalità di trattamento dei dati, nonché degli strumenti a tutela dell'interessato, con riferimento, per l'appunto, a quelli trattati dalle Autorità di pubblica sicurezza e dalle Forze di polizia. In particolare, si evidenzia che le Autorità di pubblica sicurezza e le Forze di polizia possono acquisire, nel rispetto delle vigenti disposizioni di legge, dati, informazioni, atti e documenti da altri soggetti anche per via telematica, sulla base di convenzioni stipulate dagli organi o uffici interessati, sul prototipo di convenzioni-tipo adottate dal Ministero dell'Interno su parere conforme del Garante, atte a facilitare la loro consultazione mediante reti di comunicazione elettronica, di pubblici registri, elenchi, schedari e banche dati.

La disposizione, che ricalca pressoché integralmente quella attualmente contenuta all'articolo 54, comma 1, del Codice della *privacy*, non è suscettibile di determinare nuovi o maggiori oneri per la finanza pubblica, considerato che, per le convenzioni sottoscritte con soggetti pubblici, trova applicazione il principio di gratuità, fissato dall'articolo 50, comma 2, del d.lgs. 7 marzo 2005, n. 82, recante il Codice dell'Amministrazione digitale, il quale espressamente prevede che i dati trattati da altre pubbliche Amministrazioni sono resi accessibili e fruibili senza oneri a carico dell'Amministrazione che riceve i dati.

Il Dipartimento della pubblica sicurezza assicura il periodico aggiornamento del Centro elaborazione dati, di cui all'articolo 8 della legge 1° aprile 1981, n. 121, anche attraverso interrogazioni autorizzate del casellario giudiziario e del casellario dei carichi pendenti del Ministero della Giustizia, in conformità a quanto stabilito dal D.P.R. 14 novembre 2002, n. 313 o di altre banche dati.

Si tratta di banche dati, schedari ed elenchi già esistenti e continuamente aggiornati, che non comportano, ai fini della consultazione, riflessi onerosi per la finanza pubblica.

Per eventuali interventi di adeguamento non sussistono maggiori oneri, in quanto gli stessi rientrano nell'ambito dell'assistenza tecnica di rimodulazione dell'hardware e del software, ai quali potrà provvedersi con lo stanziamento ordinario, imputabile al capitolo 7457, piano gestionale 3, iscritto nell'UdV 3.3 "Pianificazione e coordinamento Forze di Polizia" dello stato di previsione del Ministero dell'interno.

Il suddetto capitolo infatti, non solo presenta, a regime, uno stanziamento annuale di euro 8.387.270,00, ma anche risorse aggiuntive assegnate in base all'articolo 1, comma 623, della legge 21 dicembre 2016, n. 232 (legge finanziaria 2017), il quale ha previsto l'istituzione nello stato di previsione del MEF di un Fondo con una dotazione finanziaria di 70 milioni di euro per l'anno 2017 e di 180 milioni di euro per il periodo 2018-2030, per l'acquisto e l'ammodernamento dei mezzi strumentali in uso alle Forze di polizia e al Corpo nazionale dei Vigili del fuoco.

In virtù della ripartizione di tali somme, sul capitolo 7457/3 sono stati iscritti, 38 milioni di euro nel 2018, 32 milioni di euro nel 2019, 38,4 milioni di euro nel 2020 e 25 milioni di euro nel 2021.

Per quanto precede, si farà fronte alle esigenze di adeguamento informatico con le risorse disponibili a legislazione vigente, nel rispetto della clausola di invarianza finanziaria contenuta nel successivo articolo 51.

Il Capo VIII contiene le *"Disposizioni di coordinamento e abrogazioni"* ***(articoli 49-50)*** dirette a armonizzare la disciplina normativa con le altre disposizioni di riferimento del D.P.R. 196/2003 e dei decreti attuativi del medesimo anche attraverso la previsione di norme da abrogare. E', infine, dettata la clausola d'invarianza finanziaria, *in relazione alla quale si conferma che le attività conseguenti all'applicazione del decreto in esame, già espletate dalle amministrazioni a legislazione vigente, non appaiono suscettibili di determinare nuovi o maggiori oneri a carico della finanza pubblica.*

La verifica della presente relazione tecnica, effettuata ai sensi e per gli effetti dell'art. 17, comma 3, della legge 31 dicembre 2009, n. 196 ha avuto esito

[X] POSITIVO [ ] NEGATIVO

Il Ragioniere Generale dello Stato

21 FEB. 2018

MINISTERO DELLA GIUSTIZIA
UFFICIO LEGISLATIVO

SCHEMA DI DECRETO LEGISLATIVO RECANTE ATTUAZIONE DELLA DIRETTIVA 27 APRILE 2016, N. 2016/680/UE DEL PARLAMENTO EUROPEO E DEL CONSIGLIO RELATIVA ALLA PROTEZIONE DELLE PERSONE FISICHE CON RIGUARDO AL TRATTAMENTO DEI DATI PERSONALI DA PARTE DELLE AUTORITÀ COMPETENTI A FINI DI PREVENZIONE, INDAGINE, ACCERTAMENTO E PERSEGUIMENTO DI REATI O ESECUZIONE DI SANZIONI PENALI, NONCHÉ ALLA LIBERA CIRCOLAZIONE DI TALI DATI E CHE ABROGA LA DECISIONE QUADRO 2008/977/GAI DEL CONSIGLIO.

ANALISI TECNICO-NORMATIVA (ATN)

PARTE I. ASPETTI TECNICO-NORMATIVI DI DIRITTO INTERNO

1) Obiettivi e necessità dell'intervento normativo. Coerenza con il programma di Governo

Il presente schema di decreto legislativo è finalizzato al recepimento della direttiva 27 aprile 2016, n. 2016/680/UE del Parlamento europeo e del Consiglio relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio (CE)2016/680.

La necessità di provvedere all'attuazione della direttiva in esame nasce dall'esigenza di conformarsi ai principi stabiliti dal legislatore europeo in materia di tutela delle persone fisiche, al fine di fornire un livello elevato e uniforme di protezione con riguardo al trattamento dei dati personali trattati per finalità di prevenzione, accertamento e repressione di reati ed esecuzione delle pene, nonché di facilitare lo scambio di dati personali tra le autorità competenti degli Stati membri, così da garantire una efficace cooperazione giudiziaria in campo penale e di polizia.

In tale ottica e con l'ulteriore obiettivo di combinare le descritte finalità con le peculiarità proprie del procedimento e del processo penale, anche nella fase esecutiva, e delle attività delle forze di polizia a ciò funzionali, lo schema di decreto legislativo mira a creare un vero e proprio statuto sulla raccolta e il trattamento dei dati personali in ambito penale, contenente principi generali di regolamentazione della materia, rivolti anche al legislatore futuro, e disposizioni di dettaglio, nei vari settori in cui si può articolare il trattamento, modulando le esigenze di tutela dei diritti dell'interessato anche sulla base delle peculiarità proprie della giustizia penale e del contesto processuale.
In sintonia con la direttiva UE 2016/680, si fornisce una regolamentazione organica del trattamento dei dati personali delle persone fisiche per fini di prevenzione, indagine, accertamento e perseguimento di reati, la quale supera e sostituisce in gran parte quella attualmente contemplata nei titoli primo e secondo della parte seconda del Codice sul trattamento dei dati personali di cui al decreto legislativo 30 giugno 2003, n. 196, dedicate a specifici settori, in particolare quello giudiziario e quello dei trattamenti da parte delle forze di polizia.
Con l'odierno schema di decreto legislativo si assicura un completo adeguamento dell'ordinamento interno alla normativa europea, anche mediante un'opera di razionalizzazione della materia, facendo salva la regolamentazione già esistente nell'ordinamento ritenuta compatibile con quella europea.
Il presente intervento normativo risulta, pertanto, pienamente coerente con il programma di Governo.

2) Analisi del quadro normativo nazionale

Con riguardo alla tecnica redazionale, si è optato per la predisposizione di un unico corpo normativo, destinato a regolamentare il trattamento dei dati personali per finalità di prevenzione e repressione di reati, esecuzione di sanzioni penali, salvaguardia contro le minacce alla sicurezza pubblica e prevenzione delle stesse, da parte sia dell'autorità giudiziaria, sia delle forze di polizia.
Viene, dunque, adottato un testo unitario, dedicato alla complessiva disciplina del trattamento di dati personali in ambito penale, con l'obiettivo di creare un vero e proprio statuto, contenente principi generali di regolamentazione della materia, rivolti anche al legislatore futuro, e disposizioni di dettaglio, nei vari settori in cui si può articolare il trattamento dei dati personali.
In sintonia con la direttiva che si recepisce nell'ordinamento interno, si fornisce una regolamentazione organica del trattamento dei dati personali delle persone fisiche, la quale supera e sostituisce in gran parte quella attualmente contemplata nei titoli primo e secondo della parte seconda del Codice sul trattamento dei dati personali di cui al decreto legislativo 30 giugno 2003, n. 196, dedicate a specifici settori, in particolare quello giudiziario e quello dei trattamenti da parte delle forze di polizia.
Con specifico riferimento all'ambito giudiziario, attualmente trovano applicazione gli articoli da 46 a 52 del codice della privacy, dedicati ai trattamenti svolti nell'esercizio delle funzioni sia civili che penali, ivi compresi i trattamenti in materia di status giuridico ed economico del personale della magistratura che, seppure non direttamente correlati alla trattazione giudiziaria di affari e di

controversie, abbiano una diretta incidenza sulla funzione giurisdizionale, nonché quelli svolti nell'ambito di attività ispettiva su uffici giudiziari.
Per quanto concerne, invece, i trattamenti effettuati dall'autorità di pubblica sicurezza per fini di prevenzione, accertamento o repressione dei reati o di tutela della sicurezza pubblica, la disciplina dettata dalla direttiva assorbe totalmente quella oggi prevista dagli articoli da 53 a 57 del codice della privacy, che vengono conseguentemente abrogati.
Rimane, invece, del tutto compatibile con i principi enunciati nella direttiva 2016/680 quanto stabilito dall'articolo 7, comma 3, del decreto legge 18 febbraio 2015, n. 7, circa l'individuazione, con decreto adottato dal Ministro dell'interno, dei trattamenti non occasionali effettuati per fini di polizia, previsti da norme legislative o regolamentari.
In sintonia con l'opzione di compendiare in un corpo unitario tutta la materia riguardante il trattamento dei dati in ambito penale, in alcuni casi si è fatto espresso richiamo alla normativa già vigente ritenuta conforme ai principi dettati dalla direttiva, ad esempio in tema di tutela degli interessati, in altri, le disposizioni tuttora attuali sono state "trasferite" nel presente corpo normativo, come ad esempio alcune fattispecie di illecito sanzionate in via amministrativa e alcuni reati già puniti dal codice della privacy. In questo modo si è inteso anche razionalizzare e assicurare coerenza alla disciplina in vigore nell'ordinamento rispetto alle istanze di stampo europeo.

3) Incidenza delle norme proposte sulle leggi e i regolamenti vigenti

Lo schema di decreto legislativo interviene sulla normativa attualmente in vigore in materia di trattamento di dati personali, in particolare sostituisce la disciplina prevista da alcune disposizioni contenute nel Codice in materia di protezione dei dati personali di cui al decreto legislativo 30 giugno 2003, n. 196, abrogando gli articoli 53, 54, 55, 56 e 57. Altri testi normativi, invece, sono espressamente fatti salvi, come il decreto del Ministro dell'interno in data 24 maggio 2017, pubblicato sulla Gazzetta Ufficiale n. 145 del 24 giugno 2017, e i decreti del Presidente della Repubblica di attuazione dell'articolo 57 del decreto legislativo 30 giugno 2003, n. 196.

4) Analisi della compatibilità dell'intervento con i principi costituzionali

L'intervento normativo è conforme alla disciplina costituzionale.

5) Analisi della compatibilità dell'intervento con le competenze e le funzioni delle Regioni ordinarie e a statuto speciale nonché degli enti locali

Lo schema di decreto legislativo non presenta aspetti di interferenza o di incompatibilità con le competenze costituzionali delle Regioni, incidendo su materia (tutela dei diritti delle persone fisiche in campo penale e di polizia) riservata alla competenza dello Stato.

6) Verifica della compatibilità con i principi di sussidiarietà, differenziazione e adeguatezza sanciti dall'articolo 118, primo comma, della Costituzione.

Le disposizioni contenute nell'intervento normativo esaminato sono compatibili e rispettano i principi di cui all'articolo 118 della Costituzione, in quanto non prevedono né determinano, sia pure in via indiretta, nuovi o più onerosi adempimenti a carico degli enti locali.

7) Verifica dell'assenza di rilegificazioni e della piena utilizzazione delle possibilità di delegificazione e degli strumenti di semplificazione normativa

Lo schema di decreto legislativo ha ad oggetto materie assistite da riserva assoluta di legge, non suscettibili di delegificazione.

8) Verifica dell'esistenza di progetti di legge vertenti su materia analoga all'esame del Parlamento e relativo stato dell'*iter*.

Non risulta l'esistenza di progetti di legge di legge vertenti su materia analoga all'esame del Parlamento.

9) Indicazioni delle linee prevalenti della giurisprudenza ovvero della pendenza di giudizi di costituzionalità sul medesimo o analogo oggetto.

Non risulta la pendenza di giudizi di costituzionalità sul medesimo o analogo oggetto.

PARTE II. CONTESTO NORMATIVO COMUNITARIO E INTERNAZIONALE

10) Analisi della compatibilità dell'intervento con l'ordinamento europeo

Lo schema di decreto legislativo non presenta aspetti di interferenza o di incompatibilità con l'ordinamento europeo ed anzi attua nell'ordinamento interno le disposizioni contenute nella citata direttiva.

11) Verifica dell'esistenza di procedure di infrazione da parte della Commissione europea sul medesimo o analogo oggetto

Non risultano procedure di infrazione da parte della Commissione europea sul medesimo oggetto.

12) Analisi della compatibilità dell'intervento con gli obblighi internazionali

L'intervento è pienamente compatibile con gli obblighi internazionali.

13) Indicazioni delle linee prevalenti della giurisprudenza ovvero della pendenza di giudizi innanzi alla Corte di Giustizia delle Comunità europee sul medesimo o analogo oggetto.

Non risultano procedimenti pendenti avanti la Corte di Giustizia dell'Unione europea aventi il medesimo o analogo oggetto. Neppure risulta alcun orientamento giurisprudenziale relativo a tale fattispecie.

14) Indicazioni delle linee prevalenti della giurisprudenza ovvero della pendenza di giudizi innanzi alla Corte Europea dei Diritti dell'uomo sul medesimo o analogo oggetto.

Non risultano esservi pendenze o ricorsi davanti alla Corte europea dei diritti dell'Uomo, né constano orientamenti giurisprudenziali assunti dalla stessa.

15) Eventuali indicazioni sulle linee prevalenti della regolamentazione sul medesimo oggetto da parte di altri Stati membri dell'Unione Europea

Considerata l'eterogeneità dei sistemi giuridici penali europei non si hanno indicazioni sulle linee prevalenti della regolamentazione sul medesimo oggetto all'interno degli Stati membri dell'Unione europea. Una parte di essi (per quanto risulta, Germania e Austria) ha dato attuazione alla direttiva.

PARTE III. ELEMENTI DI QUALITA' SISTEMATICA E REDAZIONALE DEL TESTO

1) Individuazione delle nuove definizioni normative introdotte dal testo, della loro necessità, della coerenza con quelle già in uso

Lo schema di decreto legislativo non introduce nuove definizioni normative, essendo esaustive quelle già esistenti.

2) Verifica della correttezza dei riferimenti normativi contenuti nel progetto, con particolare riguardo alle successive modificazioni e integrazioni subite dai medesimi

I riferimenti normativi che figurano nel presente schema sono corretti.

3) Ricorso alla tecnica della novella legislativa per introdurre modificazioni e integrazioni a disposizioni vigenti

Lo schema di decreto legislativo non utilizza la tecnica della novella.

4) Individuazione di effetti abrogativi impliciti di disposizioni dell'atto normativo e loro traduzione in norme abrogative espresse nel testo normativo

Sono previste abrogazioni espresse degli articoli 53, 54, 55, 56 e 57 del Codice in materia di protezione dei dati personali di cui al decreto legislativo 30 giugno 2003, n. 196.

5) Individuazione di disposizioni dell'atto normativo aventi effetto retroattivo o di reviviscenza di norme precedentemente abrogate o di interpretazione autentica o derogatorie rispetto alla normativa vigente

Lo schema di atto normativo non contiene disposizioni aventi effetto retroattivo o di reviviscenza di norme precedentemente abrogate o di interpretazione autentica o derogatorie rispetto alla normativa vigente.

6) Verifica della presenza di deleghe aperte sul medesimo oggetto, anche a carattere integrativo o correttivo

Non sono presenti altre deleghe di carattere integrativo o correttivo.

7) Indicazione degli eventuali atti successivi attuativi; verifica della congruenza dei termini previsti per la loro adozione.

Sono previsti atti successivi attuativi di natura normativa per la regolamentazione di dettaglio della materia.

8) Verifica della piena utilizzazione e dell'aggiornamento di dati e di riferimenti statistici attinenti alla materia oggetto del provvedimento, ovvero indicazione della necessità di commissionare all'Istituto nazionale di statistica apposite elaborazioni statistiche con correlata indicazione nella relazione economico-finanziaria della sostenibilità dei relativi costi

Sono stati utilizzati i dati e i riferimenti in possesso del Ministero della giustizia.

Ministero della Giustizia
UFFICIO LEGISLATIVO

SCHEMA DI DECRETO LEGISLATIVO RECANTE "ATTUAZIONE DELLA DIRETTIVA 27 APRILE 2016, N. 2016/680/UE DEL PARLAMENTO EUROPEO E DEL CONSIGLIO RELATIVA ALLA PROTEZIONE DELLE PERSONE FISICHE CON RIGUARDO AL TRATTAMENTO DEI DATI PERSONALI DA PARTE DELLE AUTORITÀ COMPETENTI A FINI DI PREVENZIONE, INDAGINE, ACCERTAMENTO E PERSEGUIMENTO DI REATI O ESECUZIONE DI SANZIONI PENALI, NONCHÉ ALLA LIBERA CIRCOLAZIONE DI TALI DATI E CHE ABROGA LA DECISIONE QUADRO 2008/977/GAI DEL CONSIGLIO".

ANALISI DI IMPATTO DELLA REGOLAMENTAZIONE (A.I.R.)

SEZIONE 1 - IL CONTESTO E GLI OBIETTIVI

A) La rappresentazione del problema da risolvere e delle criticità constatate, anche con riferimento al contesto internazionale ed europeo, nonché delle esigenze sociali ed economiche considerate:

Il presente schema di decreto legislativo è finalizzato a recepire nell'ordinamento interno la "direttiva (UE) 2016/680 relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio".
Il provvedimento, redatto nell'esercizio della delega conferita al Governo dall'articolo 11 della legge 25 ottobre 2017, n. 163, recante "Delega al Governo per il recepimento delle direttive europee e l'attuazione di altri atti dell'Unione europea - Legge di delegazione europea 2016-2017", disciplina, in sintonia con gli obiettivi perseguiti dalla direttiva, il trattamento interamente o parzialmente automatizzato di dati personali delle persone fisiche, nonché il trattamento non automatizzato di dati personali contenuti in un archivio, o ad esso destinati, nel settore penale.

Come richiesto dal legislatore europeo, si è predisposta una disciplina organica del trattamento dei dati personali delle persone fisiche per fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, avendo cura, in ogni caso, di assicurare regole diversificate in ragione delle specifiche caratteristiche e dalla differente natura delle autorità interessate al trattamento stesso, giudiziaria e di polizia.

Si è, pertanto, creato un unico testo normativo, destinato a regolamentare il trattamento dei dati personali per finalità penale, da parte sia dell'autorità giudiziaria, sia delle forze di polizia.

La disciplina contenuta nello schema di decreto supera e sostituisce in gran parte quella attualmente contemplata nei titoli primo e secondo della parte seconda del Codice sul trattamento dei dati personali di cui al decreto legislativo 30 giugno 2003, n. 196, aggiornandola e razionalizzandola in modo da assicurare la piena conformità della normativa interna alle istanze europee.

Lo scopo perseguito dal legislatore europeo con la direttiva (UE)2016/680 è di fornire a tutte le persone fisiche un livello elevato e uniforme di tutela con riferimento al trattamento dei dati personali nello specifico settore della prevenzione, accertamento e repressione dei reati, nonché di esecuzione delle pene, e di facilitare lo scambio di dati personali tra le autorità competenti degli stati membri, così da garantire una efficace cooperazione giudiziaria in campo penale e di polizia.

In tale ottica e con l'ulteriore obiettivo di combinare le descritte finalità con le peculiarità proprie del procedimento e del processo penale, anche nella fase esecutiva, e delle attività delle forze di polizia a ciò funzionali, in modo da non comprometterne il buon esito, lo schema di decreto legislativo mira a creare un vero e proprio statuto sulla raccolta e il trattamento dei dati personali in ambito penale, contenente principi generali di regolamentazione della materia, rivolti anche al legislatore futuro, e disposizioni di dettaglio, nei vari settori in cui si può articolare il trattamento, modulando le esigenze di tutela dei diritti dell'interessato anche sulla base delle peculiarità proprie della giustizia penale e del contesto processuale.

In sintonia con i principi dettati dalla direttiva, al fine di rafforzare la protezione dell'interessato, un intero capo dello schema di decreto è dedicato alla tutela dei suoi diritti, sia mediante reclamo al garante della privacy, con riferimento al trattamento dei dati da parte delle forze di polizia, sia con ricorso giurisdizionale, per il trattamento da parte delle forze di polizia e dell'autorità giudiziaria, attraverso il richiamo alla disciplina già prevista dal codice della privacy.

Sono, inoltre, indicate sanzioni amministrative e penali, alcune anche di nuova creazione, per le violazioni della disciplina contenuta nello schema di decreto, ed è assicurato il risarcimento del danno cagionato da un trattamento o da qualsiasi altro atto compiuti in violazione delle disposizioni di cui allo schema di decreto.

B) L'indicazione degli obiettivi (di breve, medio o lungo periodo) perseguiti con l'intervento normativo:

L'obiettivo perseguito con il presente provvedimento è, anzitutto, di natura formale, essendo finalizzato all'adeguamento del diritto nazionale agli atti normativi dell'Unione europea, nonché alla predisposizione di un testo unitario in tema di trattamento dei dati personali in ambito penale, da parte delle autorità a ciò preposte, in particolare quella giudiziaria e le forze di polizia

Dal punto di vista sostanziale, lo schema di decreto è volto ad una più efficace e uniforme tutela dei diritti delle persone fisiche, assicurando tuttavia le specifiche esigenze e peculiarità del procedimento e del processo penale, nonché delle attività di polizia in materia di prevenzione e accertamento dei reati, e a facilitare lo scambio di dati personali tra le autorità competenti degli stati membri, in vista di una migliore cooperazione giudiziaria in campo penale e di polizia.

In particolare l'obiettivo che si intende perseguire:

- nel breve periodo, è quello di adottare a livello di Unione europea una più pregnante e omogena tutela dei diritti delle persone fisiche con riguardo ai dati personali, anche mediante un intervento di razionalizzazione della materia; inoltre, si prevede di migliorare gli scambi di dati tra gli Stati, con l'ulteriore risultato di facilitare e rendere più sicura la cooperazione giudiziaria in campo penale e di polizia;
- nel medio e lungo periodo, il completo recepimento della direttiva, anche attraverso l'adozione di ulteriori provvedimenti normativi volti alla disciplina di dettaglio (in particolare con riferimento alle modalità di conservazione dei dati, ai soggetti legittimati, alle condizioni di accesso, alle modalità di consultazione), è destinata a rendere maggiormente efficace la protezione dei dati personali e dei diritti degli interessati.

C) La descrizione degli indicatori che consentiranno di verificare il grado di raggiungimento degli obiettivi indicati e di monitorare l'attuazione dell'intervento nell'ambito della VIR:

Indicatori che consentono la verifica del grado di raggiungimento degli obiettivi sottesi all'adozione del presente schema di decreto legislativo sono rappresentati dai dati statistici relativi all'esercizio dei diritti da parte dell'interessato mediante richieste di informazioni, di accesso, di correzione e di cancellazione dei dati personali e delle conseguenti attività volte ad esitare tali richieste; dal numero di attività poste in essere dall'autorità di controllo (Garante della privacy) al fine di vigilare sulla corretta applicazione delle disposizioni del presente schema di decreto legislativo; dal numero di procedimenti giudiziari avviati al fine della tutela degli interessati; dal numero di sanzioni amministrative e penali irrogate per gli illeciti contemplati dal presente schema di decreto legislativo; dal numero di scambi e trasferimenti di dati tra le competenti autorità appartenenti agli Stati membri e ad altri Stati terzi o con organismi dell'Unione europea o internazionali.

D) Indicazione delle categorie dei soggetti, pubblici e privati, destinatari dei principali effetti dell'intervento regolatorio:

Risultano destinatari delle presenti disposizioni, tra i soggetti pubblici, gli appartenenti alla magistratura e all'amministrazione della giustizia, nonché alle forze di polizia preposti al trattamento dei dati personali per le finalità di cui alla direttiva che si recepisce con il presente provvedimento normativo; il garante per la protezione dei dati personale.
Tra i soggetti privati, sono interessate le persone fisiche alle quali si riferiscono i dati trattati per tali finalità.

SEZIONE 2 - PROCEDURE DI CONSULTAZIONE PRECEDENTI L'INTERVENTO

Non sono state avviate consultazioni precedentemente all'intervento normativo, in ragione della natura dello stesso, trattandosi di provvedimento il cui ambito è già delimitato con precisione sia dalla direttiva oggetto di recepimento, sia dalla legge di delegazione europea.
Per la redazione del provvedimento ci si è avvalsi dei lavori di una commissione di studio istituita presso il Ministero della giustizia, composta di professori universitari in materie giuridiche, avvocati, rappresentanti del garante per la privacy, magistrati, alle cui riunioni hanno partecipato anche rappresentanti del Ministero dell'Interno.
L'Ufficio ha, inoltre, preso parte a una riunione di coordinamento con il competente Dipartimento delle Politiche europee della Presidenza del Consiglio dei Ministri, alla quale hanno preso parte i rappresentanti delle amministrazioni interessate.

SEZIONE 3 - LA VALUTAZIONE DELL'OPZIONE DI NON INTERVENTO ("OPZIONE ZERO")

L'opzione di non intervento è stata valutata ma disattesa, stante la necessità di recepire la direttiva (UE) 2016/680, in ossequio alla delega contenuta nell'articoli 1 e 11 della legge 25 ottobre 2017, n. 163 (legge di delegazione europea 2017).
La mancata piena attuazione della direttiva esporrebbe il nostro Paese ad una possibile procedura di infrazione per inadempimento degli obblighi derivanti dal diritto dell'Unione.

SEZIONE 4 - VALUTAZIONE DELLE OPZIONI ALTERNATIVE

Tenuto conto dei limiti stringenti imposti dalla direttiva e della necessità di assicurare il suo recepimento, non è stata presa in considerazione alcuna opzione alternativa.
Sono stati fatti salvi i provvedimenti normativi già in vigore nell'ordinamento che regolano la materia, ritenuti conformi al dettato della direttiva.

SEZIONE 5 - GIUSTIFICAZIONE DELL'OPZIONE REGOLATORIA PROPOSTA E VALUTAZIONE DEGLI ONERI AMMINISTRATIVI E DELL'IMPATTO SULLE P.M.I.

A) Gli svantaggi e i vantaggi dell'opzione prescelta, per i destinatari diretti e indiretti, a breve e a medio-lungo termine, adeguatamente misurati e quantificati, anche con riferimento alla possibile incidenza sulla organizzazione e sulle attività delle pubbliche amministrazioni:

L'opzione scelta non presenta svantaggi. Il presente intervento regolatorio migliora il sistema esistente e offre un più elevato e uniforme livello di tutela dei dati personali in ambito penale, a vantaggio di tutti i cittadini. Inoltre favorisce le stesse autorità competenti, con riferimento ai trasferimenti all'estero e dall'estero dei dati personali trattati per le finalità di prevenzione, accertamento e repressione dei reati, facilitando lo scambio di tali dati così da garantire una più efficace cooperazione giudiziaria in campo penale e di polizia.

B) L'individuazione e la stima degli effetti dell'opzione prescelta sulle micro, piccole e medie imprese:

Non derivano oneri amministrativi in capo alle P.M.I.

C) L'indicazione e la stima degli oneri informativi e dei relativi costi amministrativi, introdotti o eliminati a carico di cittadini e imprese:

Non sono previsti oneri informativi a carico delle categorie sopra indicate.

D) Le condizioni e i fattori incidenti sui prevedibili effetti dell'intervento regolatorio, di cui comunque occorre tener conto per l'attuazione:

L'attuazione dell'intervento avviene tramite le risorse e le strutture interne dell'amministrazione giudiziaria, la quale è in grado di adottare immediatamente le nuove norme senza ulteriori oneri per la finanza pubblica e attraverso le strutture già esistenti. Pertanto, non sono previsti fattori che possano incidere negativamente sugli effetti prodotti dall'intervento regolatorio.

SEZIONE 6 - INCIDENZA SUL CORRETTO FUNZIONAMENTO CONCORRENZIALE DEL MERCATO E SULLA COMPETITIVITA' DEL PAESE

L'intervento regolatorio, in quanto destinato a innovare e razionalizzare gli strumenti di tutela dei dati personali in ambito penale, non ha diretta incidenza sul corretto funzionamento concorrenziale del mercato. In ogni

caso, una protezione rafforzata dei diritti dei cittadini in tema di dati personali, attuata nel rispetto delle esigenze e peculiarità delle attività di prevenzione e repressione dei reati, ed una più efficace cooperazione giudiziaria in campo penale e di polizia, contribuisce ad assicurare effetti positivi sulla competitività del Paese a livello internazionale, con particolare riferimento allo spazio dell'Unione europea. Si richiama quanto argomentato nella sezione 5 lettera A) sulle ricadute positive di una più razionale regolamentazione della materia.

SEZIONE 7 - MODALITA' ATTUATIVE DELL'INTERVENTO DI REGOLAMENTAZIONE

A) Soggetti responsabili dell'attuazione dell'intervento regolatorio

Sono responsabili dell'attuazione dell'intervento regolatorio l'autorità giudiziaria e le forze di polizia, competenti in materia di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali.

B) Le azioni per la pubblicità e per l'informazione dell'intervento

Non sono previste azioni specifiche per la pubblicità e per l'informazione dell'intervento perché diretto a soggetti specializzati. Il testo verrà diffuso in rete mediante il sito *web* del Ministero della giustizia.

C) Strumenti e modalità per il controllo e il monitoraggio dell'intervento regolatorio

Il controllo e il monitoraggio dell'intervento regolatorio in esame verrà attuato dal Ministero della giustizia attraverso le risorse in atto, senza l'introduzione di nuove forme di controllo che implichino oneri per la finanza pubblica.

D) I meccanismi eventualmente previsti per la revisione dell'intervento regolatorio

Non sono previsti specifici meccanismi per la revisione dell'intervento regolatorio.

E) Gli aspetti prioritari da monitorare in fase di attuazione dell'intervento regolatorio e considerare ai fini della VIR

A cura del Ministero della giustizia verrà effettuata, con cadenza biennale, la prevista V.I.R., nella quale saranno presi in esame i seguenti aspetti:

- verifica dell'efficacia dell'intervento mediante analisi dei flussi e dei dati statistici di cui alla Sez. I, lettera C).

SEZIONE 8 - RISPETTO DEI LIVELLI MINIMI DI REGOLAZIONE EUROPEA

L'intervento normativo si adegua al livello minimo di regolazione dell'Unione europea.