

rentemente con quanto sopra indicato, si riferiscano a principi importanti in materia di protezione dati, come ad esempio

- il soggetto che raccoglie i dati personali e le modalità per contattarlo (almeno la denominazione ufficiale del soggetto e il suo indirizzo fisico);
 - quali dati personali sono raccolti dal soggetto in questione e con quali strumenti; le finalità per cui il soggetto raccoglie i dati personali;
 - se i dati personali saranno resi noti ad altri soggetti e, in tal caso, le tipologie o i nominativi di tali soggetti e le relative finalità,
 - le opzioni in materia di privacy di cui dispongono i singoli ed i meccanismi per esercitarle con facilità, in particolare le opzioni relative all'eventualità che dati personali siano rivelati a terzi per finalità non correlate, ancorché legittime, ed ai dati personali che i singoli sono tenuti a fornire per ricevere un servizio,
 - una sintesi dei diritti di accesso, rettifica, blocco o cancellazione riconosciuti ai singoli,
 - l'ente di controllo indipendente al quale i singoli possono sottoporre reclami qualora ritengano di avere subito una violazione dei propri diritti;
- impiego di strumenti opportuni al fine di consentire ai singoli di reperire con facilità informazioni ulteriori, come ad esempio
- informazioni che un soggetto sia tenuto a fornire in base alla normativa vigente, per esempio in materia di diritto di accesso, rettifica, blocco o cancellazione, ed il periodo di conservazione dei dati personali da parte dei singoli soggetti, e
 - una spiegazione esauriente delle informazioni presentate in forma sintetica nel formato condensato, e
 - la descrizione completa delle politiche seguite dal soggetto nella gestione e nel trattamento delle informazioni.

3. La Conferenza concorda sul fatto che il formato standardizzato e condensato di cui sopra dovrebbe essere conforme a tutte le norme nazionali applicabili, e che esso debba integrare, se necessario, ed essere compatibile con le informazioni che un soggetto sia tenuto per legge a fornire ai singoli.

4. La Conferenza è consapevole dell'importanza del momento in cui l'interessato prende visione dell'informativa in materia di protezione dati e privacy. Ad esempio, è particolarmente auspicabile che tale informativa sia fornita in modo automatico nel momento in cui ai singoli è data la possibilità di scegliere quali informazioni fornire e se consentire la comunicazione di tali informazioni a terzi. In altri casi può essere opportuno lasciare che siano i singoli a reperire le informazioni in materia di privacy e protezione dati attraverso legami ipertestuali evidenti. La Conferenza è consapevole delle importanti attività svolte dal Gruppo di lavoro UE in materia di protezione dei dati ex Articolo 29, per quanto riguarda la presentazione automatica di informazioni relative a privacy e protezione dati, attraverso la Raccomandazione 2/2001 su alcuni requisiti minimi per la raccolta online di dati personali nell'Unione Europea.

5. La Conferenza ritiene che l'attività delle Autorità di protezione dati e privacy potrebbe proseguire in modo fruttuoso valutando il momento in cui presentare l'informativa nel formato condensato, che tiene conto delle caratteristiche dell'ambiente sia offline sia online.

6. La Conferenza è al corrente, inoltre, di attività correlate quali la definizione di linguaggi informatici in grado di descrivere le politiche adottate in materia di privacy. La Conferenza invita a proseguire nella messa a punto di meccanismi utili a tradurre tali politiche nel formato standardizzato e condensato prima descritto.

7. La Conferenza considera quanto sopra un primo passo volto a promuovere migliori prassi nei meccanismi con cui i vari soggetti comunicano le informazioni relative alle modalità di gestione o trattamento di dati personali. La Conferenza è al corrente delle iniziative intraprese in questo settore, e invita tali iniziative a migliorare la comunicazione fra le parti in causa (soggetti che trattano i dati e singoli individui i cui dati sono oggetto di trattamento). La Conferenza intende collaborare con i soggetti ed i gruppi di interesse impegnati in tali iniziative, e prevede di compiere passi ulteriori al fine di migliorare le comunicazioni fra singoli e soggetti che trattano i dati nell'ambito di future conferenze.

99

Risoluzione relativa alla protezione dei dati ed agli organismi internazionali

Proponente: Autorità per la privacy, Nuova Zelanda.

Co-sponsors:

- Autorità per la protezione dei dati, Irlanda
- Commissione nazionale informatica e libertà, Francia
- Autorità per la privacy e i dati personali, Hong Kong SAR
- Autorità federale per la protezione dei dati, Germania

RISOLUZIONE

La 25^{ma} Conferenza internazionale delle Autorità di protezione dati e della privacy adotta la seguente risoluzione:

La Conferenza invita

- a. gli enti internazionali e sopranazionali ad impegnarsi formalmente al rispetto di principi compatibili con i più importanti strumenti internazionali relativi a protezione dei dati e privacy;
- b. gli enti internazionali e sopranazionali che detengono o trattano dati personali a definire meccanismi opportuni onde garantire il rispetto dei principi applicabili in materia di protezione dei dati, come la creazione di autorità di controllo interne ma indipendenti sul piano operativo e dotate di poteri di controllo;
- c. gli enti internazionali e sopranazionali che partecipino alla promulgazione di norme, regole o prassi comuni tali da produrre effetti sulla gestione di dati personali nel territorio soggetto alla giurisdizione dei rispettivi componenti, ad elaborare e adottare meccanismi atti a garantire che si tenga effettivamente conto degli aspetti legati alla protezione dei dati, come il ricorso a valutazioni dell'impatto in termini di privacy e la consultazione di autorità riconosciute in materia di protezione dei dati; inoltre, chiede all'autorità che ha ospitato la 25^{ma} Conferenza Internazionale di richiamare l'attenzione degli enti pertinenti sulla presente risoluzione.

100 Risoluzione sul trasferimento di dati relativi a passeggeri

L'Autorità federale svizzera per la protezione dei dati, l'Ufficio per la protezione dei dati personali della Repubblica Ceca, l'Ombudsman per la protezione dei dati della Finlandia e l'Autorità federale tedesca per la protezione dei dati propongono che la Conferenza Internazionale adotti la seguente risoluzione:

A. LA CONFERENZA RILEVA CHE

1. Nel quadro della lotta legittima contro il terrorismo e la criminalità organizzata, in alcuni Paesi sono allo studio misure che potrebbero minacciare diritti e libertà fondamentali, in particolare il diritto alla privacy.
2. C'è il rischio di minare la democrazia e la libertà attraverso misure finalizzate a difenderle.
3. Disposizioni di legge che impongano ai fornitori di trasporto di consentire l'accesso a, o trasferire dati da, insiemi di dati relativi ai passeggeri, memorizzati nei sistemi di prenotazione aerea, potrebbero confliggere con i principi internazionali della protezione dei dati o con gli obblighi imposti alle compagnie aeree dalle normative nazionali in materia di protezione dei dati.

B. LA CONFERENZA, PERTANTO, AFFERMA CHE

1. Nella lotta contro il terrorismo e la criminalità organizzata, gli Stati dovrebbero definire la propria risposta tenendo pienamente conto di principi fondamentali della protezione dei dati, i quali costituiscono parte integrante dei valori da tutelare.
2. Qualora siano necessari trasferimenti internazionali di dati personali su base regolare, ciò dovrebbe avvenire in un contesto che tenga conto della protezione dei dati, ad esempio sulla base di un accordo internazionale che preveda norme adeguate in materia di protezione dei dati, fra cui una chiara limitazione delle relative finalità, la raccolta di dati adeguati e non eccedenti, un periodo limitato di conservazione dei dati, l'informativa per gli interessati, la garanzia dell'esercizio dei diritti riconosciuti agli interessati ed un controllo indipendente.

101

Risoluzione relativa agli aggiornamenti automatici di software

RISOLUZIONE

Le Autorità per la protezione dei dati della Germania, della Repubblica Ceca, dell'Italia, l'Ispettorato per la protezione dei dati della Repubblica di Lituania, l'Autorità per l'informazione e la privacy dello stato di Ontario e l'Autorità federale svizzera per la protezione dei dati propongono che la Conferenza Internazionale adotti la seguente risoluzione:

1. La Conferenza rileva con preoccupazione che le case produttrici di software in tutto il mondo fanno sempre più ricorso a meccanismi non trasparenti per trasferire aggiornamenti di software nel computer degli utenti.

Così facendo, esse

- sono in grado di leggere e raccogliere dati personali memorizzati nel computer dei singoli utenti (ad esempio, le impostazioni dei programmi di navigazione, e informazioni sulle abitudini di navigazione del singolo utente) senza che questi abbiano la possibilità di accorgersene, intervenire o impedirlo,
- possono assumere il controllo, almeno parziale, del computer terminale e, quindi, limitare la capacità dell'utente di far fronte agli obblighi ed alle responsabilità previsti dalla legge nei suoi riguardi, in quanto titolare del trattamento, al fine di garantire la sicurezza dei dati personali eventualmente oggetto di trattamento,
- modificano il software installato sul computer, che sarà quindi utilizzato senza essere collaudato o approvato nei modi previsti, e
- possono provocare malfunzionamenti del computer senza che sia possibile individuare la causa nell'aggiornamento.

Tutto ciò può comportare particolari problemi per la pubblica amministrazione e le aziende private, nella misura in cui sussistano specifici obblighi di legge a loro carico relativamente alle modalità di trattamento dei dati personali.

2. La Conferenza, pertanto, invita le società produttrici di software

- a. ad offrire procedure per l'aggiornamento online del software soltanto su richiesta o iniziativa dell'utente, secondo modalità trasparenti e senza consentire accessi non controllati al computer dell'utente;
- b. a chiedere la comunicazione di dati personali soltanto con il consenso informato dell'utente e nella misura in cui ciò risulti necessario per effettuare l'aggiornamento online. Gli utenti non dovrebbero essere obbligati a fornire le proprie credenziali di identificazione – anziché di autenticazione – per dare inizio alla procedura di caricamento remoto;
- c. a prevedere meccanismi di libera scelta, offrendo l'aggiornamento online esclusivamente in alternativa ad altre forme (offline) di distribuzione del software, ad esempio via CD-ROM.

3. La Conferenza promuove la definizione e l'applicazione di tecnologie per l'aggiornamento del software che siano rispettose della privacy e dell'autonomia degli utenti.

102 Risoluzione sull'identificazione attraverso radiofrequenze (RFID)

Sulla base di una proposta formulata dall'Autorità per la protezione dei dati e l'accesso alle informazioni del Brandeburgo, dal Centro indipendente per la tutela della privacy dello Schleswig-Holstein, dall'Autorità spagnola per la protezione dei dati e dall'Autorità per la protezione dei dati del Cantone Zug, Svizzera, la Conferenza internazionale delibera quanto segue:

I dispositivi basati sull'identificazione attraverso radiofrequenze (RFID) trovano impiego crescente per numerosi scopi. Pur esistendo situazioni in cui tale tecnologia può avere effetti positivi e benefici, vi sono anche implicazioni potenziali in termini di privacy. Sinora le etichette RFID vengono utilizzate soprattutto per l'identificazione e la gestione di oggetti (prodotti), per il controllo della catena distributiva, o per tutelare l'autenticità di singoli marchi; tuttavia, esse potrebbero essere messe in relazione con dati personali come quelli ricavabili dalle carte di credito, e potrebbero essere utilizzate persino per raccogliere tali dati, oppure per localizzare o profilare individui in possesso di oggetti che rechino tali etichette. La tecnologia in questione potrebbe consentire di ricostruire le attività di singoli individui e istituire collegamenti fra le informazioni raccolte e banche dati preesistenti.

La Conferenza sottolinea la necessità di tenere conto dei principi di protezione dati qualora si preveda di introdurre etichette RFID connesse a dati personali. Occorre rispettare tutti i principi fondamentali della normativa in materia di protezione dei dati e privacy nella progettazione, nella realizzazione e nell'utilizzazione di dispositivi basati sulla tecnologia RFID. In particolare,

- a) prima di ricorrere a etichette RFID connesse a dati personali, o tali da consentire la profilazione della clientela, ciascun titolare di trattamento dovrebbe valutare approcci alternativi che consentano di raggiungere lo stesso obiettivo senza raccogliere dati personali o profilare la clientela;
- b) qualora il titolare del trattamento dimostri che è indispensabile ricorrere a dati personali, questi ultimi devono essere raccolti in modo chiaro e trasparente;
- c) i dati personali possono essere utilizzati esclusivamente per lo scopo specifico per cui sono stati inizialmente raccolti, e possono essere conservati soltanto finché risultino necessari al raggiungimento (o al soddisfacimento) di tale scopo, e
- d) i singoli interessati dovrebbero avere la possibilità di cancellare i dati e di disattivare o distruggere le etichette RFID una volta che ne siano entrati in possesso.

Si dovrebbe tenere conto dei principi sopra indicati nella progettazione e nell'utilizzazione di prodotti con tecnologie RFID.

La lettura e l'attivazione remote di etichette RFID, senza che la persona in possesso dell'oggetto recante un'etichetta del genere abbia alcuna ragionevole possibilità di intervenire in tale procedimento, sarebbero fonte di ulteriori preoccupazioni in termini di privacy.

La Conferenza e l'International Working Group on Data Protection in Telecommunications intendono seguire con attenzione e in modo approfondito gli sviluppi tecnologici in questo campo, al fine di garantire il rispetto dei principi di protezione dati e privacy nell'ambito della cosiddetta "informatizzazione pervasiva" (ubiquitous computing).

**CODICE IN MATERIA DI
PROTEZIONE DEI DATI PERSONALI**

Il Codice

Codice in materia di protezione dei dati personali Decreto legislativo 30 giugno 2003, n. 196 (*)

IL PRESIDENTE DELLA REPUBBLICA

VISTI gli articoli 76 e 87 della Costituzione;

VISTO l'articolo 1 della legge 24 marzo 2001, n. 127, recante delega al Governo per l'emanazione di un testo unico in materia di trattamento dei dati personali;

VISTO l'articolo 26 della legge 3 febbraio 2003, n. 14, recante disposizioni per l'adempimento di obblighi derivanti dall'appartenenza dell'Italia alle Comunità europee (legge comunitaria 2002);

VISTA la legge 31 dicembre 1996, n. 675, e successive modificazioni;

VISTA la legge 31 dicembre 1996, n. 676, recante delega al Governo in materia di tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali;

VISTA la direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione dei dati;

VISTA la direttiva 2002/58/CE del Parlamento europeo e del Consiglio, del 12 luglio 2002, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche;

VISTA la preliminare deliberazione del Consiglio dei ministri, adottata nella riunione del 9 maggio 2003;

SENTITO il Garante per la protezione dei dati personali;

ACQUISITO il parere delle competenti Commissioni parlamentari della Camera dei deputati e del Senato della Repubblica;

VISTA la deliberazione del Consiglio dei ministri, adottata nella riunione del 27 giugno 2003;

SULLA PROPOSTA del Presidente del Consiglio dei ministri, del Ministro per la funzione pubblica e del Ministro per le politiche comunitarie, di concerto con i Ministri della giustizia, dell'economia e delle finanze, degli affari esteri e delle comunicazioni;

EMANA

il seguente decreto legislativo:

(*) Testo consolidato con la legge 26 febbraio 2004, n. 45, di conversione con modificazioni del d.l. 24 dicembre 2003, n. 354

PARTE I - DISPOSIZIONI GENERALI

TITOLO I - PRINCIPI GENERALI

Art. 1. Diritto alla protezione dei dati personali

1. Chiunque ha diritto alla protezione dei dati personali che lo riguardano.

Art. 2. Finalità

1. Il presente testo unico, di seguito denominato “codice”, garantisce 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, 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 di cui al comma 1 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.

Art. 3. Principio di necessità nel trattamento dei dati

1. I sistemi informativi e i programmi informatici sono 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.

Art. 4. Definizioni

1. Ai fini del presente codice si intende per:

- a) “trattamento”, qualunque operazione o complesso di operazioni, effettuati anche senza l’ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l’organizzazione, la conservazione, la consultazione, l’elaborazione, la modificazione, la selezione, l’estrazione, il raffronto, l’utilizzo, l’interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca di dati;
- b) “dato personale”, qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale;
- c) “dati identificativi”, i dati personali che permettono l’identificazione diretta dell’interessato;
- d) “dati sensibili”, i dati personali idonei a rivelare l’origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l’adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale;
- e) “dati giudiziari”, i dati personali idonei a rivelare provvedimenti di cui all’articolo 3, comma 1, lettere da a) a o) e da r) a u), del d.P.R. 14 novembre 2002, n. 313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale;
- f) “titolare”, 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;
- g) “responsabile”, la persona fisica, la persona giuridica, la pubblica amministrazione

- e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali;
- h) “incaricati”, le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile;
 - i) “interessato”, la persona fisica, la persona giuridica, l'ente o l'associazione cui si riferiscono i dati personali;
 - l) “comunicazione”, il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dello Stato, dal responsabile e dagli incaricati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;
 - m) “diffusione”, il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;
 - n) “dato anonimo”, il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile;
 - o) “blocco”, la conservazione di dati personali con sospensione temporanea di ogni altra operazione del trattamento;
 - p) “banca di dati”, qualsiasi complesso organizzato di dati personali, ripartito in una o più unità dislocate in uno o più siti;
 - q) “Garante”, l'autorità di cui all'articolo 153, istituita dalla legge 31 dicembre 1996, n. 675.

2. Ai fini del presente codice si intende, inoltre, per:

- a) “comunicazione elettronica”, ogni informazione scambiata o trasmessa tra un numero finito di soggetti tramite un servizio di comunicazione elettronica accessibile al pubblico. Sono escluse le informazioni trasmesse al pubblico tramite una rete di comunicazione elettronica, come parte di un servizio di radiodiffusione, salvo che le stesse informazioni siano collegate ad un abbonato o utente ricevente, identificato o identificabile;
- b) “chiamata”, la connessione istituita da un servizio telefonico accessibile al pubblico, che consente la comunicazione bidirezionale in tempo reale;
- c) “reti di comunicazione elettronica”, i sistemi di trasmissione, le apparecchiature di commutazione o di instradamento e altre risorse che consentono di trasmettere segnali via cavo, via radio, a mezzo di fibre ottiche o con altri mezzi elettromagnetici, incluse le reti satellitari, le reti terrestri mobili e fisse a commutazione di circuito e a commutazione di pacchetto, compresa Internet, le reti utilizzate per la diffusione circolare dei programmi sonori e televisivi, i sistemi per il trasporto della corrente elettrica, nella misura in cui sono utilizzati per trasmettere i segnali, le reti televisive via cavo, indipendentemente dal tipo di informazione trasportato;
- d) “rete pubblica di comunicazioni”, una rete di comunicazioni elettroniche utilizzata interamente o prevalentemente per fornire servizi di comunicazione elettronica accessibili al pubblico;
- e) “servizio di comunicazione elettronica”, i servizi consistenti esclusivamente o prevalentemente nella trasmissione di segnali su reti di comunicazioni elettroniche, compresi i servizi di telecomunicazioni e i servizi di trasmissione nelle reti utilizzate per la diffusione circolare radiotelevisiva, nei limiti previsti dall'articolo 2, lettera c), della direttiva 2002/21/CE del Parlamento europeo e del Consiglio, del 7 marzo 2002;
- f) “abbonato”, qualunque persona fisica, persona giuridica, ente o associazione parte di un contratto con un fornitore di servizi di comunicazione elettronica accessibili al pubblico per la fornitura di tali servizi, o comunque destinatario di tali servizi tramite schede prepagate;
- g) “utente”, qualsiasi persona fisica che utilizza un servizio di comunicazione elettronica accessibile al pubblico, per motivi privati o commerciali, senza esservi necessariamente abbonata;
- h) “dati relativi al traffico”, qualsiasi dato sottoposto a trattamento ai fini della trasmissione di una comunicazione su una rete di comunicazione elettronica o della relativa fatturazione;
- i) “dati relativi all'ubicazione”, ogni dato trattato in una rete di comunicazione elettronica che indica la posizione geografica dell'apparecchiatura terminale dell'utente di un servizio di comunicazione elettronica accessibile al pubblico;

- l) “servizio a valore aggiunto”, il servizio che richiede il trattamento dei dati relativi al traffico o dei dati relativi all’ubicazione diversi dai dati relativi al traffico, oltre a quanto è necessario per la trasmissione di una comunicazione o della relativa fatturazione;
 - m) “posta elettronica”, messaggi contenenti testi, voci, suoni o immagini trasmessi attraverso una rete pubblica di comunicazione, che possono essere archiviati in rete o nell’apparecchiatura terminale ricevente, fino a che il ricevente non ne ha preso conoscenza.
3. Ai fini del presente codice si intende, altresì, per:
- a) “misure minime”, il complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza che configurano il livello minimo di protezione richiesto in relazione ai rischi previsti nell’articolo 31;
 - b) “strumenti elettronici”, gli elaboratori, i programmi per elaboratori e qualunque dispositivo elettronico o comunque automatizzato con cui si effettua il trattamento;
 - c) “autenticazione informatica”, l’insieme degli strumenti elettronici e delle procedure per la verifica anche indiretta dell’identità;
 - d) “credenziali di autenticazione”, i dati ed i dispositivi, in possesso di una persona, da questa conosciuti o ad essa univocamente correlati, utilizzati per l’autenticazione informatica;
 - e) “parola chiave”, componente di una credenziale di autenticazione associata ad una persona ed a questa nota, costituita da una sequenza di caratteri o altri dati in forma elettronica;
 - f) “profilo di autorizzazione”, l’insieme delle informazioni, univocamente associate ad una persona, che consente di individuare a quali dati essa può accedere, nonché i trattamenti ad essa consentiti;
 - g) “sistema di autorizzazione”, l’insieme degli strumenti e delle procedure che abilitano l’accesso ai dati e alle modalità di trattamento degli stessi, in funzione del profilo di autorizzazione del richiedente.
4. Ai fini del presente codice si intende per:
- a) “scopi storici”, le finalità di studio, indagine, ricerca e documentazione di figure, fatti e circostanze del passato;
 - b) “scopi statistici”, le finalità di indagine statistica o di produzione di risultati statistici, anche a mezzo di sistemi informativi statistici;
 - c) “scopi scientifici”, le finalità di studio e di indagine sistematica finalizzata allo sviluppo delle conoscenze scientifiche in uno specifico settore.

Art. 5. Oggetto ed ambito di applicazione

1. Il presente codice disciplina il trattamento di dati personali, anche detenuti all’estero, effettuato da chiunque è stabilito nel territorio dello Stato o in un luogo comunque soggetto alla sovranità dello Stato.

2. Il presente codice si applica anche al trattamento di dati personali effettuato da chiunque è stabilito nel territorio di un Paese non appartenente all’Unione europea e impiega, per il trattamento, 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. In caso di applicazione del presente codice, il titolare del trattamento designa un proprio rappresentante stabilito nel territorio dello Stato ai fini dell’applicazione della disciplina sul trattamento dei dati personali.

3. Il trattamento di dati personali effettuato da persone fisiche per fini esclusivamente personali è soggetto all’applicazione del presente codice solo se i dati sono destinati ad una comunicazione sistematica o alla diffusione. Si applicano in ogni caso le disposizioni in tema di responsabilità e di sicurezza dei dati di cui agli articoli 15 e 31.

Art. 6. Disciplina del trattamento

1. Le disposizioni contenute nella presente Parte si applicano a tutti i trattamenti di dati, salvo quanto previsto, in relazione ad alcuni trattamenti, dalle disposizioni integrative o modificative della Parte II.

TITOLO II - DIRITTI DELL'INTERESSATO**Art. 7. Diritto di accesso ai dati personali ed altri diritti**

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 ai sensi dell'articolo 5, comma 2;
- 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.

3. L'interessato ha diritto di ottenere:

- a) l'aggiornamento, la rettificazione ovvero, quando vi ha interesse, l'integrazione dei dati;
- b) 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;
- c) 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.

4. L'interessato ha diritto di opporsi, in tutto o in parte:

- a) per motivi legittimi al trattamento dei dati personali che lo riguardano, ancorché pertinenti allo scopo della raccolta;
- b) 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.

Art. 8. Esercizio dei diritti

1. I diritti di cui all'articolo 7 sono 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.

2. I diritti di cui all'articolo 7 non possono essere esercitati con richiesta al titolare o al responsabile o con ricorso ai sensi dell'articolo 145, se i trattamenti di dati personali sono effettuati:

- a) in base alle disposizioni del decreto legge 3 maggio 1991, n. 143, convertito, con modificazioni, dalla legge 5 luglio 1991, n. 197, e successive modificazioni, in materia di riciclaggio;
- b) in base alle disposizioni del decreto legge 31 dicembre 1991, n. 419, convertito, con modificazioni, dalla legge 18 febbraio 1992, n. 172, e successive modificazioni, in materia di sostegno alle vittime di richieste estorsive;
- c) da Commissioni parlamentari d'inchiesta istituite ai sensi dell'articolo 82 della

Costituzione;

- d) da un soggetto pubblico, diverso dagli enti pubblici economici, in base ad espressa disposizione di legge, per esclusive finalità inerenti alla politica monetaria e valutaria, al sistema dei pagamenti, al controllo degli intermediari e dei mercati creditizi e finanziari, nonché alla tutela della loro stabilità;
- e) ai sensi dell'articolo 24, comma 1, lettera f), limitatamente al periodo durante il quale potrebbe derivarne un pregiudizio effettivo e concreto per lo svolgimento delle investigazioni difensive o per l'esercizio del diritto in sede giudiziaria;
- f) da fornitori di servizi di comunicazione elettronica accessibili al pubblico relativamente a comunicazioni telefoniche in entrata, salvo che possa derivarne un pregiudizio effettivo e concreto per lo svolgimento delle investigazioni difensive di cui alla legge 7 dicembre 2000, n. 397;
- g) per ragioni di giustizia, presso uffici giudiziari di ogni ordine e grado o il Consiglio superiore della magistratura o altri organi di autogoverno o il Ministero della giustizia;
- h) ai sensi dell'articolo 53, fermo restando quanto previsto dalla legge 1° aprile 1981, n. 121.

3. Il Garante, anche su segnalazione dell'interessato, nei casi di cui al comma 2, lettere a), b), d), e) ed f), provvede nei modi di cui agli articoli 157, 158 e 159 e, nei casi di cui alle lettere c), g) ed h) del medesimo comma, provvede nei modi di cui all'articolo 160.

4. L'esercizio dei diritti di cui all'articolo 7, quando non riguarda dati di carattere oggettivo, può avere luogo salvo che concerna la rettificazione o l'integrazione di dati personali di tipo valutativo, relativi a giudizi, opinioni o ad altri apprezzamenti di tipo soggettivo, nonché l'indicazione di condotte da tenersi o di decisioni in via di assunzione da parte del titolare del trattamento.

Art. 9. Modalità di esercizio

1. La richiesta rivolta al titolare o al responsabile può essere trasmessa anche mediante lettera raccomandata, telefax o posta elettronica. Il Garante può individuare altro idoneo sistema in riferimento a nuove soluzioni tecnologiche. Quando riguarda l'esercizio dei diritti di cui all'articolo 7, commi 1 e 2, la richiesta può essere formulata anche oralmente e in tal caso è annotata sinteticamente a cura dell'incaricato o del responsabile.

2. Nell'esercizio dei diritti di cui all'articolo 7 l'interessato può conferire, per iscritto, delega o procura a persone fisiche, enti, associazioni od organismi. L'interessato può, altresì, farsi assistere da una persona di fiducia.

3. I diritti di cui all'articolo 7 riferiti a dati personali concernenti persone decedute possono essere esercitati da chi ha un interesse proprio, o agisce a tutela dell'interessato o per ragioni familiari meritevoli di protezione.

4. L'identità dell'interessato è verificata sulla base di idonei elementi di valutazione, anche mediante atti o documenti disponibili o esibizione o allegazione di copia di un documento di riconoscimento. La persona che agisce per conto dell'interessato esibisce o allega copia della procura, ovvero della delega sottoscritta in presenza di un incaricato o sottoscritta e presentata unitamente a copia fotostatica non autenticata di un documento di riconoscimento dell'interessato. Se l'interessato è una persona giuridica, un ente o un'associazione, la richiesta è avanzata dalla persona fisica legittimata in base ai rispettivi statuti od ordinamenti.

5. La richiesta di cui all'articolo 7, commi 1 e 2, è formulata liberamente e senza costrizioni e può essere rinnovata, salva l'esistenza di giustificati motivi, con intervallo non minore di novanta giorni.

Art. 10. Riscontro all'interessato

1. Per garantire l'effettivo esercizio dei diritti di cui all'articolo 7 il titolare del trattamento è tenuto ad adottare idonee 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.

2. I dati sono estratti a cura del responsabile o degli incaricati e possono essere comunicati al richiedente anche oralmente, ovvero offerti in visione mediante strumenti elettronici, sempre che in tali casi la comprensione dei dati sia agevole, considerata anche la qualità e la quantità delle informazioni. Se vi è richiesta, si provvede alla trasposizione dei dati su supporto cartaceo o informatico, ovvero alla loro trasmissione per via telematica.

3. Salvo che la richiesta sia riferita ad un particolare trattamento o a specifici dati personali o categorie di dati personali, il riscontro all'interessato comprende tutti i dati personali che riguardano l'interessato comunque trattati dal titolare. Se la richiesta è rivolta ad un esercente una professione sanitaria o ad un organismo sanitario si osserva la disposizione di cui all'articolo 84, comma 1.

4. Quando l'estrazione dei dati risulta particolarmente difficoltosa il riscontro alla richiesta dell'interessato può avvenire anche attraverso l'esibizione o la consegna in copia di atti e documenti contenenti i dati personali richiesti.

5. Il diritto di ottenere la comunicazione in forma intelligibile dei dati non riguarda dati personali relativi a terzi, salvo che la scomposizione dei dati trattati o la privazione di alcuni elementi renda incomprensibili i dati personali relativi all'interessato.

6. La comunicazione dei dati è effettuata in forma intelligibile anche attraverso l'utilizzo di una grafia comprensibile. In caso di comunicazione di codici o sigle sono forniti, anche mediante gli incaricati, i parametri per la comprensione del relativo significato.

7. Quando, a seguito della richiesta di cui all'articolo 7, commi 1 e 2, lettere a), b) e c) non risulta confermata l'esistenza di dati che riguardano l'interessato, può essere chiesto un contributo spese non eccedente i costi effettivamente sopportati per la ricerca effettuata nel caso specifico.

8. Il contributo di cui al comma 7 non può comunque superare l'importo determinato dal Garante con provvedimento di carattere generale, che può individuarlo forfettariamente in relazione al caso in cui i dati sono trattati con strumenti elettronici e la risposta è fornita oralmente. Con il medesimo provvedimento il Garante può prevedere che il contributo possa essere chiesto quando i dati personali figurano su uno speciale supporto del quale è richiesta specificamente la riproduzione, oppure quando, presso uno o più titolari, si determina un notevole impiego di mezzi in relazione alla complessità o all'entità delle richieste ed è confermata l'esistenza di dati che riguardano l'interessato.

9. Il contributo di cui ai commi 7 e 8 è corrisposto anche mediante versamento postale o bancario, ovvero mediante carta di pagamento o di credito, ove possibile all'atto della ricezione del riscontro e comunque non oltre quindici giorni da tale riscontro.

TITOLO III - REGOLE GENERALI PER IL TRATTAMENTO DEI DATI

CAPO I - REGOLE PER TUTTI I TRATTAMENTI

Art. 11. Modalità del trattamento e requisiti dei dati

1. I dati personali oggetto di trattamento sono:
 - a) trattati in modo lecito e secondo correttezza;
 - b) raccolti e registrati per scopi determinati, espliciti e legittimi, ed utilizzati in altre operazioni del trattamento in termini compatibili con tali scopi;
 - c) esatti e, se necessario, aggiornati;

- d) pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti o successivamente trattati;
- e) conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati.

2. I dati personali trattati in violazione della disciplina rilevante in materia di trattamento dei dati personali non possono essere utilizzati.

Art. 12. Codici di deontologia e di buona condotta

1. Il Garante promuove nell'ambito delle categorie interessate, nell'osservanza del principio di rappresentatività e tenendo conto dei criteri direttivi delle raccomandazioni del Consiglio d'Europa sul trattamento di dati personali, la sottoscrizione di codici di deontologia e di buona condotta per determinati settori, ne verifica la conformità alle leggi e ai regolamenti anche attraverso l'esame di osservazioni di soggetti interessati e contribuisce a garantirne la diffusione e il rispetto.

2. I codici sono pubblicati nella *Gazzetta Ufficiale* della Repubblica italiana a cura del Garante e, con decreto del Ministro della giustizia, sono riportati nell'allegato A) del presente codice.

3. Il rispetto delle disposizioni contenute nei codici di cui al comma 1 costituisce condizione essenziale per la liceità e correttezza del trattamento dei dati personali effettuato da soggetti privati e pubblici.

4. Le disposizioni del presente articolo si applicano anche al codice di deontologia per i trattamenti di dati per finalità giornalistiche promosso dal Garante nei modi di cui al comma 1 e all'articolo 139.

Art. 13. Informativa

1. L'interessato o la persona presso la quale sono raccolti i dati personali sono previamente informati oralmente o per iscritto circa:

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

2. L'informativa di cui al comma 1 contiene anche gli elementi previsti da specifiche disposizioni del presente codice e può non comprendere gli elementi già noti alla persona che fornisce i dati o la cui conoscenza può ostacolare in concreto l'espletamento, da parte di un soggetto pubblico, di funzioni ispettive o di controllo svolte per finalità di difesa o sicurezza dello Stato oppure di prevenzione, accertamento o repressione di reati.

3. Il Garante può individuare con proprio provvedimento modalità semplificate per l'informativa fornita in particolare da servizi telefonici di assistenza e informazione al pubblico.

4. Se i dati personali non sono raccolti presso l'interessato, l'informativa di cui al comma 1, comprensiva delle categorie di dati trattati, è data al medesimo interessato all'atto della registra-