

***A TUTTI I CLIENTI
LORO SEDI***

Milano, 26 novembre 2003

Circolare n. 4/2003

**CODICE IN MATERIA DI PROTEZIONE DEI DATI PERSONALI
(DECRETO LEGISLATIVO 30 GIUGNO 2003, N. 196)**

Premessa

In attuazione delle leggi delega 31 dicembre 1996, n. 676 e 24 marzo 2001, n. 127, il Consiglio dei Ministri ha approvato il Decreto Legislativo 30 giugno 2003, n. 196, pubblicato in Gazzetta Ufficiale del 29 luglio 2003, Serie Generale n. 174, Supplemento Ordinario n. 123/L, recante il “**Codice in materia di protezione dei dati personali**” (di seguito, il “Codice” o il “Testo Unico”).

In occasione della redazione del Testo Unico i compilatori, oltre ad effettuare un’attenta opera di ricognizione e raccolta delle vigenti disposizioni in materia di tutela dei dati personali, hanno svolto un’attività di armonizzazione e adeguamento delle norme raccolte, innovando e semplificando la normativa.

A differenza dell’impostazione di altri testi unici c.d. ”misti”, nei quali sono state inserite norme sia di rango legislativo, sia di rango regolamentare, in questa occasione si è preferito adottare un Testo Unico di matrice legislativa, nel quale le vigenti disposizioni di rango regolamentare sono state assorbite dalle norme legislative ovvero eliminate in quanto ritenute non più necessarie.

Tale scelta ha comportato, sul piano sistematico, una normativa più snella e maggiormente aderente alla realtà applicativa e all’evoluzione tecnologica. Nella rielaborazione della stessa si è infatti, tenuto conto, oltre che delle interpretazioni e dei provvedimenti emanati dal legislatore, anche dei pareri espressi dal Garante per la protezione dei dati personali (di seguito, il “Garante”), nel lasso temporale intercorso tra l’entrata in vigore della legge 675/96 e l’emanazione del Testo Unico.

Cionondimeno si è pervenuti ad una disciplina per alcuni aspetti innovativa, dettata dall’esigenza di: (a) perfezionare il recepimento della normativa comunitaria, contenuta

nella Direttiva n. 95/46/CE, sulla tutela delle persone fisiche con riguardo alla tutela dei dati personali, nonché alla libera circolazione di tali dati; (b) dare attuazione alla più recente Direttiva n. 2002/58/CE, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche intendendosi per tali le informazioni “*scambiate o trasmesse tra un numero finito di soggetti tramite un servizio di comunicazione elettronica accessibile al pubblico*”.

Nell'intenzione del legislatore, il Codice ha la preminente finalità di garantire che il “*trattamento dei dati personali si svolga nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza, alla identità personale e al diritto alla protezione dei dati personali*” (cfr. art. 2, comma 1, del Codice), valorizzando “*gli aspetti di garanzia della persona*” e semplificando gli adempimenti formali posti a carico dei titolari del trattamento e le modalità di esercizio dei diritti da parte degli interessati.

Il Codice è diviso in tre parti: la prima contiene le disposizioni generali, relative alla disciplina dei trattamenti effettuati nell'ambito dei settori pubblico e privato; la seconda parte contiene norme speciali per determinati settori che integrano – e talvolta derogano – la disciplina generale; l'ultima parte contiene le disposizioni in materia di tutela amministrativa e giurisdizionale, sanzioni amministrative e penali e di disciplina dell'Ufficio del Garante.

Considerato che il Testo Unico introduce importanti modifiche all'assetto disciplinare vigente, principalmente in punto di obblighi di informativa da rendere agli interessati, di adempimenti nei confronti del Garante, di misure minime di sicurezza da adottare, si evidenzia la necessità, per tutti coloro che effettuano trattamenti di dati personali, di procedere ad una attenta revisione degli adempimenti già posti in essere, sia al fine di adeguare la propria struttura organizzativa alle nuove disposizioni in materia di misure minime di sicurezza, sia al fine di integrare i modelli di informativa e di acquisizione del consenso attualmente in uso.

Di seguito si riepilogano le principali novità introdotte dal Codice con riguardo ai trattamenti effettuati da soggetti privati ed enti pubblici economici.

1. Diritto alla protezione dei dati personali

Il legislatore ha inteso “aprire” il Codice con una norma innovativa, che introduce quale diritto fondamentale, il “*diritto – riconosciuto a chiunque - alla protezione dei dati personali*” (art. 1 del Codice).

Ponendo in correlazione l'articolo 1 e il successivo articolo 2 del Codice, è dato rilevare come il diritto alla protezione dei dati personali assuma una valenza autonoma rispetto al diritto alla riservatezza, garantendo l'uno la tutela delle informazioni concernenti la persona fisica o giuridica, l'altro la tutela della vita privata della persona.

2. Principio di semplificazione e principio di necessità nel trattamento dei dati

Il Codice codifica due importanti principi:

- (a) il **principio di semplificazione**, in base al quale l'esercizio dei diritti e delle libertà, riconosciuti all'interessato in relazione al trattamento dei propri dati personali, così come gli adempimenti cui è tenuto il titolare del trattamento, sono consentiti con modalità semplificate rispetto alla vigente disciplina, senza che la semplificazione incida comunque sul livello di garanzia (cfr. art. 2);
- (b) il **principio di necessità**, in base al quale i sistemi informativi e i programmi informatici devono essere configurati in modo tale da garantire che il trattamento dei dati personali avvenga nei soli casi in cui le finalità perseguite non consentano l'utilizzo di dati anonimi ovvero di dati che consentano l'identificazione dell'interessato solo in caso di necessità (cfr. art. 3).

Come è facilmente ipotizzabile, l'introduzione del principio di *necessità* potrebbe determinare per i titolari del trattamento l'onere di rivedere la propria organizzazione interna e i sistemi informativi adottati; ciò al fine di introdurre maggiori controlli sui trattamenti effettuati e da effettuarsi e di adeguare i trattamenti medesimi alle nuove disposizioni.

La *ratio* del principio è da ricercare nell'esigenza avvertita dal legislatore di circoscrivere l'utilizzo dei dati personali in ambienti informatici alle ipotesi in cui il trattamento con strumenti elettronici sia indispensabile per il perseguimento delle finalità in relazione alle quali i dati sono trattati. Laddove, pertanto, non sia effettivamente necessario l'utilizzo di dati personali, il titolare dovrà astenersi dall'utilizzo degli stessi; tale norma integra le disposizioni di cui all'art. 11 che codifica il principio di pertinenza e non eccedenza dei dati trattati e la violazione di tali disposizioni potrà avere rilevanza ai fini del risarcimento di eventuali danni.

3. Ambito di applicazione (art. 5)

Il legislatore ha integrato la vigente disciplina con l'inserimento della previsione secondo cui il trattamento di dati personali, effettuato da "*chiunque è stabilito nel territorio dello Stato o in un luogo comunque soggetto alla sovranità dello Stato*", è soggetto all'applicazione della legge italiana e conseguentemente agli adempimenti prescritti dal Codice.

La nuova disposizione, ponendo l'accento sul principio di "stabilimento", attrae nell'ambito di applicazione della legge anche i trattamenti di dati personali detenuti all'estero, se effettuati da soggetti stabiliti nel territorio nazionale.

La finalità sottesa alla suddetta modifica è da individuare nella volontà del legislatore di proseguire il processo di recepimento dei criteri indicati dalla Direttiva n. 95/46/CE in merito all'applicazione della normativa nazionale, già avviato con il D. lg. 28 dicembre 2001, n. 467.

4. Informativa (art. 13)

Il Codice prevede alcune novità in materia di contenuto dell'informativa preventiva da rendere agli interessati ovvero a coloro presso i quali i dati sono raccolti. In particolare, è stato previsto l'obbligo di specificare, oltre ai soggetti o le categorie di soggetti ai quali i dati personali possono essere comunicati anche i soggetti o le categorie di soggetti che possono venire a conoscenza dei dati in qualità di responsabili o incaricati del trattamento.

La norma va valutata unitamente al disposto degli artt. 4, comma 1, lett. l), e 7, comma 2, lett. e), del Codice, che, rispettivamente, contengono la nuova definizione di comunicazione e stabiliscono il diritto dell'interessato di conoscere i soggetti ai quali i dati possono essere comunicati o che ne possono venire comunque a conoscenza in qualità di rappresentante designato nel territorio dello Stato, di responsabili o incaricati.

Inoltre sono state precisate le modalità di identificazione del titolare del trattamento e i criteri di indicazione degli eventuali responsabili del trattamento. In caso di dati personali raccolti da soggetti diversi dall'interessato, l'informativa da rendere a quest'ultimo all'atto della registrazione dei dati o, quando sia prevista la comunicazione, non oltre la prima comunicazione, deve altresì contenere le informazioni in merito alle categorie di dati trattati.

Dal combinato disposto delle norme citate si desume la necessità di rivedere il contenuto dei modelli di informativa attualmente in uso nonché di predisporre idonei presidi tecnico operativi volti a consentire un tempestivo soddisfacimento delle eventuali istanze proposte dagli interessati.

Il Codice riconosce altresì al Garante la facoltà di individuare modalità semplificate per l'informativa che i sempre più diffusi “*servizi telefonici di assistenza e informazione al pubblico*” (*call center*) sono tenuti a rendere agli interessati.

La *ratio* sottesa a quest'ultima previsione va individuata nella volontà di rendere maggiormente agevole l'adempimento dell'obbligo di informativa da parte dei titolari del trattamento, ferma restando l'esigenza di garantire il rispetto dell'obbligo di informativa anche in relazione a trattamenti che non sono preceduti da un contatto diretto con l'interessato.

5. Casi nei quali può essere effettuato il trattamento senza consenso (art. 24)

Al fine di rendere omogenea e conforme alle disposizioni comunitarie la disciplina dei casi di esclusione del consenso al trattamento, il legislatore ha apportato alcune modifiche alle vigenti disposizioni in materia di trattamenti effettuati da soggetti privati ed enti pubblici economici.

In particolare, dopo un espresso rinvio ai casi di esclusione del consenso previsti nella Parte II del Codice, dedicata a specifici trattamenti e contenente norme integrative o eccezioni alle disposizioni di carattere generale, sono state parzialmente modificate talune fattispecie di trattamento senza preventivo consenso dell'interessato. Si fa riferimento alle ipotesi di:

- a) *“sussistenza di un obbligo legale”*. Al riguardo si prevede che il trattamento possa aver luogo senza il preventivo consenso dell'interessato se *“è necessario per adempiere ad un obbligo previsto dalla legge, da un regolamento o dalla normativa comunitaria”*. È dato notare come l'elemento di novità rispetto alla vigente disciplina, nella quale si fa riferimento semplicemente ai dati “raccolti e detenuti” in base a un obbligo previsto dalla legge, da un regolamento o dalla normativa comunitaria (cfr. artt. 12, comma 1, lett. a, e 20, comma 1, lett. c) della legge 675/96), debba essere ravvisato nel carattere di necessità del trattamento;
- b) *“esecuzione di misure precontrattuali adottate su richiesta”* dell'interessato, prima della conclusione del contratto. Si chiarisce che il trattamento è consentito quando lo stesso *“è necessario per adempiere, prima della conclusione del contratto, a specifiche richieste dell'interessato”* e non soltanto per dare esecuzione a *“misure precontrattuali”* su richiesta dell'interessato.

Il legislatore inoltre ha confermato l'attribuzione della delega al Garante, già introdotta con il richiamato D. Lgs. 467/2001. Come si ricorderà, la delega conferisce al Garante il potere di individuare, mediante l'adozione di propri provvedimenti - allo stato peraltro non ancora emanati - specifici casi di esclusione del consenso in applicazione della **“clausola di bilanciamento”** tra il legittimo interesse del titolare o di un terzo destinatario dei dati ed i diritti, le libertà fondamentali, la dignità o un legittimo interesse dell'interessato. L'elemento innovativo va ricercato nella delimitazione dell'ambito di operatività della delega. Infatti l'applicazione dei provvedimenti che il Garante adotterà, non potrà estendersi, per espressa previsione legislativa (cfr. art. 24, comma 1, lett. g, del Codice) alle ipotesi di trattamento concernenti la diffusione dei dati personali.

Si evidenzia altresì che, a differenza di quanto previsto dalla vigente legislazione in materia, secondo la quale è ammessa la comunicazione dei dati personali fra società controllate e/o collegate ai sensi dell'art. 2359 cod. civ. o fra società appartenenti ad un medesimo gruppo bancario anche in difetto del preventivo consenso dell'interessato, i cui trattamenti con finalità correlate siano stati notificati al Garante, per il perseguimento delle medesime finalità per le quali i dati sono stati raccolti, le nuove disposizioni ammettono la possibilità di trattare e comunicare dati personali senza il preventivo consenso dell'interessato solo nei casi individuati dal Garante in applicazione di detto principio di bilanciamento.

Al fine di uniformare la disciplina dei dati comuni a quella dei dati sensibili, è stata introdotta l'esenzione del consenso al trattamento dei dati comuni effettuato da associazioni, enti ed 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”*. Tale esenzione vale esclusivamente per i trattamenti effettuati da tali soggetti all’interno degli stessi, rimanendo esclusa in ogni caso la comunicazione all’esterno e la diffusione.

6. Garanzie per i dati sensibili (art. 26)

Unitamente alle novità introdotte in relazione al trattamento dei dati sensibili effettuato da confessioni religiose, volte a razionalizzare la disciplina e ad uniformarla al diritto comunitario (direttiva 95/46/CE), il Codice indica i casi in cui il titolare, previa autorizzazione del Garante, può procedere al trattamento dei dati sensibili senza aver acquisito il preventivo consenso scritto dell’interessato.

Altre innovazioni concernono i trattamenti svolti da:

- a) associazioni, enti e organismi senza scopo di lucro, in relazione ai quali la vigente disciplina è integrata con l’introduzione di un criterio di maggiore garanzia e trasparenza, in base al quale i dati personali degli aderenti o dei soggetti che hanno contatti regolari con l’associazione, possono essere *“trattati per il perseguimento di scopi determinati e legittimi individuati dall’atto costitutivo, dallo statuto o dal contratto collettivo”*, a condizione che il titolare abbia individuato *“espressamente le modalità di utilizzo dei dati con determinazione resa nota”* agli associati *“all’atto dell’informativa”* e che i trattamenti rientrino nel campo di applicazione delle autorizzazioni rilasciate dal Garante;
- b) titolari del trattamento, in adempimento di *“specifici obblighi o compiti previsti”* dalla normativa, anche comunitaria, in materia di gestione del rapporto di lavoro, comprese le disposizioni in materia di igiene e sicurezza del lavoro e di previdenza e assistenza. Tali trattamenti devono essere comunque effettuati nei limiti previsti dalle autorizzazioni del Garante e delle disposizioni del codice di deontologia e di buona condotta.

7. Titolare, Responsabile e Incaricati del trattamento (artt. 28-30)

Nell’intento di recepire alcuni principi ormai consolidati dalla prassi interpretativa del Garante, il legislatore chiarisce che:

- a) se *“il trattamento è effettuato da una persona giuridica, da una pubblica Amministrazione o da qualsiasi altro ente”*, titolare del trattamento medesimo è *“l’entità nel suo complesso”* e non le singole persone fisiche che prestano la loro attività nell’ambito della struttura legittimate a manifestare all’esterno la volontà del titolare del trattamento. Parimenti, si considera titolare del trattamento *“l’unità od organismo periferico che esercita un potere decisionale autonomo sulle finalità e modalità del trattamento”*.
- b) la nomina del responsabile, di esclusiva competenza del titolare del trattamento, è facoltativa.

Inoltre, con riguardo agli incaricati del trattamento, si conferma che possono rivestire la qualifica di *“incaricati”* soltanto le persone fisiche alle quali siano state impartite delle istruzioni e che gli stessi sono designati mediante atto scritto dal titolare o dal responsabile del trattamento. Si integrano le attuali disposizioni con la previsione

secondo cui l'atto di nomina deve individuare l'ambito del trattamento consentito con riguardo alle specifiche mansioni svolte dagli incaricati.

Il Codice equipara altresì alla designazione degli incaricati, la preposizione della persona fisica ad una unità organizzativa per la quale sia individuato, sempre per iscritto, l'ambito del trattamento consentito agli addetti preposti all'unità.

8. Misure minime di sicurezza (artt. 31 -36)

Il legislatore ha mantenuto la bipartizione, introdotta con il D.P.R. 28 luglio 1999, n. 318, (di seguito, anche il "Regolamento sulle misure minime di sicurezza"), tra trattamenti di dati personali effettuati con strumenti elettronici e trattamenti di dati personali effettuati senza l'ausilio di strumenti elettronici. È venuta meno l'attuale distinzione tra trattamenti dei dati effettuati mediante elaboratori non accessibili in rete e trattamenti effettuati mediante elaboratori accessibili in rete e, in tale ambito, l'ulteriore distinzione tra trattamenti effettuati mediante elaboratori accessibili da altri elaboratori solo attraverso reti non disponibili al pubblico e trattamenti effettuati mediante elaboratori accessibili mediante una rete di telecomunicazioni disponibili al pubblico.

Al fine di dare attuazione al principio di semplificazione - che, come si è più volte ribadito, è uno dei principi ispiratori del Codice, - nonché di rendere le disposizioni in materia di rispetto delle misure minime di sicurezza maggiormente aderenti alla costante evoluzione tecnologica e all'esperienza maturata nel settore, si è inteso definire in via generale le misure minime nel corpo del Codice, introducendo invece, in apposito Disciplinare Tecnico (*cf.* Allegato B al Codice, che sostituisce il vigente Regolamento sulle misure minime di sicurezza), dettagliate disposizioni di attuazione delle misure minime di sicurezza. L'Allegato sarà aggiornato periodicamente con decreto del Ministro della Giustizia di concerto con il Ministro per le innovazioni e le tecnologie e non più mediante decreto del Presidente della Repubblica.

Da un rapido esame delle disposizioni del Codice, si rileva in primo luogo che non ha specifica rilevanza formale la figura dell'amministratore di sistema, a suo tempo tipizzata nel richiamato D.P.R. n. 318/1999.

Tra le misure volte ad assicurare un livello minimo di protezione dei dati personali, da adottare nel quadro dei più generali obblighi di sicurezza, si segnalano, relativamente ai trattamenti con strumenti elettronici: il principio della riserva del trattamento a incaricati *"dotati di credenziali di autenticazione, consistenti in un codice identificativo associato ad una parola chiave ovvero in un dispositivo di autenticazione in possesso e uso esclusivo"* dell'utente o in un sistema biometrico, *"eventualmente associati a un codice identificativo o a una parola chiave"*; l'obbligo di adozione di procedure di gestione delle credenziali di autenticazione; l'utilizzazione di un sistema di autorizzazione (profilo utente); l'individuazione di procedure per la custodia delle copie di sicurezza, il ripristino della disponibilità dei dati e dei sistemi.

Più specificamente, al fine di contemperare l'esigenza di segretezza delle componenti riservate delle credenziali e la necessità di *"assicurare la disponibilità di dati o strumenti elettronici in caso di prolungata assenza o impedimento dell'incaricato"*

che renda indispensabile e indifferibile intervenire” sempre che specifiche esigenze operative e di sicurezza del sistema lo impongano, il Codice pone a carico del titolare del trattamento, l’obbligo di impartire, per iscritto, *“idonee e preventive”* istruzioni volte a *“individuare le modalità”* di gestione delle credenziali. La norma dispone inoltre che la custodia delle copie delle credenziali, organizzata pur sempre nel rispetto del principio di segretezza, è affidata a soggetti espressamente e preventivamente incaricati per iscritto. A tali soggetti è fatto obbligo di informare tempestivamente l’incaricato degli interventi eventualmente effettuati.

Il legislatore ha altresì considerato e disciplinato l’ipotesi in cui i titolari del trattamento individuino *“profili di autorizzazione di ambito diverso”*, prescrivendo, in tal caso, l’utilizzo di un *“sistema di autorizzazione”*.

Al fine di consentire che gli incaricati del trattamento accedano esclusivamente ai dati necessari per le operazioni di trattamento, il titolare del trattamento, anteriormente all’inizio del trattamento medesimo, deve individuare i *“profili di autorizzazione”*, e verificare, periodicamente e comunque almeno una volta all’anno, la sussistenza delle condizioni che costituiscono il presupposto per la concessione dei suddetti profili.

Il titolare del trattamento sarà tenuto ad attivare ulteriori misure di sicurezza, quali, a titolo esemplificativo: *“l’aggiornamento periodico dell’individuazione dell’ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici”*; l’adozione di idonei strumenti elettronici volti a prevenire rischi di intrusione.

Mette conto soffermare l’attenzione sulle disposizioni concernenti la redazione del Documento Programmatico sulla sicurezza in quanto le stesse introducono aspetti particolarmente innovativi rispetto alle disposizioni vigenti.

Come noto, l’art. 6 del vigente D.P.R. 318/99 prevede, quale presupposto dell’obbligo della redazione del suddetto documento, il trattamento dei dati *“sensibili”* - quali definiti dagli articoli 22 e 24 della legge 675/96 - effettuato mediante elaboratori accessibili mediante una rete di telecomunicazioni disponibili al pubblico. A quest’ultimo riguardo, si ricorderà che, secondo l’interpretazione consolidata e i chiarimenti forniti dallo stesso Garante, sono considerate *disponibili al pubblico* le reti che utilizzino, *“anche per sola interconnessione su linee dedicate”* la rete pubblica nonché gli elaboratori *“connessi ad una rete che ha un collegamento al mondo Internet”*.

Con le nuove disposizioni i presupposti dell’obbligo di redazione risultano più stringenti.

Infatti, avendo il Codice unificato le attuali distinzioni tra i trattamenti effettuati con modalità diverse, distinguendo esclusivamente tra trattamenti senza l’ausilio di strumenti elettronici e trattamenti con strumenti elettronici, l’obbligo di redazione del Documento Programmatico sulla sicurezza entro il 31 marzo di ciascun anno, risulta esteso a tutti i trattamenti di dati sensibili o di dati giudiziari effettuati con strumenti

elettronici, indipendentemente dalla circostanza che i trattamenti siano effettuati mediante elaboratori connessi ad una rete collegata alla rete pubblica.

Si è altresì introdotto, a carico del titolare del trattamento, uno specifico obbligo di informazione dell'avvenuta redazione o aggiornamento del Documento Programmatico sulla sicurezza, nella relazione di accompagnamento del bilancio di esercizio e si sono ampliati i contenuti del Documento medesimo.

Il contenuto minimo di tale Documento sarà infatti costituito da:

- elenco dei trattamenti di dati personali;
- distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati;
- analisi dei rischi;
- 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;
- descrizione dei criteri e delle modalità per il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento;
- previsione di interventi formativi degli incaricati del trattamento;
- descrizione dei criteri da adottare per garantire l'adozione delle misure minime di sicurezza in caso di trattamenti di dati personali affidati all'esterno della struttura del titolare;
- per gli organismi sanitari e gli esercenti le professioni sanitarie, individuazione dei criteri da adottare per la cifratura o per la separazione dei dati personali idonei a rivelare lo stato di salute e la vita sessuale dagli altri dati personali.

Si evidenzia infine l'onere del titolare del trattamento, il quale si avvalga di soggetti esterni alla propria struttura al fine di dare esecuzione alle misure minime di sicurezza, di pretendere da tale soggetto "esterno" apposito documento scritto contenente la descrizione degli interventi effettuati e attestante la conformità degli stessi alle disposizioni dell'Allegato B al Codice.

9. Notificazione (artt. 37 e 38)

Il Codice, completando l'intervento di razionalizzazione e semplificazione avviato con il D.Lgs. n. 467/2001, introduce significative semplificazioni degli adempimenti a carico del titolare del trattamento in materia di Notificazioni al Garante.

Infatti, ribaltando l'impostazione seguita dalla legge 675/96, il Codice esclude, in via generale, l'obbligo della Notificazione e della modifica della stessa attualmente posto a carico di tutti i soggetti non espressamente esentati.

La Notificazione dovrà essere effettuata solo in caso di trattamenti relativi a dati particolarmente delicati o a rischio, quali, a titolo esemplificativo, "*dati idonei a rivelare la vita sessuale o la sfera psichica*" trattati da organismi senza scopo di lucro; "*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*"; "*dati*

sensibili registrati in banche dati a fini di selezione del personale”, sempre che il trattamento avvenga per conto di terzi, “nonché dati sensibili utilizzati per sondaggi di opinione, ricerche di mercato e altre ricerche campionarie; 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”.

Si sottolinea, inoltre, che la notificazione non potrà più essere effettuata mediante il modello cartaceo ma dovrà essere trasmessa esclusivamente per via telematica, seguendo le indicazioni del Garante quanto all’uso della firma digitale.

10. Trasferimento di dati all’estero (artt. 42 – 45)

Conformemente alle innovazioni introdotte in materia di Notificazione, il legislatore ha escluso l’obbligo di notificare preventivamente al Garante il trasferimento dei dati all’estero ed ha soppresso l’obbligo di procedere al trasferimento dei dati solo dopo aver lasciato trascorrere il termine attualmente previsto dall’art. 28, comma 2 della legge 675/96.

Nella struttura del Codice si è operata con maggiore chiarezza, rispetto alle vigenti norme in materia, la distinzione tra trasferimenti di dati all’interno dell’Unione Europea e trasferimenti di dati personali verso Paesi terzi.

In particolare, in attuazione del principio sancito dalla Direttiva comunitaria 95/46, in base al quale i dati personali possono circolare liberamente tra gli Stati membri, a condizione che siano garantiti i diritti fondamentali della persona, si è enunciata una disposizione di portata generale *“le disposizioni del presente Codice non possono essere applicate in modo tale da restringere o vietare la circolazione dei dati personali fra gli Stati membri dell’Unione Europea”.*

In applicazione di tale disposizione, nessuna limitazione e/o specifico adempimento sono previsti per il trasferimento di dati all’interno dell’Unione Europea, salvo che per i trasferimenti effettuati al fine di eludere disposizioni normative, in relazione ai quali è comunque fatta salva l’adozione di eventuali provvedimenti sanzionatori.

Il trasferimento dei dati personali oggetto di trattamento verso un Paese non appartenente all’Unione Europea è consentito nei casi espressamente indicati dal legislatore negli articoli 43 e 44 senza specifici adempimenti a carico dei soggetti che effettuino i trasferimenti dei dati.

Al riguardo si sottolinea che nell’articolo 43 del Codice sono state sostanzialmente riprodotte le disposizioni già presenti nella legge 675/96 (artt. 26, comma 2 e 28, comma 4, fatta eccezione per la lett. g, in relazione alla quale il legislatore ha introdotto una specifica norma), con qualche particolarità dettata da esigenze di simmetria fra trattamenti effettuati all’interno del territorio statale e trasferimento dei dati all’estero (cfr. art. 43, comma 1, lett. b e d, del Codice).

È altresì consentito il trasferimento di dati personali in Paesi non appartenenti all'Unione Europea, quando, non sussistendo le condizioni indicate nell'art. 43 del Codice, il Garante abbia rilasciato apposita autorizzazione al trasferimento *“sulla base di adeguate garanzie per i diritti dell'interessato”*. Si precisa che tali garanzie possono essere individuate: (a) dal Garante anche in relazione a garanzie prestate con un contratto; (b) dalle decisioni della Commissione Europea volte a constatare che un Paese terzo *“garantisce un livello di protezione adeguato o che alcune clausole contrattuali offrono garanzie sufficienti”*.

11. Codici di deontologia (art. 12)

Il Codice attribuisce ai codici di deontologia e di buona condotta in materia di protezione dei dati personali il ruolo di fonti integrative della legislazione vigente. In particolare, il rispetto delle disposizioni contenute in tali Codici costituisce condizione essenziale per la liceità e correttezza del trattamento dei dati personali.

È confermata la volontà del legislatore - già espressa nella legge 675/96 e successive modifiche e integrazioni - di dare impulso alla produzione di regole elaborate direttamente dagli interessati con riguardo a trattamenti di dati personali effettuati nell'ambito di determinati settori, quali, a titolo esemplificativo, sistema bancario, finanziario, assicurativo, videosorveglianza, marketing diretto, rapporti di lavoro, Internet.

È ribadito il ruolo propulsivo del Garante, al quale è riconosciuto il potere di promuovere la sottoscrizione dei codici, verificarne la conformità alle disposizioni normative vigenti nonché di contribuire alla generale diffusione e al rispetto da parte dei soggetti pubblici e privati interessati al trattamento dei dati personali.

È evidente che la rilevanza attribuita ai codici dalle nuove disposizioni, trova la sua ragion d'essere nell'intenzione del legislatore di rendere omogenee le modalità dei trattamenti in specifici settori e, mediante un'attività di bilanciamento e di raccordo fra le esigenze della produzione, dell'economia, della sicurezza aziendale, dello svolgimento dell'attività lavorativa e i diritti spettanti agli interessati, in materia di tutela della riservatezza.

12. Sanzioni

Il legislatore, oltre ad adeguare gli importi delle sanzioni pecuniarie all'introduzione dell'Euro, ha accentuato il rigore delle sanzioni, commisurandole alla gravità delle violazioni e all'effettività delle sanzioni, e ha introdotto, quale pena accessoria da applicarsi eventualmente su richiesta espressa del Garante, la pubblicazione sulla stampa dell'ordinanza-ingiunzione.

La finalità del legislatore è quella di rendere le sanzioni amministrative un valido deterrente alle eventuali violazioni connesse con il trattamento dei dati personali.

La novità di maggior rilievo introdotta nel Codice relativamente alle sanzioni penali concerne la punibilità delle ipotesi di trattamento illecito dei dati (art. 167) solo *“se dal*

fatto derivi nocumento”, mentre la legislazione in vigore considera il nocumento una circostanza aggravante. Con l’occasione sono state altresì adeguate le pene edittali previste per tale reato.

13. Entrata in vigore e disposizioni transitorie

Il Codice entra in vigore quasi integralmente il 1° gennaio 2004, fatta eccezione per alcune disposizioni espressamente previste dall’art. 186 del D. Lgs. 196/2002. A far tempo da tale data saranno abrogati, tra gli altri provvedimenti, la legge 31 dicembre 1996, n. 675; il D.P.R. 28 luglio 1999, n. 318 e parzialmente il D.P.R. 31 marzo 1998, n. 501.

Al fine di consentire ai titolari del trattamento di adeguare alle disposizioni contenute nel Codice, le misure minime di sicurezza attualmente adottate, il legislatore ha differito al 30 giugno 2004 il termine ultimo entro il quale adottare le nuove misure minime di sicurezza individuate nel Codice stesso. Resta inteso che per le misure minime già previste dalla vigente normativa, e confermate nel Codice, tale disposizione transitoria non trova applicazione.

I titolari del trattamento che non possiedano strumenti elettronici idonei all’applicazione delle misure di sicurezza individuate dal Codice, hanno facoltà di avvalersi, ai fini dell’adeguamento, di un ulteriore anno decorrente dalla data di entrata in vigore del Codice medesimo, a condizione che predispongano un documento, avente data certa, contenente le oggettive ragioni tecniche che non consentano l’adeguamento.

Si informa che è possibile reperire il testo integrale del Codice nel sito www.garanteprivacy.it.