20
Disciplina della privacy e tutela dei dati personali

1 Il Codice della privacy

Il D.Lgs. 30 giugno 2003 che contiene il cd. Codice in materia di dati personali (cd. Codice della Privacy), rappresenta il punto di arrivo della sistemazione organica di una disciplina che, sebbene storicamente poco sentita dal nostro legislatore, era raccolta in una molteplicità di disposizioni.

Il Codice, da un punto di vista strutturale, è organizzato in 3 parti:

- la Parte prima, "**Disposizioni generali**", è dedicata ai soggetti (Titolare, Responsabile, Incaricato, interessato), agli adempimenti ed alle regole del trattamento. Le disposizioni di tale Parte (artt. 1-45) si applicano a *tutti i trattamenti*, salvo differenziazioni dovute al carattere pubblico o privato del soggetto trattante ed eventuali deroghe disposte da norme della Parte speciale;
- la Parte seconda, "**Disposizioni relative a specifici settori**", disciplina il trattamento in ambiti specifici, quale ad esempio quello giudiziario, quello sanitario, quello lavorativo, nonché il trattamento in ambito pubblico;
- la Parte terza, "**Tutela dell'interessato e sanzioni**", è, invece, dedicata alla tutela amministrativa e giurisdizionale nonché alle sanzioni amministrative ed agli illeciti penali.

2 Principi generali della disciplina

«***Chiunque ha diritto alla protezione dei dati personali che lo riguardano***». L'art. 1 del Codice introduce alla disciplina della protezione dei dati personali con un'affermazione categorica e caratterizzante la normativa: i dati personali devono essere sempre tutelati, a prescindere dal trattamento al quale sono sottoposti e dalla natura del soggetto che lo pone in essere (pubblica o privata).

Il Codice individua, poi, una serie di principi generali che devono essere rispettati nell'attività di trattamento e che assumono una particolare rilevanza in quanto costituiscono la **guida interpretativa** di tutte le successive norme.

Innanzitutto il legislatore, in coerenza con l'art. 2 Cost., ha stabilito che il trattamento deve avvenire assicurando **un elevato livello di tutela dei diritti e delle libertà fondamentali**, nonchè della dignità dell'interessato, garantendo, al contempo, il rispetto dei **principi di semplificazione** (inteso come riduzione di adempimenti e snellimento delle procedure), **armonizzazione** (da intendere come omogeneità di tutele rispetto al rango dei diritti da tutelare) ed **efficacia** (nel senso che si deve garantire il più elevato livello di osservanza dei principi che regolano la materia) delle modalità previste per l'esercizio degli stessi diritti da parte degli interessati, nonchè per l'adempimento degli obblighi da parte di chi effettua il trattamento (art. 2 c.d.p.).

3 Il dato personale

Per **dato personale** il codice intende "qualunque informazione" relativa a **persona fisica**, *identificata o identificabile, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale* (quindi, un numero di telefono, un indirizzo,

le impronte digitali o un'immagine o la voce di un soggetto). Il legislatore ha accolto una nozione ampia di dato, rientrando in essa **qualunque informazione** il cui utilizzo può portare alla **identificazione**, anche indiretta, di un soggetto.

È importante ricordare che il dato personale da tutelare può essere anche riferito a persone decedute e non necessariamente deve trattarsi di un dato scritto o testuale, applicandosi la disciplina codicistica, ad esempio, anche al trattamento di fotografie o di videoriprese.

Il legislatore ha individuato diverse categorie di dati.

Innanzitutto, vengono definiti **dati identificativi** quei dati personali che permettono l'*identificazione diretta del soggetto* cui si riferiscono mentre è considerato **dato anonimo** quel dato che *non è collegabile ad alcun soggetto*, perché raccolto in forma anonima fin dall'inizio o per come elaborato a seguito di trattamento.

Il Codice individua, poi, altre tipologie di dato personale che, come si vedrà, rivestono una particolare importanza. E così abbiamo:

- i **dati sensibili** che sono quei dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonchè i dati personali *idonei a rivelare* lo stato di salute e la vita sessuale;
- i **dati giudiziari** che sono quei dati personali idonei a rivelare informazioni personali in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi del codice di procedura penale.

4 Il trattamento dei dati

L'art. 4 del Codice, alla lett. a) del comma 1, definisce il **trattamento** come ***qualunque operazione o complesso di operazioni***, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca di dati.

Anche il compimento di una sola delle operazioni anzidette configura un'ipotesi di trattamento.

Il legislatore ha fissato alcuni principi-guida tesi a far sì che il ***trattamento sia necessario, giustificato e proporzionato***.

Innanzitutto, il **principio di necessità del trattamento**, sancito all'art. 3 del Codice, comporta che i programmi e i sistemi informativi devono essere configurati, già in origine, in modo da **ridurre al minimo l'utilizzazione di dati personali e di dati identificativi;** lo stesso trattamento deve essere escluso se le finalità con lo stesso perseguite possono essere realizzate mediante l'utilizzo di dati anonimi, ovvero di modalità che permettano di identificare l'interessato solo in caso di necessità.

Al trattamento si applicano il **principio di finalità**, sancito dall'art.11, comma 1, lett. b), c.d.p., in base al quale lo stesso è lecito soltanto se fondato su una ragione, ***determinata, esplicita e legittima*** che lo giustifica, ed il **principio di proporzionalità**, sancito dall'art.11, comma 1, lett. d), c.d.p., per cui tutti i dati personali oggetto di trattamento e le modalità del loro trattamento devono essere ***pertinenti, completi e non eccedenti*** rispetto alle finalità per le quali sono raccolti o successivamente trattati (è sproporzionato il trattamento di quei dati che, sulla scorta dello scopo dichiarato, non è necessario trattare).

5 Il Garante per la protezione dei dati personali

Il Codice della privacy attribuisce un ruolo fondamentale al Garante per la protezione dei dati personali, che, mediante l'esercizio dei poteri attribuitigli e agendo come "arbitro" delle situazioni controverse, assicura la corretta applicazione delle relative disposizioni.

Il Garante è un'**autorità amministrativa indipendente**, e, in quanto tale, agisce in piena **autonomia** e con **indipendenza** di giudizio e di valutazione. Il legislatore, infatti, da un lato, ha sottratto il Garante da qualsiasi potere diretto del Governo, e dall'altro lato ha creato un collegamento istituzionale con il Parlamento che si manifesta nella nomina dei componenti e nella relazione annuale che viene presentata dall'autorità per illustrare l'attività svolta.

Il Garante è un **organo collegiale** costituito da quattro componenti, di cui eletti due dalla Camera dei Deputati e due dal Senato della Repubblica, scelti tra persone che assicurino indipendenza di giudizio e che siano esperti di riconosciuta e comprovata competenza nelle materie del diritto o dell'informatica, garantendo al contempo la presenza di entrambe le qualifiche.

Come in ogni organo collegiale, i componenti eleggono nel loro ambito un Presidente, il cui voto nelle deliberazioni prevale in caso di parità, ed eleggono altresì un Vice-presidente, che assume le funzioni del Presidente in caso di assenza o impedimento di quest'ultimo.

Quanto alla durata in carica del Presidente e dei componenti questa è fissata in **sette anni**.

I **compiti principali del Garante** sono individuati dall'**art. 154 del Codice**, e, fatto salvo quanto previsto da specifiche disposizioni, si tratta in particolare di:

- *controllare che i trattamenti di dati personali siano conformi alla disciplina applicabile* e, eventualmente, prescrivere ai titolari o ai responsabili dei trattamenti le misure da adottare per svolgere correttamente il trattamento;
- *esaminare reclami e segnalazioni* nonché *decidere i ricorsi* presentati dagli interessati o dalle associazioni che li rappresentano ai sensi dell'art. 145 del Codice;
- *vietare* in tutto od in parte *il trattamento illecito o non corretto dei dati*, ovvero *disporre il blocco del trattamento* di dati personali, qualora per la loro natura, per le modalità o per gli effetti del loro trattamento possa derivare un rilevante pregiudizio per l'interessato;
- *adottare i provvedimenti previsti dalla normativa* in materia di dati personali (ad esempio, le autorizzazioni generali per il trattamento dei dati sensibili);
- *promuovere la sottoscrizione dei codici di deontologia e di buona condotta* in vari ambiti (credito al consumo, attività giornalistica ecc.);
- *segnalare*, quando ritenuto opportuno, al Parlamento e al Governo *l'opportunità di adottare provvedimenti normativi specifici*, la cui necessità è legata anche all'evoluzione del settore;
- *esprimere i pareri* nei casi previsti, in particolare quando richiesti dal Presidente del Consiglio o da ciascun ministro in ordine a regolamenti ed atti amministrativi suscettibili di incidere sulle materie disciplinate dal Codice.
- *predisporre una relazione annuale* sull'attività svolta e sullo stato di attuazione della normativa sulla *privacy* da trasmettere al Parlamento e al Governo;
- *curare la tenuta del registro dei trattamenti*, formato sulla base delle notificazioni di trattamento ricevute ai sensi dell'art. 37 del Codice;
- *curare l'informazione e la sensibilizzazione dei cittadini* in materia di trattamento dei dati personali, nonché sulle misure di sicurezza dei dati;
- *coinvolgere i cittadini e tutti i soggetti interessati con consultazioni pubbliche* dei cui risultati si tiene conto per la predisposizione di provvedimenti a carattere generale.
- *denunciare i fatti configurabili come reati* perseguibili d'ufficio, dei quali viene a conoscenza nell'esercizio o a causa delle funzioni.

Il Garante svolge altresì la *funzione di controllo e/o assistenza*, in materia di trattamento dei dati personali, prevista da leggi di ratifica di accordi o convenzioni internazionali, o da regolamenti comunitari (ad esempio, la L. 388/1993 di ratifica ed esecuzione dei protocolli e degli accordi di adesione all'accordo di Schengen).

Infine, rilevante è l'*attività di cooperazione* che il Garante svolge con le altre autorità amministrative indipendenti nello svolgimento dei rispettivi compiti (a tale fine, il Garante può invitare rappresentanti di un'altra autorità a partecipare alle proprie riunioni, o essere invitato alle riunioni di altra autorità, partecipando alla discussione di argomenti di comune interesse; ovvero può chiedere la collaborazione di personale specializzato addetto ad altra autorità).

Il legislatore ha attribuito al Garante una serie di **poteri**, che rendono effettivo il delicato ruolo dallo stesso rivestito nel sistema della tutela del diritto alla privacy.

Innanzitutto, viene in rilievo l'art. 157 c.d.p., che disciplina un **potere di vigilanza e controllo** che il Garante esercita principalmente a seguito di segnalazioni da parte di soggetti che ritengono sia avvenuto un trattamento illecito dei propri dati. La norma prevede che il Garante può richiedere ai soggetti coinvolti nel trattamento dei dati — al titolare, al responsabile, all'interessato e anche a terzi — di *fornire informazioni e di esibire documenti*.

Sotto altro punto di vista vengono in rilievo i cd. **accertamenti ispettivi**. Tali accertamenti possono essere realizzati sia sulla base di un programma specifico del Garante, predisposto con cadenza semestrale e che individua i settori nei quali si procederà (cd. *piano ispettivo*), che sulla scorta delle segnalazioni e dei reclami presentati. Essi vengono effettuati, solitamente, anche in collaborazione con le Unità Speciali della Guardia di Finanza - Nucleo Speciale Privacy.

L'art. 158 del Codice prevede che il Garante può disporre — anche in collaborazione con gli organi dello Stato — accessi a banche di dati e/o archivi; ispezioni e verifiche nei luoghi ove si svolge il trattamento o nei quali occorre effettuare rilevazioni comunque utili al controllo del rispetto della disciplina in materia di trattamento dei dati personali.

Quanto ai **poteri sanzionatori** il Codice distingue tra *violazioni amministrative* delle norme e *illeciti penali* commessi in relazione al trattamento dei dati. Quanto al primo aspetto, a titolo di esempio, si ricorda la previsione dell'art. 161 del Codice relativo che sanziona la violazione di quanto disposto dal precedente art. 13: si tratta del caso di omissione o inidoneità dell'informativa che deve essere resa all'interessato in ordine al trattamento dei propri dati personali, al fine di ottenere il consenso allo stesso. La sanzione pecuniaria che può essere irrogata in tale ipotesi varia da *un minimo di seimila euro ad un massimo di trentaseimila euro*.

6 Titolare, responsabile e incaricato

Il titolare è **colui che effettua il trattamento** e che ha potere decisionale autonomo in ordine alle finalità, alle modalità del trattamento dei dati personali e agli strumenti da utilizzare, compreso il profilo della sicurezza.

Il titolare può essere una *persona fisica* ma anche una *persona giuridica*, "*la pubblica amministrazione e qualsiasi altro ente, associazione od organismo*". In quest'ultima ipotesi, il titolare del trattamento è identificato **nell'entità nel suo complesso** ovvero nell'unità o nell'organismo periferico che esercita il potere decisionale.

Il titolare del trattamento può nominare un **responsabile del trattamento** dei dati, attribuendogli una serie di compiti analiticamente determinati, per iscritto, nell'atto di nomina.

La nomina del responsabile è facoltativa — per cui si tratta di un **soggetto eventuale** — e l'incarico può essere attribuito ad una *persona fisica*, ad una *persona giuridica*, alla *pubblica amministrazione* e a *qualsiasi altro ente, associazione od organismo* (art. 4, comma 1, lett. g), c.d.p.).

Il responsabile effettua il trattamento attenendosi alle istruzioni impartite dal titolare il quale, anche tramite verifiche periodiche, vigila sulla puntuale osservanza delle disposizioni in mate-

ria di *privacy* e delle istruzioni che ha impartito. Il responsabile del trattamento deve godere di un'esperienza, di una capacità e di una affidabilità tali da soddisfare le esigenze di pieno rispetto delle vigenti disposizioni in materia e se le necessità organizzative lo richiedano, il titolare può designare come responsabili *più soggetti*, provvedendo anche alla suddivisione dei compiti.

Se è facoltà del titolare nominare un responsabile del trattamento, indispensabile è l'esatta individuazione degli **incaricati del trattamento**, ossia delle *persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile* (art. 4, comma 1, lett. h), c.d.p.).

Mentre il titolare ed il responsabile possono essere indistintamente persone fisiche, persone giuridiche e pubbliche amministrazioni, gli incaricati, dovendo compiere effettivamente e concretamente le operazioni (es. gli impiegati di un ufficio) possono essere solo persone fisiche.

Le operazioni di trattamento possono essere effettuate solo da incaricati che operano sotto la *diretta autorità* del titolare o del responsabile, attenendosi alle istruzioni impartite, e la cui designazione sia stata effettuata per iscritto con puntuale individuazione dell'ambito del trattamento consentito.

La designazione è comunque valida quando, pur non essendo espressa e specifica per la singola persona, consiste nella documentata preposizione della persona fisica ad una unità organizzativa per la quale sia già stato individuato, per iscritto, l'ambito del trattamento consentito agli addetti preposti alla stessa.

7 L'interessato

I dati personali che possono essere oggetto di trattamento, inevitabilmente, appartengono ad una persona che il legislatore definisce **interessato**; l'art. 4, comma 1, lett. i) del Codice, infatti, con tale termine individua "*la persona fisica, cui si riferiscono i dati personali*".

Il Codice dedica molta attenzione all'interessato, che, quale *dominus* del dato personale, ha il potere di incidere sul trattamento da realizzare, attraverso l'esercizio di una serie di pretese, riconosciutegli dal legislatore in conformità alla previsione dell'art. 2 del Codice, che può esercitare nei confronti di chi tratta dati che lo riguardano.

In particolare, il Titolo II della Parte Prima del Codice è dedicata ai **diritti dell'interessato** e si apre, all'art. 7 del Codice, con la previsione analitica degli stessi, riconducibili, sostanzialmente, al diritto di ottenere una vasta gamma di informazioni relative ai propri dati, di chiedere ed ottenere il loro aggiornamento, la loro rettifica e/o cancellazione e di opporsi al relativo trattamento.

Specificamente, l'art. 7 c.d.p. individua i diritti in questione e stabilisce innanzitutto che l'interessato ha diritto ad ottenere la ***conferma dell'esistenza o meno di dati personali che lo riguardano***, anche se non ancora registrati, e la loro comunicazione in forma intelligibile. Inoltre, ha il diritto di ottenere l'indicazione:

- dell'origine dei propri dati personali;
- delle finalità e delle modalità del loro trattamento;
- della logica applicata al trattamento effettuato con strumenti elettronici;
- degli estremi identificativi del titolare, dei responsabili e del rappresentante designato a norma di legge;
- dei soggetti o delle categorie ai quali i dati personali possono essere comunicati.

Inoltre, è riconosciuto all'interessato il diritto ad ottenere: **l'aggiornamento, la rettificazione** ovvero, quando vi ha interesse, **l'integrazione dei dati**; **la cancellazione**, **la trasformazione** in forma anonima ovvero **il blocco** (inteso come "la conservazione di dati personali con sospensione temporanea di ogni altra operazione del trattamento") del trattamento, quando esso avvenga in violazione di legge; **una precisa e puntuale attestazione** che le operazioni citate siano state

portate a conoscenza dei soggetti ai quali i dati sono stati comunicati o diffusi, eccetto il caso in cui tale adempimento sia impossibile o comporti un impiego di mezzi manifestamente sproporzionato rispetto al diritto tutelato.

L'interessato, infine, ha il **diritto di opporsi**, in tutto o in parte, purchè per motivi legittimi, al trattamento dei dati personali che lo riguardano ancorchè pertinenti allo scopo della raccolta, e al trattamento finalizzato all'invio di materiale pubblicitario o di vendita diretta, ovvero per il compimento di ricerche di mercato o di comunicazioni commerciali.

Per l'esercizio dei propri diritti, il legislatore non richiede particolari formalità: è sufficiente presentare una **richiesta**, che deve essere idoneamente riscontrata, senza ritardo, dal chi effettua il trattamento.

La richiesta può essere presentata mediante *lettera raccomandata*, *telefax* o *posta elettronica* ovvero mediante *ulteriori soluzioni tecnologiche*, che non sono direttamente indicate dal legislatore ma rimesse all'individuazione del Garante.

Nell'esercizio dei propri diritti, l'interessato può conferire, per iscritto, **delega o procura** a persone fisiche, enti, associazioni od organismi, ovvero farsi **assistere da una persona di fiducia**. Inoltre, il legislatore riconosce la possibilità di esercitare i diritti di un defunto riconoscendo una legittimazione attiva solo a chi abbia "un interesse proprio, o agisce a tutela dell'interessato o per ragioni familiari meritevoli di protezione".

Si è detto che la richiesta deve essere riscontrata. A tal fine, l'art. 10 del Codice, disciplina le modalità in cui è possibile evadere una richiesta.

Innanzitutto, il legislatore impone al titolare del trattamento l'obbligo di agevolare l'accesso ai dati personali da parte dell'interessato e l'obbligo di semplificare le modalità e ridurre i tempi per effettuare il riscontro al richiedente, anche nell'ambito di uffici o servizi preposti alle relazioni con il pubblico.

Salvo che la richiesta sia circoscritta, il riscontro alla stessa comprende tutti i dati personali che riguardano l'interessato, comunque trattati dal titolare.

I dati sono **estratti** (dal responsabile o dall'incaricato) e possono essere **comunicati al richiedente** anche oralmente, ovvero **offerti in visione** mediante strumenti elettronici, sempre che la loro comprensione sia agevole, considerata anche la qualità e la quantità delle informazioni. Se vi è richiesta, si provvede alla **trasposizione dei dati su supporto cartaceo o informatico**, ovvero alla loro **trasmissione per via telematica**.

L'effettività della tutela degli interessati, infine, è garantita anche dall'obbligo di comunicare i dati **in forma intelligibile** — anche attraverso l'uso di una grafia comprensibile — e, nell'ipotesi di comunicazione di codici o sigle, mediante l'utilizzo di parametri per la comprensione del relativo significato.

È molto importante ricordare che il riscontro alle richieste di accesso dell'interessato deve essere effettuato "senza ritardo" (*ex* art. 8, comma 1, c.d.p.) e comunque entro e non oltre 15 giorni dal ricevimento della richiesta, altrimenti il titolare si espone al rischio di possibili azioni avanti al Garante (*ex* art. 146 c.d.p.).

8 Gli adempimenti e le regole per tutti i trattamenti

Il Capo I della Parte Prima del Codice contiene disposizioni (artt. da 11 a 17) che definiscono delle **regole generali**, applicabili a *tutti i tipi* di trattamento, che devono essere rispettate da **qualsiasi titolare**, a prescindere dalla natura giuridica — pubblica o privata — dello stesso, per garantire la legittimità del suo operato.

L'art. 11 del Codice è infatti una norma di fondamentale importanza per comprendere quando un trattamento può dirsi legittimo, in quanto contiene disposizioni incentrate ad individuare *i requisiti dei dati personali* e *le modalità con cui devono essere trattati*.

I dati personali oggetto di trattamento devono essere:

a) trattati in ***modo lecito e secondo correttezza***;
b) raccolti e registrati per ***scopi determinati, espliciti e legittimi***, ed utilizzati in altre operazioni del trattamento in termini compatibili con tali scopi;
c) ***esatti*** e, se necessario, aggiornati;
d) ***pertinenti, completi e non eccedenti*** rispetto alle finalità per le quali sono raccolti o successivamente trattati;
e) ***conservati in una forma che consenta l'identificazione dell'interessato*** per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati.

Inoltre, è sanzionata con l'**inutilizzabilità dei dati trattati** la violazione della disciplina rilevante in materia di trattamento dei dati personali.

a) L'informativa

Il titolare del trattamento ha l'obbligo di fornire all'interessato una ***comunicazione***, resa oralmente o per iscritto, con la quale quest'ultimo viene portato a conoscenza di una serie di notizie circa il trattamento al quale saranno sottoposti i propri dati. Si tratta della cd. **informativa**.

L'art. 13 del Codice dispone che ad ogni interessato è riconosciuto **il diritto all'informativa,** cioè **il diritto ad essere informato, prima del trattamento**, circa:

- le **finalità** e le **modalità** del trattamento cui sono destinati i dati;
- la **natura obbligatoria** o **facoltativa** del conferimento dei dati;
- le conseguenze di un eventuale **rifiuto di rispondere** ad una richiesta di dati personali;
- i soggetti o le categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di responsabili o incaricati, e l'ambito di diffusione dei dati medesimi;
- i diritti dell'interessato, di cui all'art. 7 del Codice;
- gli **estremi identificativi del titolare** e, se designati, del r**appresentante** nel territorio dello Stato, ai sensi dell'art. 5, e **del responsabile**. Quando il titolare ha designato più responsabili è indicato almeno uno di essi, indicando il sito della rete di comunicazione o le modalità attraverso le quali è conoscibile in modo agevole l'elenco aggiornato dei responsabili; quando è stato designato un responsabile per il riscontro all'interessato in caso di esercizio dei diritti riconosciutigli dall'art. 7, è indicato anche tale responsabile.

Sempre con riferimento al contenuto, l'informativa **può non includere gli elementi già noti** alla persona che fornisce i dati o la cui conoscenza può ostacolare in concreto l'espletamento, da parte di un soggetto pubblico, di funzioni ispettive o di controllo svolte per finalità di difesa o sicurezza dello Stato oppure di prevenzione, accertamento o repressione di reati.

Il Codice precisa anche che se i dati personali *non sono raccolti* presso l'interessato, l'informativa, comprensiva delle categorie di dati trattati, è data al medesimo interessato all'atto della registrazione dei dati o, quando è prevista la loro comunicazione, non oltre la prima comunicazione: tali previsioni non si applicano quando il trattamento avvenga obbligatoriamente per espressa previsione di una norma di legge (nazionale o comunitaria) ovvero di regolamento; quando è finalizzato all'esercizio delle indagini difensive, o, comunque, per far valere o difendere un diritto in sede giudiziaria (sempre che i dati siano trattati esclusivamente per tali finalità e per il periodo strettamente necessario al loro perseguimento); ovvero, infine, quando l'informativa stessa, a giudizio del Garante, comporti un dispendio di mezzi eccessivamente oneroso e sproporzionato rispetto al diritto tutelato oppure si riveli impossibile.

b) La notificazione

La notificazione è l'atto con cui il titolare nei casi previsti dalla legge comunica al Garante i trattamenti di dati personali ai quali intende procedere, comunicandogli le caratteristiche principali dello stesso.

A norma dell'art. 37 c.d.p., il titolare è tenuto ad effettuare la notificazione al Garante ***solo quando*** il trattamento cui intende procedere riguardi particolari tipi di dati, e specificamente:

a) **dati genetici, biometrici o dati che indicano la posizione geografica di persone od oggetti** mediante una rete di comunicazione elettronica;
b) **dati idonei a rivelare lo stato di salute e la vita sessuale**, trattati a fini di *procreazione assistita*, *prestazione di servizi sanitari* per via telematica relativi a banche di dati o alla *fornitura di beni*, *indagini epidemiologiche*, rilevazione di *malattie mentali, infettive e diffusive*, *sieropositività*, *trapianto di organi e tessuti* e monitoraggio della *spesa sanitaria*;
c) **dati idonei a rivelare la vita sessuale o la sfera psichica** trattati da associazioni, enti od organismi senza scopo di lucro, anche non riconosciuti, a carattere politico, filosofico, religioso o sindacale;
d) **dati trattati con l'ausilio di strumenti elettronici** volti a definire *il profilo o la personalità dell'interessato*, ovvero ad analizzare *abitudini o scelte di consumo*, ovvero a monitorare *l'utilizzo di servizi di comunicazione elettronica*, con esclusione dei trattamenti tecnicamente indispensabili per fornire i servizi medesimi agli utenti;
e) **dati sensibili registrati in banche di dati** a fini di *selezione del personale per conto terzi*, nonchè dati sensibili utilizzati per *sondaggi di opinione*, *ricerche di mercato* e altre ricerche campionarie;
f) **dati registrati in apposite banche di dati** gestite con strumenti elettronici e relative al *rischio sulla solvibilità economica*, alla *situazione patrimoniale*, al *corretto adempimento di obbligazioni*, a *comportamenti illeciti o fraudolenti*.

La notificazione al Garante, deve essere effettuata con **unico atto** anche quando il trattamento comporta il trasferimento dei dati all'estero.

Le notificazioni ricevute vengono inserite dal Garante in un ***registro dei trattamenti*** accessibile a chiunque secondo modalità, determinate dall'autorità stessa, che garantiscono una *consultazione gratuita per via telematica*, anche mediante convenzioni con soggetti pubblici o presso il proprio Ufficio. Le notizie accessibili tramite la consultazione del registro possono essere trattate esclusivamente per finalità di applicazione della disciplina in materia di protezione dei dati personali.

Quanto alla **procedura** da seguire per adempiere all'obbligo di notificazione, questa è regolamentata dall'art. 38 del Codice che prevede una serie di formalità piuttosto semplici da adempiere.

La notificazione del trattamento, infatti, deve **essere presentata al Garante prima dell'inizio del trattamento stesso ed una sola volta** a prescindere dal numero delle operazioni e dalla durata del trattamento da effettuare, e può riguardare uno o più trattamenti con finalità correlate.

Una nuova notificazione è richiesta solo anteriormente alla cessazione del trattamento o al mutamento di taluno degli elementi da indicare nella notificazione medesima.

Risponde all'esigenza di attuare il *principio di trasparenza* nel trattamento dei dati, la norma di chiusura di cui all'art. 38, comma 6, c.d.p., secondo la quale il titolare del trattamento che non è tenuto alla notificazione al Garante, è comunque obbligato a fornire le notizie contenute nel modello citato *a chi ne fa richiesta*, salvo che il trattamento riguardi pubblici registri, elenchi, atti o documenti conoscibili da chiunque.

c) L'autorizzazione

Il Codice della privacy prevede due diverse tipologie di autorizzazioni che possono essere rilasciate dal Garante: le cd. **autorizzazioni generali**, disciplinate dall'art. 40 c.d.p., e le **autorizzazioni specifiche** di cui al successivo art. 41 c.d.p.

L'art. 40 c.d.p. stabilisce che laddove il Codice richieda per il trattamento dei dati un'autorizzazione del Garante — per il trattamento di *dati sensibili* è richiesta dall'art. 26 c.d.p. mentre per quello dei *dati giudiziari* è necessario fare riferimento all'art. 27 c.d.p. — questa può essere rilasciata "collettivamente", facendo riferimento a determinate categorie di titolari o di trattamenti. In tal caso, si ha un'***autorizzazione generale*** — in quanto la stessa riguarda **determinati settori** — che individua il proprio ambito soggettivo ed oggettivo di operatività.

Essa infatti, si applica a **determinate categorie di soggetti e di dati personali** precisamente individuati e indica le *finalità del trattamento* e i *principali obblighi* da rispettare, stabilisce *i tempi massimi di conservazione* dei dati stessi e le *condizioni alle quali può procedersi alla divulgazione* a terzi delle informazioni raccolte e trattate.

Tali autorizzazioni sono pubblicate nella Gazzetta Ufficiale della Repubblica italiana.

9 La sicurezza dei sistemi informativi e le misure minime di sicurezza

a) La sicurezza dei sistemi informativi

Alla sicurezza dei dati e dei sistemi è dedicato il Capo I del Titolo V della Parte I del Codice, che impone al titolare dei generali obblighi di sicurezza a tutela dei dati raccolti e trattati.

L'art. 31 del Codice stabilisce che i dati personali oggetto di trattamento devono essere custoditi e controllati adottando tutte quelle regole tecniche e quegli accorgimenti (e, cioè, attraverso idonee e preventive misure di sicurezza) — anche in relazione alle conoscenze acquisite nel tempo in base al progresso tecnico — che ne assicurino in ogni momento l'integrità, preservandoli cioè da fenomeni di distruzione, perdita (anche accidentale), accesso non autorizzato, ovvero dal trattamento non consentito.

b) Le misure minime di sicurezza

Anche il Capo II del Titolo V della Parte prima del Codice è dedicato alla sicurezza e contiene una serie di disposizioni che, inserendosi nel quadro generale degli obblighi di sicurezza, impongono ai titolari del trattamento di adottare misure cd. minime, cioè volte ad assicurare un livello minimo di protezione dei dati personali. Si tratta, in sostanza, di "misure di accortezza" non derogabili *in peius*, ma da assumersi quale parametro base per ogni attività di raccolta e trattamento dei dati personali.

Peraltro, a riprova di quanto sia fondamentale il tema della sicurezza, nell'allegato B del Codice si trova un utile e completo "Disciplinare tecnico in materia di misure minime di sicurezza", in cui possono rinvenirsi le *regole tecniche* da seguire avuto riguardo al trattamento effettuato sia con strumenti elettronici sia senza l'ausilio di tali supporti.

L'art. 34 del Codice individua le misure minime di sicurezza che devono essere adottate per far sì che un **trattamento effettuato con strumenti elettronici** possa considerarsi lecito.

Quando, invece, il **trattamento è eseguito senza l'ausilio di strumenti elettronici** le misure minime di sicurezza da adottare sono di minore incidenza e comunque riconducibili, almeno: all'aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unità organizzative; alla previsione di procedure per un'idonea custodia degli atti e dei documenti affidati agli incaricati per lo svolgimento dei relativi compiti; alla previsione di

procedure per la conservazione degli atti in archivi il cui accesso deve essere riservato e possibile solo ad una cerchia selezionata di persone anche grazie ad una disciplina *ad hoc* che fissa le modalità di accesso ed è quindi finalizzata all'identificazione degli incaricati.

10 Trattamenti illeciti e risarcimento del danno

L'art. 15 del Codice dispone che i danni cagionati da un trattamento illecito di dati personali devono essere risarciti secondo le modalità prescritte dall'art. 2050 c.c.; è incluso l'obbligo di ristorare la parte danneggiata anche del danno non patrimoniale.

Circa la natura del danno, il legislatore espressamente riconosce tutela anche al danno non patrimoniale, ovvero a tutte quelle situazioni in cui, pur non essendosi verificata in capo all'interessato una *deminutio patrimonii*, tuttavia, allo stesso sono derivate conseguenze negative di altro tipo.

11 La cessazione del trattamento e il trattamento che presenta rischi specifici

L'art. 16 del Codice prevede che, quando per una qualsiasi causa, si giunga alla cessazione del trattamento dei dati, gli stessi possono essere alternativamente:

a) *distrutti*;
b) *ceduti ad un altro titolare*, purchè destinati ad essere trattati in termini compatibili con gli scopi per i quali erano stati raccolti;
c) *conservati per fini esclusivamente personali*;
d) *conservati o ceduti ad altro titolare solo per scopi storici, statistici o scientifici*, in conformità alle previsioni di legge.

Il successivo art. 17 disciplina il trattamento di dati che presenta rischi specifici. Circoscrive la portata della disposizione l'individuazione dei dati ai quali si applica: si tratta di dati comuni — la norma parla di dati *diversi da quelli sensibili e giudiziari* — il cui trattamento presenta **rischi specifici** per *i diritti e le libertà fondamentali*, nonchè per *la dignità dell'interessato*, in relazione alla natura dei dati o alle modalità del trattamento o agli effetti che può determinare. Al di là delle difficoltà legate all'esatta individuazione di tali dati, il loro **trattamento è ammesso solo nel rispetto di misure ed accorgimenti a garanzia dell'interessato**, ove prescritti.

Tali accorgimenti sono stabiliti dal Garante, in applicazione dei principi sanciti dal Codice, nell'ambito di una *verifica preliminare all'inizio del trattamento*, effettuata anche in relazione a determinate categorie di titolari o di trattamenti, ovvero *anche a seguito di un interpello del titolare*.

12 Il trattamento effettuato da privati o da enti pubblici economici

Il Capo III della Parte Prima del Codice, contenente le regole specifiche per il trattamento effettuato da privati ed enti pubblici economici, si apre con l'imposizione al titolare di uno specifico adempimento preliminare nei confronti dell'interessato: l'art. 23 del Codice, infatti, espressamente *subordina il trattamento al rilascio del consenso allo stesso da parte dell'interessato*.

Il ***consenso espresso*** dell'interessato, che può riguardare l'intero trattamento ovvero essere circoscritto ad una o più operazioni dello stesso, è validamente prestato *solo se* presenta i seguenti *requisiti*:

— deve essere stato **espresso liberamente e specificamente** in riferimento ad un trattamento chiaramente individuato;

- deve essere **documentato per iscritto;**
- deve essere stata **fornita all'interessato l'informativa**, con tutte le informazioni di cui all'art.13 c.d.p.

Per quanto riguarda la *forma* con la quale deve essere manifestato il consenso, il legislatore, al comma 4 della disposizione (poi ripreso dal successivo art. 26 del Codice), stabilisce che essa deve necessariamente essere **scritta** solo quando il trattamento riguarda **dati sensibili**.

13 Il divieto di comunicazione e diffusione dei dati raccolti

Per **comunicazione** di dati personali si intende il dare conoscenza degli stessi a uno o più **soggetti determinati** diversi dall'interessato, dal rappresentante del titolare nel territorio dello Stato, dal responsabile e dagli incaricati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione. Si ha, invece, **diffusione** se i terzi non sono determinati: "diffondere", infatti, va inteso nel senso di **dare conoscenza di dati personali a soggetti indeterminati**, in qualunque forma, anche mediante la loro messa a disposizione o comunicazione.

Il legislatore, pur sancendo un **generale divieto di comunicazione e diffusione dei dati raccolti**, non ha generalizzato la sua portata.

L'art. 25 del Codice, infatti, stabilisce che, oltre alle ipotesi di *divieto disposto dal Garante o dall'autorità giudiziaria*, la comunicazione e la diffusione sono vietate:

a) *in riferimento a dati personali dei quali è stata ordinata la cancellazione*, ovvero quando *è decorso il periodo di tempo necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati* ai sensi dell'art. 11, comma 1, lett. e), c.d.p.;
b) *per finalità diverse da quelle indicate nella notificazione del trattamento*, ove prescritta.

Al di fuori di queste ipotesi, il legislatore fa salve la comunicazione o la diffusione di dati laddove richieste da forze di polizia, dall'autorità giudiziaria, da organismi di informazione e sicurezza o da altri soggetti pubblici per finalità di difesa o di sicurezza dello Stato o di prevenzione, accertamento o repressione di reati.

14 Il trattamento dei dati sensibili effettuato da privati e da enti pubblici economici

L'art. 26 del Codice della privacy detta disposizioni volte ad assicurare che il trattamento dei dati sensibili avvenga secondo garanzie connesse alla particolare natura degli stessi.

Innanzitutto, il primo comma della norma si apre con la previsione secondo la quale il trattamento dei dati sensibili — che deve avvenire nell'osservanza dei presupposti e dei limiti stabiliti dal Codice, dalla legge e dai regolamenti — per poter essere realizzato necessita:

a) del **consenso scritto dell'interessato**
b) della **previa autorizzazione del Garante**, che deve essere rilasciata entro 45 giorni dalla richiesta.

Tale previsione non trova applicazione, ai sensi del comma 3 della norma, con riferimento al trattamento:

a) dei dati relativi agli aderenti alle confessioni religiose e ai soggetti che, per finalità religiose, hanno contatti regolari con le medesime confessioni, effettuato dai relativi organi ovvero da enti civilmente riconosciuti;

b) dei dati riguardanti l'adesione di associazioni od organizzazioni a carattere sindacale o di categoria ad altre associazioni, organizzazioni o confederazioni a carattere sindacale o di categoria;
c) dei dati contenuti nei *curricula*, spontaneamente trasmessi dagli interessati ai fini dell'eventuale instaurazione di un rapporto di lavoro.

Il legislatore dedica il quarto comma della disposizione all'individuazione dei casi in cui, pur venendo in rilievo dati sensibili, il relativo trattamento *non necessita del consenso dell'interessato* ma *solo della previa autorizzazione del Garante*. Si tratta dei casi in cui:

a) il trattamento è effettuato da associazioni, enti od organismi senza scopo di lucro, anche non riconosciuti, a carattere politico, filosofico, religioso o sindacale, ivi compresi partiti e movimenti politici, per il perseguimento di scopi determinati e legittimi, relativamente ai dati personali degli aderenti o dei soggetti che hanno contatti regolari con l'associazione, ente od organismo;
b) il trattamento è necessario per la salvaguardia della vita o dell'incolumità fisica di un terzo;
c) il trattamento è necessario per lo svolgimento delle investigazioni difensive o, comunque, per far valere o difendere in sede giudiziaria un diritto, sempre che i dati siano trattati esclusivamente per tali finalità e per il periodo strettamente necessario al loro perseguimento. Se i dati sono idonei a rivelare lo stato di salute e la vita sessuale, il diritto deve essere di rango pari a quello dell'interessato, ovvero consistente in un diritto della personalità o in un altro diritto o libertà fondamentale e inviolabile;
d) il trattamento è necessario per adempiere a specifici obblighi o compiti previsti dalla legge, da un regolamento o dalla normativa comunitaria per la gestione del rapporto di lavoro, anche in materia di igiene e sicurezza del lavoro e della popolazione e di previdenza e assistenza.

In ogni caso è fatto divieto di diffondere i dati idonei a rivelare lo stato di salute, ossia di dare conoscenza degli stessi a soggetti indeterminati, in qualunque forma, anche mediante la messa a disposizione o consultazione.

15 I principi applicabili al trattamento effettuato da un soggetto pubblico

Come si è già avuto modo di precisare, mentre le disposizioni del Capo I della Parte Prima del Codice della privacy si applicano a tutti i soggetti che effettuano un trattamento, a prescindere dalla natura giuridica del titolare, quelle contenute nel Capo II (artt. 18-22) si applicano **solo ai soggetti pubblici**, esclusi gli enti pubblici economici.

Il Capo in questione si apre con una disposizione – l'art. 28 c.d.p. – che, dettando principi generali, ha una portata onnicomprensiva: essa, infatti, interessa qualsivoglia tipologia di dato (non operando alcuna distinzione) e qualsiasi tipologia di trattamento.

La norma introduce due regole fondamentali:

a) *la strumentalità del trattamento rispetto al perseguimento dei fini istituzionali dell'ente*: il soggetto pubblico, cioè può trattare i dati personali (di qualsiasi natura) **soltanto per lo svolgimento delle funzioni istituzionali**. In ogni caso il trattamento deve avvenire nel rispetto dei presupposti e dei limiti fissati dallo stesso Codice, anche in relazione alla diversa natura dei dati, dalla legge e dai regolamenti;
b) *il divieto di acquisire il consenso dell'interessato al trattamento*: la più importante distinzione rispetto alla disciplina prevista per i privati e gli enti pubblici economici è rappresentata proprio dal fatto che i soggetti pubblici per effettuare il trattamento "**non devono richiedere il**

consenso dell'interessato". Tale regola non trova applicazione per gli esercenti le professioni sanitarie e gli organismi sanitari pubblici.

16 Il trattamento dei dati personali comuni

Il trattamento dei "*dati diversi da quelli sensibili e giudiziari*" è consentito **anche in mancanza di una norma di legge o di regolamento** che espressamente lo contempli, sempreché lo stesso sia effettuato **perseguendo finalità istituzionali**, secondo la regola generale di cui al precedente art. 18, comma 2, c.d.p.

Il trattamento di tale tipologia di dati pone soprattutto una questione di **disciplina della comunicazione e della diffusione** degli stessi, considerato che quando il *titolare del trattamento* è una *pubblica amministrazione* esso deve essere identificato con "l'entità nel suo complesso o l'unità od organismo periferico che esercita un potere decisionale del tutto autonomo sulle finalità e sulle modalità del trattamento" (art. 28 c.d.p.): nell'esercizio dell'attività amministrativa, infatti, capita di frequente che i dati personali dell'interessato alla stessa debbano essere trasmessi ad altro ufficio della stessa P.A. oppure ad altro soggetto pubblico (ad esempio per l'acquisizione di un parere).

La **comunicazione di dati personali "comuni" da parte di un soggetto pubblico ad un altro soggetto pubblico** è agevolata dal legislatore che la considera lecita se *prevista da una norma di legge o di regolamento* ovvero, in mancanza, se *necessaria per lo svolgimento di funzioni istituzionali*, e può essere iniziata solo se è decorso il termine di quarantacinque giorni dal ricevimento della comunicazione al Garante prevista dall'art. 39 del Codice, salvo diversa determinazione, anche successiva, dello stesso Garante.

La **comunicazione di dati personali "comuni" da parte di un soggetto pubblico a privati o a enti pubblici economici e la diffusione degli stessi** da parte di un soggetto pubblico sono intese in senso più restrittivo in quanto sono *ammesse esclusivamente sulla base di una norma di legge o di un regolamento*.

17 Il trattamento dei dati personali sensibili

A differenza di quanto stabilito per i dati comuni, il cui trattamento è considerato lecito col solo richiamo alle funzioni istituzionali della pubblica amministrazione, per il trattamento dei dati sensibili da parte dei soggetti pubblici il legislatore richiede una più analitica copertura normativa.

L'art. 20 del Codice della privacy dispone, infatti, che il trattamento di dati sensibili da parte di soggetti pubblici è consentito solo se **autorizzato da espressa disposizione di legge (e non anche di regolamento come richiesto per il trattamento dei dati comuni),** che specifichi:

- le *tipologie di dati* che possono essere trattati (ad es. quello sanitario, quello attinente all'orientamento politico ecc.)
- le *operazioni eseguibili* (ad es. conservazione, elaborazione, comunicazione ecc.)
- le *finalità di rilevante interesse pubblico* perseguite.

Ai sensi del Codice rientrano tra le finalità di rilevante interesse pubblico:

- l'applicazione della disciplina **del diritto di accesso** agli atti amministrativi (art. 59 c.d.p.);
- la **tenuta** degli **atti e dei registri dello stato civile, delle anagrafi e delle liste elettorali** (art. 62 c.d.p.);
- l'applicazione della disciplina in materia di **cittadinanza**, **immigrazione** e **condizione dello straniero** (art. 64 c.d.p.);

- l'applicazione della disciplina in materia di **elettorato attivo e passivo** e di **esercizio dei diritti politici** nonché della pubblicità dell'attività di organi pubblici (art. 65 c.d.p.);
- l'applicazione della disciplina in materia **tributaria e doganale** (art. 66 c.d.p.);
- l'applicazione della disciplina in materia di **attività di controllo e ispettive** (art. 67 c.d.p.);
- l'applicazione della disciplina in materia di **concessione di benefici e abilitazioni** (art. 68 c.d.p.);
- l'applicazione della disciplina in materia di **conferimento di onorificenze, ricompense e riconoscimenti** (art. 69 c.d.p.);
- l'applicazione della disciplina in materia di **rapporti tra soggetti pubblici e organizzazioni di volontariato e di obiezione di coscienza** (art. 70 c.d.p.);
- l'applicazione della disciplina in materia **di sanzioni amministrative e ricorsi** nonché quella volta a far valere il **diritto di difesa in sede amministrativa o giudiziaria** (art. 71 c.d.p.);
- lo svolgimento dei **rapporti istituzionali con enti di culto e confessioni o comunità religiose** (art. 72 c.d.p.);
- le finalità **assistenziali e sociali** (art. 73 c.d.p.);
- le finalità del SSN e degli altri **servizi sanitari pubblici** (art. 85 c.d.p.);
- attività amministrative per l'applicazione della disciplina sulla **tutela sociale della maternità e di interruzione della gravidanza, di stupefacenti e sostanze psicotrope, di assistenza, integrazione sociale e diritti degli handicappati** (art. 86 c.d.p.);
- l'istruzione in ambito scolastico, professionale, superiore o universitario (art. 95 c.d.p.);
- le finalità relative ai trattamenti effettuati per **scopi storici**, a quelli effettuati dai soggetti pubblici che fanno parte del **sistema statistico nazionale SISTAN**, ai sensi del D. Lgs. 322/1989, ed a quei trattamenti effettuati per **scopi scientifici** (art. 98 c.d.p.);
- l'instaurazione e la gestione da parte di soggetti pubblici di **rapporti di lavoro di qualunque tipo**, dipendente o autonomo, anche non retribuito o onorario o a tempo parziale o temporaneo, e di altre forme di impiego che non comportano la costituzione di un rapporto di lavoro subordinato (art. 112 c.d.p.).

Qualora la legge precisi la rilevante finalità di interesse pubblico da perseguire ma *non menzioni le categorie di dati sensibili e le operazioni eseguibili*, il trattamento è ammesso solo in riferimento ai tipi di dati e di operazioni identificati e resi pubblici **con atto di natura regolamentare** adottato in conformità al parere espresso dal Garante, ai sensi dell'art. 154, comma 1, lett. *g)*, c.d.p., anche sulla base di **schemi tipo.**

L'atto di natura regolamentare deve essere emanato dai soggetti che effettuano il trattamento, in relazione alle specifiche finalità perseguite nei singoli casi.

Se, invece, il trattamento non è previsto espressamente da una disposizione di legge, i soggetti pubblici possono **chiedere al Garante di individuare le attività**, tra quelle agli stessi demandate dalla legge, che perseguono finalità di rilevante interesse pubblico e per le quali il trattamento è conseguentemente autorizzato. Il trattamento è consentito solo se il soggetto pubblico provvede altresì a identificare e rendere pubblici i tipi di dati e di operazioni secondo le modalità anzidette.

In ogni caso quando il titolare provvede all'identificazione delle classi di dati e di operazioni, questa deve deve essere periodicamente aggiornata e integrata.

18 La tutela della privacy in ambito sanitario

L'infermiere è tenuto al **segreto d'ufficio** se pubblico impiegato e al **segreto professionale** se libero professionista.

Per i **pubblici impiegati** l'obbligo del segreto è **previsto dal contratto collettivo** e da una specifica norma di legge, l'articolo 28 della legge n. 241 del 1990 che ha sostituito l'articolo 15

del D.P.R. 3/1957, che ora testualmente recita: «L'impiegato deve mantenere il segreto d'ufficio. Non può trasmettere a chi non ne abbia diritto informazioni riguardanti provvedimenti od operazioni amministrative, in corso o in conclusione, ovvero notizie di cui sia venuto a conoscenza a causa delle sue funzioni, al di fuori delle ipotesi e delle modalità previste dalle norme sul diritto di accesso. Nell'ambito delle proprie attribuzioni, l'impiegato preposto ad un ufficio rilascia copie ed estratti di atti e documenti di ufficio nei casi non vietati dall'ordinamento». Per i liberi professionisti, invece, l'obbligo del segreto professionale è previsto direttamente dal **codice penale che include tra le categorie gravate dall'obbligo anche i medici e i loro ausiliari.**

Il **dovere al segreto per tutti gli infermieri** è, infine, ribadito anche dal **codice deontologico della categoria**, l'art. 28 del quale stabilisce che «L'infermiere rispetta il segreto professionale non solo per obbligo giuridico, ma per intima convinzione e come espressione concreta del rapporto di fiducia con l'assistito».

Il dovere del segreto si sovrappone al dovere di tutelare la riservatezza (privacy) della persona ricoverata come previsto dal Codice in materia di protezione dei dati personali; il codice di deontologia degli infermieri, infatti, ribadisce che «L'infermiere assicura e tutela la riservatezza nel trattamento dei dati relativi all'assistito. Nella raccolta, nella gestione e nel passaggio di dati, si limita a ciò che è attinente all'assistenza».

Le norme del Codice in materia di protezione dei dati personali trovano applicazione anche in un ambito come quello sanitario: è evidente, infatti, che alle persone che entrano in contatto con medici e strutture sanitarie per cure e prestazioni mediche **bisogna garantire la più assoluta riservatezza e il rispetto della dignità, anche perché i dati trattati in queste sedi sono sempre sensibili.**

Gli organismi sanitari pubblici e privati, come pure gli esercenti le professioni sanitarie, devono anzitutto **fornire al paziente un'informativa sul trattamento dei dati personali** che lo riguardano e **acquisire il consenso al loro uso.**

Non è necessario il previo consenso nei casi di rischio imminente per la salute, o quando vi è impossibilità fisica o incapacità di agire, di intendere o di volere del paziente. In questi casi il consenso al trattamento dei dati personali può essere espresso, se ne è in grado, dal paziente stesso, **successivamente alla prestazione sanitaria ricevuta**, o da un terzo (ad esempio, un familiare, un convivente, un responsabile della struttura presso cui dimora).

L'informativa fornita all'interessato deve indicare chi è il soggetto (ad esempio, il medico) che raccoglie i suoi dati, quali sono gli scopi e le modalità del trattamento, l'ambito di circolazione dei dati e se il paziente è obbligato o meno a fornirli. L'informativa deve contenere anche indicazioni sulle modalità con cui la persona interessata può esercitare i diritti riconosciuti dalla legge, come la richiesta di integrazione, aggiornamento o cancellazione dei dati trattati.

L'informativa può essere **data *una tantum* anche oralmente.** È comunque preferibile che venga fornita per iscritto, magari attraverso un pieghevole, oppure affiggendone il testo in un luogo facilmente visibile, come nella sala d'attesa.

L'organismo sanitario può dare informazioni, anche per telefono, sulla presenza di una persona al pronto soccorso o sui degenti presenti nei reparti **solo ai terzi legittimati, come parenti, familiari, conviventi, conoscenti, personale volontario.** L'interessato, se cosciente e capace, deve poter decidere a chi possono essere comunicate notizie sulla propria salute. Occorre comunque rispettare l'eventuale richiesta della persona ricoverata a **non rendere note neppure ai terzi legittimati la sua presenza nella struttura sanitaria o le informazioni sulle sue condizioni di salute.**

È assolutamente vietata la diffusione di dati idonei a rivelare lo stato di salute. La «***diffusione***» è un'ipotesi particolare di trattamento che consiste nel dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione. Non possono quindi essere resi disponibili a chiunque su Internet i dati anagrafici, l'indicazione delle diagnosi o i risultati delle analisi cliniche delle persone che si recano presso un ospedale.

Per il trattamento dei dati sensibili in ambito sanitario, tenendo sempre conto del ruolo professionale dei medici e del personale paramedico, occorre evitare che le informazioni sulla salute possano essere conosciute da soggetti non autorizzati, a causa di situazioni di promiscuità derivanti dall'organizzazione dello spazio dei locali o dalle modalità utilizzate. Pertanto vanno adottati specifici accorgimenti per garantire la riservatezza dei pazienti, ad esempio durante l'orario di visita. Fra gli altri accorgimenti va ricordato l'uso di **paraventi o simili nei reparti di rianimazione**, volti a limitare la visibilità del malato ai soli familiari e conoscenti.

Un regime particolare è previsto dal Codice per le **cartelle cliniche**: l'art. 92, infatti, prevede che nei casi in cui organismi sanitari pubblici e privati redigano e conservino una cartella clinica in conformità alla disciplina applicabile **devono essere adottati opportuni accorgimenti per assicurare la comprensibilità dei dati** e per distinguere i dati relativi al paziente da quelli eventualmente riguardanti altri interessati, ivi comprese informazioni relative a nascituri.

Le eventuali richieste di presa visione o di rilascio di copia della cartella e dell'acclusa scheda di dimissione ospedaliera da parte di soggetti diversi dall'interessato possono essere accolte, in tutto o in parte, **solo se la richiesta è giustificata dalla documentata necessità di**:

- far valere o difendere un diritto in sede giudiziaria, ai sensi dell'art. 26, comma 4, lettera *c)*, di rango pari a quello dell'interessato, ovvero consistente in un diritto della personalità o in un altro diritto o libertà fondamentale e inviolabile;
- tutelare, in conformità alla disciplina sull'accesso ai documenti amministrativi, una situazione giuridicamente rilevante di rango pari a quella dell'interessato, ovvero consistente in un diritto della personalità o in un altro diritto o libertà fondamentale e inviolabile.

Il **D.L. 5/2012**, cd. decreto semplificazioni, conv. in **L. 35/2012**, ha stabilito che nei piani di sanità nazionali e regionali si privilegia la gestione elettronica delle pratiche cliniche attraverso l'utilizzo della **cartella clinica elettronica** (art. 47bis).

Il successivo **D.L. 179/2012** (decreto Crescita bis), conv. in **L. 221/2012**, ha previsto che, a partire dal 1° gennaio 2013, le cartelle cliniche sono conservabili anche solo in forma digitale, anche dalle strutture private accreditate.

19 La tutela innanzi al Garante

a) Le forme di tutela

L'art. 141 del Codice riconosce all'interessato **tre autonome forme di tutela** del diritto alla protezione dei dati personali azionabili innanzi al Garante, disciplinandone le specifiche modalità di esercizio.

In particolare, la norma prevede:

a) un **reclamo circostanziato**, per rappresentare una violazione delle norme in materia di trattamento di dati personali;
b) una **segnalazione** (se non è possibile presentare un reclamo), al fine di sollecitare un controllo da parte del Garante sulla medesima disciplina;
c) un **ricorso**, se si intende far valere gli specifici diritti che l'art. 7 riconosce e garantisce all'interessato.

b) La tutela in sede amministrativa: il reclamo e le segnalazioni

Il **reclamo** è quello strumento di tutela amministrativa (insieme alle segnalazioni e al ricorso) che l'interessato può utilizzare per sottoporre al Garante della privacy la **violazione delle norme**

in materia di trattamento di dati personali. Il legislatore del Codice, all'art. 142, individua il *contenuto* del reclamo, senza però prevedere particolari modalità. Esso deve contenere:

- l'indicazione per quanto possibile dettagliata dei fatti e delle circostanze su cui si fonda;
- l'indicazione delle disposizioni che si presumono violate e delle misure richieste;
- gli estremi identificativi del titolare, del responsabile, ove conosciuto, e, ovviamente, dell'istante stesso.

Nel reclamo deve essere indicato anche l'indirizzo di posta elettronica, di telefax o di telefono a cui si intende ricevere le comunicazioni relative alla procedura e può essere corredato, in allegato, dalla documentazione utile ai fini del decidere.

L'atto deve essere **sottoscritto dall'interessato** o, eventualmente, dalle associazioni che lo rappresentano, anche ai sensi dell'art. 9, comma 2, del Codice stesso, e presentato al Garante senza particolari formalità.

Il Garante, inoltre, per facilitare la presentazione di un reclamo, può predisporre un *modello ad hoc* di cui deve favorire la disponibilità con strumenti elettronici: ancora una volta il legislatore considera *Internet* il canale principale attraverso il quale diffondere servizi e, come in questo caso, il *fac simile* per predisporre un reclamo.

Quanto al *procedimento* di definizione del reclamo, questo è individuato dal successivo art. 143 del Codice.

Presentato il reclamo ed esaurita l'istruttoria preliminare, se questo non è manifestamente infondato e sussistono i presupposti per adottare un provvedimento, il Garante, anche prima della definizione del procedimento, può cercare di **addivenire ad una soluzione amichevole della controversia** invitando il titolare, anche in contraddittorio con l'interessato, ad *effettuare spontaneamente il blocco del trattamento*.

In alternativa, il Garante può:

- *prescrivere al titolare misure opportune o necessarie* per rendere il trattamento conforme alle disposizioni vigenti;
- *disporre il blocco o vietare, in tutto o in parte, il trattamento* che risulta illecito, o non corretto, anche per effetto della mancata adozione delle misure necessarie da esso impartite; 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;
- *vietare in tutto o in parte il trattamento di dati relativi a singoli soggetti o a categorie di soggetti* quando si ponga in contrasto con rilevanti interessi della collettività.

Una sola norma — l'art. 144 del Codice — è dedicata alle **segnalazioni**.

Anche questo è un mezzo per sottoporre al Garante una violazione della normativa sulla privacy al fine di sollecitare un controllo. Il legislatore non ha indicato i presupposti per poter effettuare una segnalazione, limitandosi ad affermare, in negativo, che la stessa è presentabile se non è possibile presentare un reclamo.

La norma in questione, in particolare, afferma che i provvedimenti che il Garante può emanare a seguito di un reclamo, esaminati in precedenza, possono essere adottati anche a seguito di una segnalazione purchè sia stata avviata un'istruttoria preliminare e anche prima della definizione del procedimento.

Peraltro, l'art. 144 non trova alcun immediato referente normativo in un'altra disposizione previgente.

c) Il ricorso al Garante

Il **ricorso** al Garante è l'ultimo strumento di tutela amministrativa riconosciuto all'interessato. Diversamente dagli altri due, però, il ricorso ha un ambito di applicazione ben preciso, potendo essere presentato solo **far valere gli specifici diritti riconosciuti e garantiti dall'art. 7 del Codice** (si ricordano: i diritti di accesso, di rettifica, di cancellazione, di integrazione, di opposizione) e non per una generica violazione della normativa in materia.

Gli artt. 145 e seguenti del Codice sono dedicati alla disciplina del ricorso.

La prima peculiarità che viene in evidenza quando si parla del ricorso al Garante è quella della sua **alternatività rispetto al ricorso giurisdizionale**: l'art. 145 c.d.p., infatti, prevede la possibilità di far valere i menzionati diritti sia innanzi all'autorità giudiziaria che innanzi al Garante.

Il ricorso al Garante può essere validamente proposto solo dopo aver adempiuto ad una precisa formalità: salvo i casi in cui il decorso del termine esporrebbe "*taluno a pregiudizio imminente e irreparabile*", è necessario:

- che l'interessato abbia precedentemente fatto valere, nei confronti del titolare o del responsabile, i medesimi diritti;
- che sia decorso il termine (15 giorni) stabilito dalla stessa norma per il riscontro alla richiesta;
- ovvero che sia stato opposto un diniego anche parziale alla richiesta.

L'**interpello preventivo** costituisce una *condizione di ammissibilità* del successivo ricorso al Garante e si risolve in una *richiesta di conciliazione bonaria* della controversia. È cosa ovvia che, in ipotesi di *pregiudizio imminente e irreparabile*, che giustifica la proponibilità diretta del ricorso, l'interessato è tenuto a motivare in ordine allo stesso al momento della sua proposizione, per non incorrere in una pronunzia di inammissibilità del ricorso.

Presentato l'interpello, il riscontro alla richiesta da parte del titolare o del responsabile deve avvenire entro il termine di 15 giorni; in ogni caso, tale termine può essere prorogato fino a 30 giorni se il titolare o il responsabile danno comunicazione all'interessato (nel termine ordinario) della complessità delle operazioni necessarie per fornire un integrale riscontro alla richiesta ovvero della ricorrenza di altro giustificato motivo.

Solo al termine della procedura di interpello, si può proporre il **ricorso al Garante** nei confronti del titolare (e non anche nei confronti del responsabile).

Nel ricorso al Garante occorre indicare, secondo le disposizioni dell'art. 147 c.d.p.: gli estremi identificativi del ricorrente e dell'eventuale procuratore speciale, del titolare e, ove conosciuto, del responsabile eventualmente designato per il riscontro all'interessato; la data della richiesta presentata al titolare o al responsabile, oppure l'indicazione del pregiudizio imminente ed irreparabile che permette di prescindere dalla richiesta medesima e, quindi, dalla procedura di interpello; gli elementi posti a fondamento della domanda; il provvedimento richiesto al Garante; il domicilio eletto ai fini del procedimento.

Il ricorso deve essere *sottoscritto dal ricorrente o dal procuratore speciale* e allo stesso devono essere allegate:

- la copia della richiesta rivolta al titolare o al responsabile per attivare la procedura di interpello;
- la procura nei casi in cui sia stata conferita;
- la prova del versamento dei diritti di segreteria.

Inoltre, unitamente al ricorso deve essere fornita la documentazione utile per la valutazione dello stesso e deve essere fornita l'indicazione di un recapito per l'invio di comunicazioni al ricorrente o al suo procuratore speciale mediante posta elettronica, telefax o telefono.

Il ricorso è rivolto al Garante e la sottoscrizione del ricorrente è autenticata, a meno che la stessa non venga apposta presso l'Ufficio del Garante, o da un procuratore speciale iscritto all'albo degli avvocati, al quale sia stata conferita la procura, ai sensi dell'articolo 83 c.p.c, ovvero con firma digitale in conformità alla normativa vigente.

Il ricorso viene validamente proposto con la *trasmissione al Garante mediante plico raccomandato*, oppure *per via telematica*, osservando, in quest'ultimo caso, le modalità relative alla sottoscrizione con firma digitale e alla conferma del ricevimento ex art. 38, comma 2, c.d.p., ovvero, infine, può essere *presentato direttamente presso l'Ufficio del Garante*.

Fuori dei casi in cui è dichiarato inammissibile o manifestamente infondato, la presentazione del ricorso dà vita ad una *procedura* dai tempi piuttosto stringenti.

Infatti, il ricorso è comunicato - a cura dell'Ufficio del Garante - al titolare entro tre giorni con invito ad esercitare, entro i successivi dieci giorni dal suo ricevimento, la facoltà di comunicare al ricorrente e all'Ufficio la sua eventuale **adesione spontanea**. A questa consegue la dichiarazione di *non luogo a provvedere* e, su richiesta del ricorrente, è determinato in misura forfettaria l'ammontare delle spese e dei diritti inerenti al ricorso, che possono essere posti a carico della controparte o compensati, anche parzialmente, per giusti motivi.

In ipotesi di mancata adesione, alla presentazione del ricorso segue un vero e proprio procedimento dinanzi al Garante che si svolge **in contraddittorio tra le parti**: il titolare, il responsabile eventualmente designato per il riscontro, e l'interessato hanno *diritto di essere ascoltati*, personalmente o a mezzo di procuratore speciale, e hanno facoltà di *presentare memorie o documenti*.

20 La tutela giurisdizionale

L'art. 152 del Codice della privacy attribuisce alla competenza del **giudice ordinario** la cognizione di **tutte le controversie che riguardano, comunque, l'applicazione delle disposizioni codicistiche**, comprese quelle inerenti ai provvedimenti del Garante in materia di protezione dei dati personali o alla loro mancata adozione, nonchè delle **controversie a tutela di dati personali in materia di pubblica sicurezza**, previste dall'art. 10, comma 5, L. 121/1981.

Per la disciplina applicabile, il comma 1bis della disposizione rimanda all'**art. 10 D.Lgs. 1° settembre 2011, n. 150**, che ha previsto misure in materia di riduzione e semplificazione dei procedimenti civili di cognizione.

Innanzitutto, tale norma prevede che a tali controversie si applichi il **rito del lavoro**, salvo diversa previsione dello stesso articolo, e che competente a decidere sia il **Tribunale del luogo in cui ha la residenza il titolare del trattamento dei dati**.

Qualora il ricorso abbia ad oggetto provvedimenti del Garante, lo stesso deve essere proposto, a pena di inammissibilità, entro 30 giorni dalla data di comunicazione dello stesso o da quella in cui si è formato il rigetto tacito, ovvero entro 60 giorni se il ricorrente risiede all'estero.

Trova applicazione l'art. 5 del decreto legislativo in questione, per cui l'**efficacia esecutiva del provvedimento impugnato può essere sospesa dal giudice**, se richiesto e sentite le parti, con *ordinanza non impugnabile*, quando ricorrono gravi e circostanziate ragioni esplicitamente indicate nella motivazione. Inoltre, in caso di pericolo imminente di un danno grave e irreparabile, la sospensione può essere disposta con decreto pronunciato fuori udienza, ma diventa inefficace se viene confermata entro la prima udienza successiva, con l'ordinanza citata (art. 5 D.Lgs. 150/2011).

Il giudizio può concludersi anche senza una pronuncia di merito del giudice. Ciò avviene se alla prima udienza il ricorrente non compare senza addurre alcun legittimo impedimento: in tal caso, il giudice dispone la cancellazione della causa dal ruolo e dichiara l'estinzione del processo, ponendo a carico del ricorrente le spese di giudizio.

Con la sentenza che definisce il giudizio, il giudice, anche in deroga a quanto disposto dall'art. 4 L. 2248/1865, allegato E), quando lo ritenga necessario, specialmente in relazione all'eventuale atto del soggetto pubblico titolare o responsabile, prescrive le misure necessarie e dispone sul risarcimento del danno. La sentenza non è appellabile.

21 Le sanzioni

Oltre alle esaminate forme di tutela del diritto alla privacy, certamente un ulteriore deterrente alla violazione delle norme poste a protezione dei dati personali è rappresentato dalle **sanzioni amministrative di tipo pecuniario**, previste in particolare nel Capo I del Titolo III della Terza Parte del Codice.

L'art. 161 c.d.p. punisce le ipotesi di **omessa o inidonea informativa all'interessato**, cioè quelle condotte tenute in violazione dell'art. 13 del Codice, per aver il titolare completamente omesso di adempiere all'obbligo dell'informativa, o per aver proceduto a tale adempimento in modo sostanzialmente inidoneo rispetto alle modalità e alle finalità previste dalla legge: per tale violazione è prevista la sanzione amministrativa del pagamento di una somma ***da seimila euro a trentaseimila euro***.

Il successivo art. 162 c.d.p. prevede una serie di ipotesi specifiche: la norma punisce l'**illecita cessione di dati** (avvenuta in violazione dell'art. 16, comma 1, lett. b), che consente la cessione dei dati ad altro titolare, purché destinati ad un trattamento in termini compatibili agli scopi per i quali i dati sono raccolti) con una sanzione che varia ***da diecimila a sessantamila euro***; sanziona la violazione dell'art. 84, comma 1, sulla **comunicazione dei dati idonei a rivelare lo stato di salute** — per il quale tali dati possono essere **resi** noti all'interessato da parte di esercenti le professioni sanitarie ed organismi sanitari, solo per il tramite di un medico designato dall'interessato o dal titolare — con una sanzione pecuniaria che varia ***da mille euro a seimila euro***; prevede che il trattamento effettuato in violazione delle norme sulle misure minime di sicurezza sia sanzionato con il pagamento di una somma ***da diecimila euro a centoventimila euro***, ed è escluso il pagamento in misura ridotta; in caso di **inosservanza dei provvedimenti del Garante di prescrizione di misure** necessarie a rendere il trattamento conforme alle disposizioni vigenti o **di divieto** del trattamento illecito o non corretto dei dati, ai sensi dell'art. 154, comma 1, lettere c) e d), è prevista l'applicazione in sede amministrativa della sanzione del pagamento di una somma ***da trentamila euro a centottantamila euro***; la violazione del diritto di opposizione in materia di comunicazioni indesiderate nelle forme previste dall'art. 130, comma 3bis, è sanzionata con il pagamento di una somma ***da diecimila euro a centoventimila euro***.

La **violazione delle disposizioni in materia di conservazione dei dati di traffico**, di cui all'art. 132, commi 1 e 1bis, c.d.p., si applica la sanzione amministrativa pecuniaria ***da 10.000 euro a 50.000 euro*** (art. 162bis c.d.p.)

Il D.Lgs. 69/2012 ha inserito nel Capo in esame l'art. 162ter che prevede una serie di **sanzioni applicabili nei confronti di fornitori di servizi di comunicazione elettronica accessibili al pubblico**.

Quanto alle possibili **violazioni delle norme in tema di notificazione**, l'art. 163 del Codice punisce con una sanzione ***da ventimila euro a centoventimila euro*** "chiunque, essendovi tenuto, non provvede tempestivamente alla notificazione ai sensi degli articoli 37 e 38, ovvero indica in essa notizie incomplete". In realtà, l'uso del termine "chiunque" appare inadeguato potendo commettere tale illecito solo chi abbia l'obbligo giuridico di procedere alla notificazione, ovvero il titolare del trattamento; infine, in ipotesi di **omessa informazione o esibizione al Garante**, l'art. 164 c.d.p. punisce "chiunque omette di fornire le informazioni o di esibire i documenti richiesti dal Garante" con la sanzione amministrativa del pagamento di una somma ***da diecimila euro a sessantamila euro***.

In tutte le ipotesi in cui si applicano sanzioni pecuniarie, l'art. 164bis del Codice prevede che i limiti massimi e minimi delle sanzioni possono essere applicati in **misura pari ai due quinti** se il fatto è di **minore gravità**; per valutare la gravità si ha riguardo alla natura anche economica o sociale dell'attività svolta.

Lo stesso articolo 164bis prevede, poi, alcune **ipotesi aggravate** molto severe.

Innanzitutto in caso di *più violazioni* di un'unica o di più disposizioni, commesse anche in tempi diversi in relazione a banche di dati di particolare rilevanza o dimensioni, si applica la sanzione amministrativa del pagamento di una somma **da cinquantamila euro a trecentomila euro** e non è ammesso il pagamento in misura ridotta. Questa norma non trova applicazione per le violazioni degli art. 162, comma 2, 162bis e 164.

I limiti minimo e massimo delle sanzioni sono **raddoppiati** in altri casi di maggiore gravità e, in particolare, di maggiore rilevanza del pregiudizio per uno o più interessati, ovvero quando la violazione coinvolge numerosi interessati. Infine, le dette sanzioni possono essere aumentate **fino al quadruplo** quando le stesse possono risultare inefficaci in ragione delle condizioni economiche del contravventore.

Un deterrente alla commissione di violazioni del Codice della privacy è rappresentato dalla previsione di un'ulteriore sanzione accessoria: per tutte le violazioni amministrative può essere applicata la **sanzione della pubblicazione dell'ordinanza-ingiunzione,** per intero o per estratto, in uno o più giornali indicati nel provvedimento che la applica. Tale pubblicazione ha luogo *a cura e spese del contravventore.*

Quanto al procedimento di applicazione delle sanzioni amministrative, l'art. 166 riconosce la competenza al Garante e dispone l'applicazione delle norme di cui alla L. 689/1981.

22 Gli illeciti penali

Il legislatore prevede delle ipotesi di reato conseguenti a particolari condotte tenute in violazione delle norme del Codice.

Il **reato di trattamento illecito di dati**, previsto dall'art. 167 del Codice, punisce la condotta di chiunque *al fine di trarre per sé o per altri profitto o di recare ad altri un danno*, procede al trattamento dei dati personali in violazione delle norme dettate in tema di principi applicabili a tutti i trattamenti effettuati da soggetti pubblici (art. 18), ovvero in tema di principi applicabili al trattamento di dati diversi da quelli sensibili e giudiziari (art. 19), o ancora in tema di consenso (art. 23), ovvero, infine, in tema di dati relativi al traffico (art. 123), di dati relativi all'ubicazione (art. 126), di comunicazioni indesiderate (art. 130), ovvero in applicazione della norma in materia di elenchi abbonati (art. 129).

In tale ampia previsione, il legislatore non specifica il tipo di profitto — ovvero se lo stesso debba essere ingiusto — né il tipo di danno-patrimoniale o anche non patrimoniale ma richiede per l'effettiva punibilità che **dal fatto derivi un nocumento**. La pena è quella della *reclusione da sei a diciotto mesi* o, se il fatto consiste nella comunicazione o diffusione, quella della reclusione *da sei a ventiquattro mesi*.

Ugualmente, è punita la condotta di "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 17, 20, 21, 22, commi 8 e 11, 25, 26, 27 e 45".

Le norme richiamate sono quelle dettate in tema di trattamento che presenta rischi specifici (art. 17), di principi applicabili al trattamento di dati sensibili (art. 20), di principi applicabili al trattamento di dati giudiziari (art. 21), di principi applicabili al trattamento di dati sensibili e giudiziari (art. 22), ovvero ancora in tema di divieti di comunicazione e diffusione (art. 25), di garanzie per i dati sensibili (art. 26), di garanzie per i dati giudiziari (art. 27) e, infine, di trasferimenti vietati all'estero (art. 45).

La sanzione prevista è la *reclusione da uno a tre anni* se dal fatto deriva un nocumento e salvo che il fatto costituisca più grave reato.

Il **reato di falsità nelle dichiarazioni e notificazioni al Garante** è previsto dall'art. 168 del Codice, che punisce, con la *reclusione da sei mesi a tre anni*, chiunque nella notificazione o 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*.

Tale fattispecie, che opera con la clausola "salvo che il fatto costituisca più grave reato", può ascriversi alla categoria dei **reati comuni;** benché, infatti, la notificazione di cui all'art. 37 sia un obbligo che incombe solo sul titolare del trattamento, la portata della norma è così ampia da ricomprendere anche condotte che possono validamente essere poste in essere anche da "chiunque".

L'art. 169 del Codice punisce con l'*arresto sino a due anni* chi, essendovi tenuto, **omette di adottare le misure minime di sicurezza** previste dal precedente art. 33.

Tale reato omissivo è un **reato proprio** perché può essere contestato soltanto a chi per legge è tenuto ad adottare le misure di sicurezza, ovvero al titolare del trattamento.

Infine, l'art. 170 del Codice punisce con la *reclusione da tre mesi a due anni* l'**inosservanza di taluni provvedimenti del Garante** adottati nelle ipotesi di cui agli artt. 26, comma 2, 90, 150, commi 1 e 2, e 143, comma 1, lett. c); mentre il successivo art. 171 espressamente prevede che la violazione delle disposizioni di cui agli artt. 113, comma 1, e 114 è punita con le sanzioni di cui all'art. 38 L. 20 maggio 1970, n. 300 (Statuto dei lavoratori).

Regola comune alle diverse fattispecie di reato ora esaminate è la pena accessoria della **pubblicazione della sentenza di condanna** prevista, per i soli delitti, dall'art. 172 del Codice.