

# Sulla nozione di dato personale, sulla nozione di trattamento e dei soggetti che lo effettuano nel recente codice della privacy

Luca Benci\*

## **LA LEGGE 31 DICEMBRE 1996, N. 675 “TUTELA DELLE PERSONE E DI ALTRI SOGGETTI**

rispetto al trattamento dei dati personali” vera e propria “legge madre” e la successiva gemella legge 31 dicembre 1996, n. 676 “Delega al Governo in materia di tutela delle persone e di altri soggetti al trattamento dei dati personali” hanno subito una serie di modificazioni e integrazioni con fonti di carattere legislativo e regolamentare. Tali modifiche, talvolta incoerenti e provvisorie, hanno reso difficile la comprensione globale del testo e la ricognizione del testo vigente (si pensi che solo la legge 675/96 ha subito ben nove modifiche nel giro di pochissimi anni). La forte frammentazione del quadro normativo ha portato il legislatore all’esigenza di armonizzazione del quadro stesso dando vita a un vero e proprio testo unico.

L’art. 1 della legge 24 marzo 2001, n. 127 “Differimento del termine per l’eser-

cizio della delega prevista dalla legge 31 dicembre 1996, n. 676 in materia di dati personali”. Si legge infatti al quarto comma dell’art. 1 che il “Governo ..... emana entro diciotto mesi un testo unico delle disposizioni in materia di tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali e delle disposizioni connesse, coordinandovi le norme vigenti ed apportando alle medesime le integrazioni e modificazioni necessarie al predetto coordinamento o per assicurare la migliore attuazione”. Una delega ampia quindi, non meramente ricognitiva<sup>1</sup> della legislazione esistente, che il legislatore delegato ha ampiamente usato con l’emanazione del D.Lgs 30 giugno 2003, n. 196 “Codice in materia di protezione dei dati personali”<sup>2</sup> la cui ampiezza ha fatto a taluni parlare di delega in bianco e di rischio di illegittimità costituzionale. Tra

---

\* Giurista, Cedipros, Firenze

1. È stata istituita presso il Dipartimento della Funzione Pubblica una commissione di studio – c.d. Commissione Bianca, dal nome del presidente il prof. Massimo Bianca dell’Università di Roma - che ha lavorato all’armonizzazione e all’adeguamento delle norme riunite all’interno del testo unico. Tale opera di armonizzazione non si è spinta nel settore sanitario – per precisazione della Commissione – a riassorbire nel testo unico anche disposizione pre-normativa privacy quali ad esempio le norme contenute nella normativa sull’AIDS.

2. In GU n.174 del 29-7-2003 - Suppl. Ordinario n.123).

l'altro nel frattempo si sono intrecciate e inserite nuove normative dell'Unione europea che hanno fatto slittare i tempi di emanazione del nuovo codice<sup>3</sup>.

#### IL DIRITTO ALLA PRIVACY

Il Testo unico sulla privacy precisa in modo enfatico e rituale, all'art. 1, che "chiunque ha diritto alla protezione dei dati personali che lo riguardano". Il diritto alla privacy si pone quindi come un diritto forte della personalità e si aggiunge agli altri diritti protetti dal nostro ordinamento. Rispetto alla legge 675/1996 il diritto viene affermato ben più chiaramente<sup>4</sup>. Tale diritto appartiene indistintamente a "chiunque", *c i t t a d i n o e n o n , p e r s o n a f i s i c a o p e r s o n a g i u r i d i c a , m a g g i o r e n n e o m i n o r e n n e*, come concretizzazione di un diritto inviolabile dell'uomo. Di conseguenza anche lo straniero (la norma ripetiamo parla di chiunque e non dei cittadini) pure senza essere regolarmente residente ha diritto alla protezione dei dati<sup>5</sup>. La protezione dei dati personali deve svolgersi "nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezio-

ne dei dati personali".

Il principio della protezione dei dati personali, pur essendo codificata solo all'interno di una norma legislativa ordinaria, si sta trasformando in un principio costituzionale essendo prevista nella bozza di Costituzione europea all'art. 50<sup>6</sup>.

Si arriva a parlare non soltanto del diritto alla riservatezza come diritto costituzionale ma si va ben oltre arrivando a parlare di "costituzionalizzazione della persona" tenendo presenti i rischi che l'intreccio tra biologia, tecnologia ed elettronica ha aperto" con la conseguenza che il corpo umano viene di fatto trasformato in una password per l'accesso a determinati servizi<sup>7</sup>.

Questo lavoro si pone l'obiettivo di razionalizzare i concetti di dati personali, di trattamento e delle nozioni dei soggetti che trattano i dati in modo unitario. La frammentazione delle norme e la dispersione all'interno di numerosi articoli del codice della privacy rendono difficoltoso l'inquadramento unitario di tutti i singoli aspetti. Da qui l'esigenza di una riunificazione.

#### I DATI PERSONALI

L'espressione dati personali è sinonimo di informazione<sup>8</sup> e rientra di conse-

3. Il riferimento è alla direttiva 2002/58/CE del 12 luglio 2002 che ha fatto slittare al 30 giugno 2003 i termini previsti della delega legislativa.

4. Il primo comma dell'art. 1 della legge 31 dicembre 1996, n. 675 "Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali" recitava testualmente: La presente legge garantisce che il trattamento dei dati personali si svolga nel rispetto dei diritti, delle libertà fondamentali, nonché della dignità delle persone fisiche, con particolare riferimento alla riservatezza e alla identità personale; garantisce altresì i diritti delle persone giuridiche e di ogni altro ente o associazione.

5. Bardusco A., in *AAVV, Codice della privacy – commento al Decreto legislativo 30 giugno 2003, n. 196, tomo I, Giuffrè 2004*.

6. Bozza di costituzione europea approvata dalla Conferenza dei rappresentanti dei Governi degli Stati membri a Bruxelles il 25 giugno 2004, testo provvisorio redatto dal Segretariato della Conferenza intergovernativa, articolo I-50 Protezione dei dati di carattere personale: 1. Ogni individuo ha diritto alla protezione dei dati di carattere personale che lo riguardano. 2. La legge o la legge quadro europea stabilisce le norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale da parte delle istituzioni, degli organi e degli organismi dell'Unione, e da parte degli altri stati membri nell'esercizio di attività che rientrano nel campo di applicazione del diritto dell'Unione, e le norme relative alla libera circolazione di tali dati. Il rispetto di tali norme è soggetto al controllo di autorità indipendenti.

7. Vedi Relazione del Garante 2002, Discorso del Presidente, p. 3 e ss., in [www.garanteprivacy.it](http://www.garanteprivacy.it)

8. Imperiali R., Imperiali R., *Codice della privacy – commento alla normativa sulla protezione dei dati personali*, ed. Il Sole 24 ore, 2004.

guenza in tale categoria concettuale “qualsiasi elemento che abbia un contenuto informativo” con la conseguenza che rientrano tra i dati personali non soltanto le espressioni alfabetiche ma anche immagini o suoni. Si pensi all'immagine radiologica e/o alle cassette della videosorveglianza presenti in molte terapie intensive.

I dati personali – come categoria concettuale – compongono una ampia famiglia di dati o come è stata definita una sorta di “categoria madre” che possono essere suddivisi in più categorie e, in realtà, con diversi criteri di classificazione. In base agli adempimenti previsti dalla legge sulla *privacy* i dati personali possono essere suddivisi in:

- 1) dati comuni;
- 2) dati identificativi;
- 3) dati sensibili (con la sottospecie dei dati genetici);
- 4) dati giudiziari.

A questi devono essere aggiunti una serie di dati come i dati anonimi.....

È ovvio che questi dati sono tutti personali, ma la legge sembra farne delle categorie a parte quando invece concettualmente sono collegate tra di loro in un rapporto di *genus a species*.

Andiamo a vedere allora la classificazione dei dati personali operata dal legislatore e le relative definizioni.

- a) “dato personale”, qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale;
- b) “dati identificativi”, i dati personali che permettono l'identificazione diretta dell'interessato;
- c) “dati sensibili”, i 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, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale;

- d) “dati giudiziari”, i dati personali idonei a rivelare provvedimenti di cui all'articolo 3, comma 1, lettere da a) a o) e da r) a u), del d.P.R. 14 novembre 2002, n. 313, 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 degli articoli 60 e 61 del codice di procedura penale.

I dati comuni sono l'unica categoria a non avere una definizione legislativa e si pongono come una categoria residuale non soltanto dei dati sensibili ma oggi anche dei dati identificativi.

I dati identificativi – come definizione generale – sono oggi presenti nel codice e non erano presenti come categoria generale nella classificazione che dei dati personali faceva la legge 675/1996. Erano però contenuti nel D. Lgs 30 luglio 1999, n. 281 “Disposizione in materia di trattamento dei dati personali per finalità storiche, statistiche e di ricerca scientifica”.

La nozione di dato sensibile si pone sostanzialmente come una categorie chiusa avente carattere tassativo e non estensibile con interpretazioni per analogia, date le regole rigorose a cui sono sottoposti. L'unica parte non tassativa è quella relativa al riferimento alle convinzioni religiose, filosofiche *o di altro genere, laddove l'espressione “o di altro genere” autorizza l'estensione di stili e di impostazioni vita di difficile tipizzazione ma comunque riconducibili in un qualche modo alle convinzioni filosofiche.*

All'interno dei dati sensibili non pare di cogliere una gerarchia di dati più importanti anche se la dottrina giuridica – a proposito dei dati inerenti alla salute – li ha classificati come dati “super-sensibili”. Non vi è dubbio però che gli eventi internazionali accaduti dopo l'11 settembre 2001 hanno fatto salire di importanza i dati legati alla religione o alla etnia di provenienza.

All'interno dei dati sensibili inerenti alla salute, vi sono norme più restrittive per alcune materie e che sono contenute nella legge 135/1990 sulla rilevazione statistica della infezione da HIV, sulla interruzione volontaria della gravidanza e sulla legge sulla violenza sessuale.

Si contrappongono ontologicamente ai dati personali i dati anonimi, dato che l'anonimato è il contrario di identificabilità<sup>9</sup>. Il dato anonimo può essere tale sin dall'origine o diventarlo in seguito al trattamento come specifica la nozione che il legislatore ha dettato: “il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile”. Quindi un dato è veramente anonimo quando sia dalla fase iniziale o anche successivamente l'informazione non è suscettibile di un collegamento personale né direttamente né indirettamente.

Per banca di dati si intende invece “qualsiasi complesso organizzato di dati personali, ripartito in una o più unità dislocate in uno o più siti”. L'elemento caratterizzante della banca dati è quello relativo al fatto che i dati siano contenuti all'interno di un “complesso organizzato di dati”.

#### IL TRATTAMENTO DEI DATI

La legge definisce trattamento “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”.

Rispetto alla previgente normativa troviamo la novità della consultazione dei dati. Si distingue cioè la raccolta e la registrazione dalla consultazione che evidentemente riguarda terze persone che come tali però devono essere incaricate comunque del trattamento dei dati. La dottrina giuridica ha avuto modo di classificare gli atti potenzialmente lesivi che possono essere compiuti nelle operazioni di trattamento e che possono essere così classificati: 1) atti che possono essere compiuti nella fase **preliminare**, di raccolta e di registrazione; 2) atti che possono essere compiuti nella fase di **elaborazione**, che raggruppa l'organizzazione, l'elaborazione in senso stretto, la modificazione, la selezione, l'estrazione, il raffronto, l'interconnessione e l'utilizzo; atti che possono essere compiuti nella fase della **circolazione e/o divulgazione** riguardanti la comunicazione e la diffusione. Sarebbe da registrarsi una ulteriore fase residuale comprendente la conservazione, il blocco, la cancellazione e la diffusione. Tutte queste fasi possono essere compiute con o senza l'ausilio di strumenti elettronici.

9. Imperiali R., Imperiali R., *Codice della privacy – commento alla normativa sulla protezione dei dati personali*, ed. Il Sole 24 ore, 2004, p. 65.

Per altro si rileva che la normativa italiana è ben più rigorosa di quella europea nella parte in cui tutela i dati personali anche se non inseriti organicamente all'interno di una banca dati, al contrario della direttiva 95/46/CE che tutela solo i dati destinati a figurare in una banca dati. La norma italiana ha evidentemente voluto combattere eventuali comportamenti elusivi della norma.

Il trattamento può avvenire direttamente all'interno della struttura o esternamente alla struttura stessa attraverso le varie forme ad esempio di **outsourcing informatico** che comprende tra gli altri il **disaster recovery**, gestione del server, gestione dei siti web, gestione della rete, gestione della sicurezza informatica. Realizzano forme di gestione esternalizzata di trattamento di dati anche l'attribuzione a strutture diverse da quelle aziendali di dati come la gestione della portineria, della vigilanza, della pulizia dei locali, del servizio postale interno ecc.

Come regola generale i dati devono essere trattati:

- 1) in modo lecito e secondo correttezza;
- 2) raccolti e registrati per scopi determinati, espliciti e legittimi;
- 3) esatti e se necessario aggiornati;
- 4) pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono stati raccolti o successivamente trattati;
- 5) conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati.

L'interessato ha diritto di essere previamente informato, oralmente o per scritto, di conoscere:

- a) le finalità e le modalità del trattamento cui sono destinati i dati;

- b) la natura obbligatoria o facoltativa del conferimento dei dati;
- c) le conseguenze di un eventuale rifiuto di rispondere;
- d) 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;
- e) i diritti riconosciuti a lui dal codice della privacy come interessato;
- f) gli estremi identificativi del titolare e, se designati, del rappresentante nel territorio dello Stato ai sensi dell'articolo 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 di cui all'articolo 7, è indicato tale responsabile.

L'informativa può non comprendere elementi già noti o notizie che possono ostacolare 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.

Salvo quanto vedremo successivamente per gli esercenti le professioni sanitarie i soggetti pubblici non devono richiedere il consenso all'interessato

La legge prevede inoltre alcuni **casi di esclusione dal consenso al trattamento dei dati** e li elenca in modo tassativo. Non deve quindi essere chiesto il consenso quando:

- a) i dati sono trattati in base ad un obbligo previsto dalla legge, da un regolamento o dalla normativa comunitaria;

- b) i dati sono trattati ai fini dello svolgimento delle investigazioni difensive di cui alla legge 7 dicembre 2000, n. 397, 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;
- c) l'informativa all'interessato comporta un impiego di mezzi che il Garante, prescrivendo eventuali misure appropriate, dichiara manifestamente sproporzionati rispetto al diritto tutelato, ovvero si riveli, a giudizio del Garante, impossibile;
- d) riguarda dati provenienti da pubblici registri, elenchi, atti o documenti conoscibili da chiunque, fermi restando i limiti e le modalità che le leggi, i regolamenti o la normativa comunitaria stabiliscono per la pubblicità degli atti;
- e) è necessario per la salvaguardia della vita o dell'incolumità fisica di un terzo. Se la medesima finalità riguarda l'interessato e quest'ultimo non può prestare il proprio consenso per impossibilità fisica, per incapacità di agire o per incapacità di intendere o di volere, il consenso è manifestato da chi esercita legalmente la potestà, ovvero da un prossimo congiunto, da un familiare, da un convivente o, in loro assenza, dal responsabile della struttura presso cui dimora l'interessato. Si applica la disposizione di cui all'articolo 82, comma 2;
- f) è necessario, in conformità ai rispettivi codici di deontologia di cui all'allegato A), per esclusivi scopi scientifici o statistici, ovvero per esclusivi scopi storici presso archivi privati dichiarati di notevole interesse storico ai sensi dell'articolo 6, comma 2, del decreto legislativo 29 ottobre

1999, n. 490, di approvazione del testo unico in materia di beni culturali e ambientali o, secondo quanto previsto dai medesimi codici, presso altri archivi privati.

In caso di **cessazione** del trattamento

In caso di cessazione, per qualsiasi causa, di un trattamento i dati devono essere:

- a) distrutti;
- b) ceduti ad altro titolare, purché destinati ad un trattamento in termini compatibili agli scopi per i quali i dati sono raccolti;
- c) conservati per fini esclusivamente personali e non destinati ad una comunicazione sistematica o alla diffusione;
- d) conservati o ceduti ad altro titolare, per scopi storici, statistici o scientifici, in conformità alla legge, ai regolamenti, alla normativa comunitaria e ai codici di deontologia e di buona condotta sottoscritti ai sensi dell'articolo 12.

Per quanto riguarda gli **enti pubblici** il trattamento dei dati – diversi da quelli sensibili e giudiziari, per i quali vige una disciplina diversa - è consentito soltanto per lo svolgimento delle funzioni istituzionali “anche in mancanza di una norma di legge o di un regolamento che lo preveda espressamente” (art. 19 codice privacy).

La comunicazione di un ente pubblico ad un altro ente pubblico è ammessa solo quando prevista da una norma di legge o di regolamento. In mancanza di tali norme la comunicazione è ammessa quando è necessaria per lo svolgimento delle funzioni istituzionali pur con delle restrizioni.

La **comunicazione da parte di un soggetto pubblico a privati** è ammessa solo quando prevista da legge o regolamento. Il trattamento dei dati sensibili da

parte di enti pubblici è consentito “solo se autorizzato da espressa disposizione di legge nella quale sono specificati i tipi di dati che possono essere trattati e di operazioni eseguibili e le finalità di rilevante interesse pubblico perseguite”.

Nei casi in cui una disposizione di legge specifica la finalità di rilevante interesse pubblico ma non i tipi di dati sensibili e le operazioni eseguibili, il trattamento è consentito solo in riferimento ai tipi di dati e di operazioni identificati e resi pubblici a cura dei soggetti che effettuano il trattamento.

I dati sensibili e giudiziari indispensabili per svolgere attività istituzionali possono essere trattati solo se non sia possibile avvalersi di dati anonimi. Qualora siano raccolti presso elenchi, registri o banche dati, tenute con l'ausilio di strumenti elettronici, sono trattati con tecniche di cifratura o mediante l'utilizzazione di codici identificativi o di altre soluzioni che li rendono temporaneamente non leggibili e permettono di identificare gli interessati solo in caso di necessità.

I dati idonei a rivelare lo stato di salute e la vita sessuale sono conservati separatamente da altri dati personali. I dati personali idonei a rivelare lo stato di salute non possono essere diffusi.

I privati (e gli enti pubblici economici) possono trattare dati personali solo con il consenso espresso dell'interessato che può riguardare l'intero trattamento oppure una o più operazioni. Il consenso deve essere espresso in forma scritta.

I **dati sensibili** possono essere oggetto di trattamento “solo con il consenso scritto dell'interessato e previa autorizzazione del Garante, nell'osservanza dei presupposti e dei limiti stabiliti dal presente codice (della privacy), nonché dalle leggi e dai regolamenti”. Il Garante comunica la decisione entro

quarantacinque giorni dalla richiesta. Decorso tale termine la mancata pronuncia equivale a rigetto.

La **notifica al Garante** è dovuta solo se il trattamento riguarda (riportiamo per esteso gli artt. 37, 38, 39, 40 e 41 del codice della privacy):

- 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, o 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, nonché 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.

2. Il Garante può individuare altri tratta-

menti suscettibili di recare pregiudizio ai diritti e alle libertà dell'interessato, in ragione delle relative modalità o della natura dei dati personali, con proprio provvedimento adottato anche ai sensi dell'articolo 17. Con analogo provvedimento pubblicato sulla Gazzetta ufficiale della Repubblica italiana il Garante può anche individuare, nell'ambito dei trattamenti di cui al comma 1, eventuali trattamenti non suscettibili di recare detto pregiudizio e pertanto sottratti all'obbligo di notificazione.

3. La notificazione è effettuata con unico atto anche quando il trattamento comporta il trasferimento all'estero dei dati.
4. Il Garante inserisce le notificazioni ricevute in un registro dei trattamenti accessibile a chiunque e determina le modalità per la sua 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 per esclusive finalità di applicazione della disciplina in materia di protezione dei dati personali.

#### Art. 38

##### Modalità di notificazione

1. La notificazione del trattamento è presentata al Garante prima dell'inizio del trattamento ed una sola volta, a prescindere dal numero delle operazioni e della durata del trattamento da effettuare, e può anche riguardare uno o più trattamenti con finalità correlate.
2. La notificazione è validamente effettuata solo se è trasmessa per via telematica utilizzando il modello predisposto dal Garante e osservando le prescrizioni da questi impartite, anche per quanto riguarda le modalità di sottoscrizione con firma digitale e di conferma del ricevimento della notificazione.
3. Il Garante favorisce la disponibilità del modello per via telematica e la notifica-

zione anche attraverso convenzioni stipulate con soggetti autorizzati in base alla normativa vigente, anche presso associazioni di categoria e ordini professionali.

4. Una nuova notificazione è richiesta solo anteriormente alla cessazione del trattamento o al mutamento di taluno degli elementi da indicare nella notificazione medesima.
5. Il Garante può individuare altro idoneo sistema per la notificazione in riferimento a nuove soluzioni tecnologiche previste dalla normativa vigente.
6. Il titolare del trattamento che non è tenuto alla notificazione al Garante ai sensi dell'articolo 37 fornisce le notizie contenute nel modello di cui al comma 2 a chi ne fa richiesta, salvo che il trattamento riguardi pubblici registri, elenchi, atti o documenti conoscibili da chiunque.

#### Art. 39

##### Obblighi di comunicazione

1. Il titolare del trattamento è tenuto a comunicare previamente al Garante le seguenti circostanze:
  - a) comunicazione di dati personali da parte di un soggetto pubblico ad altro soggetto pubblico non prevista da una norma di legge o di regolamento, effettuata in qualunque forma anche mediante convenzione;
  - b) trattamento di dati idonei a rivelare lo stato di salute previsto dal programma di ricerca biomedica o sanitaria di cui all'articolo 110, comma 1, primo periodo.
2. I trattamenti oggetto di comunicazione ai sensi del comma 1 possono essere iniziati decorsi quarantacinque giorni dal ricevimento della comunicazione salvo diversa determinazione anche successiva del Garante.

La comunicazione di cui al comma 1 è inviata utilizzando il modello predispo-

sto e reso disponibile dal Garante, e trasmessa a quest'ultimo per via telematica osservando le modalità di sottoscrizione con firma digitale e conferma del ricevimento di cui all'articolo 38, comma 2, oppure mediante telefax o lettera raccomandata.

Art. 40

Autorizzazioni generali

Le disposizioni del presente codice che prevedono un'autorizzazione del Garante sono applicate anche mediante il rilascio di autorizzazioni relative a determinate categorie di titolari o di trattamenti, pubblicate nella Gazzetta Ufficiale della Repubblica italiana.

Art. 41

Richieste di autorizzazione

1. Il titolare del trattamento che rientra nell'ambito di applicazione di un'autorizzazione rilasciata ai sensi dell'articolo 40 non è tenuto a presentare al Garante una richiesta di autorizzazione se il trattamento che intende effettuare è conforme alle relative prescrizioni.
2. Se una richiesta di autorizzazione riguarda un trattamento autorizzato ai sensi dell'articolo 40 il Garante può provvedere comunque sulla richiesta se le specifiche modalità del trattamento lo giustificano.
3. L'eventuale richiesta di autorizzazione è formulata utilizzando esclusivamente il modello predisposto e reso disponibile dal Garante e trasmessa a quest'ultimo per via telematica, osservando le modalità di sottoscrizione e conferma del ricevimento di cui all'articolo 38, comma 2. La medesima richiesta e l'autorizzazione possono essere trasmesse anche mediante telefax o lettera raccomandata.
4. Se il richiedente è invitato dal Garante a fornire informazioni o ad esibire docu-

menti, il termine di quarantacinque giorni di cui all'articolo 26, comma 2, decorre dalla data di scadenza del termine fissato per l'adempimento richiesto.

5. In presenza di particolari circostanze, il Garante può rilasciare un'autorizzazione provvisoria a tempo determinato.

**SOGGETTI CHE EFFETTUANO IL TRATTAMENTO DEI DATI: IL TITOLARE, IL RESPONSABILE E L'INCARICATO**

I soggetti che effettuano o che possono effettuare il trattamento dei dati sono tre: il titolare, il responsabile e l'interessato.

Il **titolare** viene definito come "la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza". L'art. 28 Codice privacy precisa che quando il trattamento "è effettuato da una persona giuridica, da una pubblica amministrazione o da un qualsiasi altro ente, associazione od organismo, titolare del trattamento è 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, ivi compreso il profilo della sicurezza". Il titolare è quindi il principale centro di imputazione giuridica delle scelte di fondo sulle finalità e sull'ampiezza dei trattamenti dei dati. Il titolare è il soggetto a cui spettano le più importanti decisioni in merito alla acquisizione, alla cessione, alla distruzione dei dati<sup>10</sup>. Assume quindi la qualità di titolare il soggetto a cui spetta il potere decisio-

10. Buttarelli, in Acciai R., *Privacy e banche dati pubbliche – il trattamento dei dati personali nelle pubbliche amministrazioni*, Padova, 2001, p. 54 e ss.

nale in merito alle finalità, alle modalità e agli strumenti utilizzati ivi compreso il profilo della sicurezza. Rispetto alla normativa previgente è prevista la contitolarità del trattamento. Oltre ad essere una persona fisica il titolare può essere una persona giuridica, ivi compresa una pubblica amministrazione che può essere sia centralizzata sia decentrata. In quest'ultimo caso deve essere un soggetto che abbia signoria autonoma sul trattamento dei dati.

Gli obblighi del titolare sono numerosi e possono essere così sintetizzati:

- 1) adottare misure idonee per agevolare l'accesso ai dati;
- 2) distruggere, cedere o conservare i dati nel caso di cessazione di un trattamento;
- 3) adottare le misure prescritte dal Garante a garanzia dell'interessato;
- 4) notificare preventivamente al Garante il trattamento avente ad oggetto dati sensibili;
- 5) fornire a chiunque ne faccia richiesta, le notizie contenute nel modello di cui al comma 2 dell'art. 38;
- 6) comunicare preventivamente al Garante i flussi comunicativi tra soggetti pubblici effettuati in qualunque forma nei casi in cui tali flussi comunicativi non siano previsti da alcuna norma;
- 7) comunicare preventivamente al Garante il trattamento di dati idonei a rivelare lo stato di salute previsto da programma di ricerca biomedica o sanitaria;
- 8) nel caso di esercenti le professioni sanitarie o organismi sanitari, designare un medico per la rivelazione all'interessato dei dati personali idonei a rivelare lo stato di salute;
- 9) fornire ed esibire, a norma dell'art. 157, le informazioni e i documenti necessari al Garante per l'esercizio delle proprie attività;

- 10) adottare le eventuali misure prescritte dal Garante al fine di rendere il trattamento conforme alle disposizioni vigenti;
- 11) eseguire, su disposizione del Garante, il blocco del trattamento risultante illecito o non corretto, a seguito della procedura di accertamento del Garante;
- 12) eseguire, nei casi in cui l'accesso ai dati e agli strumenti elettronici sia consentito esclusivamente mediante uso della componente riservata della credenziale per l'autenticazione;
- 13) nel caso di titolare di un trattamento di dati sensibili o di dati giudiziari, redigere entro il 31 marzo di ogni anno (anche attraverso il responsabile, se designato) un documento programmatico sulla sicurezza;
- 14) la nomina del responsabile per il trattamento (adempimento facoltativo).

Il **responsabile** "è la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali".

Il responsabile deve essere individuato e nominato dal titolare anche se la sua designazione non è obbligatoria. Se questa viene effettuata il responsabile deve essere individuato "tra soggetti che per esperienza, capacità ed affidabilità forniscano idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza". Possono essere previsti più responsabili ove la situazione organizzativa lo consiglia. I compiti affidati al responsabile o ai responsabili sono "analiticamente specificati per iscritto dal titolare" e il responsabile o i responsabili effettuano il trattamento "attenendosi

alle istruzioni impartite dal titolare” il quale anche attraverso verifiche periodiche, vigila sulla loro puntuale osservanza.

Possono essere nominati responsabili sia soggetti pubblici che privati sia elementi interni che esterni all’organizzazione, come del resto può essere designato responsabile anche una persona giuridica esterna o persone fisiche non legate con il titolare da un rapporto di lavoro subordinato. Fondamentale qualità per essere designati responsabili è “la preposizione al trattamento dei dati personali da parte del titolare”. In questo caso resta comunque da parte del titolare, il mantenimento “di un potere direttivo sul responsabile in ordine al trattamento dei dati”<sup>11</sup>.

È importante sottolineare come non esista un automatismo *ratione officii* in virtù del quale un responsabile di una funzione organizzativa sia da considerarsi anche responsabile del trattamento dei dati.

Oltre alle istruzioni impartite dal titolare si possono annoverare tra i compiti del responsabile i seguenti:

2. l'estrazione, ai fini dell'esercizio del diritto di accesso degli interessati dei dati e la comunicazione ai richiedenti (vedi artt. 7, 8 e 9);
3. adozione delle misure prescritte dal Garante a garanzia dell'interessato;
4. la comunicazione al titolare dell'invito a esercitare entro dieci giorni dal suo ricevimento la facoltà di comunicare al ricorrente e all'ufficio la propria eventuale adesione spontanea.

Oltre ad effettuare il trattamento dei dati il responsabile può autorizzare le persone fisiche al trattamento dei dati, conferendogli la qualità di incaricato. Ne consegue un potere di controllo su

tali soggetti e impartire agli stessi istruzioni scritte.

Gli *incaricati* del trattamento sono coloro che operano sotto la diretta autorità del titolare o del responsabile, attenendosi alle istruzioni impartite”. La loro designazione “è effettuata per iscritto e individua puntualmente l’ambito del trattamento consentito”. Per essere nominati incaricati quindi bisogna essere una persona fisica, essere i soggetti che materialmente effettuano le operazioni di trattamento, avere una autorizzazione del titolare o del responsabile e agire sotto la diretta autorità del titolare o del responsabile. Oltre alla designazione scritta si considera tale (la designazione) anche “la documentata preposizione della persona fisica ad una unità per la quale è individuata per iscritto, l’ambito del trattamento consentito agli addetti all’unità medesima” (art. 30 codice privacy). Si apre quindi la strada a un a designazione con modulistica standard contenente una sorta di regolamento privacy di reparto valdo per tutti gli incaricati con le specifiche che il responsabile o il titolare riterranno opportune in relazione all’organizzazione del lavoro.

Il disciplinare tecnico sulla redazione del Documento programmatico sulla sicurezza stabilisce, per gli incaricati, la previsione di “interventi formativi ... per renderli edotti dei rischi che incombono sui dati, delle misure per prevenire eventi dannosi, della protezione dei dati personali più rilevanti e delle modalità per l’aggiornamento sulle misure minime di sicurezza adottate dal titolare.

---

11.AAVV, *Codice della privacy*, cit. p. 469.