



*Dispensa:  
Il Codice sulla  
Privacy*

*a cura dello  
Studio Rag. Donatella Tomassini*

novembre '05

## INDICE

<b>PRIVACY</b> .....	<b>pag.</b>	<b>3</b>
Introduzione.....	pag.	3
Il Codice della Privacy.....	pag.	4
Articolazione del Codice della Privacy.....	pag.	4
<b>LA NOTIFICAZIONE DEL TRATTAMENTO DEI DATI</b> .....	<b>pag.</b>	<b>6</b>
Sanzioni in caso di inadempimento della notificazione.....	pag.	7
Soggetti tenuti alla notificazione e ambiti di trattamento.....	pag.	7
Obbligo di notificazione a seguito della deliberazione 1/04 del Garante.....	pag.	7
<b>TRATTAMENTO</b> .....	<b>pag.</b>	<b>12</b>
La responsabilità civile del trattamento di dati personali.....	pag.	12
Titolare del trattamento.....	pag.	12
Responsabile del trattamento.....	pag.	12
Incaricato del trattamento.....	pag.	13
Responsabili “di fatto”.....	pag.	13
<b>MISURA DI SICUREZZA</b> .....	<b>pag.</b>	<b>15</b>
Trattamento di dati comuni e sensibili con strumenti elettronici.....	pag.	15
Sistema di autenticazione informatica e autorizzazione.....	pag.	15
Misure di sicurezza per la prevenzione di intrusioni o perdita di dati.....	pag.	16
Documento programmatico sulla sicurezza.....	pag.	16
Trattamenti senza l’ausilio di strumenti elettronici.....	pag.	17
Trattamenti con strumenti elettronici.....	pag.	18
Misure di “tutela e garanzia”.....	pag.	18
Misure idonee.....	pag.	18
Misure minime.....	pag.	19
Sanzioni per l’omissione di misure di sicurezza.....	pag.	19
Termini per l’adozione delle nuove misure minime.....	pag.	19
Casi di esclusione dell’obbligo di informativa.....	pag.	19
Consenso informato ed esercizio dei diritti.....	pag.	20
Diritti di informazione.....	pag.	20
Diritti pretensivi.....	pag.	20
Diritti oppositivi.....	pag.	20
Modulo del Garante.....	pag.	21
Consenso informato, informativa e autorizzazioni.....	pag.	21
Consenso dell’interessato.....	pag.	21
Casi di consenso non necessario.....	pag.	21
Autorizzazione specifiche del Garante.....	pag.	22
Autorizzazioni generali del Garante.....	pag.	22
Sanzioni trattamento illecito.....	pag.	23
Sanzioni per mancanza del consenso.....	pag.	23
La comunicazione preventiva al Garante.....	pag.	23
Operazioni conseguenti alla cessazione di un trattamento.....	pag.	23
Sanzioni per omessa comunicazione al Garante.....	pag.	24
Principi secondo cui deve avvenire il trattamento e sanzioni generali.....	pag.	24
Sanzioni generali.....	pag.	24
Sanzioni per omessa o inadeguata informativa.....	pag.	24
Casistica particolare: pensionati, case vacanza, attività alberghiere.....	pag.	25

# PRIVACY

## Introduzione

La definizione del termine "privacy" è quella che si adatta al pensiero della classe borghese, di circoscrivere uno spazio individualistico ed intimo da difendere dalle intrusioni esterne.

La tutela della "riservatezza", che viene realizzata attraverso il riferimento a questa accezione della privacy, è tipicamente quella delle persone "in vista" prese di mira dalla stampa scandalistica e mondana o dai servizi giornalistici di approfondimento più "critici" e quella non meno "conservatrice" dei contribuenti che intendono mantenere il segreto sulla consistenza dei propri patrimoni o sul proprio tenore di vita.

Nel medesimo concetto tradizionale di privacy, tuttavia, si riconoscono anche coloro che intendono opporsi alla diffusione ingiustificata di notizie che possano fomentare l'esclusione sociale, la stigmatizzazione dei soggetti deboli o diversi e la discriminazione per motivi legati alle opinioni politiche, religiose o sindacali.

Il vasto movimento riformatore che ha coinvolto l'Europa tra gli anni '70 e gli anni '90 fa riferimento alla seconda accezione della privacy quella ispirata alle preoccupazioni per gli utenti dei nuovi servizi interattivi, sottoposti ad un costante controllo ed incrocio dei dati relativi alle proprie scelte, gusti, interessi. Da ciò deriva la possibilità di una serie di impieghi secondari dei dati, nella forma di profili riguardanti singoli individui, famiglie, gruppi. Si tratta di una nuova "merce" il cui commercio può determinare rischi di tipo più o meno tradizionale per la privacy: ma può soprattutto modificare i rapporti tra fornitori e consumatori di beni e servizi, riducendo l'autonomia di questi ultimi in modo tale da incidere sul modello complessivo di organizzazione sociale ed economica.

Il nuovo Codice D.Lgs. 30 giugno 2003, n. 196 prende posizione rispetto al tema della definizione giuridicamente rilevante della privacy costituendo, a favore di tutti i soggetti sia persone fisiche sia persone giuridiche, una posizione giuridica attiva consistente nel "diritto alla protezione dei dati personali".

Il Codice, in particolare, stabilisce una serie di sanzioni amministrative e penali e rafforza la tutela civilistica del diritto alla riservatezza ispirandosi ai seguenti principi generali

- 1) Il trattamento 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 protezione dei dati personali;
- 2) Il trattamento dei dati personali è disciplinato assicurando un elevato livello di tutela dei diritti e delle libertà delle persone nel rispetto dei principi di semplificazione, armonizzazione ed efficacia delle modalità previste per il loro esercizio da parte degli interessati, nonché per l'adempimento degli obblighi da parte dei titolari del trattamento;
- 3) La disciplina generale relativa al trattamento dei dati è tendenzialmente uniforme per ogni tipo di trattamento; particolari norme sono tuttavia dettate per il trattamento di dati in ambito pubblico; si conferma pertanto il tendenziale dualismo tra la disciplina privatistica e quella pubblicistica della privacy, all'interno del quale fatica a trovare una giusta collocazione l'ambito del Terzo Settore;
- 4) Le garanzie previste dal Codice si estendono anche ai trattamenti di dati personali detenuti all'estero, se vengono effettuati da un soggetto che sia "stabilito nel territorio dello Stato o in un luogo comunque soggetto alla sovranità dello Stato";
- 5) Le garanzie previste dal Codice si estendono anche ai trattamenti di dati personali se vengono impiegati strumenti situati nel territorio dello Stato anche diversi da quelli elettronici, salvo che essi siano utilizzati solo ai fini di transito nel territorio dell'Unione europea, anche se chi effettua il trattamento è stabilito nel territorio di un Paese non appartenente all'Unione europea.

Il trattamento di dati personali effettuato da persone fisiche per fini esclusivamente personali non è soggetto all'applicazione della disciplina del Codice; si applicano, tuttavia, in ogni caso le disposizioni in tema di responsabilità e di sicurezza dei dati e, la disciplina generale trova integrale

applicazione se i dati, pur raccolti da privati per fini personali, sono destinati ad una comunicazione sistematica o alla diffusione.

Non si realizza trattamento di dati personali, e quindi non si applica il Codice, qualora i dati siano resi anonimi, cioè non siano in alcun modo riconducibili a specifiche persone fisiche o giuridiche

L'art. 3 del Codice stabilisce un principio generale relativo al trattamento di dati realizzati mediante il ricorso a sistemi informativi ed a programmi informatici; questi devono essere configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalità che permettano di identificare l'interessato solo in caso di necessità.

### **Il codice della Privacy**

L'attività legislativa italiana ha avuto avvio con l'approvazione da parte del Consiglio d'Europa, a Strasburgo il 28 gennaio 1981, della Convenzione n. 108 "per la protezione delle persone in relazione all'elaborazione automatica dei dati a carattere personale". La successiva intensa attività della Commissione Europea, culminata nell'adozione della Direttiva 95/46/CE del 24 ottobre 1995, in merito a "Tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione dei dati" (G.U. C.E. n. 1. 281/31 del 23 novembre 1995)

La prima legge italiana in materia di privacy è stata la legge n. 675/1996 del 31/12/1996

La fretta con cui il testo di legge è stato esaminato dal Parlamento, per consentirne l'approvazione entro gli stretti termini richiesti da esigenze internazionali, avrebbe imposto la previsione di un secondo strumento di produzione normativa: la legge di delega n. 676/1996 che conferiva all'Esecutivo il potere di emanare uno o più decreti legislativi contenenti disposizioni integrative e correttive della legge appena approvata; anche per questo la legge nasceva, per così dire, all'insegna della provvisorietà e dell'incertezza.

Dal 1996 al 2004 si è verificata una brusca inversione di tendenza.

La produzione legislativa e normativa in tema di privacy è stata sovrabbondante ed il tema della tutela dei dati personali è penetrato profondamente nella coscienza collettiva, il nuovo Codice della privacy è perciò innanzi tutto un Testo Unico, che realizza il coordinamento e la armonizzazione di una produzione legislativa ampia e dettagliata quant'altre mai.

Nella G.U. 29 luglio 2003, Serie generale n. 174, Supplemento ordinario n. 123/L è stato pubblicato l'atteso Codice in materia di protezione dei dati personali.

Il Codice D.Lgs. 30 giugno 2003, n. 196 è entrato in vigore il 1° gennaio 2004, sostituendo integralmente la legge n. 675/1996 e molte disposizioni di legge e di regolamento dettate in materia, ponendosi, come il primo Testo Unico in materia di trattamento di dati personali in Italia.

### **Articolazione del codice della privacy**

Il Testo Unico è composto di 186 articoli suddivisi in tre ampie parti oltre a vari allegati di fondamentale importanza riguardanti: i Codici di Deontologia (all. A.), il Disciplinare Tecnico in materia di misure minime di sicurezza ed i Trattamenti non occasionali in campo giudiziario e di polizia.

La Prima Parte, artt. 1-45, è dedicata alle disposizioni generali in materia di protezione dei dati, Titolo I, e, in ossequio a tali enunciazioni di principio sono posti diritti in capo agli interessati, Titolo II, e correlativi obblighi a carico di chi intenda effettuare trattamento di dati personali altrui; la legge traccia, inoltre, distinzioni tra regole valide per tutti coloro che operano trattamenti di dati e regole specifiche dettate per soggetti pubblici e soggetti privati, Titoli III - IV.

Infine, sono poste le norme fondamentali in materia di sicurezza dei dati e dei sistemi, Titolo V, adempimenti connessi con l'inizio o la cessazione del trattamento dei dati o con il loro trasferimento all'estero, Titoli VI-VII.

La Seconda Parte è dedicata alle disposizioni relative a specifici settori, artt. 46-180, e raccoglie norme di contenuto eterogeneo; si segnalano per il loro rilievo nel campo di attività degli enti non profit le norme a tutela dei minori, Titolo I, capo II; le norme in tema di trattamenti in ambito pubblico spesso coinvolgenti forme di collaborazione-convenzione con il privato sociale, Titolo IV; le norme dettate in tema di trattamento in ambito sanitario, Titolo V; ed infine quelle per il trattamento di dati storici, scientifici e statistici, Titolo VII, che può riguardare direttamente l'attività degli enti non profit ad indirizzo culturale o indirettamente anche quelli dediti ad attività socio-assistenziale che intendano operare un monitoraggio delle propri interventi.

La Terza Parte è dedicata alle sanzioni civili, penali ed amministrative poste a presidio dei diritti sanciti dal Codice.

## LA NOTIFICAZIONE DEL TRATTAMENTO DEI DATI

In base all'art. 38 del Codice "la notificazione del trattamento è presentata al Garante prima dell'inizio del trattamento ed una sola volta, a prescindere dal numero delle operazioni e dalla durata del trattamento da effettuare, e può anche riguardare uno o più trattamenti con finalità correlate" mentre "una nuova notificazione è richiesta solo anteriormente alla cessazione del trattamento (art. 16 del Codice della privacy) o al mutamento di taluno degli elementi da indicare nella notificazione medesima".

Come si è accennato in precedenza, ma è bene ribadirlo, la situazione più comune è quella per cui gli Enti non profit, tenuti alla notificazione in base all'art. 37 del Codice, abbiano già iniziato un trattamento anteriormente al 1° gennaio 2004; orbene, indipendentemente dalla circostanza che lo abbiano notificato in passato o meno, i titolari di simili trattamenti dovevano procedere alla nuova notificazione entro il 30 aprile 2004.

Tutte le notificazioni successive al 1° gennaio 2004 sono considerate dal Garante "nuove notificazioni", anche se in passato i trattamenti di cui sopra siano stati notificati in base alla legge n. 675/1996. Quest'ultima circostanza può riguardare, ad esempio, le cooperative sociali di tipo A, che già anteriormente erano soggette all'obbligo (sia pur in forma semplificata) di notificazione. Solo le "ulteriori eventuali notificazioni" costituiranno ai fini della tenuta del Registro delle semplici "modifiche del trattamento", oppure "cessazioni del trattamento". Superando le incertezze che si erano manifestate in passato, è stato previsto il caso, non infrequente, di "contitolarietà del trattamento"; in questa circostanza è previsto che ciascun contitolare sia tenuto ad effettuare un'autonoma notificazione, nella quale indicherà tutti gli altri contitolari, sottoscrivendo, ovviamente, solo la propria notificazione.

Quanto al contenuto della notificazione essa consta di una parte generale in cui è richiesto di indicare i dati del titolare del trattamento (specificando l'esistenza di eventuali contitolari e del responsabile del trattamento) e di una parte relativa al tipo di trattamento soggetto a notificazione. Compilando la parte specifica relativa alla propria attività, il titolare dovrà indicare:

- 1) la categoria di dati trattati
- 2) le categorie di interessati cui si riferiscono i dati
- 3) le finalità del trattamento
- 4) le modalità del trattamento.

scegliendo le risposte da apposite tabelle allegate alla modulistica consultabile sul sito del Garante. Completa il contenuto della notificazione l'indicazione della eventuale comunicazione o diffusione dei dati all'esterno dell'Ente, il luogo di loro custodia, le misure di sicurezza adottate, l'eventuale utilizzo di siti web per il trattamento dei dati ed il loro trasferimento all'estero.

Quanto alle modalità di notificazione si rileva, innanzi tutto, secondo l'art. 38 del Codice che obbligatoriamente il titolare deve procedere ad una trasmissione "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".

Le istruzioni in sede di prima applicazione della normativa fornite dal Garante sono le seguenti: "La "nuova notificazione" va eseguita unicamente in via telematica, compilando i campi del modello disponibile sul sito Internet <http://www.garanteprivacy.it>. A differenza della notificazione prevista dalla legge n. 675/1996, non è quindi possibile utilizzare modelli cartacei o dischetti, né per la compilazione, né per l'invio. Per quanto riguarda la modifica della notificazione, l'attività del notificante è semplificata. Si può richiamare a video la notificazione già trasmessa, apportando le modifiche necessarie per i soli riquadri interessati. La notificazione, così modificata, è trasmessa osservando la procedura telematica prevista per la nuova notificazione"

Si segnala inoltre che ogni notificazione inviata al Garante (prima notificazione, modifica o cessazione del trattamento) deve essere accompagnata dal pagamento dei diritti di segreteria, il cui importo è fissato in euro 150,00.

Sempre dalla lettura delle istruzioni del Garante si evince che non è stata prevista, in ossequio al dettato dell'art. 38 del Codice, altra forma di sottoscrizione della notificazione che la firma digitale ( art. 10, comma 3, D.P.R. n. 445/2000 ). A tal fine, il titolare del trattamento deve munirsi di un dispositivo di firma digitale disponibile presso uno dei certificatori accreditati ai sensi dell'art. 2, comma 1, lett. c), D.Lgs. n. 10/2002 ovvero può avvalersi dell'operato di professionisti o altri soggetti in grado di effettuare l'invio telematico con firma digitale. Eseguite le operazioni (inserimento dei dati, pagamento dei diritti di segreteria, apposizione della firma digitale e trasmissione in via telematica) e trasmessa la notificazione in via telematica, verrà inviato dal Garante con l'indicazione di giorno, ora e minuto, un ID permanente (C.U.N.) da conservare a cura del notificante. Il C.U.N. verrà comunicato al solo notificante per posta elettronica. Solo con l'inserimento del C.U.N. il notificante potrà accedere, in tempi successivi, alla notificazione per modificarla o per provvedere alla notificazione della cessazione del trattamento.

Il problema della notificazione per gli Enti No Profit si pone, ordinariamente, in occasione dell'inizio del trattamento, della sua cessazione o in seguito al mutamento di taluno degli elementi della notificazione iniziale.

Lo scopo dell'adempimento è chiarissimo: le notificazioni provenienti da tutto il Paese vengono inserite in uno specifico "registro dei trattamenti" tenuto dal Garante (art. 154, comma 1 lett. l del Codice Privacy), ove sono consultabili da chiunque con modalità agevoli.

Ciascun Ente, inoltre, a richiesta di qualunque soggetto i cui dati siano stati fatti oggetto di trattamento deve essere in grado di fornire le informazioni contenute sul modello.

Il tema riveste dunque un indubbio interesse generale sia perché può essere utile a ciascuna organizzazione poter consultare, in sede di tutela dei diritti propri o dei propri assistiti, il registro generale delle notificazioni, sia perché il contenuto standard della notificazione segna la misura minima delle informazioni che il titolare e/o i responsabili del trattamento devono essere costantemente in grado di fornire.

### **Sanzioni in caso di inadempimento della notificazione**

Dopo il 30 aprile 2004, sono scattate le sanzioni amministrative: l'Art. 163 (Omessa o incompleta notificazione) dispone infatti che "Chiunque, essendovi tenuto, non provvede tempestivamente alla notificazione ai sensi degli articoli 37 e 38, ovvero indica in essa notizie incomplete, è punito con la sanzione amministrativa del pagamento di una somma da 10.000 euro a 60.000 euro e con la sanzione amministrativa accessoria della pubblicazione dell'ordinanza-ingiunzione, per intero o per estratto, in uno o più giornali indicati nel provvedimento che la applica."

Ancor più grave, e di diversa natura, la sanzione prevista per il caso di false dichiarazioni o attestazioni in sede di notifica. Tale comportamento integra, infatti, gli estremi del reato previsto dall'art. 168 del Codice e punito, salvo che il fatto costituisca più grave reato, con la reclusione da sei mesi a tre anni".

### **Soggetti tenuti alla notificazione e ambiti di trattamento**

L'art. 37 del Codice della Privacy individua "in positivo" le tipologie dei trattamenti oggetto di notificazione al Garante in quanto suscettibili di recare pregiudizio ai diritti e alle libertà dell'interessato.

Gli ambiti di trattamento che interessano potenzialmente gli enti non profit sono molteplici.

Seguendo, dunque, l'elencazione dell'art. 37 del Codice, per chiarezza espositiva, ricordiamo qui di seguito quali trattamenti devono essere notificati, integrando il testo di legge, con le restrizioni introdotte dal Garante il 31 marzo 2004 ( deliberazione n. 1/2004 del Garante ) e le precisazioni del 23 e 26 aprile.

### **Obbligo di notificazione a seguito della deliberazione 1/04 del Garante**

Sono tenuti alla notificazione i titolari che effettuino il trattamento di:

A) dati genetici, biometrici o dati che indicano la posizione geografica di persone od oggetti mediante una rete di comunicazione elettronica

- Tuttavia l'ambito di applicazione della norma è stato ristretto dal Garante (prov. 1/2004) che ha escluso i trattamenti effettuati da esercenti professioni sanitarie ed avvocati in relazione ai dati biometrici o genetici; con il chiarimento del 23 aprile il Garante ha specificato che l'esonero di cui sopra "opera anche nel caso in cui l'attività sia prestata in forma associata. L'esonero opera inoltre per l'attività svolta da medici titolari di un trattamento in materia di igiene e sicurezza del lavoro e della popolazione."

- Quanto alla individuazione della posizione geografica dei soggetti, è stato specificato dal garante che sono da notificare i soli trattamenti che permettano la localizzazione in forma "continuativa", con il chiarimento del 23 aprile il Garante ha precisato che "Non devono essere notificati al Garante i trattamenti di dati personali che consentano solo una rilevazione non continuativa del passaggio o della presenza di persone o oggetti, effettuata, ad esempio, all'atto della:

a) registrazione di ingressi o uscite presso luoghi di lavoro, tramite tessere elettromagnetiche, codici di accesso o altri dispositivi, a meno che, mediante la rete di comunicazione elettronica, sia possibile tracciare gli spostamenti di interessati in determinati luoghi o aree sul territorio. Non devono essere inoltre trattati dati biometrici, perché in tal caso la notificazione è necessaria;

b) rilevazione di immagini o suoni, anche con impianti a circuito chiuso, presso immobili o edifici ove si svolgono attività del titolare del trattamento (locali commerciali, professionali o dell'ente, nonché le relative aree perimetrali, adibite a parcheggi o a carico/scarico merci, accessi, uscite di emergenza), a meno che, anche mediante interazione con altri sistemi, il titolare possa rilevare le diverse ubicazioni o spostamenti di una persona o di un oggetto in determinati luoghi o aree sul territorio;

c) lettura di carte elettroniche per fornire beni, prestazioni o servizi quali, ad esempio, carte di pagamento, carte di credito o di fidelizzazione. I dati non devono essere peraltro rilevati con strumenti elettronici volti ad analizzare abitudini o scelte di consumo, poiché in tal caso la notificazione è necessaria"

Per tutti gli altri soggetti, ivi compresi gli enti non profit, e le cooperative che effettuino trattamenti di simili dati, l'obbligo di notifica sussiste e deve essere osservato prima dell'inizio del trattamento o, per i trattamenti già iniziati, alla data di entrata in vigore del Codice sulla privacy (1 gennaio 2004), entro il 30 aprile 2004.

In particolare, il Garante ha chiarito con atto del 26 aprile 2004 che: "L'esonero non opera invece per i trattamenti di dati genetici e biometrici effettuati da strutture sanitarie pubbliche o private (ospedali, case di cura e di riposo aziende sanitarie laboratori di analisi cliniche, associazioni sportive). L'esonero è stato infatti disposto solo in favore di persone fisiche esercenti le professioni sanitarie e non per i trattamenti in quanto tali".

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 diffuse, sieropositività, trapianto di organi e tessuti e monitoraggio della spesa sanitaria

- In relazione a simili trattamenti il Garante ha ribadito che è tenuto alla notifica solo il soggetto che eroga servizi sanitari per via telematica relativi ad una banca dati o alla fornitura di beni.

Nei propri chiarimenti resi tra il 23 ed il 26 aprile il Garante ha ulteriormente specificato che: "Non devono essere notificati i trattamenti di dati sanitari -e/o sulla vita sessuale- effettuati nell'ambito di servizi di assistenza o consultazione sanitaria per via telefonica, come i servizi telefonici gestiti in ambito assicurativo e che consentono il consulto di esercenti professioni sanitarie".

- Le considerazioni sull'esonero espresse in tema di dati genetici e biometrici per i professionisti che effettuano il trattamento individualmente o in forma associata valgono anche per i trattamenti relativi a procreazione assistita, trapianti, indagini epidemiologiche, rilevazione di malattie mentali, infettive, diffuse e sieropositività.

Nell'esonero rientrano anche i trattamenti effettuati da un medico specialista nell'ambito di un'attività di consulenza o di procreazione assistita, sempre che non siano effettuati in modo sistematico.

- Per quanto riguarda malattie infettive il trattamento da notificare è solo quello che deve essere effettuato "a fini di rilevazione" di tali patologie e in linea generale riguarda gestori di strutture anziché singoli professionisti che occasionalmente vengono a conoscenza di tali.

- Le prestazioni di servizi sanitari on line vanno notificate solo se i servizi sono:

a) relativi ad una banca dati o siano prestati per via telematica

b) relativi alla fornitura di beni.

Non vanno quindi notificati:

a) i trattamenti di dati sanitari nell'ambito della teleassistenza (consultazione di specialisti per via telefonica)

b) i trattamenti di dati organizzati in banche dati trattati manualmente (archivi cartacei)

c) i trattamenti di dati organizzate in banche dati informatizzate ma non collegate ad una rete telematica

Non devono, infine, notificare i medici che usano unicamente un computer nel proprio ufficio; usano la posta elettronica per dialogare con i pazienti, effettuano prenotazioni per gli assistiti, ecc.

Anche sulla base di altri esempi sono stati considerati quindi esonerati dalla notificazione diversi trattamenti effettuati nell'ambito della cd. medicina in rete. Per altri casi di accesso a banche dati da parte di medici è stato precisato che la notificazione compete invece alla a.s.l. o all'ente locale.

- Monitoraggio della spesa sanitaria; igiene e sicurezza del lavoro.

Poiché non rientrano nel monitoraggio della spesa sanitaria non vanno notificati i trattamenti di dati sanitari effettuati da strutture convenzionate con il Servizio sanitario nazionale, solo per ottenere il rimborso delle prestazioni specialistiche erogate.

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

Il Garante ha ribadito che: "Non vanno notificati al Garante i trattamenti effettuati da associazioni, enti od organismi che non hanno carattere politico, sindacale, religioso o filosofico, come ad esempio cooperative che svolgono attività di ricovero e assistenza a malati psichici.

Il Provvedimento del garante n. 1 del 31 marzo 2004 laddove esclude (punto 3) la notificazione per i trattamenti di dati idonei a rivelare la sfera psichica di lavoratori in materia di rapporto di lavoro e di previdenza, si riferisce anche ai casi in cui si deve adempiere a specifici obblighi stabiliti in sede di contrattazione collettiva e giuridicamente rilevanti in base alla normativa in materia ".

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.

In relazione a tale previsione, che può indirettamente coinvolgere anche Enti non profit o Cooperative il Garante ha ritenuto opportuno chiarire ulteriormente che:

- Ai fini dell'obbligo di notificazione, gli strumenti elettronici utilizzati devono essere configurati e impiegati per definire o valutare il profilo o la personalità dell'interessato, oppure per analizzare le sue abitudini o scelte di consumo.

- I sistemi o programmi informatici devono essere finalizzati a registrare, elaborare o raffrontare specifiche annotazioni per studiare il comportamento o le preferenze di singoli interessati od utenti individuati nominativamente o identificabili anche indirettamente attraverso appositi codici.

- Non devono essere quindi notificati i trattamenti di dati effettuati al solo fine di:

- fornire all'interessato beni, prestazioni o servizi, con l'ausilio di strumenti elettronici finalizzati alla gestione del relativo rapporto e dei connessi adempimenti contabili o fiscali, all'invio di eventuali

comunicazioni informative commerciali e al controllo della qualità di servizi offerti senza procedere ad alcuna profilazione degli interessati;

- verificare l'identità o il profilo di autorizzazione di utenti o incaricati, nell'ambito di sistemi di autenticazione informatica o di autorizzazione per l'accesso a dati o sistemi (ad esempio, per accedere ad una banca di dati personali o a determinati contenuti di un sito web). Anche in questo caso, tuttavia, se sono trattati dati biometrici la notificazione è necessaria ( art. 37, comma 1, lett. a), D.Lgs. n. 196/2003 );

- registrare gli accessi ad un sito web, se i dati sono memorizzati esclusivamente per il tempo tecnicamente indispensabile ai fini di sicurezza del sistema o di elaborazione statistica in forma anonima.

Si tratta quindi di precisazioni che circoscrivono ulteriormente l'obbligo limitandolo a casi in cui effettivamente la creazione del profilo utente non è funzionale alla mera attuazione delle prestazioni richieste dall'utente.

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.

Il Garante in questo settore ha semplicemente ribadito le esclusioni decise con il provvedimento n. 1 del 2004 per cui non sono da notificare i trattamenti effettuati:

a) al solo fine di selezione di personale per conto esclusivamente di soggetti appartenenti al medesimo gruppo bancario o societario;

b) da soggetti pubblici per adempiere esclusivamente a specifici obblighi o compiti previsti dalla normativa in materia di occupazione e mercato del lavoro;

c) da associazioni o organizzazioni di categoria al solo fine di svolgere ricerche campionarie relativamente a dati riguardanti l'adesione alla medesima associazione o organizzazione".

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

Il Garante ha fornito in questo campo importanti delucidazioni che si riportano per esteso:

"Non devono essere notificati i trattamenti effettuati da soggetti che utilizzano banche di dati centralizzate o sistemi informativi gestiti autonomamente da altri soggetti -titolari del relativo trattamento- e che, pur comunicando a questi ultimi alcuni dati personali, non hanno alcun potere decisionale in ordine alle finalità e alle modalità del trattamento e agli strumenti utilizzati in tali ambiti. Ciò anche quando, per mere ragioni tecniche, una copia della banca di dati gestita dal terzo autonomo titolare del trattamento, risieda presso il soggetto abilitato unicamente a consultarla in tale forma.

Ad esempio, banche, uffici postali e società emittenti carte di pagamento non devono notificare i trattamenti di dati effettuati nell'ambito dell'archivio informatizzato degli assegni bancari e postali e delle carte di pagamento istituito ai sensi del d.lg. n. 507/1999 (c.d. Centrale di allarme interbancaria-CAI) e gestito dalla Banca di Italia in qualità di titolare del trattamento (art. 10-bis, comma 2, l. n. 386/1990; art. 1, comma 4, d. m. n. 458/2001).

In riferimento ai casi indicati nella Deliberazione del 31 marzo 2004, n. 1 del Garante , si ritiene utile infine precisare che:

a) non devono essere notificati (punto 6, lett. b) i trattamenti relativi a clienti o fornitori effettuati da liberi professionisti od organismi (es.: CAAF) per adempimenti fiscali (ad es., in qualità di intermediari necessari per presentare le dichiarazioni dei redditi) o contabili (es.: redazione di bilanci), oppure per svolgere investigazioni difensive o curare la difesa in sede giudiziaria di diritti degli assistiti;

b) i trattamenti relativi alla fornitura di beni, prestazioni o servizi (ad esempio, concernenti clienti, fornitori o dipendenti) o ad adempimenti contabili o fiscali, e che non devono essere notificati in base alla deliberazione n. 1/2004 (punto 6, lett. b) ), riguardano anche dati di cui sia necessario il trattamento in sede pre-contrattuale;

c) i trattamenti relativi ad obbligazioni, comportamenti illeciti o fraudolenti che non devono essere notificati in quanto trattati solo per adempiere ad obblighi normativi in materia di rapporto di lavoro, previdenza o assistenza (punto 6, lett. c)), comprendono quelli concernenti eventuali obblighi derivanti dalla contrattazione collettiva, giuridicamente rilevanti in base alla normativa in materia;

d) sono sottratti all'obbligo di notificazione i soggetti pubblici che utilizzano la banca di dati elettronica per riscuotere tributi, applicare sanzioni amministrative o rilasciare licenze, concessioni o autorizzazioni ( punto 6, lett. d) del Deliberazione n. 1/2004 ). Devono invece notificare i soggetti privati concessionari di servizi di riscossione di tributi che esercitano le medesime attività, a meno che essi svolgano formalmente ed effettivamente le funzioni di "responsabile del trattamento" per conto del soggetto pubblico conformemente alle disposizioni vigenti su tale designazione ( art. 29 del codice della privacy );

e) non sono sottratti all'obbligo di notificazione i trattamenti di immagini o suoni che, benché registrati temporaneamente, siano inseriti in apposite banche di dati elettroniche relative a comportamenti illeciti o fraudolenti ( punto 6, lett. e), Del. n. 1/2004 )."

L'elenco delle materie soggette a notificazione di cui al citato art. 37 non è però un numero chiuso. Lo stesso Garante ha la facoltà di estendere o restringere l'ambito di operatività delle norme citate in ragione del rischio cui sono potenzialmente sottoposti i diritti dell'interessato. In quest'ottica i trattamenti di dati effettuati da enti non profit che in futuro potrebbero essere interessati dall'applicazione della norma sono molti di più; anche sotto questo profilo è opportuno procedere ad una frequente verifica dell'evoluzione normativa per non incorrere nelle sanzioni specificamente previste per l'omissione di notifica.

L'adempimento deve essere preventivo, cioè deve precedere l'inizio del trattamento, tuttavia, per i trattamenti già iniziati alla data di entrata in vigore del Codice, e quindi la gran maggioranza dei trattamenti effettuati dagli enti non profit, molto opportunamente il Legislatore ha previsto una norma transitoria che ha consentito l'adeguamento entro il 30 aprile 2004 ( art. 181 cod. Privacy ).

## TRATTAMENTO

### **La responsabilità civile da trattamento di dati personali**

L'art. 15 del Codice della privacy impone a chiunque cagiona danno ad altri per effetto del trattamento di dati personali di risarcire il danno.

Ciò significa concretamente che potrebbero essere chiamati a rispondere del danno non solo il Titolare, ma anche gli altri soggetti che avrebbero dovuto impedire il realizzarsi dell'evento dannoso o che con il proprio comportamento vi hanno dato direttamente causa.

Nel settore non profit, la questione risarcitoria potrebbe assumere rilievo e proporzioni rilevanti soprattutto per i componenti degli organi amministrativi.

Le figure soggettive rilevanti ai fini dell'individuazione della responsabilità in ordine al trattamento dei dati personali sono essenzialmente tre:

- 1) **il titolare del trattamento**
- 2) **il responsabile del trattamento**
- 3) **l'incaricato del trattamento.**

### **Titolare del trattamento**

Il titolare del trattamento è 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".

Titolare del trattamento è, nel settore non profit, sempre coincidente con l'Ente, l'Associazione, la Fondazione o l'Organizzazione di volontariato "cui competono sempre le decisioni ultime in questa materia", anche se la volontà dell'Ente è espressa attraverso l'organo o gli organi a ciò deputati dall'atto costitutivo o dallo statuto dei vari Enti: il Consiglio Direttivo, il Presidente.

Invero solo le Associazioni giuridicamente riconosciute e le Fondazioni godono di una autonomia patrimoniale perfetta per cui solo questi Enti risponderanno esclusivamente con il proprio patrimonio degli eventuali danni causati dal trattamento antigiuridico dei dati personali altrui effettuato dai propri incaricati. In ogni altro caso si porrebbe il problema della responsabilità solidale degli amministratori della Associazione non riconosciuta o del Comitato ex art. 38 c.c, qualora sia ravvisabile un collegamento tra la loro opera dispiegata in concreto e l'evento dannoso.

### **Responsabile del Trattamento**

Il Responsabile del Trattamento è definito come 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 titolare del trattamento potrà, in sostanza, scegliere "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" un collaboratore cui delegare alcuni dei propri compiti (art. 29). I compiti, affidati al responsabile, dovranno tuttavia essere analiticamente specificati per iscritto. A sua volta il responsabile dovrà effettuare il trattamento attenendosi alle istruzioni impartite dal titolare il quale, anche tramite verifiche periodiche, vigilerà sulla puntuale osservanza delle disposizioni di legge e delle proprie istruzioni.

Ove necessario, per esigenze organizzative, possono essere designati responsabili più soggetti, anche mediante suddivisione di compiti.

Qualora nominato, alla responsabilità del Titolare si aggiungerà la responsabilità solidale di tale soggetto, alleggerendo, indirettamente, quella soggettiva e personale degli amministratori cui potrà essere solo imputato di non avere scelto oculatamente il Responsabile (culpa in eligendo) o di non avere vigilato sulla sua attività (culpa in vigilando).

### **Incaricato del trattamento**

L'incaricato del trattamento, è la persona fisica e non anche - come nel caso dei Responsabili - la persona giuridica, "autorizzata a compiere operazioni di trattamento dal titolare o dal responsabile"; anche in questo caso la designazione è effettuata per iscritto e individua puntualmente l'ambito del trattamento consentito ad una determinata persona o ad un gruppo di persone in relazione alla funzione esercitata all'interno dell'Organizzazione (amministratori, revisori, assistenti sociali, volontari, impiegati amministrativi).

Gli incaricati non sono quindi solo coloro che svolgono attività meramente esecutive; il loro ruolo nell'organizzazione può anche essere di vertice ma rispetto al trattamento dei dati non hanno capacità decisionali autonome; come specifica l'art 30 del codice, "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".

Anche rispetto a queste figure soggettive può operare il concorso, interno, di responsabilità nei confronti del danneggiato, tenendo conto della adeguatezza delle istruzioni impartite dal Responsabile e dal Titolare e della diligenza utilizzata nello svolgimento dai propri compiti.

### **Responsabili "di fatto"**

Chiunque, e non solo le figure soggettive autorizzate ad effettuare i trattamenti, può essere chiamato a rispondere dei danni cagionati.

Possono rientrare in questa categoria i responsabili "di fatto", cioè chi abbia operato come responsabile della privacy al fuori di una formale investitura; o soggetti che pur operando per l'Ente in questione non siano stati incaricati del trattamento dei dati che hanno, in fatto, operato. Allo stesso modo gli amministratori dell'Ente, sia riconosciuto sia non riconosciuto, possono essere chiamati personalmente a concorrere alla responsabilità dell'Ente qualora sia dimostrata una loro personale colpa nella causazione dell'evento; ad esempio per non aver deliberato la spesa occorrente all'adozione delle misure evidenziate dal responsabile del trattamento che siano apparse come idonee ad evitare il danno.

L'art. 15 del Codice della privacy , rubricato "Danni cagionati per effetto del trattamento" stabilisce che: "Chiunque cagiona danno ad altri per effetto del trattamento di dati personali è tenuto al risarcimento ai sensi dell'articolo 2050 del codice civile. Il danno non patrimoniale è risarcibile anche in caso di violazione dell'articolo 11 ."

Ciò significa, concretamente che, oltre alle specifiche sanzioni di tipo penale o amministrativo che presidiano il rispetto delle norme poste a tutela della privacy, il Titolare del trattamento dei dati può essere in ogni caso chiamato a risarcire il danno cagionato all'interessato in conseguenza del trattamento errato o fraudolento dei dati personali altrui.

La disciplina del risarcimento del danno in questo settore è, tuttavia, particolarmente rigorosa.

Il Codice sulla privacy dispone che il risarcimento seguirà non la regola generale di cui all'art 2043 del c.c. che impone a chiunque lamenti di avere subito un danno di provare in giudizio gli elementi costitutivi del proprio diritto, bensì la ben più favorevole per i danneggiati regola di cui all'art. 2050 del c.c..

Ciò concretamente significa che si opera, in giudizio, una sorta di inversione dell'onere della prova tale per cui il Titolare del trattamento o chiunque vi sia obbligato può evitare la condanna solo se prova "di avere adottato tutte le misure idonee ad evitare il danno".

Al riguardo si segnala l'orientamento giurisprudenziale per cui "la presunzione di responsabilità contemplata dalla norma dell'art. 2050 c.c. per le attività pericolose può essere vinta solo con una prova particolarmente rigorosa, essendo posto a carico dell'esercente l'attività pericolosa l'onere di dimostrare l'adozione di "tutte le misure idonee ad evitare il danno": pertanto non basta la prova negativa di non aver commesso alcuna violazione delle norme di legge o di comune prudenza, ma occorre quella positiva di aver impiegato ogni cura o misura atta ad impedire l'evento dannoso, di

guisa che anche il fatto del danneggiato o del terzo può produrre effetti liberatori solo se per la sua incidenza e rilevanza sia tale da escludere, in modo certo, il nesso causale tra attività pericolosa e l'evento e non già quando costituisce elemento concorrente nella produzione del danno, inserendosi in una situazione di pericolo che ne abbia reso possibile l'insorgenza a causa dell'inidoneità delle misure preventive adottate." (Cass. Sez. III, sent. n. 5960 del 21 novembre 1984).

Infine si osservi, rispetto al tema della quantificazione del danno, che seppur l'interessato non fosse in grado di dimostrare di avere patito un danno patrimoniale in conseguenza del trattamento illegittimo, potrebbe chiedere comunque il risarcimento del danno "non patrimoniale" che è risarcibile, oltre le norme comuni, anche in caso di violazione delle regole sul trattamento dei dati.

## MISURE DI SICUREZZA

### **Trattamento di dati comuni e sensibili con strumenti elettronici**

Il soggetto che deve porre in essere le misure sotto elencate è il Titolare del trattamento, cioè l'Associazione o la Fondazione nel suo complesso, a mezzo dell'attività dei propri organi direttivi.

L'esecuzione di tali misure può essere delegata al Responsabile della privacy, da designarsi per iscritto sempre a cura del Titolare.

Le misure minime per il trattamento con strumenti elettronici di dati comuni e sensibili sono elencate dal Disciplinare Tecnico in materia di sicurezza (allegato B del Codice), ulteriormente specificate in molteplici e complesse modalità tecniche che qui di seguito vengono sinteticamente esposte.

### **Sistema di autenticazione informatica e autorizzazione**

Il titolare, direttamente o attraverso il responsabile della privacy, deve dotare ogni incaricato del trattamento di dati personali di (una o più) credenziali di autenticazione che consentano il superamento di una procedura di autenticazione relativa ad uno specifico trattamento o ad un insieme di trattamenti. Le credenziali di autenticazione consistono in un codice per l'identificazione dell'incaricato associato ad una parola chiave riservata conosciuta solamente dal medesimo oppure in un dispositivo di autenticazione in possesso ed uso esclusivo dell'incaricato, eventualmente associato ad un codice identificativo o ad una parola chiave, oppure in una caratteristica biometrica dell'incaricato, eventualmente associata ad un codice identificativo o ad una parola chiave.

Il titolare deve prescrivere all'incaricato di adottare le cautele che si rendono necessarie per assicurare la segretezza della componente riservata della credenziale e la diligente custodia dei dispositivi in possesso ed uso esclusivo dell'incaricato stesso.

Le disposizioni seguenti non si applicano ai trattamenti dei dati personali destinati alla diffusione.

La parola chiave, quando è prevista dal sistema di autenticazione, deve essere composta da almeno otto caratteri oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito; essa non deve contenere riferimenti agevolmente riconducibili all'incaricato e va modificata da quest'ultimo al primo utilizzo e, successivamente, almeno ogni sei mesi. In caso di trattamento di dati sensibili e di dati giudiziari, è necessario modificare la parola chiave almeno ogni tre mesi.

Il codice per l'identificazione, laddove utilizzato, non può essere assegnato ad altri incaricati, neppure in tempi diversi. Le credenziali di autenticazione non utilizzate da almeno sei mesi sono da disattivare, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica. Le credenziali vanno disattivate anche in caso di perdita della qualità che consente all'incaricato l'accesso ai dati personali. Il titolare deve impartire istruzioni agli incaricati perché non sia lasciato incustodito e accessibile a terzi lo strumento elettronico durante una sessione di trattamento.

Quando l'accesso ai dati e agli strumenti elettronici è consentito esclusivamente mediante uso della componente riservata della credenziale per l'autenticazione, sono da individuare per iscritto le modalità con le quali il titolare può assicurare la disponibilità di dati o strumenti elettronici in caso di prolungata assenza o impedimento dell'incaricato che renda indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema. In tal caso la custodia delle copie delle credenziali va organizzata garantendo la relativa segretezza ed individuando preventivamente per iscritto i soggetti incaricati della loro custodia, i quali devono informare tempestivamente l'incaricato dell'intervento effettuato.

Quando per gli incaricati sono individuati profili di autorizzazione di ambito diverso va utilizzato un sistema di autorizzazione. I profili di autorizzazione, per ciascun incaricato o per classi omogenee di incaricati, devono essere individuati e configurati dal titolare anteriormente all'inizio del trattamento, in modo da limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento. Periodicamente, e comunque almeno annualmente, bisogna verificare poi la sussistenza delle condizioni per la conservazione dei profili di autorizzazione.

### **Misure di sicurezza per la prevenzione di intrusioni o perdita di dati**

Il titolare o il responsabile, ove designato, debbono redigere una lista degli incaricati, anche per classi omogenee di incarico, e dei relativi profili di autorizzazione; tali liste vanno aggiornate, almeno una volta l'anno, per consentire ai singoli incaricati e agli addetti alla gestione o alla manutenzione degli strumenti elettronici un accesso selettivo ai dati che devono poter trattare.

Il titolare deve impartire le opportune disposizioni affinché i dati personali siano protetti contro il rischio di intrusione di virus informatici, mediante l'attivazione di idonei strumenti elettronici da aggiornare con cadenza almeno semestrale.

Gli aggiornamenti periodici dei programmi per elaboratore, volti a prevenire la vulnerabilità di strumenti elettronici e a correggerne difetti, sono da effettuare almeno annualmente.

In caso di trattamento di dati sensibili o giudiziari l'aggiornamento deve essere almeno semestrale.

Il titolare deve impartire istruzioni organizzative e tecniche che prevedono il salvataggio dei dati con frequenza almeno settimanale.

### **Documento programmatico sulla sicurezza**

Tra le misure minime più impegnative vi è senza dubbio la redazione del documento programmatico di sicurezza, adempimento cui il Disciplinare tecnico dedica la regola 19.

In base a tale disposizione, i soggetti tenuti alla redazione del DPS sono esclusivamente i titolari di un trattamento di dati sensibili o di dati giudiziari effettuato con strumenti elettronici (cfr. anche la Guida operativa per redigere il Documento programmatico sulla sicurezza (DPS)).

Entro il 31 marzo di ogni anno, il titolare di un trattamento di dati sensibili o di dati giudiziari redige anche attraverso il responsabile, se designato, un documento programmatico sulla sicurezza.

Il termine per la redazione del documento, da parte dei soggetti che vi siano tenuti per la prima volta, è stato prorogato prima al 30 giugno 2005 poi al 31/12/2005.

Il documento programmatico deve contenere idonee informazioni riguardo:

- l'elenco dei trattamenti di dati personali;
- la distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati;
- l'analisi dei rischi che incombono sui dati;
- le misure da adottare per garantire l'integrità e la disponibilità dei dati, nonché la protezione delle aree e dei locali, rilevanti ai fini della loro custodia e accessibilità;
- la descrizione dei criteri e delle modalità per il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento;
- la previsione di interventi formativi degli incaricati del trattamento, per renderli edotti dei rischi che incombono sui dati, delle misure disponibili per prevenire eventi dannosi, dei profili della disciplina sulla protezione dei dati personali più rilevanti in rapporto alle relative attività, delle responsabilità che ne derivano e delle modalità per aggiornarsi sulle misure minime adottate dal titolare. La formazione va programmata già al momento dell'ingresso in servizio, nonché in occasione di cambiamenti di mansioni o di introduzione di nuovi significativi strumenti, rilevanti rispetto al trattamento di dati personali;
- la descrizione dei criteri da adottare per garantire l'adozione delle misure minime di sicurezza in caso di trattamenti di dati personali affidati, in conformità al codice, all'esterno della struttura del titolare;
- per i dati personali idonei a rivelare lo stato di salute e la vita sessuale, l'individuazione dei criteri da adottare per la cifratura o per la separazione di tali dati dagli altri dati personali dell'interessato.

### **Altre misure per il trattamento di dati sensibili o giudiziari**

I dati sensibili o giudiziari vanno protetti contro l'accesso abusivo ad un sistema informatico o telematico mediante l'utilizzo di idonei strumenti elettronici.

Il titolare o il responsabile, se designato, deve provvedere ad impartire istruzioni organizzative e tecniche per la custodia e l'uso dei supporti rimovibili su cui sono memorizzati i dati al fine di evitare accessi non autorizzati e trattamenti non consentiti. Tali supporti rimovibili, se non utilizzati,

devono essere distrutti o resi inutilizzabili, ovvero possono essere riutilizzati da altri incaricati, non autorizzati al trattamento degli stessi dati, se le informazioni precedentemente in essi contenute non sono intelligibili e tecnicamente in alcun modo ricostruibili.

Vanno adottate idonee misure per garantire il ripristino dell'accesso ai dati in caso di danneggiamento degli stessi o degli strumenti elettronici, in tempi certi compatibili con i diritti degli interessati e non superiori a sette giorni.

Gli organismi sanitari e gli esercenti le professioni sanitarie devono effettuare il trattamento dei dati idonei a rivelare lo stato di salute e la vita sessuale contenuti in elenchi, registri o banche di dati con tecniche di cifratura o mediante l'utilizzazione di codici identificativi o di altre soluzioni che, considerato il numero e la natura dei dati trattati, li rendono temporaneamente inintelligibili anche a chi è autorizzato ad accedervi e permettono di identificare gli interessati solo in caso di necessità, anche al fine di consentire il trattamento disgiunto dei medesimi dati dagli altri dati personali che permettono di identificare direttamente gli interessati.

I dati relativi all'identità genetica vanno trattati esclusivamente all'interno di locali protetti accessibili ai soli incaricati dei trattamenti ed ai soggetti specificatamente autorizzati ad accedervi; il trasporto dei dati all'esterno dei locali riservati al loro trattamento deve avvenire in contenitori muniti di serratura o dispositivi equipollenti; il trasferimento dei dati in formato elettronico deve essere cifrato.

### **Trattamenti senza l'ausilio di strumenti elettronici**

Per i Trattamenti senza l'ausilio di strumenti elettronici sono previste le seguenti misure minime:

- aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unità organizzative;
- previsione di procedure per un'idonea custodia di atti e documenti affidati agli incaricati per lo svolgimento dei relativi compiti;
- previsione di procedure per la conservazione di determinati atti in archivi ad accesso selezionato e disciplina delle modalità di accesso finalizzata all'identificazione degli incaricati.

Il soggetto che deve porre in essere le misure sopra elencate è il Titolare del trattamento, cioè l'Associazione o la Fondazione nel suo complesso, a mezzo dell'attività dei propri organi direttivi. L'esecuzione di tali misure può essere delegata al Responsabile della privacy, da designarsi per iscritto sempre a cura del Titolare.

Si segnala che, anche quando il trattamento dei dati avviene senza l'ausilio degli strumenti elettronici, vi sono comunque alcuni adempimenti da rispettare, delineati dal Disciplinare Tecnico in materia di sicurezza e qui sinteticamente riportati:

1. Il titolare, direttamente o attraverso il responsabile della privacy, deve impartire agli incaricati istruzioni scritte finalizzate al controllo e alla custodia, per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento, degli atti e dei documenti contenenti dati personali.
2. Nell'ambito dell'aggiornamento periodico con cadenza almeno annuale dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati, la lista degli incaricati può essere redatta anche per classi omogenee di incarico e dei relativi profili di autorizzazione.
3. Quando gli atti e i documenti contenenti dati sensibili o giudiziari sono affidati agli incaricati del trattamento per lo svolgimento dei relativi compiti, i medesimi atti e documenti devono essere controllati e custoditi dagli incaricati fino alla restituzione, in maniera che ad essi non accedano persone prive di autorizzazione, e vanno restituiti al termine delle operazioni affidate.
4. L'accesso agli archivi contenenti dati sensibili o giudiziari deve essere controllato. Le persone ammesse, a qualunque titolo, dopo l'orario di chiusura, sono da identificare e registrare. Quando gli archivi non sono dotati di strumenti elettronici per il controllo degli accessi o di incaricati della vigilanza, le persone che vi accedono devono essere preventivamente autorizzate.

### **Trattamenti con strumenti elettronici**

Per i Trattamenti con strumenti elettronici sono previste le seguenti misure minime:

- autenticazione informatica;
- adozione di procedure di gestione delle credenziali di autenticazione;
- utilizzazione di un sistema di autorizzazione;
- aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici;
- protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di dati, ad accessi non consentiti e a determinati programmi informatici;
- adozione di procedure per la custodia di copie di sicurezza, il ripristino della disponibilità dei dati e dei sistemi;
- tenuta di un aggiornato documento programmatico sulla sicurezza;
- adozione di tecniche di cifratura o di codici identificativi per determinati trattamenti di dati idonei a rivelare lo stato di salute o la vita sessuale effettuati da organismi sanitari.

### **Misure di "tutela e garanzia"**

Si segnalano, inoltre, per la loro importanza le misure di "tutela e garanzia" previste dal Disciplinare Tecnico.

In base alla regola n. 25. il titolare può adottare misure minime di sicurezza avvalendosi di soggetti esterni alla propria struttura, per provvedere alla esecuzione, in tal caso dovrà farsi rilasciare dall'installatore "una descrizione scritta dell'intervento effettuato che ne attesta la conformità alle disposizioni del presente disciplinare tecnico".

In base alla regola 26 il titolare dovrà riferire, nella relazione accompagnatoria del bilancio d'esercizio, se dovuta, dell'avvenuta redazione o aggiornamento del documento programmatico sulla sicurezza. Tale regola riguarda tutti gli Enti non profit che per legge o per statuto siano tenuti alla elaborazione del bilancio.

La ratio della norma è, palesemente, quella di responsabilizzare gli organi di vertice degli Enti che con scadenza per lo meno annuale dovranno vigilare sull'operato del Responsabile ed interrogarsi sullo stato di attuazione del Dps.

Una eventuale omissione di tale regola chiamerà in causa l'eventuale responsabilità del Titolare per culpa in vigilando e potrebbe configurare anche una concorrente responsabilità personale degli amministratori.

### **Misure idonee**

Strettamente connessa alla responsabilità ex art.2050 c.c. per il trattamento antigiuridico dei dati personali è la disciplina codicistica delle misure di sicurezza.

La legge impone al Titolare il risarcimento extracontrattuale, pertanto, se non prova di avere adottato tutte le misure idonee a evitare l'evento dannoso conseguente al trattamento dei dati personali, è pienamente comprensibile l'imposizione in capo al Titolare di uno speculare dovere positivo: l'adozione di ogni misura atta a prevenire danni a terzi; in altre parole il titolare dovrà approntare le prassi, i protocolli, le procedure e gli strumenti tecnici idonei ad evitare che il trattamento dei dati personali altrui possa cagionare all'interessato un danno.

Tale obbligo generale, specificazione del generale principio giuridico del *neminem laedere*, trova una compiuta disciplina nel Codice della privacy all'articolo 31 che impone al Titolare di adoperarsi affinché i dati personali oggetto di trattamento siano "custoditi e controllati, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta".

### **Misure minime**

Un rilievo particolare hanno le misure minime di sicurezza.

Nel quadro dei più generali obblighi di sicurezza indicati nella parte dedicata alle "Misure idonee", o previsti da speciali disposizioni, i Titolari del trattamento sono comunque tenuti ad adottare le misure minime specificate dal Codice e dal Disciplinare tecnico, volte ad assicurare un livello minimo di protezione dei dati personali.

Tali misure sono diversamente declinate qualora il Titolare adotti o meno strumenti elettronici nel trattamento dei dati.

### **Sanzioni per l'omissione di misure di sicurezza**

Ai sensi dell'art. 169 del codice della privacy (Misure di sicurezza), chiunque, essendovi tenuto, omette di adottare le misure minime previste dall'articolo 33 è punito con l'arresto sino a due anni o con l'ammenda da 10.000 euro a 50.000 euro.

All'autore del reato, all'atto dell'accertamento o, nei casi complessi, anche con successivo atto del Garante, e' impartita una prescrizione fissando un termine per la regolarizzazione non eccedente il periodo di tempo tecnicamente necessario, prorogabile in caso di particolare complessità o per l'oggettiva difficoltà dell'adempimento e comunque non superiore a sei mesi.

Nei sessanta giorni successivi allo scadere del termine, se risulta l'adempimento alla prescrizione, l'autore del reato e' ammesso dal Garante a pagare una somma pari al quarto del massimo dell'ammenda stabilita per la contravvenzione.

L'adempimento e il pagamento estinguono il reato.

La condanna per uno dei delitti previsti dal codice della privacy importa la pubblicazione della sentenza.

### **Termini per l'adozione delle "nuove" misure minime**

Il Legislatore, per venire incontro a non poche richieste provenienti soprattutto dagli operatori economici, si è visto costretto a differire il termine di adeguamento delle proprie strutture dei titolari alle nuove misure minime di sicurezza - originariamente previsto per il 30 giugno del 2004 - prima al 31 dicembre 2004, con D.L. 24 Giugno 2004, n. 158 e successivamente al 30 giugno 2005, con il D.L. 9 novembre 2004, n. 266.

Infine, la Legge 1° marzo 2005, n.26 "Conversione in legge, con modificazioni, del decreto-legge 30 dicembre 2004, n. 314, recante proroga di termini", pubblicata sulla GU n. 50 del 2 marzo 2005, ha ulteriormente differito il termine per la redazione del Documento programmatico in materia di sicurezza sino al 31 dicembre 2005 insieme alle altre misure di sicurezza c.d. nuove, cioè che non erano previste dal D.P.R. 28 luglio 1999, n. 318; conseguentemente scivola al 31 marzo 2006 la data, ulteriormente, prevista per l'adeguamento alle misure minime di cui all'articolo 34 (secondo modalità tecniche di cui all'allegato B), nel caso in cui il titolare, entro il termine del 31 dicembre 2005 descriva in un documento a data certa, da conservare presso la propria struttura, le obiettive ragioni tecniche per cui i propri strumenti elettronici non consentono in tutto o in parte l'immediata applicazione delle misure di cui sopra. In questo secondo caso il titolare è, comunque, tenuto ad adottare ogni possibile misura di sicurezza in relazione agli strumenti elettronici detenuti in modo da evitare, anche sulla base di idonee misure organizzative, logistiche o procedurali, un incremento dei rischi.

### **Casi di esclusione dell'obbligo di informativa**

Se i dati personali non sono raccolti presso l'interessato, l'informativa, comprensiva delle categorie dei 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 salvo che:

- a) i dati siano trattati in base ad un obbligo previsto dalla legge, da un regolamento o dalla normativa comunitaria;
- b) i dati siano 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 comporti un impiego di mezzi che il Garante, prescrivendo eventuali misure appropriate, dichiari manifestamente sproporzionati rispetto al diritto tutelato, ovvero si riveli, a giudizio del Garante, impossibile.

### **Consenso informato ed esercizio dei diritti**

Il Titolare, o quando è stato designato un responsabile per il riscontro all'interessato, deve essere in grado di rispondere all'interessato che eserciti i diritti di cui all'articolo 7 del Codice sulla privacy.

Si tratta, non solo di diritti di informazione e diritti pretensivi ma anche oppositivi molto importanti e potenzialmente onerosi per il titolare, in quanto appunto, soggetto passivo degli obblighi; passiamo ad illustrarne il contenuto.

### **Diritti di informazione**

1) L'interessato ha diritto di 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.

2) L'interessato ha diritto di ottenere l'indicazione:

a) dell'origine dei dati personali;

b) delle finalità e modalità del trattamento;

c) della logica applicata in caso di trattamento effettuato con l'ausilio di strumenti elettronici;

d) degli estremi identificativi del titolare, dei responsabili e del rappresentante designato nel territorio dello Stato,

e) dei soggetti o delle categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di rappresentante designato nel territorio dello Stato, di responsabili o incaricati.

### **Diritti pretensivi**

1) l'aggiornamento, la rettificazione ovvero, quando vi ha interesse, l'integrazione dei dati;

2) la cancellazione, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge, compresi quelli di cui non è necessaria la conservazione in relazione agli scopi per i quali i dati sono stati raccolti o successivamente trattati;

3) l'attestazione che le operazioni di cui alle lettere a) e b) sono state portate a conoscenza, anche per quanto riguarda il loro contenuto, di coloro ai quali i dati sono stati comunicati o diffusi, eccettuato il caso in cui tale adempimento si rivela impossibile o comporta un impiego di mezzi manifestamente sproporzionato rispetto al diritto tutelato.

### **Diritti oppositivi**

1) L'interessato ha diritto di opporsi, in tutto o in parte al trattamento dei dati personali, per motivi legittimi che lo riguardano, ancorchè pertinenti allo scopo della raccolta;

2) L'interessato ha diritto di opporsi al trattamento di dati personali che lo riguardano a fini di invio di materiale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato o di comunicazione commerciale.

Il titolare deve quindi predisporre una struttura in grado non solo di dare esecuzione a tali richieste dell'interessato, valutandone la fondatezza o il ricorrere di uno dei casi in cui è possibile opporre un rifiuto ( art. 8 comma II, Codice ), ma di farlo in tempi molto rapidi; infatti il codice consente (art 8 comma I) che i diritti di cui all'articolo 7 siano esercitati "con richiesta rivolta senza formalità al titolare o al responsabile, anche per il tramite di un incaricato, alla quale è fornito idoneo riscontro senza ritardo". Inoltre, l'art. 10 (Riscontro all'interessato), per garantire l'effettivo esercizio dei diritti di cui all'articolo 7 impone al titolare l'adozione delle misure volte, in particolare:

a) ad agevolare l'accesso ai dati personali da parte dell'interessato, anche attraverso l'impiego di appositi programmi per elaboratore finalizzati ad un'accurata selezione dei dati che riguardano singoli interessati identificati o identificabili;

b) a semplificare le modalità e a ridurre i tempi per il riscontro al richiedente, anche nell'ambito di uffici o servizi preposti alle relazioni con il pubblico.

### **Modulo del Garante**

Per favorire l'adempimento di questi obblighi il Garante ha predisposto un modulo che ha la finalità di semplificare e canalizzare le richieste degli interessati.

#### **Consenso informato, informativa, autorizzazioni**

Il trattamento dei dati personali può avvenire lecitamente solo dopo che sia stato acquisito il consenso informato degli interessati.

Tali condizioni sono soddisfatte non solo sollecitando l'acquisizione di una manifestazione di volontà dell'interessato espressa liberamente e specificamente in riferimento ad un trattamento chiaramente individuato; ma anche attraverso la garanzia di una piena consapevolezza del significato del consenso così espresso.

La consapevolezza viene assicurata, principalmente, attraverso la trasmissione all'interessato di tutta una serie di elementi di valutazione, con lo strumento dell'informativa (art. 13 Codice); tale strumento consente, infatti, all'interessato di esprimere consapevolmente, se richiesto, il consenso al trattamento e, in ogni caso, di esercitare i diritti che la legge gli attribuisce specificamente (art. 7 Codice) e di cui deve essere, anche indirettamente, reso edotto.

L'informativa è pertanto da considerarsi il primo e più generale degli adempimenti previsti dal Codice, non solo perché ordinariamente precede l'inizio del trattamento, sia nel settore pubblico sia in quello privato, ma soprattutto perché, anche quando il titolare è esentato dall'ottenere il consenso, deve comunque predisporre una adeguata informativa per l'interessato.

Il Titolare deve pertanto, nel rispetto del principio di trasparenza, predisporre un testo chiaro ed esaustivo, in cui non potranno, quindi, mancare riferimenti chiari alle finalità ed alle 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; 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 di cui all'articolo 7 ; 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 assumere forme molto semplificate, in relazione alle esigenze di una efficace e chiara comunicazione; così ad esempio è inutile fornire nuovamente elementi già noti all'interessato, e si possono evitare lunghe trascrizioni o letture di testi o documenti facilmente accessibili all'interessato cui si può fare riferimento per relationem.

#### **Consenso dell'interessato**

Il Titolare del trattamento di dati sensibili o giudiziari, ai sensi dell'art 26, comma 1, del codice della privacy, deve acquisire il consenso dell'interessato che deve essere manifestato, in questo caso, sempre ed esclusivamente in forma scritta.

Rispetto al trattamento di dati comuni, ancor più limitati sono i casi in cui il consenso non è invece richiesto ( art. 26, comma 4 )

Oltre che il consenso scritto dell'interessato, è, tuttavia, necessaria anche la previa autorizzazione del Garante per il trattamento.

#### **Casi di consenso non necessario**

Il consenso espresso dell'interessato non è necessario:

- a) per adempiere ad un obbligo previsto dalla legge, da un regolamento o dalla normativa comunitaria;
- b) per eseguire obblighi derivanti da un contratto del quale è parte l'interessato o per adempiere, prima della conclusione del contratto, a specifiche richieste dell'interessato;
- c) per trattare 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 conoscibilità e pubblicità dei dati;
- d) per trattare dati relativi allo svolgimento di attività economiche, trattati nel rispetto della vigente normativa in materia di segreto aziendale e industriale;
- e) per effettuare trattamenti indispensabili 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) con esclusione della comunicazione all'esterno e della diffusione, è effettuato da associazioni, enti od organismi senza scopo di lucro, anche non riconosciuti, in riferimento a soggetti che hanno con essi contatti regolari o ad aderenti, per il perseguimento di scopi determinati e legittimi individuati dall'atto costitutivo, dallo statuto o dal contratto collettivo, e con modalità di utilizzo previste espressamente con determinazione resa nota agli interessati all'atto dell'informativa ai sensi dell'articolo 13.

#### **Autorizzazione specifiche del Garante**

Il Garante comunica la decisione adottata sulla richiesta di autorizzazione entro quarantacinque giorni, decorsi i quali, la mancata pronuncia equivale a rigetto. Con il provvedimento di autorizzazione, ovvero successivamente, anche sulla base di eventuali verifiche, il Garante può prescrivere misure e accorgimenti a garanzia dell'interessato, che il titolare del trattamento è tenuto ad adottare.

Ai sensi dell'art. 40 del codice della privacy, in luogo di una specifica autorizzazione, il titolare si può giovare di autorizzazioni generali, cioè relative a determinate categorie di titolari o di trattamenti, pubblicate nella Gazzetta Ufficiale della Repubblica italiana.

#### **Autorizzazioni generali del Garante**

Le autorizzazioni generali (pubblicate sulla Gazzetta ufficiale n. 190 del 14 agosto 2004) hanno durata annuale, ma sono state prorogate, con provvedimento del Garante del 1° luglio 2005 e rimarranno, quindi, in vigore fino al 31 dicembre 2005.

I sette provvedimenti, di fondamentale importanza per gli Enti non profit sono i seguenti:

1. Autorizzazione 30 giugno 2004, n.1/2004 : autorizzazione al trattamento dei dati sensibili nei rapporti di lavoro.
2. Autorizzazione 30 giugno 2004, n.2/2004 : autorizzazione al trattamento dei dati sensibili idonei a rivelare lo stato di salute e la vita sessuale.
3. Autorizzazione 30 giugno 2004, n.3/2004 : autorizzazione al trattamento dei dati sensibili da parte di organismi di tipo associativo e delle fondazioni.
4. Autorizzazione 30 giugno 2004, n.4/2004 : autorizzazione al trattamento di dati sensibili da parte dei liberi professionisti.
5. Autorizzazione 30 giugno 2004, n.5/2004 : autorizzazione al trattamento dei dati sensibili da parte di diverse categorie di privati.
6. Autorizzazione 30 giugno 2004, n.6/2004 : autorizzazione al trattamento dei dati sensibili da parte degli investigatori privati.
7. Autorizzazione 30 giugno 2004, n.7/2004 : autorizzazione al trattamento dei dati a carattere giudiziario da parte di privati, enti pubblici economici e di soggetti pubblici.

Le Organizzazioni di Volontariato e gli altri enti non profit, hanno dovuto uniformarsi alle nuove prescrizioni contenute in dette Autorizzazioni, entro il 30 settembre 2004 e ora, per effetto della citata proroga, potranno continuare a rispettare fino al 31 dicembre 2005 le medesime prescrizioni, senza che sia necessario presentare al Garante un'apposita istanza o comunicazione.

L'importanza della conoscenza e della scrupolosa osservanza delle autorizzazioni generali si comprende alla luce del fatto che la necessità di operare trattamenti di dati sensibili, previa autorizzazione o sotto la copertura di una autorizzazione generale, patisce pochissime eccezioni, concernenti solo due categorie di enti: le confessioni religiose e le associazioni sindacali o di categoria di secondo grado.

Per la precisione ai sensi dell'art 26, comma 3, del D.Lgs. n. 196/2003 sono leciti pur senza necessità di autorizzazione e di consenso scritto dell'interessato i trattamenti:

a) dei dati relativi agli aderenti alle confessioni religiose e ai soggetti che con riferimento a finalità di natura esclusivamente religiosa hanno contatti regolari con le medesime confessioni, effettuato dai relativi organi, ovvero da enti civilmente riconosciuti, sempre che i dati non siano diffusi o comunicati fuori delle medesime confessioni. Queste ultime determinano idonee garanzie relativamente ai trattamenti effettuati, nel rispetto dei principi indicati al riguardo con autorizzazione del Garante;

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". Sono previsti, invero, dal Codice alcuni limitatissimi ed eccezionali casi in cui il trattamento di dati sensibili è possibile e lecito non solo in assenza del consenso dell'interessato ma anche dell'autorizzazione del Garante ex art 26, comma 3.

#### **Sanzioni trattamento illecito**

Ai sensi dell'art. 167 il Trattamento illecito di dati in violazione di quanto disposto dagli artt. 26 e 27, al fine di trarne per sé o per altri profitto o di recare ad altri un danno, salvo che il fatto costituisca più grave reato, e' punito, se dal fatto deriva nocumento, con la reclusione da uno a tre anni.

La condanna per uno dei delitti previsti dal presente codice importa la pubblicazione della sentenza.

#### **Sanzioni per mancanza del consenso**

Ai sensi dell'art. 167, il trattamento illecito di dati in violazione di quanto disposto dall'art. 23 del Codice, al fine di trarne per sé o per altri profitto o di recare ad altri un danno, è punito se dal fatto deriva nocumento, con la reclusione da sei a diciotto mesi o, se il fatto consiste nella comunicazione o diffusione, con la reclusione da sei a ventiquattro mesi, salvo che il fatto costituisca più grave reato,

La condanna per uno dei delitti previsti dal codice importa la pubblicazione della sentenza.

#### **La comunicazione preventiva al Garante**

Il Titolare del trattamento è tenuto a comunicare previamente al Garante, nel settore privato, ai sensi dell'art. 39 del Codice, l'inizio di uno specifico trattamento: quello di dati idonei a rivelare lo stato di salute previsto dal programma di ricerca biomedica o sanitaria per scopi scientifici ( art. 110, comma 1, primo periodo, codice della privacy ).

I trattamenti oggetto di comunicazione possono essere iniziati decorsi quarantacinque giorni dal ricevimento della comunicazione salvo diversa determinazione anche successiva del Garante.

#### **Operazioni conseguenti alla cessazione di un trattamento**

Il Titolare del trattamento, ai sensi dell'art. 16, in caso di cessazione, per qualsiasi causa, di un trattamento deve provvedere affinché i dati siano:

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.

La cessione dei dati in violazione di dell'art 16 o di altre disposizioni rilevanti in materia di trattamento dei dati personali è inefficace, con la conseguenza che il titolare continuerà a rispondere dell'uso che dei dati venga effettuato.

### **Sanzioni per omessa comunicazione al Garante**

Ai sensi dell'art. 162, la cessione dei dati in violazione di quanto previsto dall'articolo 16, comma 1, lettera b), o di altre disposizioni in materia di disciplina del trattamento dei dati personali è punita con la sanzione amministrativa del pagamento di una somma da 5.000 euro a 30.000 euro.

In tali casi, può essere irrogata anche la sanzione accessoria della pubblicazione dell'ordinanza ingiunzione.

### **Principi secondo cui deve avvenire il trattamento e sanzioni generali**

Secondo quanto previsto dal Codice all'art. 11, il trattamento dei dati personali deve avvenire nel rispetto di alcuni fondamentali principi così sintetizzabili:

a) i dati devono venir trattati in modo lecito e secondo correttezza;

b) i dati devono essere raccolti e registrati per scopi determinati, espliciti e legittimi, ed utilizzati in altre operazioni del trattamento in termini compatibili con tali scopi;

c) i dati raccolti devono essere esatti e, se necessario, aggiornati;

d) i dati raccolti devono essere pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti o successivamente trattati;

e) i dati devono essere 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.

### **Sanzioni generali**

Ai sensi dell'art. 167 del codice della privacy il Trattamento illecito di dati in violazione di quanto disposto dall'art. 11, al fine di trarne per sé o per altri profitto e/o di recare ad altri un danno, salvo che il fatto non costituisca più grave reato, è punito con la reclusione da uno a tre anni.

La condanna per uno dei delitti previsti dal codice importa la pubblicazione della sentenza.

Anche in assenza di una espressa richiesta in tal senso da parte dell'interessato, i dati personali trattati in violazione della disciplina in materia di privacy "non possono essere utilizzati".

L'inutilizzabilità dei dati comporta che essi possano essere conservati dal titolare ma non possono essere oggetto di alcun'altra operazione.

### **Sanzioni per omessa o inidonea informativa**

Ai sensi dell'art. 161 la omessa o inidonea informativa all'interessato è punita con la sanzione amministrativa del pagamento di una somma da tremila euro a diciottomila euro o, nei casi di dati sensibili o giudiziari o di trattamenti che presentano rischi specifici ai sensi dell'articolo 17 o, comunque, di maggiore rilevanza del pregiudizio per uno o più interessati, da 5.000 euro a 30.000 euro.

La somma può essere aumentata sino al triplo quando risulta inefficace in ragione delle condizioni economiche del contravventore.

In tali casi può essere irrogata anche la sanzione accessoria della pubblicazione dell'ordinanza ingiunzione.

## **Casistica particolare**

### **Pensionati, case vacanza, attività alberghiere**

Non sono pochi gli enti non profit (enti religiosi, fondazioni, associazioni) che nel quadro di attività sociali e culturali gestiscono strutture (come le case per le vacanze sociali, i pensionati per lavoratori o per studenti universitari, ecc.) che sono sottoposte alla disciplina degli alberghi quanto alla compilazione delle così dette "schede d'albergo".

In proposito, si è espresso il Garante, con un parere del 1° giugno 2005, in occasione della approvazione dello schema di decreto che regola le modalità di trasmissione alle questure dei dati delle persone che alloggiano negli alberghi, in particolare attraverso reti telematiche.

In base alle disposizioni del T.U. di pubblica sicurezza in vigore, albergatori, gestori di pensioni, appartamenti per vacanze, affittacamere, gestori di campeggi, ecc. possono conservare solo dati eventualmente necessari a fini fiscali e contabili (ad esempio, informazioni da inserire nella fattura o ricevuta). Sulle schede dovranno essere riportate solo le generalità, non la residenza del cliente e la data di arrivo. Infine, sempre dal punto di vista dei gestori delle strutture alberghiere, il Garante ha stabilito che la consegna dei dati alle autorità di p.s. dovrà essere "diretta", specie per le schede cartacee, senza il tramite di altri enti o soggetti.

Infine, il Garante ha auspicato l'adozione di un "decreto ministeriale che, dando ordine alla materia e certezza agli operatori nell'applicazione delle norme", sostituisca la congerie di precedenti decreti, alcuni dei quali abrogati o adottati senza il previsto parere del Garante, che si sono stratificati nel tempo.