SENATO DELLA REPUBBLICA

XVI LEGISLATURA

Doc. CXXXVI
n. 1

RELAZIONE

SULL'ATTIVITÀ SVOLTA DAL GARANTE E SULLO STATO DI ATTUAZIONE DEL CODICE IN MATERIA DI PROTEZIONE DEI DATI PERSONALI

(ANNO 2007)

(Articolo 154, comma 1, lettera m), *del decreto legislativo 30 giugno 2003, n. 196)*

Presentata dal Garante per la protezione dei dati personali

(PIZZETTI)

Comunicata alla Presidenza il 25 luglio 2008

TIPOGRAFIA DEL SENATO (100)

INDICE GENERALE

I. STATO DI ATTUAZIONE DEL CODICE IN MATERIA DI PROTEZIONE DEI DATI PERSONALI

DOCUMENTAZIONE
Provvedimenti del Garante
Regolamenti e provvedimenti generali

Elenco delle abbreviazioni

La presente Relazione è riferita al 2007 e contiene talune notizie già anticipate nella precedente Relazione, nonché alcune ulteriori informazioni, aggiornate al 24 aprile 2008, relative a sviluppi che si è ritenuto opportuno menzionare.

ad es.	ad esempio
art.	articolo
Bollettino	Bollettino del Garante per la protezione dei dati personali "Cittadini e Società dell'Informazione"
c.c.	codice civile
c.p.c.	codice di procedura civile
c.p.p.	codice di procedura penale
cd.	cosiddetto/a
cfr.	confronta
Cost.	Costituzione
d.l.	decreto-legge
d.lg.	decreto legislativo
d.m.	decreto ministeriale
d.P.C.M.	decreto del Presidente del Consiglio dei ministri
d.P.R.	decreto del Presidente della Repubblica
G.U.	Gazzetta Ufficiale
l.	legge
lett.	lettera
n.	numero
p.	pagina
p.a.	Pubblica amministrazione
par.	paragrafo
Provv.	provvedimento del Garante per la protezione dei dati personali
Relazione	Relazione del Garante
r.d.	regio decreto
reg.	regolamento
T.U.	testo unico
u.s.	ultimo scorso
Ue	Unione europea
v.	vedi

Stato di attuazione del Codice in materia di protezione dei dati personali

I - Stato di attuazione del Codice in materia di protezione dei dati personali

1 Principali interventi dell'Autorità nel 2007

1.1. *Provvedimenti più significativi*

1.1.1 *Banche dati Dna, Ris dell'Arma dei carabinieri e Ced del Dipartimento di pubblica sicurezza*

Il Garante ha inviato al Parlamento e al Governo una segnalazione, adottata il 19 settembre 2007 [doc. *web* n. 1456163], in relazione alle iniziative legislative che si sono registrate sul finire della XV legislatura per l'istituzione di una banca dati del Dna a fini di sicurezza e giustizia, con la quale ha individuato gli aspetti per i quali l'Autorità ritiene opportuno un intervento normativo e ha indicato le garanzie da assicurare alle persone interessate.

Il Garante, nel condividere l'esigenza di disciplinare organicamente la materia e potenziare le tecniche di indagine, anche per scopi di cooperazione internazionale, ha osservato che vi sono rilevanti effetti sui diritti e le libertà fondamentali delle persone; pertanto, una normativa adeguata sull'uso e la gestione dei dati relativi al Dna per finalità di accertamento e repressione dei reati dovrebbe prendere in esame alcuni profili fondamentali. In particolare, l'Autorità ha richiamato l'attenzione del Parlamento e del Governo sui seguenti aspetti:

- la banca dati dovrebbe avere esclusive finalità specifiche di identificazione delle persone, anche in armonia con quanto previsto dal Trattato di *Prüm* sulla cooperazione transfrontaliera e dalla normativa europea;
- la banca dati deve contenere solo profili Dna (sequenze alfanumeriche) e le relative informazioni non devono essere duplicate in altri archivi di singole forze di polizia;
- considerata la particolare delicatezza e natura dei dati genetici, che riguardano non soltanto l'individuo, ma il suo intero gruppo biologico, i relativi campioni non devono essere conservati in forma di banca dati e devono essere applicati sistemi di analisi che non consentano di individuare patologie di cui sia eventualmente affetto l'interessato;
- gli operatori che possono accedere ai dati devono essere individuati con modalità selettive e solo in rapporto ad attività investigative previste o disposte per legge;
- sempre per la particolare delicatezza di queste informazioni, occorre assicu-

rare un elevato livello di sicurezza e qualità dei dati tale da consentire il tracciamento di ogni accesso e lo svolgimento periodico di adeguate procedure di controllo;

- occorrono specifiche indicazioni circa le modalità con le quali le persone i cui dati sono conservati possano esercitare i diritti loro riconosciuti dal Codice *privacy*, ovvero l'accesso, l'aggiornamento, o l'eventuale cancellazione dei dati.

L'Autorità ha inoltre raccomandato di prestare la massima attenzione all'ambito della raccolta dei dati e ai motivi che la giustificano. L'istituzione di una banca dati a livello nazionale non impone necessariamente l'introduzione di un prelievo obbligatorio del Dna poiché un tale archivio può essere utilmente composto da dati raccolti nell'ambito di procedimenti penali, già molto numerosi. Tuttavia, per il caso in cui il Parlamento ritenesse di stabilire un prelievo obbligatorio per alcune categorie di soggetti (fermati, arrestati, indagati, imputati o condannati), l'Autorità ha sottolineato la necessità di individuare in maniera proporzionata i soggetti interessati e i relativi reati, da definire sulla base della loro gravità.

Il Garante ha infine concordato sull'utilità di specifiche previsioni che confermino i compiti di vigilanza e controllo dell'Autorità stessa su tali trattamenti di dati, anche con riferimento a un eventuale rapporto periodico al Parlamento.

Le indicazioni espresse nella segnalazione sono state richiamate e specificate nel parere che il Garante ha reso successivamente sullo schema di disegno di legge presentato dal Governo per l'istituzione della banca dati (*Parere* 15 ottobre 2007 [doc. *web* n. 1448799]).

Nel corso del 2007 è altresì proseguita l'istruttoria sull'utilizzo dei dati genetici per finalità di polizia giudiziaria da parte del Reparto investigazioni scientifiche dell'Arma dei carabinieri di Parma (*v. Relazione* 2006, p. 138). Al termine degli accertamenti, con *provvedimento* del 19 luglio 2007 adottato ai sensi degli artt. 143, 144, 154 e 160 del Codice, il Garante ha prescritto all'Arma dei carabinieri-Reparto investigazioni scientifiche di Parma di effettuare l'ulteriore utilizzo dei campioni biologici e dei profili genetici, anche con specifico riferimento all'attività di comparazione, in conformità a quanto disposto dalle competenti autorità giudiziarie e alle condizioni e nei limiti previsti dal codice di procedura penale; ha, altresì, impartito una serie di prescrizioni per rafforzare il livello di protezione dei profili genetici e dei campioni biologici conservati presso il Reparto.

Analogamente, seppure in relazione a profili tematici diversi da quelli sopra menzionati, con il *provvedimento* adottato l'8 maggio 2007 e relativo ai trattamenti dei dati posti in essere presso il Centro elaborazione dati (Ced) del Dipartimento della pubblica sicurezza del Ministero dell'interno, sulla base di accertamenti avviati nel 2006 (*cfr. Relazione* 2006, p. 72-73), il Garante ha prescritto le modificazioni da apportare ai trattamenti di dati personali svolti presso il Centro allo scopo di dare attuazione agli obblighi stabiliti dal Codice e dai princìpi posti nella Raccomandazione n. R(87) 15 del Consiglio d'Europa. Ciò, con particolare riferimento alla pertinenza e aggiornamento dei dati, alle informazioni acquisite da attività amministrative, ai tempi di conservazione dei dati, alla connessione con altre banche dati e all'esercizio dei diritti da parte degli interessati.

1.1.2. *Conservazione e sicurezza dei dati di traffico telefonico e telematico*

Vi sono stati alcuni interventi di particolare rilievo sulla conservazione dei dati di traffico telefonico e telematico volti a contemperare le esigenze di tutela della sfera privata di milioni di cittadini e le esigenze funzionali della magistratura e delle forze di polizia.

Con deliberazione del 19 settembre 2007 [doc. *web* n. 1442463], il Garante ha avviato una consultazione pubblica sulle regole essenziali per la messa in sicurezza dei dati conservati a fini di accertamento e repressione dei reati. Sono state interpellate le istituzioni interessate (in particolare Ministero della giustizia, Ministero dell'interno e Csm), le aziende e le relative associazioni di categoria, nonché le associazioni dei consumatori, allo scopo di adottare un provvedimento definitivo sulla base delle osservazioni pervenute.

Il documento oggetto della consultazione, frutto di un'attività anche ispettiva molto articolata, iniziata alla fine del 2005, indica in maniera organica le misure da rispettare per la conservazione dei dati a fini di giustizia da parte dei fornitori di servizi di comunicazione elettronica.

In particolare il documento, nel chiarire i soggetti destinatari e i dati oggetto di conservazione, stabilisce prescrizioni tecnico organizzative riguardo alla loro tenuta e alla loro messa in sicurezza.

Sono esclusi dall'ambito di applicazione di queste misure i gestori di esercizi pubblici e *Internet café*, di siti Internet che diffondono contenuti sulla rete (*"content provider"*), e di motori di ricerca, nonché le aziende o le amministrazioni pubbliche che mettono a disposizione del personale reti telefoniche e informatiche (*ad es.*, centralini aziendali) o che si avvalgono di *server* messi a disposizione da altri soggetti.

Le garanzie di base per la messa in sicurezza dei dati sono state poi individuate con *provvedimento* del 17 gennaio 2008, (in *G.U.* n. 30 del 5 febbraio 2008 [doc. *web* n. 1482111]), anche alla luce delle osservazioni pervenute nel corso della consultazione pubblica.

I dati di traffico telefonico e Internet sono particolarmente delicati: numero chiamato, data, ora, durata della chiamata, localizzazione del chiamante nel caso del cellulare, dati inerenti agli *Sms* o *Mms*, indirizzi *e-mail* contattati, data, ora e durata degli accessi alla rete consentono infatti di ricostruire tutte le relazioni di una persona e le sue abitudini.

Le garanzie riguardano, in sintesi:

Accesso ai dati: quest'ultimo è consentito solo al personale incaricato e mediante avanzati sistemi di autenticazione informatica, anche con l'uso di dati biometrici (*ad es.*, impronte digitali). Sono compresi nell'ambito applicativo della prescrizione, salvo limitati casi di necessità, gli amministratori di sistema, figure chiave della sicurezza delle banche dati sul cui ruolo, spesso sottovalutato anche nei settori più delicati, l'Autorità avvierà una più approfondita riflessione.

Accesso ai locali: i locali in cui sono ospitati i sistemi di elaborazione che trattano dati di traffico telefonico per esclusive finalità di giustizia devono disporre di sistemi biometrici di controllo degli accessi. In ogni caso, i sistemi che trattano dati di traffico di qualsiasi natura vanno installati in locali ad accesso selezionato.

Sistemi di autorizzazione: le funzioni tra chi assegna le credenziali di autenticazione e chi accede ai dati devono essere separate rigidamente. I profili di autorizzazione da attribuire agli incaricati devono essere differenziati a seconda che il trattamento dei dati di traffico sia effettuato per scopi di ordinaria gestione o per quelli di accertamento e repressione dei reati.

Tracciamento dell'attività del personale incaricato: ogni accesso effettuato e ogni operazione compiuta da parte degli incaricati e degli amministratori di sistema devono essere registrati in appositi *audit log*.

Conservazione separata: i dati tenuti per esclusive finalità di accertamento e repressione dei reati devono essere conservati separatamente da quelli utiliz-

zati per funzioni aziendali (*ad es.*, fatturazione, *marketing*, antifrode, statistiche) e i sistemi di elaborazione che li trattano vanno sottoposti a rigide misure di sicurezza fisica e controllo degli accessi.

Cancellazione dei dati: una volta decorso il tempo previsto di conservazione i dati devono essere immediatamente cancellati o resi anonimi, eliminandoli anche dalle copie di *backup* create per il salvataggio dei dati.

Controlli interni: devono essere effettuati controlli periodici sulla legittimità degli accessi ai dati da parte degli incaricati, sul rispetto delle norme di legge e delle misure organizzative tecniche e di sicurezza prescritte dal Garante, sull'effettiva cancellazione dei dati una volta decorsi i termini di conservazione.

Sistemi di cifratura: contro i rischi di acquisizione indebita, anche fortuita, delle informazioni registrate da parte di incaricati di mansioni tecniche (amministratori di sistema, amministratori di *database*, manutentori *hardware* e *software*), i dati di traffico trattati per esclusive finalità di giustizia devono essere protetti con tecniche crittografiche.

I fornitori di servizi di comunicazione elettronica dovranno applicare tali misure entro il 31 ottobre 2008. L'introduzione di alcune di esse è stata disposta dal Garante anche in relazione alla conservazione dei dati per finalità non di giustizia, (fatturazione, commercializzazione di servizi, statistica *ecc.*), al fine di favorire un quadro più ampio di sicurezza di dati e sistemi.

Prima del recente recepimento della direttiva europea in materia, il *cd.* decreto "milleproroghe" (d.l. 31 dicembre 2007, n. 248 conv. con legge 28 febbraio 2008, n. 31), ha, tuttavia, stabilito che i tempi di conservazione potevano, in sostanza, giungere a otto per i dati di traffico telefonico e superare i tre per quelli telematici.

Con lettere inviate al Presidente della Camera dei Deputati ed al Ministro delle Politiche Europee, il Garante ha quindi ribadito le proprie preoccupazioni sui tempi di conservazione dei dati detenuti per finalità di giustizia. L'Autorità ha richiamato l'esigenza che il bilanciamento degli interessi coinvolti sia conforme alle prescrizioni della predetta direttiva comunitaria (la *cd.* "direttiva Frattini") e che quest'ultima, la quale prevede tempi di conservazione dei dati di traffico sia telefonico che telematico compresi tra un minimo di sei mesi ed un massimo di due anni, fosse tempestivamente recepita; ha perciò auspicato l'introduzione di alcune modifiche correttive in sede di conversione del decreto, affinché fosse specificato che il periodo di conservazione dei dati era prorogato solo fino all'entrata in vigore del decreto di recepimento della direttiva e, comunque, non oltre il 31 dicembre 2008.

Con i provvedimenti del 10 gennaio 2008, a tutela degli utenti di alcuni dei maggiori gestori di servizi telefonici e telematici, è stata imposta a Telecom Italia S.p.A. [doc. *web* n. 1524263], Vodafone Omnitel N.V., [doc. *web* n. 1484758], e H3G S.p.A. [doc. *web* n. 1484726], la cancellazione di informazioni, conservate illegittimamente, riguardanti i siti Internet visitati dagli utenti. A Vodafone, H3G e Wind telecomunicazioni S.p.A. è stata impartita l'adozione di specifiche misure tecniche per la messa in sicurezza dei dati personali conservati a fini di giustizia.

I gestori devono infatti conservare esclusivamente i dati di traffico telematico funzionali alla fornitura e alla fatturazione del servizio di connessione e non i dati di traffico apparentemente "esterni" alla comunicazione (pagine *web* visitate o gli indirizzi *Ip* di destinazione) e che possono peraltro coincidere di fatto con il "contenuto" della comunicazione, consentendo di ricostruire meglio relazioni personali e sociali, convinzioni religiose, orientamenti politici, abitudini sessuali e stato di salute.

La mancata adozione di alcune misure di sicurezza e l'indebita conservazione dei dati sulla navigazione in Internet era emersa nel corso dell'attività ispettiva disposta dal Garante anche nell'ultimo anno al fine di verificare il rispetto del Codice e delle

prescrizioni impartite dall'Autorità con il *provvedimento* del 15 dicembre 2005 [doc. *web* n. 1203890] riguardo alla protezione dei dati di traffico telefonico conservati a fini di giustizia e alle modalità con le quali i gestori di telefonia, fissa e mobile, adempiono alle richieste dell'autorità giudiziaria in materia di intercettazioni.

1.1.3. *Posta elettronica e rete Internet*

Soggetti privati come le società non possono svolgere attività di monitoraggio sistematico finalizzato all'individuazione di utenti che si scambiano *file* musicali o giochi su Internet.

Questa la decisione adottata il 28 febbraio 2008 [doc. *web* n. 1495246] al termine dell'istruttoria avviata sul "caso Peppermint", la società discografica con sede in Germania che aveva svolto, attraverso una società svizzera (la Logistep, utilizzata anche dalla società Techland sp. z.o.o., la quale commercializza giochi elettronici avente sede in Polonia), un monitoraggio delle reti *peer to peer* (P2p). Tramite l'utilizzo di uno specifico *software*, le società avevano individuato numerosissimi indirizzi Ip (che identificano i *computer* collegati ad Internet) relativi a utenti ritenuti responsabili dello scambio illegale di *file*: erano poi risalite ai nominativi degli utenti, anche italiani, al prevalente fine di potere ottenere un risarcimento del danno.

Il Garante ha ritenuto illecita l'attività svolta dalle società, richiamando anche la decisione dell'omologa autorità svizzera del 9 gennaio 2008 (*cfr. www.edoeb.admin.ch*).

Al riguardo, sono state altresì considerate le ordinanze con cui il Tribunale di Roma –come richiesto dal Garante– ha rigettato alcuni ricorsi con i quali le società Peppermint e Techland intendevano ottenere da taluni fornitori di servizi di comunicazione elettronica la trasmissione delle generalità dei soggetti ritenuti responsabili di aver scambiato *file* protetti dal diritto d'autore tramite reti *peer to peer*. Tale profilo della comunicazione dei dati di traffico è stato esaminato, da ultimo, dalla Corte di giustizia delle Comunità europee la quale si è pronunciata su una questione per molti aspetti simile (sentenza 29 gennaio 2008, pronunciata nella causa C-275/06 Promusicae c/ Telefonica de Espana Sau), escludendo la possibilità che tali dati potessero essere messi a disposizione per controversie civili relative ai diritti di proprietà intellettuale (*cfr.* punto 48 della sentenza; artt. 15, n. 2, e 18 della direttiva 2000/31/Ce relativa a taluni aspetti giuridici dei servizi della Società dell'informazione, in particolare il commercio elettronico, nel mercato interno; artt. 8, nn. 1 e 2 direttiva 2001/29/Ce sull'armonizzazione di taluni aspetti del diritto d'autore e dei diritti connessi nella società dell'informazione; art. 8 direttiva 2004/48/Ce sul rispetto dei diritti di proprietà intellettuale; artt. 17, n. 2 e 47 Carta dei diritti fondamentali dell'Unione europea).

La decisione del Garante del 28 febbraio ricorda che la direttiva europea sulle comunicazioni elettroniche vieta ai privati di poter effettuare monitoraggi, ossia trattamenti di dati massivi, capillari e prolungati, specie nei riguardi di un numero elevato di soggetti; ritiene poi violato il principio di finalità, essendo le reti P2p finalizzate allo scambio tra utenti di dati e *file* per scopi personali. Il predetto utilizzo dei dati dell'utente può avvenire, dunque, soltanto per queste finalità e non per scopi ulteriori quali quelli perseguiti dalle società Peppermint e Techland (cioè il monitoraggio e la ricerca di dati per la richiesta di un risarcimento del danno).

Infine, non sono stati rispettati i princìpi di trasparenza e correttezza in quanto i dati sono stati raccolti ad insaputa sia degli interessati, sia di abbonati che non erano necessariamente coinvolti nello scambio di *file*.

Nel *provvedimento* si è stabilito quindi che entro il 31 marzo 2008 le società che

hanno effettuato il monitoraggio dovevano cancellare i dati personali degli utenti che hanno scambiato *file* musicali e giochi attraverso il sistema P2p.

1.1.4. *Misure in materia di propaganda elettorale*

In vista dell'avvio della campagna elettorale, con deliberazione del 28 febbraio 2008 (in *G.U.* n. 58 dell'8 marzo 2008 [doc. *web* n. 1493909]), l'Autorità ha consentito a partiti e candidati di non adempiere temporaneamente all'obbligo di informativa fino al 31 luglio 2008, rispetto ai dati raccolti da registri ed elenchi pubblici, in caso di invio di materiale propagandistico di dimensioni ridotte (*cd.* "santini").

La deliberazione richiama le modalità –fissate da uno specifico *provvedimento* generale del 7 settembre 2005 (in *G.U.* 12 settembre 2005, n. 212 [doc. *web* n. 1165613])– in base alle quali chi effettua propaganda elettorale può utilizzare correttamente i dati personali dei cittadini (*ad es.*, indirizzo, telefono, *e-mail ecc.*).

Per contattare gli elettori e inviare materiale di propaganda, partiti, organismi politici, comitati promotori, sostenitori e singoli candidati possono usare, senza il consenso dei cittadini, i dati contenuti nelle liste elettorali detenute dai comuni. Possono essere usati anche altri elenchi e registri in materia di elettorato passivo ed attivo (*ad es.*, elenco degli elettori italiani residenti all'estero) nonché altre fonti documentali detenute da soggetti pubblici se liberamente accessibili a chiunque e secondo le modalità eventualmente stabilite per accedere ad esse. Partiti e candidati possono inoltre usare lecitamente i dati personali di iscritti ed aderenti.

Per i titolari di cariche elettive vi è la possibilità di utilizzare dati raccolti nel quadro delle relazioni interpersonali con cittadini ed elettori.

Per particolari modalità di comunicazione elettronica come *Sms*, *e-mail*, *Mms*, telefonate preregistrate e *fax*, è necessario il consenso dell'interessato, che deve precedere la chiamata o il messaggio. Il consenso deve essere parimenti ottenuto nel caso si utilizzino dati raccolti automaticamente su Internet o ricavati da *forum* o *newsgroup*, liste abbonati a un *provider* o dati presenti sul *web* per altre finalità.

Possono essere presi in considerazione anche i dati degli abbonati presenti nei nuovi elenchi telefonici accanto ai quali figurino i due simboli che attestano la disponibilità a ricevere posta o telefonate. Sono ugualmente utilizzabili, se si è ottenuto preventivamente il consenso degli interessati, i dati relativi a simpatizzanti o ad altre persone già contattate per singole iniziative o che vi hanno partecipato (*ad es. referendum*, proposte di legge, raccolte di firme).

Non sono invece in alcun modo utilizzabili, neanche da titolari di cariche elettive, gli archivi dello stato civile, l'anagrafe dei residenti, gli indirizzi raccolti per svolgere attività e compiti istituzionali o per prestazioni di servizi, anche di cura, le liste elettorali di sezione già utilizzate nei seggi, nonché i dati annotati privatamente nei seggi da scrutatori e rappresentanti di lista, durante operazioni elettorali.

Un *provvedimento* di analogo contenuto era stato adottato il 3 maggio 2007 (in *G.U.* n. 130 del 7 giugno 2007 [doc. *web* n. 1409206]) in vista delle elezioni amministrative.

1.1.5. *Trattamento di dati personali di lavoratori per la gestione del rapporto di lavoro in ambito pubblico*

Sono state individuate in un quadro unitario le misure e gli accorgimenti da adottare per garantire la riservatezza dei dati personali dei dipendenti pubblici senza venire meno al principio di trasparenza della pubblica amministrazione. Le linee-guida del 14 giugno 2007 (in *G.U.* 13 luglio 2007, n. 161 [doc. *web* n. 1417809]), che seguono quelle adottate per i lavoratori privati (in *G.U.* 7 dicembre 2006, n. 285 [doc. *web* n. 1364099]), oltre a fornire orientamenti utili per cittadini e amministra-

zioni pubbliche rispondono anche a numerose segnalazioni e quesiti rivolti Garante. Questi, in sintesi, alcuni dei punti principali del *provvedimento*.

Assenze per malattia, certificati e visite mediche

In caso di assenza per malattia, all'amministrazione vanno consegnati certificati medici privi di diagnosi e con la sola indicazione dell'inizio e della durata dell'infermità. Se il lavoratore produce documentazione in cui è presente anche la diagnosi, l'ufficio deve astenersi dall'utilizzare queste informazioni e deve invitare il personale a non produrre altri certificati aventi le stesse caratteristiche. Particolari cautele devono essere adottate dall'ente pubblico quando tratta dati sulla salute dei dipendenti nei casi di visite medico legali, denunce di infortunio all'Inail, abilitazioni al porto d'armi e alla guida.

Diffusione dei dati in Internet

Nell'utilizzare Internet come strumento di diffusione di dati personali (*ad es.*, per graduatorie e giudizi di valutazione), occorre prevedere forme adeguate di selezione delle informazioni che potrebbero essere altrimenti reperite indiscriminatamente mediante un comune motore di ricerca esterno ai siti. Nelle graduatorie relative a concorsi o selezioni vanno riportati solo dati effettivamente pertinenti (si pensi ad elenchi nominativi abbinati ai risultati, agli elenchi di ammessi alle prove scritte o orali, ai recapiti telefonici, al codice fiscale, *ecc.*). É sempre vietata la diffusione di informazioni sulla salute del lavoratore o dei familiari interessati.

Dati biometrici dei lavoratori pubblici

Anche nell'ambito del pubblico impiego non è consentito un uso generalizzato dei dati biometrici dei dipendenti (in particolare impronte digitali, iride) per controllare le presenze o gli accessi sul luogo di lavoro. Il Garante può autorizzare l'attivazione di tali sistemi di rilevazione solo in presenza di particolari esigenze (*ad es.*, per l'accesso ad aree adibite alla sicurezza dello Stato o alla conservazione di oggetti di particolare valore) e con precise garanzie (verifica preliminare dell'Autorità, impiego di codice cifrato dell'impronta memorizzato nel solo *badge* del dipendente e non in archivi centralizzati).

Comunicazioni tra amministrazione e lavoratore

Per prevenire la conoscenza ingiustificata di dati da parte di persone non autorizzate, l'amministrazione deve adottare forme di comunicazione con il dipendente protette e individualizzate, inoltrando, ad esempio note in busta chiusa o inviandole a una *e-mail* personale o invitando l'interessato a ritirare personalmente la documentazione.

1.1.6. *Trattamento di dati personali della clientela in ambito bancario*

Con *provvedimento* generale del 25 ottobre 2007 (in *G.U.* n. 273 del 23 novembre 2007 [doc. *web* n. 1457247]), sono state adottate, anche alla luce delle segnalazioni e dei reclami pervenuti all'Autorità, le linee-guida sul "trattamento dei dati personali della clientela in ambito bancario", con le quali sono state individuate alcune garanzie per il corretto uso dei dati personali dei clienti da parte degli istituti bancari e degli operatori postali. Il Garante ha evidenziato, in particolare, che le comunicazioni di informazioni bancarie a terzi devono essere effettuate solo nei casi espressamente previsti dalla legge, dal Codice o quando sia l'interessato stesso ad autorizzare terzi (familiari, coniuge, professionisti legati da una rapporto di lavoro) ad operare per suo conto o a conoscere il tipo di rapporto intrattenuto con la banca. Le banche possono registrare le telefonate effettuate dalla clientela per dare particolari ordini e istruzioni o nei servizi di *"telephone banking"*, ma devono informare gli interessati. È inoltre necessario adottate misure di sicurezza contro l'alterazione o l'uso indebito del contenuto delle conversazioni. Occorre poi evitare indebite comunicazioni di dati a terzi: il personale deve pertanto astenersi dall'effettuare telefonate e colloqui con la clientela ad alta voce e in presenza di terzi e occorre predisporre distanze di cortesia agli sportelli. Le informazioni dei clienti trattate dalle banche devono essere sempre esatte e aggiornate e il cliente ha diritto ad ottenere la comunicazione in forma intelligibile dei

dati che lo riguardano (comprese le operazioni effettuate, le registrazioni telefoniche e gli ordini di investimento), ma non di quelli riferiti ad altre persone (se presenti, nella copia dei documenti da consegnare al cliente devono essere quindi oscurati). Nel caso infine che i titolari del trattamento siano cessionari di sportelli bancari essi possono effettuare l'informativa mediante pubblicazione della stessa nella Gazzetta ufficiale e una successiva comunicazione agli interessati alla prima occasione utile.

1.1.7. *Trattamento di dati personali in ambito assicurativo*

Con *provvedimento* del 26 aprile 2007 [doc. *web* n. 1410057] sono state individuate modalità più snelle per l'adempimento dell'obbligo dell'informativa da parte di imprese di assicurazione, con specifico riferimento alla pluralità di soggetti (persone fisiche e giuridiche, operanti in Italia e all'estero) che possono venire a conoscenza delle informazioni relative a una specifica posizione assicurativa (*cd.* "catena assicurativa"). In sostanza, il Garante (tenendo in considerazione la previsione contenuta nell'art. 13 della direttiva 95/46/Ce oltre alle indicazioni formulate dalla Raccomandazione del Consiglio d'Europa Rec (2002)9, del 18 settembre 2002), ha autorizzato le imprese di assicurazione stipulanti a rendere l'informativa alla clientela *una tantum*, in sede di conclusione del contratto di assicurazione, anche nell'interesse dei diversi soggetti che, in qualità di autonomi titolari del trattamento, utilizzano dati personali relativi al medesimo rischio assicurato.

Come chiarito in passato (*cfr. Provv.* 28 maggio 1997 [doc. *web* n. 40425]), l'informativa deve riferirsi a tutte le operazioni necessarie a dare corretta esecuzione al rapporto contrattuale, nonché agli altri trattamenti che (talora anche in base a esplicite previsioni di legge) possono essere effettuati lecitamente; deve poi illustrare i flussi comunicativi e indicare con precisione le finalità in concreto perseguite dall'impresa di assicurazione, nonché i soggetti o le tipologie di soggetti ai quali i dati possono essere comunicati (in qualità di autonomi titolari del trattamento) o che possono venirne a conoscenza quali "responsabili del trattamento".

Con il *provvedimento* sono state fornite, altresì, precisazioni in ordine alla formulazione che la modulistica in uso presso il settore assicurativo deve contenere nelle ipotesi in cui sia necessario il consenso dell'interessato. Salvo, infatti, il caso in cui il consenso non è richiesto (ovvero quando i dati sono necessari per instaurare o per dare esecuzione a un contratto di assicurazione, oppure sono trattati sulla base di uno dei presupposti di cui all'art. 24 del Codice), nei casi in cui il consenso dell'interessato è invece necessario (ad esempio, per il trattamento dei dati sensibili per i quali occorre comunque un consenso manifestato in forma scritta), l'impresa assicuratrice stipulante può circoscrivere la formula di consenso ai soli trattamenti da essa effettuati, oppure formularla in modo da ricomprendere, nei limiti del medesimo rischio assicurato, anche gli specifici trattamenti ulteriori effettuati da altri titolari appartenenti alla *cd.* "catena assicurativa".

Da ultimo, in considerazione del particolare ruolo svolto dai riassicuratori -che non instaurano un rapporto contrattuale con i soggetti coinvolti nel contratto di assicurazione- il Garante ha stabilito che l'eventuale comunicazione di dati (ad eccezione dei dati di natura sensibile) da parte della compagnia assicuratrice al riassicuratore rientra nell'ambito di applicazione dell'istituto del bilanciamento degli interessi tenuto conto del legittimo interesse dei titolari del trattamento coinvolti, e non richiede pertanto il consenso dell'interessato (art. 24, comma 1, lett. *g*), del Codice).

1.1.8. *Guida pratica e misure di semplificazione per le piccole e medie imprese*

Per facilitare le piccole e medie imprese nell'assolvimento degli obblighi che la normativa sulla *privacy* impone a chi raccoglie, utilizza e conserva dati personali è

stata anzitutto messa a punto una "Guida pratica e misure di semplificazione per le piccole e medie imprese" (in *G.U.* 21 giugno 2007, n. 142 [doc. *web* n. 1412271]), integrata da un questionario volto ad agevolare gli imprenditori nella più rapida verifica degli adempimenti previsti dal Codice. La guida chiarisce, in relazione alle circostanze concrete, chi può essere individuato quale titolare o responsabile del trattamento; in quali casi il trattamento deve essere notificato; quando occorre fornire l'informativa e quando è necessario acquisire il consenso dell'interessato; le misure da adottare per la sicurezza dei dati, i requisiti per il trasferimento dei dati in Paesi extracomunitari e i doveri del titolare del trattamento in caso di esercizio dei diritti da parte degli interessati ai sensi dell'art. 7 del Codice. La guida intende quindi rispondere all'esigenza, evidenziata dalle associazioni di categoria, di facilitare l'adempimento degli obblighi contenuti nella disciplina di protezione dei dati personali talvolta ritenuti onerosi per l'ordinaria attività di impresa. L'illustrazione di tali adempimenti mira peraltro a evidenziare come una corretta protezione dei dati personali possa rendere più efficiente l'attività d'impresa e incrementare la fiducia di consumatori e utenti.

1.1.9. *Bollette telefoniche: anche le ultime tre cifre possono essere "in chiaro"*

Con *provvedimento* del 13 marzo 2008 (in *G.U.* n. 79 del 3 aprile 2008, [doc. *web* n. 1501106]), le compagnie telefoniche sono state autorizzate ad emettere fatture dettagliate senza il mascheramento delle ultime tre cifre dei numeri chiamati. Gli abbonati che intendono continuare a ricevere bollette con la fatturazione dettagliata, ma con le ultime tre cifre oscurate, dovranno richiederlo espressamente al proprio gestore.

L'*autorizzazione generale* del Garante è stata rilasciata al termine di un'istruttoria preliminare avviata nel 2007, volta a verificare le modalità con le quali i gestori consentono agli utenti di effettuare chiamate addebitandone il costo non in fattura, ma attraverso carte di pagamento, anche prepagate.

La decisione tiene conto delle esigenze, manifestate più volte in questi anni da diversi abbonati, di poter verificare più agevolmente l'esattezza degli addebiti e le chiamate effettuate. L'abbonato, infatti, poteva conoscere i numeri totalmente in chiaro solo per contestare addebiti determinati o riferiti a periodi limitati.

A partire dal 1° luglio 2008, i gestori di telefonia fissa e mobile possono indicare nella fatturazione dettagliata i numeri completi delle comunicazioni. I gestori telefonici potranno esercitare tale facoltà a condizione che, come richiesto dal Garante, tutti gli abbonati vengano preventivamente portati a conoscenza di questa possibilità, mediante un'apposita informativa da inserire all'interno di almeno due fatture e nel sito *web* del fornitore.

L'informativa dovrà citare la decisione del fornitore di avvalersi dell'autorizzazione del Garante e specificare che tutti gli abbonati, che abbiano fatto o faranno richiesta di fatturazione dettagliata, la riceveranno "in chiaro", salvo che intendano mantenere il mascheramento delle ultime tre cifre.

Il Garante ha prescritto inoltre che nell'informativa i gestori invitino tutti gli abbonati che vorranno ricevere la fatturazione dettagliata in chiaro a informare quanti utilizzano la stessa utenza che la fatturazione perverrà completa di tutti i numeri chiamati.

1.1.10. *Pubblicazione e diffusione di atti e documenti di enti locali*

Con il *provvedimento* del 19 aprile 2007 ("Linee-guida in materia di trattamento di dati personali per finalità di pubblicazione e diffusione di atti e documenti di enti locali", in *G.U.* n. 120 del 25 maggio 2007 [doc. *web* n. 1407101]), il Garante ha definito princìpi e limiti che gli enti locali sono tenuti a rispettare riguardo al trat-

tamento di dati personali effettuato nelle attività connesse alla pubblicazione e diffusione di atti e documenti. Particolare attenzione è stata prestata alla diffusione di dati personali contenuti in atti e deliberazioni dai quali possono emergere delicate informazioni su condizioni di salute, *handicap* o situazioni di disagio (*ad es.*, di cittadini che concorrono per l'assegnazione di alloggi popolari, assistenza e contributi o per l'ammissione di minori agli asili nido).

Prima di pubblicare gli atti, renderli accessibili a terzi o metterli in rete, l'ente locale deve valutare se le finalità di trasparenza possono essere perseguite senza divulgare dati personali o attraverso modalità che permettano di identificare gli interessati solo se necessario. Negli atti, devono poi comparire solo dati pertinenti e non eccedenti rispetto alle finalità che l'ente intende raggiungere. I dati sensibili e giudiziari possono essere diffusi solo se realmente indispensabili e se l'ente abbia adottato il regolamento previsto dal Codice sull'uso di questi dati. É sempre vietato, comunque, diffondere informazioni sulla salute.

L'impiego delle nuove tecnologie impone all'ente locale sia di assicurare sempre l'esattezza, l'aggiornamento e la pertinenza dei dati pubblicati in rete, sia di garantire il diritto all'oblìo delle persone interessate: ad esempio, trascorso un certo periodo dalla pubblicazione, risulta spesso necessario collocare determinati documenti in una parte del sito dove non sono più rintracciabili direttamente dai motori di ricerca esterni.

Specifiche cautele vanno adottate anche nel pubblicare gli elenchi delle persone che usufruiscono di crediti, sussidi o sovvenzioni: ad esempio, possono essere a volte pubblicati i nominativi dei beneficiari e la data di nascita, ma senza diffondere indirizzi, codici fiscali, coordinate bancarie o particolari della vita privata che possano creare imbarazzo agli interessati.

Le deliberazioni che approvano graduatorie dei vincitori dei pubblici concorsi possono essere pubblicate integralmente anche *on-line*, ma per visionare elaborati, verbali o titoli occorre prevedere accessi selezionati dei partecipanti, ad esempio attraverso una chiave personale (*username* e *password*, numero di protocollo o altri estremi identificativi).

1.1.11. *Maggiori garanzie a tutela degli invalidi civili*

Il Garante ha ricevuto alcune segnalazioni da parte di invalidi civili che lamentavano una violazione delle disposizioni in materia di protezione dei dati personali determinata dall'indicazione dei dati relativi alla diagnosi nelle istanze volte all'accertamento sanitario dell'invalidità civile e in alcuni tipi di certificazioni che attestano il riconoscimento della invalidità civile per finalità amministrative. Con *provvedimento* del 21 marzo 2007 (*G.U.* n. 82 del 7 aprile 2007 [doc. *web* n. 1395821]), l'Autorità ha pertanto indicato alcune misure per garantire un elevato livello di tutela della riservatezza anche in questo settore. Considerata la particolare natura delle informazioni richieste agli interessati, il Garante ha richiamato l'attenzione sull'obbligo degli uffici competenti alla ricezione delle istanze di adottare accorgimenti necessari a garantire un livello elevato di tutela dei diritti degli interessati, quali distanze di cortesia, spazi per colloqui riservati, consegna della documentazione in busta chiusa e obbligo di impartire precise istruzioni al personale sanitario (*v.* anche *Provv.* del 9 novembre 2005, sul rispetto della dignità delle persone nelle strutture sanitarie [doc. *web* n. 1191411]).

Le aziende sanitarie locali, inoltre, non devono indicare la diagnosi sui certificati che attestano il riconoscimento dell'invalidità civile per l'iscrizione alle liste del collocamento obbligatorie o per la richiesta di esenzione dalle tasse scolastiche o universitarie, specie nei casi in cui si riscontri lo stato di sieropositività o l'infezione da Hiv.

Riportare le patologie nei verbali delle commissioni mediche che accertano tipo e grado di invalidità è prescritto dalla normativa anche in vista di eventuali revisioni o ricorsi. Non è invece giustificato indicare gli stessi dati nelle certificazioni per l'iscrizione al collocamento o per ottenere un'esenzione dalle tasse scolastiche, sia perché non indispensabili, sia in ragione del quadro normativo di riferimento. Vi sono infatti alcune norme che prevedono tutele rafforzate per specifiche patologie (*ad es.*, la l. n. 135/1990, che limita la comunicazione dei risultati di accertamenti per l'infezione da Hiv alla sola persona che si è sottoposta agli esami). Inoltre, per avere diritto ad alcuni benefici o all'iscrizione a categorie protette, la normativa di settore prescrive spesso specifici requisiti quali l'appartenenza a una famiglia in disagiate condizioni economiche, o l'aver subito una riduzione della capacità lavorativa *ecc.*, tra i quali non risulta la patologia sofferta. Anche ai fini del collocamento, infine, è prevista solo una valutazione delle funzionalità della persona disabile, per individuarne le capacità lavorative.

Sulla base di tali presupposti normativi il Garante ha pertanto ritenuto necessario prescrivere alle aziende sanitarie locali, al fine di rendere il trattamento conforme alle norme in materia di protezione dei dati, di rilasciare le certificazioni che attestano il riconoscimento dell'invalidità civile per finalità connesse all'iscrizione alle liste del collocamento obbligatorio o alla richiesta di esenzione dalle tasse scolastiche e universitarie, senza indicare i dati personali relativi alla diagnosi.

1.1.12. *Accesso dei medici a zone a traffico limitato*

A seguito di alcune segnalazioni, il Garante si è pronunciato in merito alla legittimità della richiesta, rivolta da alcune amministrazioni comunali ai medici privi di un permesso per l'accesso ad una Ztl, di comunicare dati personali relativi alle persone visitate a domicilio in tali aree. In particolare, con il *provvedimento* del 14 giugno 2007 (in *G.U.* n. 161 del 13 luglio 2007 [doc. *web* n. 1424100], l'Autorità, ritenendo che il dovere degli organi comunali di applicare sanzioni in caso di accertata violazione delle norme di accesso e circolazione dei veicoli non debba tradursi in una indebita violazione della riservatezza dei pazienti, ha ritenuto sproporzionate e non indispensabili le richieste rivolte ai medici. L'accertamento delle violazioni per l'accesso alla Ztl, può essere perseguito infatti attraverso altre modalità, parimenti efficaci, ma rispettose del diritto alla protezione dei dati personali, quali, ad esempio, la comunicazione dell'indirizzo e del numero civico presso il quale è stato prestato intervento, la targa del veicolo del medico che ha effettuato la visita o il numero di iscrizione all'ordine professionale. Il Garante ha pertanto prescritto ai comuni di astenersi dal richiedere ai medici le generalità e altre informazioni che identificano le persone visitate a domicilio all'interno di aree Ztl. L'Autorità ha inoltre prescritto ai medici, in caso di ricorso avverso la contestazione amministrativa, di non presentare documenti contenenti le generalità e altre informazioni che identificano i pazienti visitati a domicilio, documenti che gli uffici territoriali di governo devono, pertanto, astenersi dal richiedere.

1.1.13. *Servizi telefonici. Adempimenti semplificati per i* customer care

Con il *provvedimento* del 15 novembre 2007 (in G. U. n. 285 del 7 dicembre 2007 [doc. *web* n. 1462788]), sono state prescritte misure per semplificare l'informativa fornita dalle società che (anche attraverso canali completamente automatizzati) si occupano di *customer care*, assistenza *post* vendita, prenotazioni di servizi, *phone banking* in modalità *"inbound"*, ossia a seguito di una chiamata dell'utente. È stato in primo luogo stabilito che non è necessario fornire l'informativa quando siano trattati i soli dati necessari ad assicurare il servizio richiesto, o il cliente sia già

stato informato precedentemente, *ad es.*, al momento della sottoscrizione di un contratto, o alcuni elementi dell'informativa emergano nel corso del colloquio telefonico. Per utilizzare i dati anche ad altri fini (*ad es.*, di *marketing* o profilazione) è necessario informare l'utente e ottenere un suo consenso specifico.

L'Autorità ha ricordato che, ove necessaria, l'informativa deve essere fornita con formule sintetiche, chiare e di immediata comprensione, ed ha autorizzato coloro che prestano i servizi in esame a indicare la modalità attraverso la quale l'interessato può consultare o ascoltare a richiesta un'informativa più specifica, ad esempio mediante un sito *web* o tramite operatore o messaggio registrato ascoltabile digitando una cifra sulla tastiera del telefono.

Nel *provvedimento*, adottato anche tenendo conto delle richieste di chiarimento provenienti da una associazione di categoria, l'Autorità ha inoltre invitato le società del settore ad assicurare elevati livelli di professionalità nel trattamento dei dati ponendo specifica attenzione anche al profilo della loro sicurezza.

In particolare, è stata sottolineata l'importanza di adottare adeguate cautele quando un medesimo *call center* si trovi a gestire contemporaneamente vari *database*, con tipologie diverse di informazioni, per una pluralità di committenti. Per tale motivo, prima della stipula del contratto che affida in *outsourcing* il servizio, deve essere effettuata un'attenta analisi delle implicazioni che il trattamento dei dati può comportare.

1.1.14. *Utilizzazione dei dati della clientela del mercato di energia e gas*

Con *deliberazione* del 25 luglio 2007 (in *G.U.* del 20 agosto 2007 [doc. *web* n. 1428567]), adottata al termine di una procedura di cooperazione con l'Autorità per l'energia elettrica e il gas, il Garante ha fornito una serie di indicazioni, nell'ambito della fornitura di energia elettrica e gas, per la informazione dei clienti e il corretto utilizzo dei dati che li riguardano.

La recente disciplina sulla liberalizzazione dell'energia prevede che, a partire dal 1° luglio 2007, i clienti domestici possano recedere dal contratto di fornitura di energia stipulato prima di tale data con il distributore operante nel proprio ambito territoriale e scegliere un fornitore diverso. Le società che vendono energia devono poter acquisire dalle banche dati dei distributori alcune informazioni di base relative agli utenti del mercato energetico, in modo da formulare proposte commerciali.

In base a tale *deliberazione* le società distributrici sono tenute a informare i clienti in maniera colloquiale e sintetica riguardo alla facoltà di recedere dal contratto e alla possibilità che alle aziende venditrici di energia siano forniti alcuni dati (generalità, consumi, potenza impegnata *ecc.*) al fine di far conoscere le loro migliori offerte sulla base di un profilo "minimo" del cliente medesimo. A tale proposito il Garante ha predisposto in allegato alla *deliberazione* un modello di informativa.

L'informativa deve essere recapitata insieme alla corrispondenza ordinaria riguardante la gestione del vigente contratto di fornitura o di distribuzione (*ad es.*, l'invio della bolletta), nonché resa disponibile anche sul sito Internet e attraverso i servizi di assistenza e informazione al pubblico.

Le proposte commerciali dei venditori devono essere rigorosamente cartacee: non è quindi consentito il *marketing* telefonico o per via telematica. I dati dei clienti non possono essere comunicati a terzi.

I dati personali dei clienti che non rispondono alle offerte commerciali devono essere cancellati non più tardi di sei mesi dall'invio della proposta.

1.1.15. *Schema preliminare del codice di deontologia e di buona condotta per il trattamento dei dati personali effettuato per svolgere investigazioni difensive o per far valere o difendere un diritto in sede giudiziaria*

I lavori di redazione del codice di deontologia e di buona condotta per il trattamento dei dati personali effettuato per svolgere investigazioni difensive o per far valere o difendere un diritto in sede giudiziaria (art. 135 del Codice) si sono susseguiti con notevole intensità nel corso del 2007, specie nell'ambito di riunioni promosse dall'Autorità con i soggetti interessati.

Gli incontri, caratterizzati da elevato spirito di collaborazione, hanno reso possibile la definizione, negli ultimi mesi dell'anno, di uno schema preliminare di codice, sottoposto dalle medesime categorie interessate all'esame del Garante per le valutazioni di cui all'art. 6 del regolamento del Garante n. 2/2006.

Lo schema (che, sulla base di una prima verifica, il 20 marzo 2008 è stato ritenuto dall'Autorità conforme alla normativa vigente), è rimasto accessibile anche tramite il sito *web* del Garante [doc. *web* n. 1503511], al fine di consentire entro il 30 aprile 2008 (avviso in *G.U.* n. 83 dell'8 aprile 2008) la raccolta di eventuali osservazioni da parte dei "soggetti interessati" prima della sua formale sottoscrizione (art. 12 del Codice; artt. 5 e 6 del regolamento del Garante n. 2/2006).

Le principali novità introdotte nello schema del codice riguardano l'ambito di applicazione, i tempi di conservazione delle informazioni, i rapporti con i terzi e con la stampa e le modalità di trattamento dei dati personali per le finalità di difesa di un diritto in sede giudiziaria. Riguardo a quest'ultimo aspetto lo schema di codice sollecita i soggetti coinvolti a prestare specifica attenzione all'adozione di idonee cautele per prevenire l'ingiustificata raccolta, utilizzazione o conoscenza di dati con riferimento allo scambio di corrispondenza, specie per via telematica, all'esercizio contiguo di attività autonome all'interno di uno studio, all'utilizzo di particolari dispositivi o supporti, specialmente se elettronici, come le registrazioni audio/video o i tabulati di flussi telefonici o informatici, e all'acquisizione informale di notizie, dati e documenti connotati da un alto grado di confidenzialità o che possano comportare, comunque, rischi specifici per gli interessati.

1.2. *Rapporti con il Parlamento e altre istituzioni*

1.2.1. *Le audizioni del Garante in Parlamento*

Anche nel 2007 il Garante ha partecipato ad alcune audizioni presso commissioni della Camera e del Senato o altri organismi anche bicamerali su temi d'interesse all'esame del Parlamento, nell'ambito di indagini conoscitive o nel corso dei lavori per l'approvazione di proposte di legge aventi riflessi in materia di protezione dei dati personali.

In questo quadro si collocano, in particolare:

- il 28 novembre 2007, presso la Commissione politiche dell'Unione europea della Camera, un'audizione nell'ambito dei lavori per l'approvazione di due disegni di legge di ratifica di accordi internazionali concernenti il funzionamento del sistema satellitare Galileo, nel corso della quale sono state esaminate le implicazioni che il sistema presenta in relazione alla tutela dei dati personali, con specifico riferimento al contesto comunitario (*v.* anche *par.* 2.2.);
- il 17 luglio 2007, presso la Commissione di vigilanza sull'anagrafe tributaria, un'audizione nell'ambito dell'indagine conoscitiva sulle modalità di gestione e utilizzo dei dati dell'anagrafe tributaria;
- il 16 maggio 2007, presso il Comitato parlamentare di controllo sull'attua-

zione dell'Accordo di Schengen, un'audizione nell'ambito dell'indagine conoscitiva in materia di immigrazione che ha riguardato le problematiche connesse all'applicazione del Trattato di Prüm, con specifico riferimento alla raccolta e conservazione di dati relativi al Dna delle persone ed alle implicazioni sulla protezione dei dati personali;

- il 2 maggio 2007, presso la Commissione affari costituzionali del Senato, un'audizione nell'ambito dell'indagine conoscitiva sui rapporti fra libertà di informazione, sviluppo delle comunicazioni, tutela dei diritti della persona e sicurezza pubblica (una prima audizione del Garante si era tenuta nel novembre-dicembre 2006);
- il 13 marzo 2007, presso le Commissioni cultura e comunicazioni della Camera riunite, un'audizione nell'ambito della discussione del disegno di legge presentato dal Governo per la disciplina del settore televisivo nella fase di transizione al digitale;
- il 6 marzo 2007, innanzi all'ufficio di presidenza della Commissione finanze e tesoro del Senato, un'audizione (informale) nell'ambito della discussione di un disegno di legge relativo all'istituzione di un sistema di prevenzione delle frodi nel settore del credito al consumo;
- il 23 gennaio 2007, presso la Commissione igiene e sanità del Senato, un'audizione (informale) che ha avuto ad oggetto i disegni di legge in materia di "testamento biologico". L'intervento del Garante ha riguardato, in particolare, l'esame delle problematiche che emergono con riguardo alla protezione dei dati personali, come, ad esempio, le modalità di raccolta e di conservazione delle *cd.* "dichiarazioni anticipate di volontà", i soggetti legittimati a trattare i dati e il consenso informato dei pazienti;
- il 16 gennaio 2007, presso il Comitato parlamentare di controllo sull'attuazione dell'Accordo di Schengen, un'audizione che ha avuto per oggetto, in particolare, l'esame delle questioni attinenti alla evoluzione del sistema informativo Schengen (*cd.* "Sis-II") e allo scambio crescente di informazioni e di dati tra le forze di polizia. L'audizione ha riguardato anche il Trattato di Prüm, nonché lo sviluppo della cooperazione dell'Unione europea con gli Stati Uniti, in merito alle problematiche del *cd.* "Pnr" (*Passenger name record*) e del caso Swift e i connessi riflessi sui diritti fondamentali dei cittadini.

1.2.2. *L'Autorità e le attività di sindacato ispettivo del Parlamento*

Anche nel 2007 l'Autorità ha fornito propri contributi conoscitivi in riferimento ad atti di sindacato ispettivo e ad attività di indirizzo del Parlamento riguardanti profili attinenti alla protezione dei dati personali.

Sono stati forniti al Governo elementi di valutazione in relazione ad atti di sindacato ispettivo fra i quali si ricordano, in particolare:

- un'interrogazione a risposta immediata presentata in Commissione giustizia della Camera dall'on. Balducci, relativa al caso "Peppermint" (*Nota* 13 giugno 2007). L'Autorità ha precisato che il Garante si è costituito in giudizio presso il Tribunale di Roma nelle controversie instaurate dalle società Peppermint Jam Records GmbH, tedesca, e *T*echland sp. z.o.o., polacca, nei riguardi di alcuni fornitori di servizi di comunicazione elettronica, al fine di verificare se nella vicenda siano state rispettate le garanzie previste per i cittadini dalla normativa in materia di protezione dei dati personali. L'Autorità ha precisato di aver avviato un distinto procedimento amministrativo di controllo per verificare autonomamente la liceità e la correttezza dei trattamenti di dati personali effettuati dalle predette società, e di aver rivolto una richie-

sta di collaborazione alle Autorità per la protezione dei dati personali nei Paesi interessati, in particolare per quanto riguarda altre eventuali informazioni utili o per agevolare, se necessario, un'idonea risposta alle richieste istruttorie rivolte alle società (sugli sviluppi del caso in questione *v. par.* 20.5);

- un'interrogazione a risposta scritta presentata dall'on. Urso, relativa all'invio massiccio e indiscriminato di *e-mail* pubblicitarie non richieste (*spamming*) che interessa singoli utenti della rete Internet e piccole e medie imprese costrette a sopportarne i costi (*Nota* 23 febbraio 2007). Al riguardo, l'Autorità ha ricordato che dopo una serie di interventi mirati che hanno portato a sospendere l'attività illecita di alcune aziende e persone fisiche e a denunciarne talune all'autorità giudiziaria, nel 2003 il Garante ha adottato un *provvedimento* generale (*Provv.* 29 maggio 2003 [doc. *web* n. 29840]) con il quale, sulla base della normativa all'epoca vigente (l. n. 675/1996 e d.lg. n. 171/1998) ha precisato vari aspetti legati all'invio di *e-mail* promozionali o pubblicitarie, anche alla luce della direttiva europea 2002/58/Ce poi recepita con il Codice in materia di protezione dei dati personali. I princìpi organicamente riassunti dal Garante nel *provvedimento* sono stati "confermati" e implementati dal Codice mediante specifiche garanzie a tutela dell'interessato previste, in particolare, nell'articolo 130. L'Autorità ha infine informato che continuano a pervenire al Garante numerosi reclami e segnalazioni con i quali sono lamentate ripetute violazioni del diritto al corretto e lecito utilizzo dei dati personali nell'invio dei messaggi promozionali e che particolare preoccupazione desta, poi, l'incremento delle segnalazioni che lamentano l'invio di *e-mail* riconducibili al fenomeno denominato *"phishing"*, volto ad acquisire fraudolentemente informazioni personali del destinatario dell'*e-mail*. Il Garante, anche in relazione a tale specifico fenomeno, ha, perciò, intensificato le attività di controllo e verifica dell'attività svolte da diversi operatori che, direttamente o per mezzo di soggetti specializzati, svolgono campagne pubblicitarie e di *direct marketing* utilizzando lo strumento della posta elettronica.

1.2.3. *L'attività consultiva del Garante sugli atti del Governo*

Nel quadro dell'attività consultiva prevista dal Codice in relazione a norme regolamentari e ad atti amministrativi suscettibili di incidere sulla protezione dei dati personali (art. 154, comma 4, del Codice), il Garante ha espresso anche nel 2007 diversi pareri i quali hanno riguardato, in particolare:

- uno schema di provvedimento dell'Agenzia delle entrate in materia di comunicazione in via telematica alla predetta agenzia dei dati acquisiti nell'attività di gestione del servizio di smaltimento dei rifiuti (art. 1, commi 106, 107 e 108 della l. 27 dicembre 2006, n. 296) (*Parere* 6 dicembre 2007 [doc. *web* n. 1470750]);
- uno schema di decreto interministeriale predisposto dal Ministero delle comunicazioni recante recepimento del codice di autoregolamentazione delle trasmissioni di commento degli avvenimenti sportivi denominato "Codice *media* e sport" (*Parere* 11 ottobre 2007 [doc. *web* n. 1449705]);
- uno schema di decreto predisposto dal Ministero dell'interno recante regole tecniche in materia di carta d'identità e documento d'identità elettronici (*Parere* 1° agosto 2007 [doc. *web* n. 1436216]);
- uno schema di decreto predisposto dalla Presidenza del Consiglio dei ministri-Dipartimento delle politiche per la famiglia, sul coordinamento delle attività delle pubbliche amministrazioni per la tutela dei minori dallo sfrutta-

mento e dall'abuso sessuale (*Parere* 25 luglio 2007 [doc. *web* n. 1436237]);
- uno schema di decreto predisposto dal Ministero dell'economia e delle finanze in materia di pagamenti da parte delle pubbliche amministrazioni (*Parere* 25 luglio 2007 [doc. *web* n. 1434395]);
- uno schema di decreto predisposto dal Ministero della giustizia in materia di rilascio di certificati del casellario giudiziale (*Parere* 25 luglio 2007 [doc. *web* n. 1431017]);
- uno schema di provvedimento dell'Agenzia delle entrate in materia di individuazione degli elementi informativi e di definizione delle modalità tecniche e dei termini relativi alla trasmissione di determinati elenchi (art. 37, commi 8 e 9, d.l. 4 luglio 2006, n. 223, convertito dalla l. 4 agosto 2006, n. 248) (*Parere* 26 aprile 2007 [doc. *web* n. 1402616]);
- uno schema di provvedimento dell'Agenzia delle entrate in materia di modalità e termini per la comunicazione dei corrispettivi giornalieri (art. 37, comma 34, d.l. n. 223/2006) (*Parere* 12 aprile [2007 doc. *web* n. 1402655]);
- uno schema di regolamento recante norme in materia di composizione e compiti della Commissione per le adozioni internazionali (*Parere* 12 aprile 2007 [doc. *web* n. 1401738]);
- uno schema di decreto del Ministero dell'università e della ricerca riguardante le prove di ammissione a corsi di laurea per l'anno accademico 2007-2008 *(Parere* 4 aprile 2007 [doc. *web* n. 1401716]);
- uno schema di decreto predisposto dal Ministero dell'economia e delle finanze in materia di archivi informatici delle tasse automobilistiche (*Parere* 16 marzo 2007 [doc. *web* n. 1397123]);
- uno schema di decreto recante regole procedurali di carattere tecnico operativo per l'attuazione del d.P.R. 14 novembre 2002, n. 313 recante il testo unico in materia di casellario giudiziale (*Parere* 18 gennaio 2007 [doc. *web* n. 1381963]);
- uno schema di decreto riguardante l'istituzione dei registri e delle cartelle sanitarie e di rischio dei lavoratori esposti ad agenti cancerogeni o biologici (*Parere* 11 gennaio 2007 [doc. *web* n. 1388712]);
- due schemi di provvedimenti dell'Agenzia delle entrate in materia di modalità e termini per la comunicazione all'anagrafe tributaria dei dati relativi alle somme di denaro erogate da imprese, intermediari e altri operatori del settore delle assicurazioni, nonché di altre informazioni da parte di operatori finanziari (artt. 35, comma 27, e 37, commi 4 e 5, d.l. n. 223/2006) (*Pareri* 11 gennaio 2007 [doc. *web* nn. 1381575 e 1381941]);
- uno schema di provvedimento recante modalità di trasmissione dei dati relativi ai crediti d'imposta per la ricerca scientifica e tecnologica, di cui all'art. 5 della l. 27 dicembre 1997, n. 449 (*Parere* 25 gennaio 2007 [doc. *web* n. 1381925]).

A fronte dei diversi pareri sopra menzionati, continuano tuttavia a registrarsi casi di mancata consultazione dell'Autorità, fra i quali in particolare:
- decreto del Ministro della salute 21 dicembre 2007 (*G.U.* 16 gennaio 2008, n. 13) recante "Istituzione del sistema informativo dei servizi trasfusionali";
- decreto del Direttore dell'Agenzia del territorio 13 novembre 2007 (*G.U.* 24 novembre 2007, n. 274, S.O. n. 243) recante "Definizione delle regole tecnico-economiche per l'utilizzo dei dati catastali per via telematica da parte dei sistemi informatici di altre amministrazioni, ai sensi dell'articolo 59, comma 7-*bis,* del d.lg. 7 marzo 2005, n. 82";
- decreti del Direttore dell'Agenzia del territorio 6 novembre 2007 (*G.U.* 13

novembre 2007, n. 264) e 4 maggio 2007 (*G.U.* 10 maggio 2007, n. 107) in materia di accesso al sistema telematico dell'Agenzia del territorio per la consultazione delle banche dati ipotecaria e catastale;

- decreto del vice Ministro dell'economia e delle finanze 3 ottobre 2007 (*G.U.* 8 novembre 2007, n. 260) recante "Individuazione dei soggetti esonerati dall'obbligo della tracciabilità dei pagamenti";
- tre decreti del Ministro del lavoro adottati di concerto con il Ministro per le riforme e le innovazioni nella pubblica amministrazione 30 ottobre 2007 (*G.U.* 27 dicembre 2007, n. 299), in materia di comunicazioni telematiche dovute dai datori di lavoro ai servizi competenti, scheda anagrafico-professionale e *standard* tecnici della borsa continua nazionale del lavoro;
- decreto del Presidente della Repubblica 22 giugno 2007, n. 116 (*G.U.* 2 agosto 2007, n. 178) recante "Regolamento di attuazione dell'articolo 1, comma 345, della l. 23 dicembre 2005, n. 266, in materia di depositi dormienti";
- decreto del presidente del Consiglio dei ministri 14 giugno 2007 (*G.U.* 5 luglio 2007, n. 154) e relativo comunicato di rettifica (*G.U.* 9 agosto 2007, n. 184) in materia di "Decentramento delle funzioni catastali ai comuni, ai sensi dell'articolo 1, comma 197, della l. 27 dicembre 2006, n. 296.";
- decreto del Ministro dell'economia e delle finanze 8 giugno 2007 (*G.U.* 18 giugno 2007, n. 139) recante "Criteri e modalità per la concessione di contributi per l'acquisto di *pc* da parte di collaboratori coordinati e continuativi e di collaboratori a progetto, in attuazione dell'articolo 1, comma 298, della legge 27 dicembre 2006, n. 296 (legge finanziaria 2007)";
- decreto 23 maggio 2007 e provvedimento 25 maggio 2007 del Direttore dell'Agenzia del territorio (*G.U.* 29 maggio 2007, n. 123) che, rispettivamente, istituiscono, presso il servizio di pubblicità immobiliare dell'Agenzia, il registro delle comunicazioni in materia di cancellazione di ipoteche e definiscono le relative modalità di trasmissione da parte del creditore, ai sensi dell'articolo 13, comma 8-*septies*, del d.l. 31 gennaio 2007, n. 7, convertito dalla l. 2 aprile 2007, n. 40.

1.2.4. *Altri pareri*

Su espressa richiesta, il Garante ha espresso parere anche su alcuni altri atti normativi del Governo e, in particolare, sui seguenti provvedimenti:

- uno schema di decreto legislativo volto a dare attuazione alla legge 3 agosto 2007, n. 123, in materia di salute e sicurezza nei luoghi di lavoro (*Parere* 31 marzo 2008);
- uno schema di decreto legislativo per l'attuazione della direttiva 2006/24/Ce riguardante la conservazione di dati di traffico trattati nell'ambito della fornitura di servizi di comunicazione elettronica (*Parere* 5 marzo 2008);
- uno schema di decreto legislativo recante norma di attuazione in materia di dichiarazione di appartenenza o aggregazione al gruppo linguistico in provincia di Bolzano (*Parere* 10 gennaio 2008 [doc. *web* n. 1484669]);
- un disegno di legge per l'istituzione di una banca dati contenente profili del Dna delle persone a fini di giustizia, presentato dal Governo anche in attuazione del Trattato di Prüm (*Parere* 15 ottobre 2007 [doc. *web* n. 1448799]);
- uno schema di decreto legislativo per il recepimento della direttiva 2004/82/Ce concernente l'obbligo dei vettori aerei di comunicare i dati relativi alle persone trasportate (*Parere* 13 febbraio 2007 [doc. *web* n. 1388444]).

2 Quadro normativo in materia di protezione dei dati personali

2.1. *Il percorso di "stabilizzazione" delle garanzie previste nel Codice.*

Le *Relazioni* del Garante degli scorsi anni hanno evidenziato il percorso normativo attraverso il quale sono state introdotte nel nostro ordinamento importanti garanzie per i diritti fondamentali della persona rispetto al trattamento dei dati personali che hanno trovato, poi, nel Codice in materia di protezione di dati personali (decreto legislativo 30 giugno 2003, n. 196), il loro pieno consolidamento, in particolare con il riconoscimento del diritto alla protezione dei dati personali.

Nelle *Relazioni* del 2004 e del 2005 si erano, tuttavia, evidenziati alcuni circoscritti interventi modificativi del Codice, in materia di conservazione dei dati di traffico telefonico e telematico e in ambito sanitario, sui quali l'Autorità aveva richiamato l'attenzione per evitare segnali in parziale controtendenza rispetto a quel percorso di "stabilizzazione" delle regole per la protezione dei dati.

Mentre nel 2006 il Codice non aveva subito modifiche significative (salva la reiterazione di proroghe già disposte negli anni precedenti per adottare le misure minime di sicurezza e i regolamenti sul trattamento dei dati sensibili e giudiziari delle pubbliche amministrazioni), sul finire della XV legislatura si è registrato un nuovo intervento integrativo del Codice con riferimento ai dati di traffico telematico, ad opera della legge 18 marzo 2008, n. 48, di ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica.

La predetta Convenzione, come si dirà più diffusamente in altra parte della *Relazione* (*par.* 2.2.), prevede che ciascuno Stato membro introduca misure sostanziali e procedurali in ambito penale per il contrasto dei crimini informatici e per la raccolta di prove elettroniche utili nelle indagini concernenti qualunque reato, anche non informatico.

In tale quadro, la Convenzione reca alcune disposizioni che consentono, anche per finalità di collaborazione internazionale, la conservazione temporanea (per un periodo di tempo non superiore a novanta giorni, ma prorogabile) di specifici dati informatici, inclusi i dati sul traffico, già in possesso dei fornitori di servizi di comunicazione elettronica o comunque sotto il loro controllo (*cd.* "congelamento"), quando la disponibilità dei medesimi dati da parte delle competenti autorità sia necessaria e vi sia motivo di ritenere che i dati stessi, anche in ragione della loro particolare vulnerabilità, possano essere cancellati o modificati (artt. 16 e 17 Conv.).

In Europa, la conservazione dei dati di traffico per finalità di giustizia e, in particolare, per il perseguimento e la repressione di reati gravi, è oggetto della direttiva 2006/24/Ce, in fase di recepimento nei vari Paesi. Inoltre, l'istituto del "congelamento" dei dati trova, di regola, la sua naturale esplicazione in ordinamenti nei quali la conservazione sistematica dei dati di traffico non è consentita o è prevista per periodi di tempo assai ristretti.

La predetta legge n. 48/2008 (art. 10), integrando l'articolo 132 del Codice (nuovi commi 4-*ter*, 4-*quater* e 4-*quinquies*), ha previsto che specifici organi di polizia possano ordinare ai fornitori di servizi di comunicazione elettronica di conservare e proteggere, per un periodo non superiore a novanta giorni (prorogabile non

oltre i sei mesi) dati relativi al traffico telematico, esclusi comunque i contenuti delle comunicazioni, ai fini dello svolgimento di investigazioni preventive o per finalità di accertamento e repressione di specifici reati. I provvedimenti degli organi di polizia sono poi comunicati al pubblico ministero per la convalida.

Tali disposizioni -oltre a presentare possibili profili meritevoli di approfondimento con riferimento all'art. 15 *Cost.*, in base al quale la libertà di ogni forma di comunicazione può essere limitata solo per atto motivato dell'autorità giudiziaria- dovranno essere comunque applicate alla stregua dei princìpi di finalità e di proporzionalità, in una prospettiva di selettività dei provvedimenti e tenendo conto delle garanzie previste dalla predetta direttiva europea sulla conservazione dei dati di traffico.

Ulteriori modifiche del menzionato art. 132 sono state da ultimo previste dal richiamato decreto legislativo di recepimento della *cd.* "Direttiva Frattini".

2.2. *Novità normative con riflessi in materia di protezione dei dati personali*

Nel corso del 2007 sono stati approvati alcuni provvedimenti normativi che hanno riguardato il trattamento dei dati personali e l'attività del Garante.

Criminalità informatica

Vanno ricordati, in particolare:

- la menzionata legge 18 marzo 2008, n. 48, recante ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica. Come ricordato (*v. par.* 2.1.) la Convenzione, aperta alla firma a Budapest il 23 novembre 2001 ed entrata in vigore il 1° luglio 2004, reca misure da adottare a livello nazionale in tema di diritto penale sostanziale e processuale, nonché disposizioni in materia di cooperazione internazionale. In particolare, essa prevede alcune fattispecie di reato che le parti devono introdurre come, ad esempio: l'accesso illegale a un sistema informatico; le intercettazioni illegali di dati informatici; l'attentato all'integrità di dati o di sistemi informatici; la cancellazione, l'alterazione e la soppressione dei dati informatici; l'abuso di dispositivi, compresi i programmi informatici, specialmente concepiti per permettere la commissione dei delitti sopraccitati, nonché di parole chiave o di codici di accesso o di sistemi analoghi che consentano di accedere a un sistema informatico; le falsificazioni informatiche e la frode informatica. La Convenzione prevede, inoltre, misure procedurali che riguardano il perseguimento dei predetti reati, fra le quali: la comunicazione rapida dei dati conservati, compresi quelli relativi al traffico; l'ordine di esibizione; la perquisizione e il sequestro dei dati informatici; la raccolta dei dati di traffico in tempo reale; l'intercettazione del contenuto dei dati; essa prevede infine talune misure giurisdizionali. La Convenzione di Budapest non regola, comunque, solo i *cd.* "reati informatici", ma riguarda, in termini più generali, anche le procedure e le modalità di applicazione di vari atti di indagine penale (ispezioni, perquisizioni, sequestri anche di corrispondenza, custodia, accertamenti urgenti, *ecc.*) per reati non informatici, ovvero "di tipo tradizionale" per i quali ricorra un'esigenza probatoria che presuppone la ricerca di mezzi di prova su o mediante strumenti elettronici (*cfr.* artt. 14 e 19 Conv.).
  La Convenzione prevede inoltre varie forme di collaborazione e di mutua assistenza fra gli Stati firmatari, anche a fini di estradizione, non solo relativamente a reati "collegati a sistemi e dati informatici", ma anche "per raccogliere le prove in forma elettronica" di qualsiasi tipo di reato, informatico e non. Ciò può avvenire in casi numericamente elevati, venendo in considerazione reati puniti con pena non inferiore nel massimo a un anno (artt. 23 e

24 Conv.). In tale ampia prospettiva, le attività di indagine penale svolte nei vari Paesi, anche quando derivano da richieste di cooperazione internazionale disciplinate dalla Convenzione, potranno quindi comportare la raccolta e lo scambio di una notevole quantità di dati personali, riguardanti il traffico telefonico o telematico, anche non connessi direttamente a forme di criminalità informatica o che comunque possono riguardare attività del tutto lecite. L'impatto delle misure è quindi particolarmente significativo sui diritti e sulle libertà degli interessati. Va tenuto conto che, in proposito, si sono avuti, di recente, alcuni esempi significativi di perquisizioni presso redazioni giornalistiche e giornalisti disposte dalla autorità giudiziaria.

Nel corso dei lavori preparatori della Convenzione, il Gruppo dei Garanti europei (in particolare con il *Parere n.* 4/2001, adottato il 22 marzo 2001) ha evidenziato diversi profili critici riguardanti la rispondenza del progetto di convenzione ai princìpi in materia di protezione dei dati personali sanciti nella Convenzione del Consiglio d'Europa n. 108 del 1981 e negli altri strumenti normativi successivamente intervenuti in materia. Il testo definitivo della Convenzione ha recepito solo in parte le obiezioni e i suggerimenti avanzati dai Garanti europei nell'ottica di una maggiore attenzione alle esigenze di protezione dei dati personali. Un punto importante che è stato accolto, in parte, riguarda l'invito dei Garanti a specificare maggiormente i criteri che possono giustificare l'adozione delle misure previste dalla Convenzione, in termini di necessità, adeguatezza e proporzionalità, come richiesto dai menzionati strumenti normativi di protezione dei dati.

In questo senso, l'articolo 15 della Convenzione obbliga gli Stati firmatari ad assoggettare l'applicazione delle misure di assistenza alle norme di diritto interno. Tali misure devono prevedere condizioni idonee a garantire una tutela adeguata dei diritti fondamentali della persona (in particolare, di quelli previsti dalla Convenzione per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali, il cui articolo 8 sancisce, com'è noto, il diritto alla riservatezza); devono altresì assicurare specificamente il rispetto del "principio di proporzionalità".

L'applicazione del principio di proporzionalità è, quindi, prevista dalla Convenzione in termini di obbligatorietà, ai fini della corretta attuazione della Convenzione stessa. La legge n. 48/2008 non ha previsto, in tal senso, un'unica norma a carattere generale da integrare, poi, nella legislazione processuale penale. Risulta, quindi, necessario che tale principio sia adeguatamente sviluppato nella legislazione mediante l'inserimento, in ciascuna delle pertinenti disposizioni di legge che disciplinano l'attività di indagine e istruttoria nell'ambito del processo penale, di un'apposita previsione in base alla quale gli atti di indagine e processuali dovranno essere adottati dall'autorità giudiziaria o di polizia in chiave di proporzionalità e di selettività, in relazione, cioè, a dati e informazioni pertinenti e non eccedenti rispetto all'indagine in corso e con modalità parimenti proporzionate. Tali "clausole di proporzionalità" devono risultare operanti anche per altri atti di indagine previsti dalla Convenzione e già disciplinati dalla legislazione nazionale, come, ad esempio, le intercettazioni di comunicazioni e di conversazioni e in particolare di quelle "di nuova generazione", come quelle vocali effettuate in rete (*Voip, ecc.*). Qualora non si ottenga dal legislatore la menzione espressa del principio di proporzionalità nelle norme di legge sugli atti di indagine, è, comunque, più che opportuna un'azione di continua sensibilizzazione delle competenti autorità investigative affinché il principio di proporzionalità men-

zionato nella Convenzione sia rispettato in concreto negli atti di indagine. Analoga esigenza di applicazione in chiave di proporzionalità si pone, poi, per le disposizioni della legge di ratifica che hanno introdotto il *cd.* "congelamento" temporaneo e urgente dei dati di traffico telematico (*cfr. par.* 2.1.).

- la legge 25 febbraio 2008, n. 34, recante disposizioni per l'adempimento di obblighi derivanti dall'appartenenza dell'Italia alle Comunità europee. Tra le direttive cui il Governo è delegato a dare attuazione figura la direttiva 2006/86/Ce del 24 ottobre 2006, relativa alla conservazione, alla distribuzione e alla rintracciabilità dei tessuti e delle cellule umani. La legge attribuisce, inoltre, delega al Governo per l'adozione di decreti legislativi di attuazione di alcune decisioni quadro adottate nell'ambito della cooperazione di polizia e giudiziaria in materia penale (art. 28);

Legge comunitaria 2007

- la legge 18 marzo 2008, n. 53, di ratifica ed esecuzione di accordi di cooperazione relativi rispettivamente, a un sistema globale di navigazione satellitare civile (Gnss) tra la Comunità europea e i suoi Stati membri e Israele e, in pari data, la legge n. 54, di ratifica ed esecuzione di: 1) Accordo di cooperazione relativo ad un sistema globale di navigazione satellitare civile (Gnss)-Galileo tra la Comunità europea ed i suoi Stati membri e la Repubblica popolare cinese, fatto a Pechino il 30 ottobre 2003; 2) Accordo concernente la promozione, la fornitura e l'uso dei sistemi di navigazione satellitare Galileo e Gps e applicazioni correlate tra gli Stati uniti d'America, da un lato, e la Comunità europea e i suoi Stati membri, dall'altro. In merito a tali atti il 28 novembre 2007 si è tenuta presso la Commissione politiche dell'Unione europea della Camera un'audizione del Garante, nel corso della quale sono state esaminate le implicazioni che il sistema satellitare Galileo presenta in relazione alla tutela dei dati personali (*v. par.* 1.2.1.);

Sistema satellitare Galileo

- il decreto legge 31 dicembre 2007, n. 248, convertito dalla legge 28 febbraio 2008, n. 31, recante proroga di termini previsti da disposizioni legislative e disposizioni urgenti in materia finanziaria (*cd.* decreto "milleproroghe"). L'articolo 34, in materia di contrasto del terrorismo internazionale, proroga il termine di conservazione dei dati di traffico telefonico e telematico per i fornitori di reti pubbliche di comunicazioni o di servizi di comunicazione elettronica, già fissato al 31 dicembre 2007 (art. 6, comma 1, d.l. 27 luglio 2005, n. 144, conv. dalla l. 31 luglio 2005, n. 155).
  Per armonizzare i periodi di conservazione dei dati di traffico con le prescrizioni contenute nella pertinente direttiva europea in materia (direttiva 2006/24/Ce *cd.* "Frattini") il termine è prorogato alla data di entrata in vigore del decreto legislativo di attuazione della predetta direttiva -che dovrà individuare, appunto, specifici termini di conservazione dei dati- e comunque non oltre il 31 dicembre 2008;

Conservazione dei dati di traffico

- il medesimo decreto legge n. 248/2007, all'art. 47-*quater*, equipara la durata in carica del presidente e dei membri del Garante -unitamente a quelli della Consob e dell'Autorità per la vigilanza sui contratti pubblici- a quella del presidente e dei membri dell'Autorità garante della concorrenza e del mercato e dell'Autorità per le garanzie nelle comunicazioni (sette anni, non prorogabili), nelle more dell'approvazione della legge di riordino delle autorità indipendenti;

Durata in carica dei membri delle autorità indipendenti

- la legge 24 dicembre 2007, n. 244, che reca alcune disposizioni di interesse per gli aspetti concernenti la protezione dei dati personali, tra le quali si segnalano quelle relative a: 1) l'individuazione, con decreto interministeriale,

Legge finanziaria 2008

degli Stati o territori che consentono un adeguato scambio di informazioni (*white list*), nell'ambito delle disposizioni relative ai redditi prodotti all'estero e ai rapporti internazionali, recate dal testo unico delle imposte sui redditi di cui al d.P.R. n. 917/1986 (art. 1, comma 83); 2) la comunicazione mensile, in via telematica, dei dati retributivi, prevista al fine di semplificare la dichiarazione annuale presentata dai sostituti d'imposta tenuti al rilascio della certificazione unica, rimettendo a un decreto interministeriale la definizione delle modalità attuative e di condivisione dei dati tra Inps, Inpdap e l'Agenzia delle entrate (art. 1, commi 121 e 122); 3) l'introduzione della fatturazione elettronica per l'emissione, la trasmissione, la conservazione e l'archiviazione delle fatture emesse nei rapporti con le amministrazioni dello Stato e con gli enti pubblici nazionali, con l'osservanza del Codice dell'amministrazione digitale e attraverso il sistema di interscambio istituito e gestito dal Ministero dell'economia e delle finanze (art. 1, commi 209-213); 4) la comunicazione all'anagrafe tributaria di dati e notizie su contratti di somministrazione di servizi di telefonia, fissa, mobile e satellitare (*cd.* "catasto telefonico") raccolti dai relativi fornitori, a fini di contrasto all'evasione fiscale (art. 1, comma 222), in merito alla quale il Garante ha segnalato alla competente commissione parlamentare la criticità di una raccolta generalizzata di nuovi dati relativi a tutte le utenze telefoniche, anche mobili, e la necessità del ricorso a modalità proporzionate e selettive, che evitino l'afflusso indiscriminato di diversi milioni di dati relativi a cittadini non interessati a tali verifiche fiscali; 5) l'individuazione con decreto del Ministro dell'economia e delle finanze dei casi e delle modalità con cui, previa autorizzazione del direttore dell'Agenzia delle entrate e ai soli fini della riscossione delle entrate degli enti locali, i soggetti tenuti all'accertamento e alla riscossione dei tributi e di tutte le entrate possono accedere a dati e informazioni disponibili presso il sistema informativo dell'Agenzia delle entrate e prendere visione di atti riguardanti i beni dei debitori e dei coobbligati (art. 1, comma 225); 6) in relazione al sistema informativo della fiscalità, l'individuazione in capo al Ministero dell'economia e delle finanze della contitolarità delle banche di dati che lo compongono, ritenuta funzionale al sistema integrato delle banche dati in materia tributaria e finanziaria di cui all'art. 1, comma 57, della legge finanziaria 2007 (art. 1, comma 274); 7) la dichiarazione sostitutiva unica, con le informazioni necessarie per la determinazione dell'indicatore della situazione economica equivalente (I.s.e.e.) dei soggetti che richiedono prestazioni sociali agevolate, che il richiedente la prestazione può presentare anche direttamente all'Agenzia delle entrate in via telematica, ove intenda far rilevare i mutamenti delle condizioni familiari ed economiche del proprio nucleo familiare; si prevede inoltre che tramite convenzione tra la predetta Agenzia e l'Inps siano definite le modalità per lo scambio delle informazioni necessarie all'attuazione della disposizione, nel rispetto delle garanzie previste dal Codice (art. 1, comma 344); 8) la realizzazione di un "sistema unico nazionale" -articolato su base distrettuale di corte d'appello- delle intercettazioni telefoniche, ambientali e altre forme di comunicazione informatica o telematica disposte o autorizzate dall'autorità giudiziaria, il cui avvio è demandato al Ministero della giustizia (art. 2, comma 82); 9) l'istituzione, presso il Ministero dello sviluppo economico, del Garante per la sorveglianza dei prezzi, con il compito di sovrintendere alla tenuta ed elaborazione delle informazioni richieste agli "uffici prezzi" delle camere di commercio e ad altri organi (Istat, uffici del Ministero delle politiche agricole,

alimentari e forestali, Dipartimento per la programmazione e il coordinamento della politica economica della Presidenza del Consiglio dei ministri) e di renderle note –anche in via telematica– avvalendosi del portale delle imprese gestito dalla rete informatica delle camere di commercio; si segnala, in proposito, la particolare criticità della disposizione in base alla quale le informazioni riferite ai prezzi al consumo, anche nominative, sono in ogni caso sottratte all'applicazione della disciplina in materia di protezione dei dati personali, sulla quale l'Autorità nel corso dei lavori per l'approvazione della legge ha richiamato vivamente l'attenzione del competente ministero per le gravi implicazioni che possono derivarne sui diritti delle persone (art. 2, comma 199); 10) la definizione, con regolamento dell'Autorità per le garanzie nelle comunicazioni e nel rispetto dei princìpi di riservatezza previsti dal Codice, delle modalità di comunicazione dell'adempimento degli obblighi relativi alla promozione della distribuzione e della produzione di opere europee (art. 2, comma 301); 11) l'introduzione dell'azione collettiva risarcitoria, quale nuovo strumento generale di tutela dei diritti dei consumatori e degli utenti (*cd.* "*class action*"), attraverso la modifica del codice del consumo (art. 140 *bis*). Si prevede, in particolare, che il giudice chiamato a pronunciarsi sull'ammissibilità della domanda possa differire la pronuncia quando sul medesimo oggetto è in corso un'istruttoria davanti a un'autorità indipendente (art. 2, commi 445-449); 12) l'identificazione da parte del Cnipa di soluzioni tecniche e funzionali atte a garantire la salvaguardia dei dati e delle applicazioni informatiche e la continuità operativa dei servizi informatici e telematici, al fine di salvaguardare e di garantire l'integrità del patrimonio informativo gestito dalle amministrazioni pubbliche, anche ai sensi del Codice dell'amministrazione digitale e del Codice in materia di protezione dei dati personali (art. 2, comma 582); 13) con riguardo alle misure che le pubbliche amministrazioni devono individuare per il contenimento delle spese di funzionamento, l'individuazione –nel rispetto della normativa sulla tutela della riservatezza– di forme di verifica del corretto utilizzo delle utenze relative alle apparecchiature di telefonia mobile (art. 2, comma 595); 14) la pubblicazione degli atti comportanti spese a fini retributivi da parte di pubbliche amministrazioni statali, agenzie, società non quotate a totale o prevalente partecipazione pubblica e altri enti pubblici, sul relativo sito *web*, con l'indicazione nominativa dei destinatari e dell'ammontare del compenso (art. 3, comma 44);

- il decreto legge 1° ottobre 2007, n. 159, convertito dalla legge 29 novembre 2007, n. 222, recante interventi urgenti in materia economico-finanziaria, che tocca anche aspetti concernenti la protezione dei dati personali, fra i quali si ricordano in particolare: 1) il *cd.* "blocco dei pagamenti pubblici" di importo superiore a 10.000 euro nei confronti di cittadini che a loro volta sono debitori verso la pubblica amministrazione, per i quali si prevede la possibilità che l'importo di riferimento sia modificato con mero decreto ministeriale (art. 19); 2) l'istituzione dell'Osservatorio nazionale e degli osservatori regionali sulle politiche abitative, al fine di assicurare la formazione e la condivisione delle banche dati necessarie per la programmazione degli interventi di edilizia residenziale con finalità sociali, nonché allo scopo di monitorare il fenomeno dell'occupazione abusiva degli alloggi. Si prevede, inoltre, che i soggetti gestori del patrimonio immobiliare debbano assicurare, attraverso un sistema di banche dati consultabile via Internet, tutte le informazioni necessarie al pubblico, permettendo al contempo un delicato controllo

Collegato alla legge finanziaria 2008

incrociato dei dati nell'ambito del sistema integrato gestito dall'amministrazione finanziaria competente (art. 21); 3) la realizzazione, da parte del Ministero della giustizia, della "banca dati" delle misure cautelari prevista dalle norme di attuazione del codice di procedura penale, al fine di potenziare gli strumenti di conoscenza dei precedenti giudiziari individuali, nonché il rafforzamento della struttura informatica del Registro generale del casellario giudiziale e la sua integrazione su base nazionale con i carichi pendenti (art. 38); 4) il sistema integrato dell'anagrafe tributaria (art. 1, commi 56 e 57, legge finanziaria 2007), che viene finalizzato non solo alla condivisione e alla gestione integrata delle informazioni, ma anche al "costante scambio" delle informazioni medesime, e la cui effettiva realizzazione viene assicurata anche attraverso l'attività di indirizzo del Ministero dell'economia nei confronti di tutte le strutture dell'amministrazione finanziaria, ritenuta necessaria a garantire la razionalizzazione ed omogenee modalità di gestione del sistema informativo della fiscalità (art. 39, comma 4);

Riforma dei servizi di informazione e di sicurezza

- la legge 3 agosto 2007, n. 124, di riforma del sistema di informazione per la sicurezza della Repubblica e della disciplina del segreto di Stato.

Nel periodo d'interesse, il Governo ha inoltre adottato alcuni decreti legislativi di interesse per l'Autorità, fra i quali, in particolare:

Raccolta di sangue e servizi trasfusionali

- il decreto legislativo 20 dicembre 2007, n. 261, recante la revisione del decreto legislativo 19 agosto 2005, n. 191, di attuazione della direttiva 2002/98/Ce, che stabilisce norme di qualità e di sicurezza per la raccolta, il controllo, la lavorazione, la conservazione e la distribuzione del sangue umano e dei suoi componenti. In particolare, si prevede che tutti i dati raccolti, comprese le informazioni di carattere genetico, cui hanno accesso terzi, siano resi anonimi in modo tale che il donatore non sia più identificabile, e che si adottino misure di protezione dei dati tali da scongiurare divulgazioni indebite di tali informazioni, garantendo al tempo stesso la tracciabilità delle donazioni (art. 22);
- il decreto legislativo 9 novembre 2007, n. 207, di attuazione della direttiva 2005/61/Ce che applica la direttiva 2002/98/Ce per quanto riguarda le prescrizioni in tema di rintracciabilità del sangue e degli emocomponenti destinati a trasfusioni e la notifica di effetti indesiderati ed incidenti gravi; tutte attività che devono esplicarsi nel rispetto della "normativa vigente", tra cui, segnatamente, quella in materia di protezione dei dati personali (artt. 2, 3 e 4);
- il decreto legislativo 9 novembre 2007, n. 208, di attuazione della direttiva 2005/62/Ce che applica la direttiva 2002/98/Ce per quanto riguarda le norme e le specifiche comunitarie relative ad un sistema di qualità per i servizi trasfusionali, che prevede, tra l'altro, a garanzia della riservatezza dei donatori di sangue, la disponibilità di un'area riservata e separata, destinata al colloquio con il candidato donatore e al ristoro/riposo *post* donazione; nonché la conservazione della documentazione relativa alle registrazioni di ciascuna attività svolta dai servizi trasfusionali e dalle unità di raccolta, effettuata secondo procedure che garantiscano la protezione dei dati e la tutela della riservatezza "sulla scorta delle regolazioni e normative vigenti" (allegato I, punti 3.2, 5 e 6.1);

Contrasto del riciclaggio

- il decreto legislativo 21 novembre 2007, n. 231, di recepimento della direttiva 2005/60/Ce e della direttiva 2006/70/Ce concernente la prevenzione dell'utilizzo del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo. Il decreto, previsto dalla legge comunitaria 2005 (l. n. 29/2006), ha inteso coordinare le disposizioni

in materia di rango primario e secondario succedutesi nel tempo, e che hanno esteso le misure antiriciclaggio, originariamente introdotte nel settore del credito e dell'intermediazione finanziaria, a diverse professioni (notai, altri liberi professionisti legali, ragionieri, commercialisti, consulenti tributari e del lavoro e agenti immobiliari) e ad attività d'impresa ritenute particolarmente suscettibili di utilizzazione a fini di riciclaggio (agenzie di recupero crediti, custodia e trasporto di valori, commercio di cose antiche o di preziosi, case d'asta o case da gioco). Il decreto ha confermato e, in parte, ampliato tale intervento estensivo, sulla base di quanto previsto dalla citata direttiva europea. Come rilevato dal Garante nel parere reso sullo schema (*v. par.* 1.2.3.2.), la particolare ampiezza del novero dei soggetti tenuti agli obblighi di identificazione della clientela, di registrazione delle operazioni e (in alcuni casi) di segnalazione di quelle sospette impone da tempo una riflessione di fondo sul crescente impatto che la normativa antiriciclaggio assume sempre più in settori via nuovi, nonché sulle connesse implicazioni che ne derivano per i diritti delle persone e sul piano della protezione dei dati personali. La direttiva 2005/60/Ce prevede infatti anche un incremento dei controlli sui soggetti che effettuano operazioni "sospette", stabilendo che debba essere identificato anche il "titolare effettivo" dell'operazione stessa (vale a dire la persona che esercita un controllo sul cliente o per conto della quale l'attività o l'operazione vengono effettuate); prevede, altresì, verifiche sulla clientela calibrate rispetto al "rischio" di riciclaggio associato al cliente (*cd.* "approccio basato sul rischio"). La medesima direttiva europea menziona, al contempo, la necessità di rispettare i diritti fondamentali delle persone e i princìpi riconosciuti, in particolare, dalla Carta dei diritti fondamentali dell'Unione europea, il cui articolo 8 garantisce ad ogni individuo il diritto alla protezione dei dati personali che lo riguardano. In tale quadro, il descritto e rilevante ampliamento, soggettivo e oggettivo, della normativa a livello europeo e, conseguentemente, di quella nazionale di attuazione, ne rende necessaria un'applicazion rigorosa in chiave di effettiva necessità, proporzionalità e selettività degli interventi di monitoraggio e di prevenzione (artt. 2 e 11 del Codice), anche in considerazione degli enormi flussi informativi previsti dal decreto legislativo. Al riguardo si segnala, in particolare, che l'art. 36, comma 6, del decreto prevede che i dati e le informazioni raccolti per finalità antiriciclaggio, debitamente registrate, siano poi "utilizzabili ai fini fiscali secondo le disposizioni vigenti"; nel parere espresso il Garante ha richiesto che tale utilizzabilità vi sia solo in caso di accertato riciclaggio, per assicurare il rispetto dei princìpi di finalità e proporzionalità nel trattamento dei dati (art. 11 del Codice);

- il decreto legislativo 6 novembre 2007, n. 191, che attua la direttiva 2004/23/Ce sulla definizione di norme di qualità e di sicurezza per la donazione, l'approvvigionamento, il controllo, la lavorazione, la conservazione, lo stoccaggio e la distribuzione di tessuti e cellule umani; si prevede, in particolare, che tutti i dati, comprese le informazioni genetiche, ai quali hanno accesso terzi, siano resi anonimi in modo tale che né il donatore, né il ricevente siano identificabili (art. 14); tra le informazioni da fornire ai donatori o ai soggetti legittimati a esprimere il consenso alla donazione figurano quelle relative alla protezione dei dati e alla riservatezza medica (art. 15 e allegato 1);

Tessuti e cellule umane

- il decreto legislativo 6 novembre 2007, n. 198, di attuazione della direttiva 2005/14/Ce sull'assicurazione della responsabilità civile risultante dalla circolazione di autoveicoli, che –modificando il codice delle assicurazioni pri-

Dati riguardanti la copertura assicurativa dei veicoli

vate (art. 142 *bis*)– prevede a favore del danneggiato il diritto di ottenere dal Centro di informazione italiano, istituito presso l'Isvap, i dati riguardanti la copertura assicurativa del veicolo che ha causato il sinistro, il numero di polizza e la data di scadenza della stessa (art. 1, comma 5);

Sperimentazione di farmaci

- il decreto legislativo 6 novembre 2007, n. 200, di attuazione della direttiva 2005/28/Ce, recante princìpi e linee-guida dettagliate per la buona pratica clinica relativa ai medicinali in fase di sperimentazione a uso umano, nonché requisiti per l'autorizzazione alla fabbricazione o importazione di tali medicinali; tra i princìpi di buona pratica clinica si prevede la garanzia della riservatezza dei documenti che potrebbero identificare i soggetti in sperimentazione (art. 3, comma 11) e si dedica un'apposita previsione alla riservatezza dei dati e dei rapporti d'ispezione (art. 30, commi 1 e 2);

Commercio a distanza di servizi finanziari

- il decreto legislativo 23 ottobre 2007, n. 221, recante disposizioni correttive ed integrative del Codice del consumo (d.lg. 6 settembre 2005, n. 206) che traspone in tale codice la disciplina relativa alla commercializzazione a distanza di servizi finanziari ai consumatori, già contenuta nel decreto legislativo n. 190 del 2005; si registra, in particolare, che il nuovo articolo 67-*sexiesdecies* del predetto Codice reca la disciplina delle comunicazioni non richieste in caso di utilizzo di tecniche di comunicazione a distanza;

Pratiche commerciali sleali

- il decreto legislativo 2 agosto 2007, n. 146, recante attuazione della direttiva 2005/29/Ce relativa alle pratiche commerciali sleali fra imprese e consumatori. Per quanto di specifico interesse in materia di protezione dei dati personali, il decreto modifica il Codice del consumo (art. 26, comma 1, lett. *c*) d.lg. n. 206/2005) inserendo fra le pratiche commerciali definite "aggressive" anche le ripetute e non richieste sollecitazioni commerciali per telefono, via *fax*, per posta elettronica o mediante altro mezzo di comunicazione a distanza, fuori dalle circostanze in cui esse risultino giustificate ai fini dell'esecuzione di un'obbligazione contrattuale e fatta salva la disciplina in materia prevista dal medesimo Codice del consumo (art. 58) e dal Codice in materia di protezione dei dati personali (art. 130);

Comunicazioni dei vettori aerei

- il decreto legislativo 2 agosto 2007, n. 144, con il quale è stata recepita la direttiva 2004/82/Ce concernente l'obbligo dei vettori aerei di comunicare i dati relativi alle persone trasportate, sul cui schema il Garante ha espresso parere (*v. par.* 1.2.3.2.).

2.2.1. *I regolamenti sui procedimenti presso il Garante*

Regolamento sulle procedure

Il 14 dicembre 2007 sono stati adottati due regolamenti del Garante, entrambi pubblicati in *G.U.* n. 7 del 9 gennaio 2008.

Il primo (Regolamento n. 1/2007 [doc. *web* n. 1477480]) disciplina le procedure con le quali il Garante svolge i compiti previsti per legge ai fini del rispetto della normativa sulla protezione dei dati personali (art. 154 del Codice).

Dopo l'entrata in vigore del Codice e sulla base dell'esperienza acquisita, è emersa infatti l'esigenza di consolidare alcune concrete modalità attuative delle disposizioni relative allo svolgimento dei compiti dell'Autorità, e, in particolare, alle procedure di tutela degli interessati, avviate d'ufficio o su loro istanza, tenendo conto anche delle risorse del Garante e delle entrate disponibili in base al bilancio di previsione.

Il regolamento evidenzia che l'Autorità continuerà ad ispirare la propria azione a princìpi di trasparenza, ragionevolezza, proporzionalità e non discriminazione, realizzando l'interesse pubblico connesso a ciascuna attività secondo criteri di buona amministrazione, economicità e adeguatezza e valorizzando l'utilizzo di tecniche informatiche e della telematica. A tal fine, si terrà conto in particolare di alcuni fat-

tori, quali la natura e della gravità degli illeciti da accertare in rapporto ai loro effetti e all'entità del danno che può derivarne per uno o più interessati, come pure la probabilità di comprovare la sussistenza degli illeciti segnalati (art. 3).

Sulla base di questi criteri (*v.* anche art. 2, comma 1, lett. *a*) e *c*), del regolamento n. 1/2000) il Garante determina e aggiorna con cadenza almeno semestrale la programmazione dei lavori del collegio, le linee di priorità nell'esame di reclami e segnalazioni da parte dell'ufficio e la programmazione delle attività ispettive (art. 4), in modo da trovare il miglior equilibrio tra le risorse disponibili e le questioni da trattare.

Nel quadro di priorità così determinato, il regolamento disciplina lo svolgimento delle procedure anche in applicazione dei princìpi contenuti nella legge n. 241 del 1990 ed evidenzia, tra l'altro, i diversi casi in cui, al termine dell'istruttoria preliminare, non si ravvisano gli estremi per un provvedimento di divieto o blocco del trattamento ai sensi dell'art. 143 del Codice; tra questi casi, vi rientrano, le condotte ormai prive di effetti, anche per il tempo trascorso, quelle per le quali il titolare ha nella sostanza posto rimedio a quanto lamentato dagli interessati, oppure può essere sufficiente richiamare un provvedimento generale del Garante (art. 11).

Nel contempo, si è ravvisata la necessità di verificare la perdurante attualità e la persistenza dei presupposti per adottare provvedimenti in ordine a fatti oggetto di segnalazioni e reclami pervenuti all'Autorità prima dell'insediamento dell'attuale collegio; si è perciò previsto che, salvi alcuni casi, siano improcedibili segnalazioni e reclami anteriori al 30 aprile 2005 per i quali non sia stata presentata nei termini indicati dal regolamento una motivata richiesta di trattazione (art. 21).

L'esplicita indicazione dei criteri di priorità e di trattazione è apparsa, oltre che rispettosa di esigenze normative, utile per orientare in concreto gli interessati, in modo che le segnalazioni e i reclami consentano di intervenire sui casi di rilievo e, insieme, di fornire gli elementi di valutazione necessari all'Autorità per il migliore svolgimento delle sue funzioni.

Regolamento sulla durata dei procedimenti e sulle unità organizzative competenti

Il secondo regolamento (n. 2/2007 [doc. *web* n. 1477624]) individua i termini per lo svolgimento dei procedimenti e le unità organizzative responsabili ai sensi degli artt. 2 e 4 della l. n. 241/1990 e successive modificazioni. Anche questo regolamento riguarda sia i procedimenti avviati d'ufficio, sia quelli avviati su istanza di parte. Al testo sono allegate al testo due tabelle, la tab. A, che contiene una ricognizione dei termini già stabiliti per legge, la tab. B, invece, con cui sono determinati i termini non previsti direttamente dalla legge. Quest'ultima tabella che è stata oggetto di un comunicato di rettifica pubblicato nella *Gazzetta Ufficiale* 7 giugno 2008, n. 132, è divisa in due parti, relative la prima a procedimenti disciplinati dal Codice, e, la seconda, a procedimenti inerenti al personale dell'Ufficio. I termini stabiliti dalla legge si riferiscono alla data di adozione del provvedimento finale da parte del Collegio del Garante. Quelli determinati dal regolamento, invece si riferiscono alla data in cui l'unità organizzativa competente conclude l'esame dell'affare; in questi casi bisogna aggiungere il termine per l'adozione del provvedimento finale, non superiore a sessanta giorni, decorrenti dalla data di ricezione degli atti da parte del collegio (*v.* art. 15 del regolamento del Garante n. 1/2000 [doc. *web* n. 1098801]).

2.3. *Il monitoraggio delle leggi regionali*

Nel corso del 2007 è proseguita l'attività di monitoraggio degli atti delle regioni e degli enti locali.

L'attività in parola, svolta con finalità anzitutto conoscitive, ha avuto per oggetto la conformità degli atti normativi, anche in *itinere*, alla disciplina nazionale in mate-

ria di protezione dei dati personali, alla luce della nota sentenza n. 271/2005 della Corte costituzionale, che riconduce la protezione dei dati alla materia dell'ordinamento civile e, quindi, alla esclusiva competenza statale.

Va premesso che il quadro giurisprudenziale di riferimento non ha presentato variazioni rispetto all'anno precedente e che oggetto di analisi e di verifica sono risultati principalmente i settori attinenti alle politiche sociali e familiari nonché i procedimenti elettorali e quelli amministrativi.

Con specifico riferimento alle richieste di parere pervenute dalla Presidenza del Consiglio dei ministri relative a leggi già approvate è stato nella gran parte dei casi riscontrato, come già lo scorso anno, un sostanziale corretto svolgimento della potestà legislativa regionale.

Tra i parametri costituzionali venuti in considerazione, si segnala quello dell'art. 48 della Costituzione sulla segretezza del voto, che acquista particolare rilievo nelle ipotesi in cui venga disciplinato il *cd.* "voto elettronico".

A fronte di innovative modalità di votazione che in via sperimentale cominciano ad essere disciplinate si è infatti ritenuto doveroso verificare se la segretezza e, quindi, la protezione delle opinioni politiche del votante prevista dalla Costituzione, sia assicurata in termini adeguati.

In sede di approfondimento da parte dell'Autorità, è emerso tra l'altro che il problema si può porre in particolare per i voti "nulli", che sono comunque espressione della non comprimibile libertà di scelta dell'elettore e che potrebbero anche indirettamente risultare riconoscibili nel caso in cui, ad esempio, la procedura per esprimerli risultasse, per ragioni tecniche, più lunga di quella necessaria per esprimere un voto valido, e quindi richiedesse una maggiore permanenza dell'elettore in cabina.

A fronte di alcuni testi normativi suscettibili di applicazione non pienamente conforme alla normativa nazionale, ma che di per sé non apparivano in violazione dell'esclusiva competenza legislativa statale, l'Autorità ha indicato la necessità di utilizzare lo strumento regolamentare previsto dagli artt. 19 e 20 del Codice per assicurare la piena conformità della disciplina regionale –relativa alla comunicazione di dati comuni a soggetti privati ovvero alla loro diffusione, nonché al trattamento dei dati sensibili– ai limiti posti dal Codice.

Con riferimento all'esame dei testi legislativi e regolamentari in *itinere* effettuato nel corso dell'anno, si sono registrati poi profili e problematiche di interesse similari a quelli riguardanti gli atti legislativi già pubblicati sulla *Gazzetta Ufficiale.*

L'attività di monitoraggio, seppure a campione e limitatamente a quanto pubblicato sui siti istituzionali, ha riguardato anche taluni provvedimenti amministrativi delle regioni e degli enti locali tra i quali vanno menzionate alcune deliberazioni comunali istitutive di registri di unioni di fatto, la deliberazione di una giunta regionale in materia di registri pubblici delle assistenti familiari e un regolamento regionale in materia di sistema informativo geografico regionale.

Al riguardo si è evidenziato che lo svolgimento da parte di enti locali di compiti conoscitivi informativi e statistici risponde all'esigenza di assicurare la circolazione delle informazioni tra amministrazioni locali, regionali e statali, ma va seguito con attenzione in particolare per quanto attiene al grado di pervasività dei sistemi in concreto posti in essere.

Per quanto attiene alle convivenze di fatto, si è confermato che risultano rispettose delle esigenze di protezione dei dati personali quelle deliberazioni che ricollegano effetti al dato obiettivamente riscontrabile della comune residenza dei soggetti interessati, evitando, in linea con il principio di essenzialità nel trattamento dei dati, di attribuire rilievo a profili più direttamente attinenti alla sfera affettiva o sessuale, e senza interferire con la disciplina in materia di registri anagrafici e di stato civile.

L'attività svolta dal Garante

II - L'attività svolta dal Garante

3 Il Garante e le pubbliche amministrazioni

3.1. *Profili introduttivi*

Nel settore pubblico si continuano a registrare ritardi e difficoltà nella rigorosa applicazione della normativa e dei princìpi in materia di protezione dei dati personali.

Nel corso del 2007 è proseguita da parte delle pubbliche amministrazioni l'attività necessaria all'adozione dei regolamenti per il trattamento dei dati sensibili e giudiziari, nonché l'adeguamento degli assetti organizzativi e funzionali alle disposizioni del Codice e, in alcuni casi, l'adozione delle norme regolamentari in funzione integrativa della normativa statale.

Il varo dei predetti regolamenti, oltre a costituire un adempimento necessario, ha offerto alle amministrazioni pubbliche un'importante occasione per proseguire il processo di ammodernamento delle proprie strutture anche alla luce dei diritti e delle libertà fondamentali delle persone.

Nel 2007 l'Autorità è stata altresì chiamata a verificare il rispetto della disciplina in materia di protezione dei dati personali in diversi settori fra i quali quello riguardante il trattamento delle informazioni genetiche e dei campioni biologici; si è conclusa, infatti, l'ultima fase di approfondimento in ordine all'individuazione delle cautele da osservare in relazione al trattamento di tale categoria di informazioni ed è stata così adottata nel mese di febbraio l'*autorizzazione generale* per il trattamento dei dati genetici [doc. *web* n. 1389918], la cui predisposizione ha impegnato lungamente l'Autorità, anche in collaborazione con esperti del settore (*v. Relazione* 2006, p. 64).

Inoltre, le numerosissime comunicazioni pervenute all'Autorità ai sensi degli artt. 19, comma 2 e 39, comma 1, lett. *a*), del Codice hanno contribuito a far emergere l'esistenza di flussi di informazioni personali diversi da quelle sensibili e giudiziarie tra enti pubblici, anche in assenza di norme di legge e di regolamento, ma necessari per l'esercizio delle funzioni istituzionali di uno degli enti coinvolti.

Il Garante ha inoltre continuato a verificare la corretta interpretazione ed applicazione della normativa in materia di protezione dei dati in tutti gli ambiti pubblici, per garantire il rispetto della dignità e della riservatezza dei cittadini soprattutto in quei particolari settori, quali quello sanitario, dove, per la particolare delicatezza delle informazioni trattate, risulta imprescindibile l'adozione di misure ed accorgimenti ancora più incisivi di quelli normalmente previsti a tutela degli interessati.

Obiettivo prioritario del Garante è, quindi, tuttora, la "messa in sicurezza" dei trattamenti più delicati (si pensi al trattamento dei dati sensibili e giudiziari, non-

ché agli accessi alle grandi banche di dati) e delle modalità più pericolose di trattamento delle informazioni come quella delle interconnessioni.

Le pagine che seguono dànno conto –con un'esposizione casistica, in ragione del rilievo delle norme che nei diversi settori regolano il trattamento di dati da parte dei soggetti pubblici– delle molteplici direzioni nelle quali l'Autorità, pur con risorse assai limitate, è stata chiamata ad intervenire.

3.2. *I regolamenti sui trattamenti di dati sensibili e giudiziari*

3.2.1. *I regolamenti delle amministrazioni centrali*

Il processo di adeguamento al sistema di garanzie previsto dal Codice per il trattamento dei dati sensibili e giudiziari è proseguito nel corso dell'anno per talune amministrazioni centrali che non vi avevano provveduto entro il termine del 28 febbraio 2007. Il Garante è stato quindi chiamato ad esprimere il previsto parere sugli schemi di regolamento predisposti dall'Aifa-Agenzia italiana del farmaco (*Parere* 12 aprile 2007 [doc. *web* n. 1403241]), dall'Isfol-Istituto per lo sviluppo della formazione professionale dei lavoratori (*Parere* 26 aprile 2007 [doc. *web* n. 1407772]), dal Coni-Comitato olimpico nazionale italiano, (*Parere* 19 settembre 2007 [doc. *web* n. 1443411]) e dalla Sspal-Scuola superiore della pubblica amministrazione locale (*Parere* 7 febbraio 2008 [doc. *web* n. 1491594].

In tutti questi casi, l'Autorità ha subordinato l'adozione del parere favorevole al rispetto di talune condizioni, evidenziando che eventuali trattamenti di dati sensibili o giudiziari, effettuati oltre la scadenza di legge e nelle more dell'adozione di un regolamento conforme al parere espresso dal Garante, possono essere effettuati lecitamente solo sulla base di una specifica previsione legislativa. In alcune circostanze, inoltre, è stata rilevata la non corretta individuazione delle disposizioni del Codice relative alle finalità di rilevante interesse pubblico perseguite nello svolgimento delle attività poste in essere di volta in volta (*cfr. Pareri* all'Isfol, al Coni e alla Sspal). In alcuni casi, il Garante non ha ritenuto comprovata l'indispensabilità dell'utilizzo di talune categorie di informazioni sensibili per perseguire le attività menzionate negli schemi. In particolare, è stato richiesto alla Scuola superiore della pubblica amministrazione locale di valutare ulteriormente l'indispensabilità dell'utilizzo di dati personali attinenti allo stato di salute per elaborare studi e ricerche nell'ambito delle scienze mediche; ciò, in ragione delle finalità istituzionali della scuola, strettamente connesse alle esigenze di formazione, aggiornamento e specializzazione degli amministratori pubblici locali. Un riesame della valutazione di indispensabilità è stato richiesto anche all'Agenzia italiana del farmaco in ordine all'utilizzo di informazioni sensibili –in luogo di dati anonimi o diversi da quelli sensibili– per monitorare le sperimentazioni cliniche di medicinali presso l'Osservatorio nazionale sulla sperimentazione clinica che fa capo all'Agenzia.

L'Autorità ha precisato ancora che interconnessioni e raffronti, anche in applicazione del criterio di indispensabilità, devono essere limitati alle ipotesi in cui sussista una base normativa che li autorizzi (art. 22, commi 9 e 11, del Codice). Al riguardo, precisando che l'"interconnessione" evidenzia una relazione tra sistemi informativi reciprocamente accessibili a determinate condizioni, il Garante ha richiesto di verificare se, nei singoli casi, l'operazione consiste in una interconnessione o in un diverso tipo di collegamento per via telematica volto a ottenere informazioni o certificazioni dal medesimo o da altri titolari del trattamento, senza una consultazione

diretta di banche dati (*cfr. ad es., Parere* alla Sspal). Taluni specifici rilievi sono stati poi formulati all'Aifa riguardo alle operazioni di interconnessione e raffronto indicate nello schema di regolamento nell'ambito della "rete nazionale ed internazionale di farmacovigilanza". Fermi restando i flussi telematici di informazioni previsti per legge (in particolare, dal d.lg. 24 aprile 2006, n. 219), l'Autorità non ha ritenuto che le disposizioni primarie richiamate nello schema consentissero l'interconnessione informatica tra il sistema dell'Agenzia e quelli delle aziende farmaceutiche idonea a raffrontare dati sensibili detenuti da distinti titolari del trattamento.

3.2.2. *I regolamenti delle regioni e degli enti locali*

Sono continuate a pervenire da parte di enti regionali e locali numerose richieste di parere (art. 20, comma 2 e 154, commi 1, lett. *g*) e 5, del Codice) aventi per oggetto schemi di regolamento riguardanti trattamenti di dati sensibili e giudiziari ritenuti non ricompresi, per tipologia di dati o di operazioni, né negli schemi-tipo di regolamento, sui quali il Garante si è espresso favorevolmente, predisposti dall'Anci-Associazione nazionale dei comuni italiani [doc. *web* n. 1174532], dall'Uncem-Unione nazionale comuni comunità enti montani [doc. *web* n. 1182195], dall'Upi-Unione delle province d'Italia [doc. *web* n. 1174562], dalla Conferenza regioni e delle province autonome [doc. *web* n. 1272225], né nei pareri con i quali il Garante si è espresso positivamente con riferimento a ulteriori trattamenti di dati sensibili e giudiziari non considerati nei predetti schemi-tipo (*Relazione 2006*, pp. 34 e 35 [doc. *web* nn. 1213424, 1298732, 1314392, 1370369, 1377640, 1434995]).

In particolare, è pervenuta all'Autorità una specifica richiesta di parere dalla Provincia autonoma di Trento in ordine a una scheda, da allegare al regolamento già adottato, che identifica i tipi di dati e di operazioni eseguibili dall'amministrazione in relazione alle specifiche finalità perseguite nell'ambito del sistema educativo di istruzione e formazione provinciale (artt. 73, 86, comma 1, lettera *c*) e 95 del Codice). In ordine alla medesima scheda, predisposta al termine di una collaborazione informale avviata con l'Ufficio del Garante, l'Autorità ha espresso parere favorevole (*Parere* 10 gennaio 2008, [doc. *web* n. 1482234]).

Altre richieste di parere pervenute dagli enti locali hanno posto problematiche interpretative per molti versi omogenee.

Sono numerosi, infatti, i casi in cui si è reso necessario richiamare gli enti locali al rispetto del principio di indispensabilità di dati sensibili o giudiziari trattati e di operazioni eseguibili (art. 22, comma 5, del Codice).

Ad esempio, laddove non è risultata comprovata, dalla descrizione del trattamento, l'indispensabilità dell'utilizzo di dati idonei a rivelare lo stato di salute dei familiari dell'interessato per la gestione di albi comunali di associazioni e organizzazioni di volontariato, l'amministrazione interessata è stata invitata a espungere i dati in questione dallo schema di regolamento, ferma restando la possibilità di verificare nuovamente l'indispensabilità e di documentarla adeguatamente al fine di richiedere al Garante uno specifico parere in proposito (*Nota* 8 maggio 2007).

Analoghe considerazioni sono state formulate nei confronti di un comune, che aveva individuato i dati idonei a rivelare l'origine razziale ed etnica ai fini della concessione di contributi per l'abbattimento delle barriere architettoniche, senza comprovare nella descrizione del trattamento l'indispensabilità dell'utilizzo di tali informazioni per perseguire le finalità connesse all'erogazione dei contributi in questione (*Nota* 31 maggio 2007).

I medesimi princìpi sono stati rappresentati ad altri enti locali che hanno invece individuato, quali dati necessari per il perseguimento di specifiche finalità istituzionali, lo stato di salute relativo ai familiari del dipendente, la vita sessuale per perse-

guire scopi socio-assistenziali e psico-sociali in favore di soggetti immigrati (*Nota* 2 agosto 2007), l'anamnesi familiare per perseguire finalità in materia di protezione civile (*Nota* 18 giugno 2007) e i dati idonei a rivelare l'adesione a sindacati nel quadro della gestione dell'anagrafe della popolazione residente (*Nota* 21 giugno 2007).

Un ulteriore aspetto di valutazione ha riguardato i destinatari delle comunicazioni aventi a oggetto dati sensibili o giudiziari ad opera degli enti locali. È stato così evidenziato che eventuali, ulteriori destinatari del flusso informativo possono essere identificati solo nei limiti delle categorie già indicate nelle corrispondenti schede degli schemi tipo in relazione alle finalità di rilevante interesse pubblico ivi specificate. È stato comunque sottolineato che, ai fini di una corretta applicazione del Codice, l'ente locale, qualora intenda avvalersi di soggetti esterni per lo svolgimento di attività istituzionali in *cd.* "*outsourcing*", deve designare tali soggetti quali responsabili del trattamento (art. 29 del Codice). In tal caso, poiché la trasmissione di dati personali a un soggetto designato responsabile del trattamento non costituisce una comunicazione ai sensi del citato art. 4, comma 1, lett. *l*), del Codice, non occorre riportare tale indicazione nello schema di regolamento (*Nota* 15 ottobre 2007).

Un caso particolare ha poi riguardato il trattamento di dati personali effettuato dalle farmacie comunali nell'ambito delle attività di prenotazione presso il competente centro unico di prenotazione (cup) delle prestazioni sanitarie. È stato evidenziato che si tratta di una funzione istituzionale che attiene non alle strutture comunali, bensì alle regioni. Queste ultime, infatti, si possono avvalere delle farmacie aperte al pubblico per attuare le prenotazioni di prestazioni specialistiche per via informatica tramite il cup, nel caso ne ravvisino la necessità (*v.* art. 2, comma 3, del d.P.R. 8 luglio 1998, n. 371). In particolare, i dati immessi nella banca dati relativa ai cup sono gestiti dalle singole aziende sanitarie, come è stato espressamente rappresentato nello schema-tipo di regolamento per i trattamenti dei dati sensibili e giudiziari di competenza delle regioni e delle province autonome (*cfr.* scheda n. 8 dell'allegato B dello schema-tipo citato), sul quale il Garante ha espresso parere positivo il 13 aprile 2006 (*cfr. Relazione* 2005, p. 21 [doc. *web* n. 1272225]). In relazione a tali profili, è stato quindi fatto presente al comune di espungere il riferimento al trattamento in questione dallo schema di regolamento (*Nota* 21 dicembre 2007).

Con specifico riferimento alle province, il Garante è stato interpellato in ordine ai trattamenti di dati sensibili e giudiziari effettuati dalla consigliera o dal consigliere di parità. A tale proposito, è stato rappresentato che la provincia, nei limiti e in considerazione delle competenze ad essa attribuite dalla legge, può avvalersi dello schema di regolamento per il trattamento dei dati sensibili e giudiziari predisposto dal Ministero del lavoro e della previdenza sociale –sul quale il Garante ha espresso parere favorevole il 28 febbraio 2007 [doc. *web* n. 1409015]– e che prevede espressamente, nella scheda n. 12, il trattamento di dati sensibili e giudiziari finalizzato, tra l'altro, a "garantire le pari opportunità" (art. 112, comma 2, lett. *b*), del Codice). Nell'ipotesi in cui i tipi di dati personali trattati e le operazioni su di essi eseguibili, siano pienamente conformi a quelli individuati nella citata scheda n. 12 del predetto schema di regolamento, non si rende necessario chiedere il parere specifico ai sensi dell'art. 20, comma 2, del Codice (*Nota* 24 ottobre 2007).

Taluni consorzi e autorità d'ambito territoriale si sono rivolti al Garante presentando richieste di parere su schemi di regolamento per il trattamento dei dati sensibili e giudiziari in considerazione della loro particolare conformazione istituzionale. Ad essi si è ritenuto applicabile il regime previsto per gli enti locali e, quindi, la possibilità di fare riferimento ai sopra citati schemi tipo di regolamento predisposti per comuni, comunità montane e province laddove effettuino il trattamento di dati personali in qualità di titolari autonomi del trattamento (artt. 4, comma 1, lett. *f*),

e 28 del Codice). Ciò, in relazione alle rilevanti finalità di interesse pubblico perseguite di volta in volta, nei limiti ed in considerazione delle competenze ad essi attribuiti dalla legge e svolte per conto di comuni e province.

Il Garante è stato altresì interpellato in ordine al trattamento di dati sensibili effettuato da una prefettura in collaborazione con taluni comuni di una provincia siciliana, finalizzato al riconoscimento di benefici economici in favore di cittadini minorati, invalidi, ciechi e sordomuti civili ai sensi della normativa di riferimento (*v.* l. 26 maggio 1970, n. 382; l. 30 marzo 1971, n. 118; l. 11 febbraio 1980, n. 18; l. 21 novembre 1988, n. 508; l. 11 ottobre 1990, n. 289).

In proposito, l'Ufficio ha osservato che, per effetto del conferimento di funzioni e di compiti amministrativi dello Stato alle regioni e agli enti locali, l'esercizio delle predette funzioni è stato delegato alle regioni (art. 130 d.lg. 30 marzo 1998, n. 112). Nelle more dell'effettiva decorrenza dell'esercizio di tali funzioni (art. 10 d.lg. n. 112/1998 *cit.* e art. 5 d.P.C.M. 26 maggio 2000), in Sicilia, in particolare, permane la competenza per la concessione delle provvidenze economiche a favore di invalidi civili in capo al Ministero dell'interno, che agisce tramite le prefetture-Utg (art. 11 d.lg. 30 luglio 1999, n. 300); il trattamento in questione è quindi lecito nei limiti di quanto espressamente previsto dal regolamento per il trattamento dei dati sensibili e giudiziari del Ministero dell'interno. Tale regolamento, infatti, disciplina il trattamento di dati idonei a rivelare lo stato di salute e giudiziari ai fini della concessione *"da parte delle Prefetture della Sicilia, dell'assegno, della pensione di invalidità e dell'indennità di accompagnamento per gli invalidi civili, i ciechi ed i sordomuti ... per le provvidenze economiche liquidate dall'Inps"* (scheda n. 4 - d.m. 21 giugno 2006, n. 244, in *G.U.* 9 agosto 2006, n. 184), sul quale il Garante ha espresso parere favorevole il 28 aprile 2006 [doc. *web* n. 1289890] (*Nota* 8 maggio 2007).

3.3. *La trasparenza dell'attività amministrativa e l'accesso ai documenti amministrativi*

L'Autorità è stata chiamata in numerose occasioni a fornire indicazioni sul delicato bilanciamento tra trasparenza amministrativa e diritto degli interessati alla riservatezza.

Al riguardo è stato evidenziato che non spetta all'Autorità verificare, caso per caso, la sussistenza dei requisiti previsti in materia di accesso alla luce dello specifico quadro normativo di riferimento; tale valutazione è rimessa all'amministrazione interpellata ed è sindacabile davanti al giudice competente.

Il principio è stato rappresentato a chi aveva segnalato al Garante il diniego opposto da un corpo di polizia locale, alla richiesta, formulata ai sensi della specifica disciplina del codice delle assicurazioni private (d.lg. 7 settembre 2005, n. 209), di ottenere taluni dati riguardanti il proprietario e il conducente di un'autovettura coinvolta in un sinistro stradale con il segnalante medesimo (*Nota* 8 giugno 2007).

Analogamente, su una richiesta di intervento indirizzata all'Autorità, per vedere soddisfatta un'istanza di accesso ai documenti amministrativi detenuti da un comune, l'Ufficio ha risposto che gli artt. 59 e 60 del Codice non hanno abrogato le disposizioni sulla trasparenza amministrativa (artt. 22 e ss., l. 7 agosto 1990, n. 241, così come modificata dalla l. 11 febbraio 2005, n. 15; art. 2 d.P.R. 12 aprile 2006, n. 184); spetta quindi all'amministrazione destinataria della richiesta di accesso esaminare l'istanza, nonché valutare se sussistano ragioni per le quali il documento può essere sottratto alla conoscibilità del richiedente (*Nota* 17 ottobre 2007).

Anche in caso di differimento dell'accesso, le scelte dell'amministrazione sono sindacabili non dinanzi all'Autorità (il cui ambito di competenza è limitato alla pro-

tezione dei dati personali), ma solo innanzi al tribunale amministrativo regionale, ovvero mediante richiesta di riesame della suddetta determinazione, al difensore civico competente per ambito territoriale (art. 25, legge 7 agosto 1990, n. 241; *Nota* 25 gennaio 2008).

I predetti princìpi sono stati richiamati anche in occasione di una richiesta di intervento nei confronti dell'Autorità per le garanzie nelle comunicazioni, per il silenzio da questa opposto in ordine a una istanza di accesso a taluni documenti amministrativi; in particolare, è stato evidenziato che nei confronti delle autorità di garanzia e di vigilanza il diritto di prendere visione e di estrarre copia di documenti amministrativi si esercita nell'ambito dei rispettivi ordinamenti (artt. 22, 23 e ss., l. n. 7 agosto 1990, n. 241; *Nota* 7 marzo 2008).

Sono state, invece, formulate osservazioni diverse con riferimento alle richieste di accesso agli archivi comunali per effettuare ricerche storiche; in proposito è stato fatto presente che se l'accesso viene effettuato per finalità di studio, indagine, ricerca e documentazione di figure, fatti e circostanze del passato (art. 4, comma 4, lett. *d*), del Codice), per il corretto trattamento dei dati personali raccolti devono essere osservate specifiche disposizioni legislative (artt. 101 e ss. del Codice; d.lg. 29 ottobre 1999, n. 490, modificato dal d.lg. 22 gennaio 2004, n. 42, richiamato dall'art. 103 del Codice), nonché il codice di deontologia e di buona condotta per i trattamenti di dati personali per scopi storici (*Provv.* 14 marzo 2001, in *G.U.* 5 aprile 2001, n. 80, Allegato A.2. al Codice [doc. *web* n. 488272]) (*Nota* 1 febbraio 2008).

In altri casi l'Autorità è stata chiamata a chiarire la differenza intercorrente tra l'esercizio del diritto di accesso alla documentazione amministrativa e il diritto di accesso ai dati personali. In particolare, una persona aveva lamentato il rifiuto opposto da un consultorio familiare alla richiesta di accedere a documenti amministrativi contenenti anche suoi dati personali. A tale proposito è stato ricordato che l'interessato ha diritto di ottenere dal titolare del trattamento la conferma dell'esistenza o meno di dati personali che lo riguardano e la comunicazione in forma intelligibile (art. 7 del Codice). Qualora, sulla base di tale riscontro, risulti che le informazioni sono state raccolte in contrasto con le prescrizioni di legge, ovvero sono inesatte o incomplete, si può chiedere, a seconda dei casi, l'aggiornamento, la rettificazione, l'integrazione o la cancellazione dei dati (artt. 7, 8, 9 e 10 del Codice). In caso di mancata risposta dopo 15 giorni dalla presentazione della richiesta di accesso ai dati personali, è possibile presentare ricorso al Garante secondo le modalità prescritte dagli artt. 145 e ss. del Codice. Alternativamente, ci si può rivolgere all'autorità giudiziaria ordinaria (*Nota* 8 febbraio 2008).

L'Autorità, tenendo conto del rilevante numero di quesiti, richieste di parere, segnalazioni e reclami, pervenuti nel tempo, ha adottato "Linee-guida in materia di trattamento di dati personali per finalità di pubblicazione e diffusione di atti e documenti di enti locali", che indicano le modalità con le quali gli enti locali possono dare pubblicità alla propria attività istituzionale proteggendo i dati personali contenuti in atti e documenti resi accessibili ai cittadini.

I princìpi fondamentali contenuti nelle linee-guida (*Provv.* 19 aprile 2007 [doc. *web* n. 1407101], in *G.U.* 25 maggio 2007, n. 120) si possono sintetizzare nei termini di seguito indicati.

La diffusione di dati personali è legittima solo se è prevista da una norma di legge o di regolamento (artt. 4, comma 1, lett. *m*), e 19, comma 3, del Codice); prima di pubblicare gli atti, renderli accessibili a terzi o metterli in rete, l'ente locale deve valutare se le finalità di trasparenza possano essere perseguite senza divulgarli, o attraverso modalità che permettano di identificare gli interessati solo se necessario (art. 3 del Codice). Negli atti devono comparire solo dati pertinenti e non eccedenti

rispetto alle finalità che l'ente intende raggiungere (art. 11, comma 1, lett. *d*), del Codice). I dati sensibili e giudiziari possono essere diffusi solo se realmente indispensabili (artt. 3, 4, comma 1, lett. *d*) ed *e*), 22, commi 3, 8 e 9, del Codice) e se l'ente abbia adottato –anche in conformità agli schemi tipo sui quali il Garante ha espresso parere favorevole– il regolamento previsto dal Codice sull'uso di questi dati (artt. 20, comma 2, 21 comma 2 e 181, comma 1, lett. *a*), del Codice). É sempre vietato diffondere informazioni sulla salute (artt. 22, comma 8, 65, comma 5 e 68, comma 3 del Codice);

La pubblicazione obbligatoria tramite affissione all'albo pretorio per quindici giorni consecutivi (art. 124 d.lg. 18 agosto 2000, n. 267) di tutte le deliberazioni degli enti locali non autorizzate, di per sé, a trasporre tutte le deliberazioni così pubblicate in una sezione del sito Internet dell'ente liberamente consultabile.

Nell'ambito del regolamento che deve assicurare il diritto dei cittadini all'accesso alle informazioni di cui è in possesso l'amministrazione (art. 10 d.lg. n. 267/2000), l'ente locale può valorizzare anche l'utilizzo di reti civiche e telematiche; non può, invece, rendere inefficaci eventuali limiti, cautele e modalità previsti da norme di settore.

Dopo aver valutato se includere i documenti diffusi in sezioni del sito che li rendano direttamente individuabili in rete a partire anche da motori di ricerca esterni al sito stesso, l'ente deve individuare –con regolamento– periodi di tempo congrui rispetto alle finalità perseguite. Decorsi tali periodi, determinati documenti o sezioni del sito dovrebbero rimanere in rete, ma essere consultabili solo a partire dal sito stesso, senza essere più rintracciabili dai motori di ricerca esterni, per evitare un sacrificio sproporzionato dei diritti degli interessati, specie se si tratta di provvedimenti risalenti nel tempo e che hanno raggiunto le loro finalità. L'ente locale, oltre ad assicurare l'esattezza, l'aggiornamento e la pertinenza e non eccedenza dei dati, deve quindi garantire il rispetto del diritto all'oblìo dell'interessato una volta perseguite le finalità poste alla base del trattamento (art. 11, comma 1, lett. *c*), *d*) ed *e*), del Codice); laddove la finalità da perseguire riguardi prevalentemente solo una o alcune categorie di persone (*ad es.*, concorsi o selezioni pubbliche), andrebbero previste forme di accesso in rete selezionato, attribuendo agli interessati una chiave personale (*username* e *password*; n. di protocollo o altri estremi identificativi di una pratica forniti dall'ente agli aventi diritto);

Agli enti locali sono applicabili anche le disposizioni del Codice che riguardano i trattamenti di dati personali finalizzati alla pubblicazione o alla diffusione occasionale di articoli, saggi o altre manifestazioni del pensiero. É parimenti applicabile il codice di deontologia per l'attività giornalistica (art. 136, comma 1, lett. *c*); (*Provv.* 29 luglio 1998, in *G.U.* n. 179/1998, Allegato A.1. al Codice [doc *web* n. 487496]), nonché il codice deontologico per il trattamenti di dati a scopi storici (artt. 4, comma 4, lett. *a*), 101 e ss. del Codice; d.lg. n. 490/1999, modificato dal d.lg. n. 42/2004, richiamato dall'art. 103 del Codice; *Provv.* del 14 marzo 2001, in *G.U.* n. 80/2001, Allegato A.2. al Codice [doc. *web n.* 488272]).

Specifiche cautele vanno adottate nel pubblicare gli elenchi delle persone che usufruiscono di crediti, sussidi, sovvenzioni o servizi (si pensi all'albo dei beneficiari di provvidenze di natura economica di cui al d.P.R. n. 118/2000; alle graduatorie dei vincitori di concorsi per accedere agli impieghi nelle pubbliche amministrazioni locali; agli asili nido; all'assegnazione di alloggi di edilizia agevolata; alle domande di mobilità); ad esempio, possono essere pubblicati i nominativi e la data di nascita dei beneficiari senza diffondere dati superflui (quali recapiti telefonici, indirizzi, codici fiscali, coordinate bancarie o altri particolari della vita privata che possano esporre l'interessato a conseguenze indesiderate, o creare imbarazzo o disagio), spe-

cie in riferimento a fasce deboli della popolazione (minori di età, anziani, soggetti inseriti in programmi di recupero e di reinserimento sociale).

A seguito dell'adozione delle predette linee-guida, l'Ufficio ha fornito numerosi chiarimenti in ordine alle particolari cautele per tutelare, nei diversi casi, il diritto alla riservatezza dell'interessato.

In particolare, un'amministrazione locale aveva chiesto chiarimenti in ordine alla possibilità di rendere pubblici taluni dati personali pur in assenza di un'espressa autorizzazione da parte degli interessati; l'Ufficio ha sottolineato che i soggetti pubblici possono trattare dati personali soltanto per lo svolgimento delle funzioni istituzionali –nel rispetto dei presupposti e dei limiti stabiliti dal Codice, dalla legge e dai regolamenti– e non sono tenuti ad acquisire il consenso degli interessati, se non a determinate condizioni (art. 18, commi 2, 3 e 4) (*Nota* 14 febbraio 2008).

Un soggetto aveva lamentato l'affissione all'albo pretorio di un avviso di asta di un immobile e la diffusione di tale notizia da parte dei funzionari del comune; è stato fatto presente che se le informazioni riportate nell'avviso di vendita dell'immobile non si configurano quali dati personali –poiché non rendono identificabili, sia pure indirettamente, gli interessati secondo quanto previsto dall'art. 4 comma 1, lett. *b*)– non risultano applicabili al trattamento in questione le disposizioni del Codice, ferma restando la possibilità di ricorrere presso le competenti sedi giudiziarie per il reato di diffamazione di cui all'art. 595 c.p., per chi si ritenga leso nella propria reputazione (*Nota* 15 gennaio 2008).

Il Ministero dell'interno-Dipartimento per gli affari interni e territoriali ha posto la questione dell'utilizzo delle videoconferenze nelle sedute degli organi collegiali degli enti locali, nonché della diffusione delle relative immagini anche tramite l'accesso del pubblico alla postazione corrispondente. In proposito è stato evidenziato che gli artt. 10 e 38 del d.lg. 18 agosto 2000, n. 267 garantiscono espressamente la pubblicità degli atti e delle sedute del consiglio comunale, rinviando a uno specifico regolamento l'introduzione di eventuali limiti a detto regime di pubblicità. Tale regolamento può, dunque, costituire la fonte idonea a disciplinare i limiti e le modalità di pubblicità delle sedute consiliari, ivi compresi eventuali divieti di registrazioni da parte di terzi, nonché l'utilizzo di sistemi di videoconferenza (*Nota* 3 gennaio 2008). Anche in tale ipotesi, si rende necessario da parte del titolare del trattamento osservare le specifiche garanzie individuate nel citato *provvedimento* del Garante del 19 aprile 2007 (doc *web* n. 1407101).

Tra i casi più rilevanti, si registra la richiesta di esame di uno schema di regolamento comunale volto a introdurre l'obbligo, in capo ai consiglieri comunali, agli assessori, al direttore e alle altre figure apicali dei servizi comunali, di dichiarare la loro appartenenza a "persone giuridiche" che abbiano rapporti contrattuali con l'ente medesimo, al fine di pubblicare successivamente le predette informazioni.

Pur evidenziando che l'Autorità è tenuta ad esprimersi solo in relazione alle richieste di consultazione presentate dal Presidente del Consiglio dei ministri e da ciascun ministro in relazione alla predisposizione di norme regolamentari e di atti amministrativi suscettibili di incidere sulle materie disciplinate dal Codice medesimo (art. 154, comma 4, del Codice), è stato rappresentato che l'appartenenza a "persone giuridiche", in taluni casi, può configurarsi quale dato personale di natura sensibile (art. 4, comma 1, lett. *d*), del Codice) (*Nota* 20 marzo 2008).

Fermo restando che il trattamento dei dati sensibili da parte dei soggetti pubblici è consentito solo nei limiti di quanto stabilito dall'art. 20 del Codice, è stato rilevato che il Garante ha ritenuto lecito unicamente l'utilizzo dei dati personali (nonché l'espletamento delle operazioni) individuati nello schema-tipo di regolamento predisposto dall'Anci [doc. *web* n. 1174532] - sul quale l'Autorità si è espressa positiva-

mente il 21 settembre 2005 [doc. *web* n. 1170239]- con la scheda riguardante la gestione dei dati relativi agli organi istituzionali dell'ente, dei difensori civici, nonché dei rappresentanti dell'ente presso enti, aziende e istituzioni. In tale scheda sono stati individuati i tipi di dati sensibili e giudiziari trattabili, e le operazioni su di essi eseguibili, in riferimento alle finalità di rilevante interesse pubblico perseguite, sia di applicazione della disciplina in materia di elettorato attivo e passivo e di esercizio di altri diritti politici, nonché di esercizio del mandato degli organi rappresentativi, designazione e nomina di rappresentanti in commissioni, enti e uffici (art. 65, comma 1, lett. *a*), e 2, lett. *c*) ed *e*), del Codice), sia di accertamento dei requisiti di onorabilità e di professionalità per le nomine, per i profili di competenza del soggetto pubblico, a uffici e a cariche direttive di persone giuridiche (art. 69 del Codice).

Il comune è stato comunque invitato a sottoporre al Garante, per l'espressione di un parere ai sensi dell'art. 20, comma 2, del Codice, eventuali ulteriori tipologie di dati personali che intende trattare, ovvero di operazioni eseguibili, documentandoli adeguatamente sotto il profilo della loro indispensabilità rispetto alla specifica finalità di rilevante interesse pubblico perseguita.

Anche nel corso dell'anno di riferimento sono state numerosissime le richieste di chiarimenti pervenute in ordine al contemperamento delle regole in materia di protezione dei dati personali con il diritto dei consiglieri comunali di accedere a notizie e informazioni in possesso del comune.

Sono stati forniti chiarimenti a un comune sulla condotta tenuta di un consigliere comunale il quale, dopo aver esercitato l'accesso ai dati contenuti nell'anagrafe della popolazione residente, ottenendo l'elenco di cittadini minorenni ricompresi in una determinata fascia di età, aveva successivamente trasmesso tale elenco a una società sportiva. Quest'ultima aveva utilizzato i dati personali in questione inviando ai minori una comunicazione promozionale in ordine all'attività esercitata e pubblicizzando, altresì, la proposta di adesione alla medesima tramite la richiesta di pagamento di una quota associativa. L'Ufficio ha rilevato che, in linea generale, il comune aveva agito correttamente nei confronti della richiesta di accesso formulata dal consigliere comunale ai sensi dell'art. 43 del d.lg. n. 267/2000, in quanto all'ampia e qualificata pretesa non sono opponibili profili di riservatezza, a condizione che i documenti e le informazioni richiesti siano pertinenti all'esercizio del mandato. Non è apparsa invece conforme al quadro normativo di riferimento la trasmissione ad un soggetto privato dei dati anagrafici legittimamente ottenuti, in quanto tale comunicazione non risultava direttamente funzionale alla cura di un interesse connesso al mandato conferito al consigliere comunale (*Nota* 28 novembre 2007).

Un comune si era rivolto all'Autorità chiedendo se un consigliere comunale potesse utilizzare la *mailing-list* dei dipendenti dell'amministrazione medesima per inviare comunicazioni di tipo politico; è stato al riguardo fatto presente che il Garante è intervenuto sull'argomento con l'adozione delle "Linee-guida in materia di trattamento di dati personali di lavoratori per finalità di gestione del rapporto di lavoro in ambito pubblico" (*Provv.* 14 giugno 2007, in *G.U.* 13 luglio 2007, n. 161, [doc. *web* n. 1417809]). In tale *provvedimento* è stato evidenziato, tra l'altro, che determinati dati personali concernenti i dipendenti delle pubbliche amministrazioni sono utilizzabili da terzi (in particolare, gli indirizzi di posta elettronica) solo in relazione ad eventi, comunicazioni e scopi correlati alle funzioni istituzionali e al ruolo ricoperto dall'interessato all'interno dell'amministrazione (*Nota* 19 marzo 2008).

Con riferimento, invece, alla lamentata diffusione di taluni documenti amministrativi da parte di un consigliere comunale, il quale ne aveva fatto richiesta ai sensi dell'art. 43 del d.lg. n. 267/2000, l'Ufficio ha evidenziato la necessità che i dati personali così acquisiti dagli aventi diritto siano utilizzati effettivamente per le sole fina-

lità realmente pertinenti al mandato, rispettando il dovere di segreto nei casi specificamente determinati dalla legge, nonché i divieti di divulgazione dei dati personali (si pensi ad esempio all'art. 22, comma 8, del Codice che vieta la diffusione dei dati idonei a rivelare lo stato di salute) (*Nota* 20 marzo 2008).

Un comune si era rivolto all'Ufficio chiedendo chiarimenti sull'accesso degli assessori comunali agli atti dell'ente; è stato ribadito che la disciplina sull'ordinamento degli enti locali non prevede per gli assessori un diritto di accesso analogo a quello riconosciuto ai consiglieri comunali. Le norme dispongono, invece, che il sindaco e i singoli assessori per gli specifici settori ad essi delegati debbano solo sovrintendere al funzionamento degli uffici e dei servizi, non con atti di diretta gestione, ma con direttive generali. L'ordinamento degli enti locali, infatti, prevede che si applichino le norme sulla distinzione tra le funzioni di indirizzo e controllo politico-amministrativo, che spettano agli organi di governo dell'ente, e quelle di attuazione e gestione amministrativa, che spettano ai dirigenti. Pertanto, solo nel caso il trattamento di dati personali, anche di natura sensibile, sia effettivamente indispensabile all'assessore per espletare la funzione di controllo politico-amministrativo sull'andamento dell'ufficio del personale, l'acquisizione dei dati può risultare conforme alle norme rilevanti in tema di protezione dei dati (art. 67, comma 1, lett. *a*) e *b*), del Codice; *v.* scheda n. 33 dello schema-tipo Anci e il *Parere* del Garante del 7 dicembre 2006, [doc. *web* n. 1370369]). Se invece mancano le ricordate finalità di rilevante interesse pubblico, la comunicazione di questi dati non è legittima e l'accesso da parte dell'assessore non è quindi consentito (*Nota* 11 marzo 2008).

3.4. *La documentazione anagrafica e la materia elettorale*

La disciplina in materia di anagrafe della popolazione residente continua a suscitare interrogativi, in particolare per quanto riguarda le possibilità offerte dall'innovazione tecnologica.

Un'amministrazione aveva interpellato l'Autorità su un progetto con cui, per semplificare e ridurre l'impatto della richiesta di certificati anagrafici da parte di enti pubblici e soggetti privati, si intendeva potenziare il sistema di autocertificazione precompilata *on-line*; è stato fatto presente che la disciplina in materia di protezione dei dati personali non ha modificato espressamente la normativa di settore, in particolare l'ordinamento anagrafico (d.P.R. 30 maggio 1989, n. 223). In linea generale sono state ritenute insussistenti, in base alle disposizioni del Codice, ragioni ostative alla realizzazione dell'iniziativa in questione, fermo restando l'onere dell'amministrazione di valutare la compatibilità del progetto con il quadro normativo di settore (*Nota* 3 gennaio 2008).

Un comune aveva comunicato al Garante, per evitare qualsiasi profilo di responsabilità, l'avvenuto rilascio di dati personali a un soggetto privato ai sensi dell'art. 34 d.P.R. n. 223/1989; è stato evidenziato che la norma in questione non prevede il rilascio di elenchi di dati anagrafici a soggetti privati, ai quali l'ufficiale di anagrafe rilascia dati anagrafici, resi anonimi ed aggregati, unicamente qualora ne sia fatta richiesta per fini statistici e di ricerca (art. 34, comma 2, d.P.R. n. 223/1989 citato). Pertanto, il semplice inoltro al Garante di comunicazioni non esime da eventuali responsabilità; è compito di ogni singola amministrazione verificare la compatibilità della trasmissione di dati personali a soggetti privati con la disciplina di riferimento (*Nota* 8 febbraio 2008).

Un comune aveva interpellato l'Autorità sulla trasmissione all'Agenzia delle entrate di Torino di elenchi dei dati contenuti nell'anagrafe della popolazione resi-

dente; è stato sottolineato che l'ufficiale dell'anagrafe rilascia elenchi di iscritti nell'anagrafe della popolazione residente esclusivamente ad amministrazioni pubbliche che ne facciano motivata richiesta, "per esclusivo uso di pubblica utilità" (art. 34, comma 1, d.P.R. n. 223/1989).

Pertanto, in tale caso, come in ogni altra ipotesi in cui una puntuale disposizione normativa preveda la comunicazione ad altri soggetti pubblici, il comune deve semplicemente applicare in modo corretto la norma di legge o di regolamento che disciplina tale flusso di dati personali, senza effettuare alcuna comunicazione al Garante (art. 19, comma 2, del Codice) (*Nota* 21 febbraio 2008).

In materia elettorale, il Ministero degli affari esteri-Direzione generale per gli italiani all'estero e le politiche migratorie aveva chiesto di conoscere se i dati personali legittimamente detenuti da un candidato ai tempi delle elezioni politiche del 2006, contenuti nelle liste elettorali dei cittadini italiani residenti nella sua circoscrizione, potessero essere utilizzati dal medesimo soggetto per sostenere la candidatura di un altro soggetto a cariche elettive proprie di un ordinamento straniero.

L'Ufficio ha evidenziato che tale elenco provvisorio è soggetto a un particolare regime di conoscibilità, espressamente vincolato dalla disciplina di riferimento al perseguimento di specifiche finalità. Poiché le limitazioni al relativo utilizzo non derivano dalla normativa in materia di protezione dei dati personali, è stato rappresentata al Ministero l'opportunità di valutare se la finalità di carattere politico-elettorale in questione possa essere perseguita mediante l'applicazione della norma in questione ovvero di altre diverse disposizioni di settore in vigore (*Nota* 11 luglio 2007).

Una persona aveva lamentato, invece, il diniego di accesso, opposto dalla commissione elettorale circondariale competente per territorio, a tutta la documentazione riguardante la consultazione elettorale del 27-28 maggio 2007, ivi compresa quella relativa alle sottoscrizioni delle liste elettorali; è stato fatto presente che il trattamento effettuato da parte della commissione elettorale circondariale per l'applicazione della disciplina in materia di elettorato attivo e passivo e di esercizio di altri diritti politici (art. 65 del Codice) risulta lecito nei limiti di quanto espressamente previsto dal regolamento per il trattamento dei dati sensibili e giudiziari del Ministero dell'interno (d.m. 21 giugno 2006, n. 244, in *G.U.* 9 agosto 2006, n. 184-scheda n. 13), sul quale il Garante ha espresso parere favorevole il 28 aprile 2007 [doc. *web* n. 1289890]. Spetta, quindi, all'amministrazione destinataria della richiesta di accesso verificare l'interesse e i motivi sottesi alla relativa istanza di accesso presentata ai sensi della legge 7 agosto 1990, n. 241, anche alla luce dei princìpi di pertinenza, non eccedenza e indispensabilità (artt. 11, comma 1, lett. *d*), e comma 22, comma 5, del Codice) (*Nota* 1 agosto 2007).

3.5. *L'istruzione*

3.5.1. *La scuola*

Nel 2007 l'Autorità ha avuto occasione di chiarire ad alcuni istituti scolastici di aver espresso, in data 26 luglio 2006, parere favorevole sullo schema di regolamento per i trattamenti di dati sensibili e giudiziari effettuati dal Ministero dell'istruzione, dalle istituzioni scolastiche ed educative e dagli istituti regionali di ricerca educativa [doc. *web* n. 1321703]. A seguito di tale parere, il Ministero ha adottato il regolamento (pubblicato in *G.U.* n. 11 del 15 gennaio 2007), al quale gli istituti scolastici devono far riferimento per trattare lecitamente i dati sensibili e giudiziari (*Note* 27 marzo 2007, 11 aprile 2007, 19 aprile 2007).

In merito ad alcuni trattamenti già identificati nel citato schema-tipo di regola-

mento sono stati forniti chiarimenti. In particolare, un genitore aveva lamentato la comunicazione al distretto sanitario competente di dati relativi all'*handicap* della figlia da parte dell'istituto scolastico. Al riguardo è stato chiarito che, in base al citato regolamento, le istituzioni scolastiche, nell'ambito delle attività propedeutiche all'avvio dell'anno scolastico, nonché dell'attività educativa, didattica e formativa e di valutazione, possono trattare i dati idonei a rivelare lo stato di salute per assicurare l'erogazione del sostegno agli alunni diversamente abili e comunicarli "*alle ausl e agli enti locali per il funzionamento dei gruppi di lavoro di istituto per l'handicap e per la predisposizione e la verifica del Piano educativo individuale, ai sensi della legge 5 febbraio 1992, n. 104*". Il trattamento dei predetti dati sensibili deve però rispettare i princìpi generali affermati dal Codice, che consentono ai soggetti pubblici di trattare solo i dati sensibili pertinenti, non eccedenti e indispensabili per svolgere attività istituzionali che non possano essere adempiute, caso per caso, mediante il trattamento di dati anonimi o di natura diversa (*Nota* 21 maggio 2007).

Di rilevante interesse in ambito scolastico è la direttiva 30 novembre 2007, adottata dal Ministero della Pubblica Istruzione con il parere favorevole del Garante [doc. *web* n. 1466996], che contiene linee di indirizzo e chiarimenti sulla normativa vigente a tutela della *privacy*, con particolare riferimento all'utilizzo di telefoni cellulari o di altri dispositivi elettronici nelle comunità scolastiche, per acquisire e/o divulgare immagini, filmati o registrazioni vocali.

Con la direttiva è stato evidenziato che quando i filmati, le immagini o i suoni, relativi ad altre persone, sono acquisiti mediante tali dispositivi per "fini esclusivamente personali", non operano gli obblighi di informativa e di acquisizione del consenso in materia di trattamento dei dati personali. Ciò, tuttavia, a condizione che le informazioni così raccolte non siano destinate ad una comunicazione sistematica o alla diffusione.

Considerato che sempre più di frequente immagini e conversazioni di studenti, docenti e persone che operano all'interno della comunità scolastica vengono, all'insaputa degli interessati, diffuse indebitamente tramite Internet o attraverso scambi reciproci di *Mms*, è stata richiamata l'attenzione sul rischio che una circolazione incontrollata di filmati, registrazioni audio, fotografie digitali possa dar luogo a gravi violazioni del diritto alla riservatezza e alla protezione dei dati personali degli interessati, soprattutto laddove tale circolazione abbia per oggetto informazioni sensibili, come, *ad es.*, quelle relative allo stato di salute, alla vita sessuale, alle convinzioni religiose, politiche e sindacali.

Nella direttiva sono stati, quindi, richiamati gli obblighi di preventiva informativa e di acquisizione del consenso dell'interessato da parte di chi raccoglie e utilizza dati personali mediante telefoni cellulari e altri dispositivi elettronici; è stato altresì posto l'accento sulla possibilità da parte delle istituzioni scolastiche autonome, nei propri regolamenti, di inibire o sottoporre a opportune cautele l'utilizzo di videotelefonini e di *Mms*, all'interno dei locali delle scuole stesse e nelle aule di lezione.

Anche nel settore scolastico, l'Autorità ha ricevuto diverse comunicazioni ai sensi dell'art. 39, comma 1, lett. *a*) del Codice. Più in particolare, un istituto tecnico industriale ha comunicato all'Ufficio di aver richiesto ai dirigenti scolastici delle scuole medie inferiori l'elenco e l'indirizzo degli studenti delle terze classi, al fine di effettuare un'adeguata iniziativa di orientamento per l'iscrizione alla scuola secondaria superiore.

Al riguardo, l'Ufficio, ha ricordato che specifiche disposizioni legislative consentono ai soggetti pubblici, ivi comprese le scuole e gli istituti scolastici di istruzione secondaria, su richiesta degli interessati, di comunicare e diffondere, anche a privati e per via telematica, dati relativi agli esiti scolastici, intermedi e finali, degli studenti e altri dati personali diversi da quelli sensibili o giudiziari, pertinenti "al fine di age-

volare l'orientamento, la formazione e l'inserimento professionale" (*cfr.* art. 96 del Codice); ha poi rappresentato che un'adeguata iniziativa di orientamento può essere svolta utilmente dai singoli istituti anche senza disporre dell'elenco di tutti gli studenti iscritti, bensì con altre modalità, ad esempio mettendo a disposizione degli stessi presso gli istituti scolastici il materiale informativo che illustri le linee distintive dei vari percorsi formativi (*Nota* 26 febbraio 2008).

A una provincia che aveva comunicato all'Ufficio di voler richiedere ai dirigenti scolastici delle scuole secondarie superiori l'elenco dei genitori degli studenti (a fini di verifica e di rendiconto dei finanziamenti elargiti, e più in generale, di assegnazione di borse di studio, contributi in denaro a studenti meritevoli, abbonamenti per trasporto pubblico ad alunni pendolari, nonché di informazione alle famiglie degli studenti sulle attività svolte dalla provincia e sulle modalità iscrizioni alle classi successive all'Università e di orientamento scolastico e professionale) è stato fatto presente che spetta all'amministrazione richiedente verificare se le finalità da porre in essere siano realizzabili sulla base di una specifica richiesta dei soggetti interessati, senza prima costituire una banca dati dei genitori degli studenti (*Nota* 25 marzo 2008).

Un comune aveva trasmesso all'Ufficio, ai sensi dell'art. 39 del Codice, la richiesta di un istituto scolastico relativa ai dati anagrafici dei genitori dei minori stranieri nati in un determinato periodo, per coinvolgere le famiglie immigrate in un progetto nato nell'ambito dell'assegnazione di contributi economici per l'integrazione scolastica e per l'accesso e la frequenza alle scuole dell'infanzia.

Al riguardo, è stato rappresentato che si può prescindere dalla comunicazione al Garante ai sensi dell'art. 39 del Codice in tutti i casi in cui vengono attivati flussi di dati consistenti nel rilascio di elenchi degli iscritti nell'anagrafe della popolazione residente verso le pubbliche amministrazioni che ne facciano motivata richiesta, per esclusivo uso di pubblica utilità. La valutazione in ordine alla sussistenza dei predetti presupposti soggettivi e oggettivi previsti dalla disciplina in materia di anagrafe della popolazione residente spetta all'amministrazione che ha effettuato la citata comunicazione (*Nota* 27 aprile 2007).

Infine, un'azienda sanitaria, aveva comunicato a questa Autorità di voler dar seguito a una richiesta del Dipartimento salute e servizi sociali di una regione, volta a creare un collegamento tra le basi dati relative ai propri assistiti e un sistema informativo integrato che gestisce l'anagrafe degli studenti per prevenire e monitorare il fenomeno dell'abbandono scolastico. L'Ufficio ha fatto presente al riguardo che, per il perseguimento di tali finalità, specifiche norme prevedono che le anagrafi regionali per l'obbligo formativo siano trasformate in anagrafi regionali degli studenti e integrate con le anagrafi comunali della popolazione. E' stato pertanto chiarito che, essendo l'integrazione delle anagrafi espressamente prevista dalla legge, non occorreva effettuare alcuna comunicazione all'Autorità, fermo restando il necessario rispetto dei princìpi di pertinenza e non eccedenza dei dati trattati rispetto alle finalità perseguite (*Nota* 21 giugno 2007).

3.5.2. *L'università*

Con specifico riferimento ai trattamenti effettuati in ambito universitario, si dà conto della comunicazione di un ateneo relativa all'intenzione di diffondere, attraverso una sezione del suo sito *web*, l'elenco dei laureati di taluni corsi con l'indicazione del titolo della tesi e del docente relatore, nonché, su base volontaria, di una scheda sintetica di presentazione del lavoro.

Si è avuto occasione di far presente che specifiche disposizioni contenute nel Codice (*cfr.* art. 100) consentono ai soggetti pubblici, ivi comprese le università e

gli enti di ricerca, di comunicare con autonome determinazioni e diffondere, anche a privati e per via telematica, dati relativi ad attività di studio e di ricerca, a laureati, dottori di ricerca, ricercatori, docenti (con esclusione dei dati sensibili o giudiziari), al fine di promuovere e sostenere la ricerca e la collaborazione in campo scientifico e tecnologico.

L'Autorità, ha ricevuto due comunicazioni da parte di università, ai sensi dell'art. 39 del Codice, aventi per oggetto l'intenzione di fornire ad enti per il diritto allo studio universitario dati relativi a studenti. In particolare, un'università aveva comunicato di voler stipulare una convenzione con l'ente regionale per il diritto allo studio universitario, allo scopo di accedere reciprocamente ai dati personali degli studenti contenuti nei rispettivi archivi; l'altro ateneo aveva manifestato il proposito di fornire all'ente per il diritto allo studio universitario dati anagrafici degli studenti e relativi alla carriera accademica e al versamento di tasse e contributi, per il controllo dei requisiti autocertificati dagli studenti.

In entrambi i casi, è stato evidenziato che le disposizioni in materia di uniformità di trattamento sul diritto agli studi universitari prevedono che gli organismi regionali di gestione e le università, per gli interventi di rispettiva competenza, al fine di controllare la veridicità delle autocertificazioni prodotte dagli studenti per gli aspetti relativi alla condizione economica, possono effettuare controlli a campione che interessino annualmente almeno il venti per cento degli idonei a beneficiare dei servizi e degli interventi non destinati alla generalità degli studenti. Detti controlli possono essere effettuati sia nei confronti degli studenti che nell'anno di riferimento abbiano presentato l'autocertificazione relativa alla condizione economica, sia rispetto a quelli che abbiano mantenuto il diritto al beneficio sulla base dei criteri di merito.

In tale quadro, l'Ufficio del Garante, come già nel 2006 (*cfr. Relazione* 2006, p. 47) ha ricordato che, in virtù dei princìpi di pertinenza e non eccedenza, non dovrebbe essere consentito per tali finalità l'accesso ai dati personali della totalità degli iscritti, potendosi ritenere lecito esclusivamente l'accesso alle informazioni personali dei soggetti che abbiano avanzato una specifica richiesta per usufruire di determinati benefici, in funzione della loro appartenenza a talune fasce di reddito o del possesso di individuati meriti accademici (*Note* 26 febbraio 2008 e 24 ottobre 2008).

3.6. *Notificazioni di atti e comunicazioni*

Notificazioni

Anche nel 2007 il Garante è intervenuto più volte per tutelare la riservatezza delle persone alle quali sono notificati atti giudiziari senza il rispetto delle modalità prescritte dai codici di rito.

Al riguardo l'Autorità ha rammentato che l'art. 174 del Codice ha previsto che, qualora la notificazione non possa essere eseguita nelle mani del destinatario, la copia dell'atto debba essere consegnata in una busta sigillata senza annotazioni dalle quali possa desumersi il contenuto dell'atto stesso.

L'Autorità ha quindi richiamato gli uffici addetti alle notificazioni istituiti presso gli uffici giudiziari al rispetto della normativa in materia.

Fornendo riscontro ad alcune segnalazioni, l'Autorità ha rappresentato che la normativa in materia di protezione dei dati personali non ha modificato l'art. 155 c.p.p., lasciando impregiudicato il potere dell'autorità giudiziaria di ricorrere, ove ne ricorrano i presupposti di legge, alla notifica "per pubblici annunzi", per favorire la conoscenza dei provvedimenti da parte delle persone interessate e l'eventuale esercizio dei diritti correlati (*Nota* 27 marzo 2007). In un altro caso, concernente la notificazione di un decreto tavolare effettuata attraverso la pubblicazione nel Bollettino ufficiale

della Regione, l'Autorità ha ribadito come nel processo civile, ai sensi dell'art. 151 c.p.c., il giudice possa prescrivere particolari forme di notificazione "quando lo consigliano circostanze particolari"; tali circostanze, nel caso segnalato, erano date dal numero estremamente elevato di destinatari della notifica del provvedimento, ossia alcune centinaia di persone (*Nota* 20 giugno 2007).

3.7. *L'attività fiscale, tributaria e doganale*

Il trattamento di dati personali nell'ambito dell'attività fiscale e tributaria è stato oggetto di particolare attenzione dell'Autorità nel corso del 2007.

Sistemi informativi della fiscalità

Oltre all'esame di segnalazioni, reclami e ricorsi in materia e ai pareri resi sui provvedimenti del Direttore dell'Agenzia delle entrate, il Garante ha aperto, in relazione a specifici fatti di cronaca riguardanti accessi abusivi all'Anagrafe tributaria, un'istruttoria preliminare sul sistema informativo della fiscalità dell'amministrazione finanziaria. Una prima fase dell'iniziativa è stata avviata, anche attraverso appositi accertamenti ispettivi, per verificare le misure di sicurezza riferite ai collegamenti da parte di enti esterni all'amministrazione finanziaria.

Audizione del presidente

L'iniziativa è stata resa nota dal presidente dell'Autorità alla Commissione parlamentare di vigilanza sull'anagrafe tributaria in occasione di un'audizione concernente l'indagine conoscitiva sulle modalità di gestione e utilizzo dei dati dell'anagrafe tributaria (6 luglio 2007).

Trasmissione di corrispettivi giornalieri

Con riferimento ai provvedimenti del Direttore dell'Agenzia delle entrate, il Garante ha espresso parere favorevole sullo schema volto a definire le modalità tecniche e i termini sulla base dei quali determinati soggetti che effettuano attività di commercio al minuto devono trasmettere telematicamente all'Agenzia l'ammontare complessivo di determinati corrispettivi giornalieri di cessioni di beni e di prestazioni di servizi. I dati oggetto della comunicazione all'anagrafe tributaria sono ordinati su scala nazionale per valutare la capacità contributiva, e poi trattati per individuare i soggetti che possiedono i requisiti fissati per l'esecuzione dei controlli fiscali e inseriti in una specifica area dedicata dell'anagrafe tributaria, al fine di assicurare la selettività degli accessi (*Parere* 12 aprile 2007 [doc. *web* n. 1402655]).

Garanzie nella comunicazione degli elenchi clienti e fornitori

Il Garante ha collaborato con l'Agenzia delle entrate alla stesura del provvedimento concernente la trasmissione in via telematica dell'elenco dei soggetti nei cui confronti sono state emesse fatture, nonché dell'elenco dei soggetti titolari di partita Iva da cui sono stati effettuati acquisti rilevanti ai fini dell'applicazione dell'imposta sul valore aggiunto.

In particolare, tenuto conto anche di alcune segnalazioni pervenute, per evitare che i dati personali dei clienti, contenuti negli elenchi oggetto di comunicazione da parte di talune categorie di soggetti obbligati (*es.*, medici), siano riferibili, ad esempio, alla specializzazione del professionista e possano quindi rivelare lo stato di salute dei clienti medesimi, è stato previsto che i soggetti obbligati alla comunicazione degli elenchi non indichino la tipologia di attività svolta; soltanto nel corso di un eventuale e successivo procedimento di accertamento verrebbero collegati i codici fiscali dei clienti con la classificazione delle categorie delle attività economiche ("Atecofin"), contenute in altra sezione dell'anagrafe tributaria.

Inoltre, durante la fase di raccolta e di archiviazione, i dati personali contenuti negli elenchi comunicati sono inseriti in un'area dedicata dell'anagrafe tributaria in modo da consentire in via primaria la sola visualizzazione -relativamente a ciascun soggetto obbligato alla trasmissione dell'elenco- di dati riepilogativi privi dei codici fiscali dei clienti. Esclusivamente attraverso un'ulteriore interrogazione possono

essere acquisiti, a cura dei soli soggetti che svolgono le attività relative al procedimento di accertamento, i singoli codici fiscali dei clienti.

Per quanto riguarda, invece, le misure di sicurezza adottate, il Garante ha ribadito l'esigenza di esaminare organicamente, in altra sede e in un contesto più ampio, il necessario incremento dei livelli di sicurezza da garantire a trattamenti di dati quali quelli disposti dal *provvedimento* in esame (*Parere* 26 aprile 2007 [doc. *web* n. 1402616]).

Partecipazione dei comuni all'accertamento fiscale del rispetto del Codice

L'Agenzia delle entrate ha chiesto il parere del Garante su uno schema di provvedimento riguardante le modalità di partecipazione dei comuni all'accertamento fiscale. In primo luogo è stato previsto che i comuni possono trasmettere all'Agenzia i dati anagrafici e il codice fiscale o la partita Iva dei soggetti in relazione ai quali siano rilevati fatti che evidenzino, senza ulteriori elaborazioni logiche, comportamenti evasivi ed elusivi (*cd.* "segnalazioni qualificate"). Le segnalazioni (su commercio e professioni, proprietà edilizie e patrimonio immobiliare, residenze fittizie all'estero, disponibilità di beni indicativi di capacità contributiva) possono riguardare informazioni non sensibili e giudiziarie qualificate, riferibili esclusivamente a situazioni di criticità già opportunamente riscontrate a livello comunale. I dati vengono inseriti all'interno di una specifica area dedicata, per assicurare la selettività degli accessi.

A loro volta i comuni che ne facciano richiesta possono ricevere dall'Agenzia delle entrate dati relativi a bonifici bancari e postali per le ristrutturazioni edilizie, informazioni su utenze (energia elettrica, acqua e gas), denunce di successioni e contratti di locazione di immobili. I comuni, in ossequio ai princìpi di pertinenza e non eccedenza, possono ottenere solo i dati relativi a soggetti fiscalmente domiciliati nel territorio comunale o, comunque, altrimenti collegati al proprio ambito territoriale di competenza.

Lo scambio di dati tra i comuni e l'Agenzia delle entrate avviene tramite il sistema telematico Siatel in modalità *web*, già utilizzato per lo scambio di informazioni tra comuni e anagrafe tributaria. Il Garante, come già rilevato nel *provvedimento* del 26 luglio 2006 [doc. *web* n. 1321668], ha evidenziato l'esigenza di irrobustire, entro un ragionevole lasso di tempo, il sistema di autenticazione degli incaricati di trattamento, e di delimitare temporalmente, e nella localizzazione sulla rete, la possibilità di accesso ai dati, per assicurare più elevati livelli di sicurezza. La delicatezza dei dati trattati e l'esigenza di mantenere una costante idoneità delle misure di sicurezza, rispetto alle potenziali minacce e all'evoluzione tecnologica, impongono infatti all'Agenzia delle entrate di adottare accorgimenti ulteriori, effettivamente idonei, con specifico riferimento ai sistemi di autenticazione e di autorizzazione, parallelamente al cospicuo incremento previsto dei flussi di dati. L'ulteriore incremento di livelli di sicurezza, tenuto anche conto del menzionato intensificarsi dei flussi di dati personali, è oggetto anche della citata istruttoria già avviata sui sistemi informativi della fiscalità (*Parere* 25 luglio 2007 [doc. *web* n. 1428047]).

Comunicazione di dati relativi allo smaltimento dei rifiuti urbani

Il Garante è intervenuto sulla comunicazione all'anagrafe tributaria, a cura dei soggetti che gestiscono (anche in regime di concessione), il servizio di smaltimento dei rifiuti urbani, delle informazioni relative agli immobili insistenti sul territorio comunale per i quali il servizio è istituito, acquisite nell'attività di gestione del servizio medesimo e rilevanti ai fini delle imposte sui redditi. I dati vengono trasmessi attraverso il servizio Entratel e sono trattati utilizzando prevalentemente sistemi di elaborazione ("*data warehouse*") volti ad eseguire analisi selettive per individuare i soggetti che possiedono i requisiti fissati per l'esecuzione dei controlli fiscali.

In proposito il Garante ha rilevato che l'Agenzia, sulla base dell'atto esaminato dal Garante con il *provvedimento* del 25 luglio, dispone già di alcune informazioni idonee a individuare situazioni di criticità derivanti dall'analisi dei dati relativi allo

smaltimento dei rifiuti (le "segnalazioni qualificate" da trasmettere possono riguardare, in particolare, "notifiche di avvisi di accertamento per omessa dichiarazione relativa alla tariffa sui rifiuti in qualità di occupante dell'immobile diverso dal titolare del diritto reale, in assenza di contratti di locazione registrati, ovvero di redditi di fabbricati dichiarati dal titolare del diritto reale ai fini dell'imposizione diretta"). Pertanto, ad avviso dell'Autorità, l'ulteriore trasmissione sistematica e indiscriminata di informazioni relative agli immobili per i quali è istituito il servizio di smaltimento dei rifiuti urbani prevista dallo schema di provvedimento in esame, non risultava né conforme alla norma primaria e giustificata, né, comunque, coordinata con i contenuti del predetto altro schema di provvedimento. L'Agenzia dell'entrate è stata quindi invitata a individuare diversamente le tipologie dei dati da trasmettere in coordinamento con il flusso di informazioni, sottoponendo un nuovo schema all'esame di questa Autorità (*Parere* 4 ottobre 2007 [doc. *web* n. 1457706]).

Sul nuovo schema di provvedimento predisposto dall'Agenzia il Garante ha poi espresso parere favorevole, demandando ad altra sede la verifica organica e in un più ampio contesto, circa l'incremento dei livelli di sicurezza nel trattamento dei dati, nonché del rispetto dei princìpi di pertinenza, non eccedenza e proporzionalità nelle singole categorie di informazioni e nella quantità dei dati nel complesso trattati rispetto alle finalità perseguite dall'Agenzia delle entrate. Le modifiche al provvedimento hanno individuato i dati minimi necessari per l'espletamento dei controlli (identificativi del soggetto che occupa l'immobile e dell' immobile) e disposto che le ulteriori informazioni sul soggetto occupante e sull'immobile vengano acquisite in sede di controllo rispettivamente dall'Anagrafe tributaria e dal sistema informativo dell'Agenzia del territorio. Circa la richiesta del Garante di coordinare il flusso di informazioni richieste con quanto disposto dall'altro *provvedimento* in materia di partecipazione dei comuni all'accertamento, l'Agenzia ha rappresentato che il proprio compito istituzionale è volto garantire, fra l'altro, che l'esplicazione dei controlli su tutto il territorio nazionale sia svolta uniformemente. Secondo l'Agenzia, poiché la partecipazione dei comuni all'accertamento dei tributi erariali attraverso la trasmissione delle *cd.* "segnalazioni qualificate", anche relative alla tariffa rifiuti, non costituisce un adempimento obbligatorio, i controlli potrebbero avere sul territorio nazionale consistenza diversa in relazione all'attività di accertamento svolta dai comuni. Pertanto, ad avviso dell'Agenzia, solo l'invio telematico dei dati in questione è in grado di consentire controlli uniformi su tutto il territorio nazionale effettuando gli incroci necessari al fine di individuare eventuali situazioni di locazioni in nero (*Parere* 6 dicembre 2007 [doc. *web* n. 1470750]).

Diffusione dei dati reddituali dei contribuenti

Il Garante si è occupato della pubblicazione degli elenchi dei contribuenti, confermando quanto evidenziato nei provvedimenti del 17 gennaio 2001 [doc. *web* n. 41031] e del 2 luglio 2003 [doc. *web* n. 1081728], nonché nella *nota* dell'Autorità del 13 ottobre 2000 (*Provv.* 18 ottobre 2007 [doc. *web* n. 1454901]).

L'Autorità ha ribadito che si possono diffondere dati sui contribuenti, individuati e resi disponibili dall'amministrazione finanziaria in base alla legge. Il Codice sulla protezione dei dati personali, infatti, non contrasta con forme di pubblicità di dati che siano di reale interesse pubblico e conformi alle norme di settore. Ai sensi dell'art. 69 del d.P.R. n. 600/1973 spettava all'amministrazione finanziaria il compito di formare e pubblicare annualmente gli elenchi dei contribuenti e individuare quali dati inserirvi. I dati sono consultabili solo dopo tale pubblicazione. Il citato art. 69 costituiva, ai sensi dell'art. 19, comma 3 del Codice, la base giuridica per pubblicare con determinate modalità elenchi dei contribuenti. Infatti, ancorché parzialmente modificato dalla legge n. 431/1991, esso recava una precisa scelta normativa di consultabi-

lità da parte di chiunque di determinate fonti, per favorire la trasparenza in materia di dati raccolti dalla pubblica amministrazione attraverso le dichiarazioni fiscali.

L'intervento del Garante è stato determinato dalla pubblicazione, da parte di due testate giornalistiche, dei dati di reddito relativi all'imponibile Irpef per l'anno 2004 di numerosi professionisti. Nella vicenda esaminata, accogliendo alcuni reclami presentati dall'Ordine dei dottori commercialisti di Bologna e da altri singoli professionisti, il Garante ha tuttavia ritenuto che la diffusione dei dati non era nel caso di specie legittima: era stato infatti il Comune di Bologna a fornire ai quotidiani i dati reddituali dei professionisti bolognesi senza attendere l'annuale formazione degli elenchi dei contribuenti da parte dell'Agenzia delle entrate, e ricavandoli direttamente e autonomamente dal sistema informativo dell'amministrazione finanziaria (sistema Siatel) che il Comune può invece utilizzare per altri scopi, solo "interni". Peraltro, ha sottolineato il Garante, per il 2004 -anno cui si riferisce il caso in esame- l'Agenzia delle entrate aveva reso disponibili i soli nomi dei contribuenti senza l'indicazione dei redditi dichiarati.

Il Garante ha dunque prescritto al Comune di Bologna di trattare i dati acquisiti direttamente dal sistema informativo Siatel solo per le finalità previste dalla legge. I quotidiani che nel caso di specie hanno pubblicato i dati dei contribuenti dovranno, da parte loro, astenersi dall'ulteriore pubblicazione, anche sui loro siti *web*, perché tali dati erano stati comunicati dal Comune in contrasto con le previsioni di legge. Con particolare riferimento all'utilizzo del sistema Siatel da parte dei comuni, il Garante ha inoltre avviato appositi controlli nell'ambito della più ampia attività istruttoria relativa al sistema informativo della fiscalità, anche presso il Comune di Bologna.

Variazioni anagrafiche

Specifici accertamenti sono stati poi avviati in relazione alla tracciabilità delle variazioni anagrafiche all'interno dei sistemi informativi della fiscalità. In particolare, con riferimento alle modifiche sui dati anagrafici che hanno conseguenze sul codice fiscale, il Garante ha chiesto all'Agenzia delle entrate chiarimenti in ordine alle cautele adottabili al fine di evitare che informazioni delicate in materia di anagrafe e di stato civile possano involontariamente emergere dalle generiche consultazioni del sistema informativo della fiscalità (*Nota* 4 maggio 2007).

Scontrino fiscale parlante

Sono pervenute all'Autorità numerose segnalazioni sul trattamento dei dati personali connessi al "scontrino parlante". La nuova disciplina fiscale prevede che lo scontrino fiscale per l'acquisto di farmaci ai fini della detrazione o della deduzione delle spese sanitarie debba indicare, oltre al codice fiscale del destinatario, la natura, qualità e quantità dei medicinali acquistati. L'espressa menzione della denominazione commerciale del farmaco comporta un trattamento sistematico di dati personali sulla salute del contribuente idonei a rivelarne le specifiche patologie. È stata pertanto avviata un'istruttoria preliminare volta a verificare l'indispensabilità dei dati idonei a rivelare le patologie del contribuente rispetto alle finalità perseguite che implicano il trattamento di tali informazioni da parte delle farmacie (attraverso la conservazione a fini contabili di copia dello scontrino), degli intermediari (commercialisti e caf nell'ambito dei controlli sulle dichiarazioni da presentare e della conservazione della documentazione), nonché dell'Agenzia e della Guardia di finanza (in sede di accertamento). Con riferimento al trattamento di tali dati da parte delle farmacie, l'Autorità e Federfarma hanno affrontato congiuntamente, inoltre, talune problematiche derivanti dalla concreta applicazione della predetta nuova disciplina (*Note* 4 e 14 gennaio 2008).

CreditoNet

Sono in corso approfondimenti relativi all'introduzione del servizio CreditoNet da parte del Ministero dell'economia e delle finanze, con particolare riferimento ai presupposti e alle modalità del trattamento, nonché alle tipologie di dati, anche sensibili, resi disponibili dal servizio. Tale servizio, attivo in via sperimentale presso

taluni istituti bancari, è volto a introdurre per i dipendenti pubblici una modalità semplificata per l'attivazione di prestiti da estinguersi con cessione di quote dello stipendio. Sul cedolino viene inserito un codice identificativo –con modalità *random* e diverso per ogni mensilità– che permette all'istituto di credito convenzionato con il ministero di visualizzare, attraverso il servizio CreditoNet, la dichiarazione dimostrativa della retribuzione necessaria ai fini della cessione del quinto dello stipendio (*Nota* 5 luglio 2007).

Agenzia delle dogane

Sono state sottoposte all'attenzione dell'Autorità alcune convenzioni finalizzate a trasmettere a consorzi privati istituiti per legge (Conai e Cobat) dati personali relativi alle caratteristiche di prodotti importati e alle generalità dei rispettivi importatori (imballaggi e batterie al piombo).

Al riguardo, si è fatto presente che, in considerazione della natura privatistica dei consorzi in esame, la comunicazione di dati personali da parte dell'Agenzia, ancorché finalizzata al perseguimento di un interesse pubblico, è ammessa unicamente laddove prevista da una norma di legge o di regolamento (art. 19, comma 3, del Codice) (*Note* 5 luglio 2007 e 30 gennaio 2008).

3.8. *Trattamenti effettuati presso regioni ed enti locali*

Nel 2007 sono state poste all'attenzione dell'Autorità molte questioni relative all'applicazione delle disposizioni in materia di protezione dei dati personali da parte di amministrazioni locali.

A seguito di una segnalazione è emersa la prassi, adottata presso un comune, di allegare alle delibere di giunta comunale, affisse integralmente all'albo pretorio in copia, le schede di valutazione sintetica illustranti situazioni di disagio socio-economico, sanitario e familiare, per erogare contributi assistenziali. In proposito, l'Ufficio ha evidenziato che possono essere trattati solo i dati sensibili indispensabili per svolgere attività istituzionali del comune che non possono essere adempiute, caso per caso, mediante il trattamento di dati anonimi o di dati personali di natura diversa; ciò, rispettando il divieto di diffondere i dati idonei a rivelare lo stato di salute (artt. 22, commi 3 ed 8, e 68, comma 3, del Codice). Sulla base di tale intervento, il comune ha provveduto a non accludere più ai propri provvedimenti pubblicati le schede di valutazione socio-economiche dei beneficiari, inserendo nelle pertinenti deliberazioni esclusivamente dati identificativi dei beneficiari ai fini della liquidazione del contributo concesso (*Nota* 8 maggio 2007).

Sono stati chiesti poi al Garante chiarimenti in ordine alle ipotesi in cui la polizia municipale deve considerarsi esonerata dall'obbligo di fornire l'informativa di cui all'art. 13 del Codice. A tale proposito, si è considerato che l'applicabilità della predetta norma è esclusa limitatamente al trattamento di dati personali effettuato "per finalità di tutela dell'ordine e della sicurezza pubblica, prevenzione, accertamento o repressione dei reati, effettuati in base ad espressa disposizione di legge che preveda specificamente il trattamento" medesimo (art. 53 del Codice); l'Ufficio ha quindi invitato la Polizia municipale a qualificare di volta in volta, nei limiti e in considerazione delle competenze ad essa attribuiti dalla legge, il tipo di attività esercitata, verificando se le finalità perseguite nei singoli casi rientrino tra quelle sopra evidenziate (*Nota* 10 ottobre 2007).

In un altro caso posto è stato lamentato che un'amministrazione comunale, nell'erogare un contributo economico, aveva notificato copia dell'atto in questione, nella quale veniva fatto esplicito riferimento ai dati sensibili del beneficiario, soggetto minore di età, non in mani proprie del destinatario, bensì depositandola nella

cassetta della posta, senza inserirla in busta chiusa e sigillata. A seguito dell'intervento dell'Ufficio, il comune si è impegnato a recapitare i provvedimenti aventi per oggetto dati sensibili o giudiziari con modalità maggiormente rispettose della dignità e della riservatezza degli interessati come, ad esempio, tramite la loro consegna in plico chiuso oppure invitando l'interessato a ritirare personalmente la documentazione presso l'ufficio competente (*Nota* 17 ottobre 2007).

È giunta a conclusione una vicenda riguardante il trattamento di dati personali dei destinatari di verbali di contravvenzione per infrazioni al Codice della strada (d.lg. 30 aprile 1992, n. 285) che, secondo una segnalazione, non veniva effettuato direttamente dal comune quale titolare del trattamento, bensì da una società esterna alla quale era stato affidato il servizio di elaborazione, stampa tipografica e notificazione dei verbali di contestazione. L'intervento dell'Ufficio ha portato l'amministrazione comunale a conformare la configurazione in *outsourcing* del servizio in questione alle disposizioni del Codice. In particolare, il comune ha correttamente designato le società esterne preposte al trattamento dei dati quali responsabili e le persone fisiche autorizzate a compiere operazioni di trattamento dei dati personali quali incaricati ai sensi degli artt. 29 e 30 del Codice (*Nota* 28 novembre 2007).

Ha poi trovato ulteriore definizione la questione riguardante le richieste di rilascio delle banche dati delle utenze di servizi pubblici presentate dai comuni alle relative aziende erogatrici. Interpellato sul punto da un comune, l'Ufficio ha evidenziato che il Garante, il 25 luglio 2007, ha espresso parere favorevole [doc. *web* n. 1428047] sullo schema di provvedimento del Direttore dell'Agenzia delle entrate concernente le modalità di partecipazione dei comuni all'accertamento fiscale ai sensi del citato art. 1, comma 2, del d.l. 30 settembre 2005, n. 203, convertito, con modificazioni, dalla legge 2 dicembre 2005, n. 248. Nel predetto provvedimento, adottato il 3 dicembre 2007 (prot. n. 187461/07; in *G.U.* 17 dicembre 2007, n. 292), è previsto che, entro tre mesi dalla data della sua pubblicazione, l'Agenzia delle entrate renda disponibili ai comuni che ne facciano richiesta i flussi informativi relativi ai contratti di somministrazione di energia elettrica, gas e acqua disponibili in anagrafe tributaria (*Nota* 11 febbraio 2008).

Anche nel corso del 2007 le amministrazioni pubbliche hanno rappresentato al Garante, ai sensi degli artt. 19, comma 2, e 39, comma 1, lett. *a*), del Codice, l'intenzione di comunicare dati personali, diversi da quelli sensibili e giudiziari, ad altri soggetti pubblici per lo svolgimento di funzioni istituzionali, anche in assenza di una norma di legge o di regolamento.

Tra i casi più rilevanti, numerosi comuni, hanno rappresentato l'intenzione di trasmettere a un consorzio generale di bonifica taluni dati personali riguardanti sia i cittadini iscritti nell'anagrafe della popolazione residente, sia i contribuenti iscritti nella banca dati i.c.i. e nella banca dati t.a.r.s.u.. Ciò, al fine di conseguire l'allineamento delle banche dati catastali con la banca dati toponomastica.

Per quanto riguarda la trasmissione dei dati anagrafici, è stato fatto presente che il comune non è tenuto ad effettuare alcuna comunicazione al Garante, dovendo applicare semplicemente in modo corretto la disposizione regolamentare (art. 34, comma 1, d.P.R. n. 223/1989 cit.) che rende ammissibile la comunicazione dei dati ad un altro soggetto pubblico. Con riferimento, invece, alla comunicazione di dati personali estrapolati dalle banche dati dell'i.c.i. e della t.a.r.s.u. al predetto consorzio, in assenza di specifiche disposizioni normative di settore che autorizzino tale flusso di dati, è stato ritenuto possibile effettuare l'operazione in questione laddove il comune medesimo lo reputi realmente necessario all'esplicazione delle rispettive funzioni istituzionali. Ciò, inoltre, sempreché siano rispettati i princìpi di pertinenza e di non eccedenza e non si determini, presso l'amministrazione "ricevente",

un afflusso esuberante di dati rispetto alle finalità perseguite. A tal fine, il comune è stato invitato a individuare puntualmente, nell'ambito delle predette banche dati, i dati personali necessari e strettamente pertinenti al raggiungimento dello scopo istituzionale perseguito (*Nota* 29 novembre 2007).

Sotto un diverso profilo, un comune ha interpellato l'Autorità in ordine alla richiesta avanzata da una provincia di ricevere taluni dati personali dei contribuenti iscritti nella banca dati i.c.i., per completare il *database* per lo svolgimento di funzioni istituzionali in materia di esercizio e manutenzione degli impianti termici. Si è considerato che la normativa di settore stabilisce che, al fine di istituire il relativo catasto o completare quello già esistente, i comuni trasmettono alla provincia e alla regione, anche in via informatica, i dati ottenuti dalle società distributrici di combustibile per il funzionamento degli impianti in questione (art. 17 d.P.R. 21 dicembre 1999, n. 551); pertanto, è stato fatto presente che il comune e la provincia, senza alcuna comunicazione al Garante, devono applicare in modo corretto la predetta disposizione regolamentare che ammette la comunicazione di determinate informazioni a un altro soggetto pubblico (*Nota* 21 dicembre 2007).

3.9. *L'attività giudiziaria*

Pubblicità dei dati nei procedimenti di espropriazione forzata

Nel 2007 sono pervenute al Garante numerose segnalazioni relative al regime di pubblicità nell'ambito dei procedimenti di espropriazione forzata.

Le questioni attenevano all'applicazione della riforma del processo esecutivo (decreto legge 14 marzo 2005, n. 35, convertito, con modificazioni, dalla legge 1 maggio 2005, n. 80) entrata in vigore il 1 marzo 2006, la quale, nel riformulare l'art. 490, comma 2, c.p.c., prevede la pubblicazione in appositi siti Internet di copia dell'ordinanza del giudice che dispone sulla vendita forzata, nonché della relazione di stima dei beni da espropriare. Nei casi segnalati erano stati diffusi nominativi di debitori sottoposti alle procedure esecutive, nonché di eventuali terzi (*ad es.*, dei proprietari di porzioni immobiliari confinanti con l'immobile dell'esecutato).

Con il *provvedimento* del 7 febbraio 2008 [doc. *web* n. 1490838] il Garante, ricordate le modifiche al codice di procedura civile apportate dal Codice, ha rilevato che la prevista consultabilità *on-line* di atti del procedimento esecutivo senza l'omissione delle generalità del debitore vanifica la tutela chiaramente garantita, anche in relazione ad altre forme di pubblicità meno invasive, in altra parte della stessa disposizione (art. 490, comma 3, c.p.c.). Occorre inoltre che nelle copie pubblicate di tali atti non siano riportati i dati personali di soggetti estranei alla procedura esecutiva ove ciò non sia previsto da una specifica norma di legge, trattandosi di informazioni eccedenti e non pertinenti rispetto alle finalità cui è preordinato il procedimento espropriativo. Ciò, al fine di assicurare il rispetto del principio di proporzionalità nel trattamento dei dati posto dall'art. 11, comma 1, lett. *d*), del Codice, applicabile anche in relazione ai trattamenti effettuati per ragioni di giustizia (art. 47 del Codice).

Ai sensi dell'art. 154, comma 1, lett. *c*), del Codice, il Garante ha quindi indicato, agli uffici giudiziari e ai professionisti delegati alle operazioni di vendita di non riportare nelle copie pubblicate delle ordinanze e delle relazioni di stima, oltre che nell'avviso di vendita, le generalità del debitore ed ogni altro dato personale idoneo a rivelare l'identità di quest'ultimo e di eventuali terzi non previsto dalla legge e comunque eccedente e non pertinente rispetto alle procedure di vendita in corso.

L'Autorità ha disposto la pubblicazione del *provvedimento* nella *Gazzetta Ufficiale* e l'invio di copia del medesimo al Ministero della giustizia e al Consiglio superiore della magistratura, anche per favorirne la diffusione presso gli uffici giudiziari interessati.

Dati contenuti in apparecchiature informatiche sottoposte a sequestro penale

L'Ordine dei giornalisti Trentino-Alto Adige e il sindacato dei giornalisti del Trentino-Alto Adige hanno segnalato che nel corso di una perquisizione disposta dalla Procura della Repubblica presso il Tribunale di Trento nelle redazioni dei quotidiani *"L'Adige"* e *"Il Trentino"* era stato acquisito, oltre a materiale in possesso di alcuni giornalisti oggetto di indagine, il contenuto della posta elettronica di tutti gli altri giornalisti in servizio presso i due quotidiani, mediante copia dei dati contenuti nel *server* delle redazioni. I segnalanti hanno lamentato la possibile violazione del segreto professionale dei giornalisti e del diritto alla riservatezza e segretezza della loro corrispondenza.

A seguito della richiesta volta ad acquisire ogni utile elemento di valutazione della vicenda, con particolare riferimento al principio di proporzionalità nel trattamento dei dati (art. 11, comma 1, lett. *d*), del Codice), la Procura della Repubblica di Trento ha comunicato che l'acquisizione di copia dei dati dei giornalisti era resa necessaria per non bloccare l'attività dei due quotidiani, in quanto il *server mail* delle redazioni, per il formato dei dati utilizzati, non permetteva una rapida differenziazione dei messaggi dei singoli utenti. Tale operazione era stata eseguita sulla copia mediante la consulenza tecnica successivamente disposta, nella quale era stato preso in esame solo il contenuto dei messaggi di posta dei giornalisti indagati e, fra questi, solo di quelli ritenuti utili per le indagini, selezionati mediante un'apposita procedura di ricerca.

L'Autorità ha preso atto di tali precisazioni, delle quali ha informato i segnalanti (*Nota* 4 marzo 2008).

Mezzi di prova

È stato chiesto al Garante di verificare eventuali violazioni della disciplina in materia di protezione dei dati personali in tema di ammissione di mezzi di prova nell'ambito dei procedimenti giudiziari, con particolare riferimento all'assunzione di prove testimoniali e alla produzione di documenti ad opera delle parti.

Al riguardo è stato ribadito che il Garante non ha diretta competenza in ordine alla valutazione processuale dell'ammissibilità e rilevanza delle prove in giudizio e alla determinazione all'interno del procedimento giudiziario delle modalità più opportune per procedere alla loro assunzione; anche nell'ipotesi di un trattamento di dati personali ad opera delle parti non conforme a disposizioni di legge o di regolamento, ciò compete al giudice, secondo le pertinenti disposizioni processuali nella materia civile e penale (art. 160, comma 6, del Codice).

4 La sanità

4.1. *Il trattamento di dati idonei a rivelare lo stato di salute*

4.1.1. *I trattamenti per fini amministrativi*

Anche nel corso del 2007 il trattamento dei dati idonei a rivelare lo stato di salute è stato oggetto di numerosi interventi dell'Autorità. In particolare il Garante ha esaminato i trattamenti di dati sanitari effettuati da strutture sanitarie pubbliche per finalità amministrative correlate a quelle di prevenzione, diagnosi, cura e riabilitazione e ha fornito indicazioni in merito a taluni trattamenti già identificati nello schema-tipo di regolamento per i trattamenti dei dati sensibili e giudiziari di competenza delle regioni e delle province autonome, delle aziende sanitarie, degli enti e agenzie regionali/provinciali, nonché degli enti vigilati dalle regioni/province autonome, su cui il Garante ha espresso parere favorevole (*Provv.* 13 aprile 2006 [doc. *web* n. 1272225]).

In particolare, muovendo da una segnalazione con la quale si lamentava che, nell'ambito di un'anamnesi personale effettuata nel corso di un ricovero, sarebbero stati rivolti al paziente anche quesiti volti a conoscere la religione professata e l'eventuale pratica della stessa, è stato chiarito che, in conformità al citato schema-tipo, le aziende sanitarie, nell'ambito dell'attività amministrativa, programmatoria, gestionale e di valutazione relativa alla assistenza in regime di ricovero ospedaliero e domiciliare, possono trattare dati idonei a rivelare le convinzioni religiose al fine di garantire il servizio di assistenza religiosa previsto da norme specifiche soltanto sulla base di una apposita richiesta proveniente dai soggetti interessati. In ogni caso, la raccolta di tali dati può essere effettuata solo previa verifica della loro pertinenza, completezza e indispensabilità rispetto alla finalità perseguita nel singolo caso (*Nota* 17 gennaio 2008).

Con riferimento ai flussi di dati tra amministrazioni pubbliche, una regione ha inoltrato all'Ufficio, ai sensi dell'art. 39 del Codice, la richiesta avanzata da ordini provinciali dei medici i quali, per finalità connesse all'esercizio della potestà disciplinare, hanno chiesto alle aziende sanitarie dati personali relativi ad accertamenti svolti sulla base di esposti presentati da cittadini alle aziende sanitarie in ordine ad un presunto disservizio del Ssn.

Al riguardo, è stata ritenuta lecita, in virtù dei princìpi di pertinenza e non eccedenza dei dati trattati rispetto alle finalità perseguite, esclusivamente la comunicazione delle informazioni personali inerenti lo specifico esposto presentato, individuate selettivamente, al fine di non determinare presso le amministrazioni richiedenti un afflusso esuberante di dati personali rispetto alle finalità dalle stesse perseguite.

L'amministrazione regionale è stata pertanto invitata a fornire indicazioni alle aziende sanitarie in ordine alla necessità di uniformare il trattamento di dati personali in questione ai ricordati princìpi di pertinenza e non eccedenza (*Nota* 24 ottobre 2007).

In relazione a una comunicazione pervenuta ai sensi dell'art. 39 del Codice, l'Ufficio ha ritenuto ammissibile la trasmissione, all'azienda sanitaria che ne aveva fatto richiesta, dei dati relativi alle imprese che avevano ospitato disabili con borse di

studio assegnate dalla provincia nell'ambito di un progetto di formazione professionale. Ciò, allo scopo di consentire all'azienda di espletare le proprie funzioni istituzionali in materia di prevenzione e sicurezza nei luoghi di lavoro (artt. *7-bis ss.* d.lg. 30 dicembre 1992, n. 502). La liceità di tale comunicazione è stata condizionata alla trasmissione delle sole informazioni pertinenti al raggiungimento delle finalità istituzionali perseguite dall'azienda sanitaria ricevente (artt. 11 e 19, comma 2, del Codice), vale a dire ai soli dati identificativi delle imprese e con l'esclusione di informazioni anagrafiche riferite ai soggetti beneficiari. Quest'ultima categoria di dati esula dall'ambito di applicazione della speciale disciplina prevista dall'art. 39 del Codice, applicabile esclusivamente alle comunicazioni tra soggetti pubblici di dati personali, diversi da quelli sensibili, non previste da alcuna disposizione legislativa o regolamentare (*Nota* 10 aprile 2007).

L'Autorità si è poi occupata del trattamento dei dati sanitari di pazienti per l'accesso dei medici nelle zone a traffico limitato (ztl). Con un *provvedimento* generale adottato il 14 giugno 2007, il Garante ha individuato un quadro di garanzie per i pazienti visitati nelle zone a traffico limitato nel rispetto delle disposizioni in tema di limitazione del traffico veicolare da parte dei medici che effettuano visite domiciliari nelle zone ztl [doc. *web* n. 1424100].

Nel corso dell'istruttoria, avviata a seguito di segnalazioni pervenute all'Autorità, è emersa una doppia esigenza: consentire alla categoria dei medici l'esercizio della propria attività di urgenza senza subire sanzioni e, nel contempo, garantire il diritto del paziente residente in una ztl a non subire violazioni della propria riservatezza. In particolare, era stato chiesto di valutare se le procedure adottate da alcuni comuni per verificare il rispetto delle norme di circolazione dei veicoli all'interno delle ztl (acquisizione, per ogni accesso del medico, dei dati anagrafici del paziente, del luogo e ora della visita, del codice regionale o di una dichiarazione della stessa persona visitata) fossero compatibili con le norme sulla protezione dei dati personali, e se fosse inoltre corretta la prassi di alcuni uffici territoriali di governo di chiedere un'analoga documentazione per l'accoglimento dei ricorsi presentati dai medici contro le multe.

Nel definire le segnalazioni pervenute, il Garante ha ravvisato come non indispensabili i dati richiesti dai comuni ai medici, ritenendo che l'accertamento delle violazioni per l'accesso alla ztl possa essere perseguito attraverso altre modalità, parimenti efficaci, ma rispettose del diritto alla protezione dei dati personali, quali, ad esempio, la comunicazione dell'indirizzo e del numero civico presso il quale è stato prestato l'intervento, la targa del veicolo del medico che ha effettuato la visita, la data e la fascia oraria di accesso e di uscita dall'area, il numero di iscrizione all'ordine professionale.

L'Autorità ha pertanto prescritto ai comuni, nell'ambito dell'attività di verifica del rispetto delle disposizioni in materia di accesso e circolazione veicolare, di non richiedere ai medici generalità o altre informazioni che identifichino le persone visitate a domicilio all'interno di aree ztl, e ai medici di non presentare documenti contenenti dati personali dei pazienti per la contestazione delle multe. Il Garante ha inoltre stabilito che, in caso di ricorso, gli uffici territoriali di governo non possono sollecitare la produzione di documenti contenenti generalità o altre informazioni delle persone visitate in grado di rilevare le condizioni di salute, poiché in tali circostanze è prevalente il diritto alla riservatezza dei pazienti.

Sotto altro profilo, l'Autorità è stata chiamata a valutare la liceità dell'affissione del referto medico legale sul vetro esterno del portone d'ingresso dello stabile del dipendente risultato assente alla visita di controllo.

In particolare, è stato evidenziato che la dicitura "ammalato dal ...", contenuta nel referto medico legale, costituisce un dato idoneo a rivelare lo stato di salute del soggetto cui tali dati si riferiscono, per il quale il Codice prevede una specifica tutela

tra cui il divieto di diffusione (artt. 22, comma 8 e 68, comma 3, del Codice).

Pertanto, non è risultata conforme alla disciplina in materia di protezione dei dati personali la condotta posta in essere da un'azienda sanitaria titolare del trattamento esaminato, che è stata invitata, per il futuro, ad utilizzare modalità di consegna del predetto referto idonee ad assicurare il rispetto dei diritti, delle libertà fondamentali e della dignità del dipendente destinatario della visita di controllo, qualora lo stesso risulti assente (*Nota* 25 marzo 2008).

Accesso dell'adottato alle proprie origini biologiche

L'Ufficio ha avuto occasione di pronunciarsi sul tema della conoscibilità da parte dell'adottato di informazioni relative alle proprie origini biologiche in un caso in cui un ospedale riteneva di non poter accogliere l'istanza di accesso di una persona adottata al registro dei ricoveri relativo al periodo della sua nascita, senza fargli conoscere dati sanitari riferiti anche a persone estranee alla vicenda. Ciò, sebbene l'interessato avesse ottenuto da un tribunale per i minorenni, prima dell'entrata in vigore del Codice, l'autorizzazione a conoscere i dati relativi all'identità personale della madre naturale e le altre informazioni sanitarie indispensabili per la cura della sua malattia (*Nota* 26 aprile 2007).

Al riguardo l'Ufficio, nel precisare che il tema continua a trovare una specifica disciplina nelle disposizioni vigenti in materia di stato civile, adozione e affidamento (d.lg. 30 giugno 2003, n. 196; *v.* anche artt. 400 *ss.* c.c.; legge 4 maggio 1983, n. 184; d.P.R. 3 novembre 2000, n. 396), ha sollecitato l'ospedale ad adottare ogni soluzione idonea a contemperare la legittima richiesta dell'interessato, volta a conoscere informazioni sanitarie indispensabili per la cura della sua malattia, anche in relazione alla decisione a suo tempo adottata dall'autorità giudiziaria, e la tutela dei diritti di terzi.

Nel caso di specie è stato peraltro osservato che, in base all'ordinamento dello stato civile vigente all'epoca della nascita dell'interessato, la dichiarazione di nascita era resa solo previa esibizione di un apposito certificato sanitario di assistenza contenente alcune indicazioni utilizzabili ai fini dell'individuazione della madre naturale del richiedente quali, il medico o l'ostetrica che ha assistito al parto (artt. 18, comma 2, r.d.l. 15 ottobre 1936, n. 2128 e 70, r.d. 9 luglio 1939, n. 1238 del testo allora vigente).

In tale quadro l'ospedale, al fine di dare esecuzione al provvedimento dell'autorità giudiziaria, avrebbe quindi potuto opportunamente curare direttamente -anche presso l'ufficiale dello stato civile- lo svolgimento di opportune indagini miranti a individuare la madre naturale del richiedente e la relativa documentazione sanitaria, consentendo all'interessato di conoscere i soli dati attinenti allo stato di salute della madre essenziali per la cura della sua malattia.

4.1.2. *Il trattamento di dati personali in occasione dell'accertamento dell'infezione da Hiv*

Nel corso dell'anno l'Autorità è stata nuovamente interpellata in ordine al trattamento di dati personali di una paziente da parte di un ambulatorio di malattie infettive in occasione dell'accertamento dell'infezione da Hiv.

Al riguardo, si è ribadito un principio più volte affermato ovvero che la legge 5 giugno 1990, n. 135 in tema di Aids e Hiv prevede espressamente l'obbligo di comunicare i risultati di accertamenti diagnostici diretti o indiretti per l'infezione da Hiv alla sola persona cui tali dati si riferiscono e che il Codice non contiene deroghe alle disposizioni di legge che stabiliscono divieti o limiti più restrittivi in materia di trattamento di taluni dati personali.

È stato, pertanto, ritenuto che questa normativa rappresenti un limite speciale da tenere presente e faccia parte dei divieti e limiti più restrittivi in materia di protezione di taluni dati personali richiamati anche nell'*autorizzazione generale* al trattamento dei dati idonei a rivelare lo stato di salute e la vita sessuale, rilasciata dal

Garante (*autorizzazione* n. 2/2005 [doc. *web.* n. 1203946]). Per la comunicazione ai familiari dello stato di sieropositività del paziente non si può quindi prescindere dal suo consenso e l'Autorità non dispone del potere di autorizzare, in deroga alla citata disciplina speciale, la comunicazione non consensuale della notizia della sieropositività del paziente vivente.

In tale quadro, è stata ritenuta tuttavia legittima la valutazione di opportunità effettuabile dal medico in merito alla sensibilizzazione della persona sieropositiva e all'eventuale persuasione a comunicare al *partner* la propria sieropositività oppure a manifestare il proprio consenso alla rivelazione da parte dello stesso medico. (*Nota* 16 maggio 2007).

Le tematiche connesse al trattamento di dati personali relativi allo stato di sieropositività o all'infezione da Hiv, nonché ad altre patologie invalidanti, sono state oggetto di un *provvedimento* collegiale con il quale l'Autorità ha prescritto alle aziende sanitarie locali alcune misure necessarie per conformarsi alle disposizioni in materia di protezione dei dati personali.

In particolare, alcuni invalidi civili avevano segnalato al Garante che sia nelle istanze per l'accertamento sanitario dell'invalidità civile, sia in alcuni tipi di certificazioni che attestano il riconoscimento della invalidità per finalità amministrative veniva indicata la diagnosi ed avevano, quindi, richiesto che fossero omessi da alcune certificazioni i riferimenti personali alle patologie invalidanti, specie quelli relativi allo stato di sieropositività o l'infezione da Hiv.

Muovendo da tali segnalazioni, l'Autorità ha avviato una complessa istruttoria all'esito della quale ha adottato un *provvedimento* nel quale ha ricostruito il quadro di riferimento normativo in tema di riconoscimento dell'invalidità civile; ha quindi precisato che la normativa di settore prevede espressamente che i verbali redatti dalle apposite commissioni mediche menzionino con chiarezza e precisione la diagnosi, indispensabile anche ai fini dell'eventuale revisione dell'invalidità o di ricorso alla decisione della commissione medica. Non è stato invece ritenuto giustificato indicare gli stessi dati nelle certificazioni per l'iscrizione nelle liste del collocamento obbligatorio o per l'esenzione dalle tasse scolastiche e universitarie a favore dei mutilati e degli invalidi civili. Ciò, non solo in quanto, in conformità alla normativa di settore e in applicazione dei princìpi di pertinenza, non eccedenza ed indispensabilità, l'indicazione di tali dati non risulta necessaria, ma anche in quanto specifiche disposizioni normative prevedono tutele rafforzate per particolari patologie (*cfr.* l. 5 giugno 1990, n. 135). Sono infatti risultati quali requisiti per l'esenzione dalle tasse scolastiche e universitarie l'appartenenza a famiglie di disagiata condizione economica e l'avere subito una diminuzione superiore ai due terzi della capacità lavorativa, mentre per l'iscrizione alle liste del collocamento obbligatorio è prevista solo una accertata diminuzione della capacità lavorativa superiore al quarantacinque per cento.

Pertanto, il Garante ha prescritto alle aziende sanitarie locali di non indicare la diagnosi sui certificati che attestano il riconoscimento dell'invalidità civile per l'iscrizione alle liste del collocamento obbligatorio o per la richiesta di esenzione da tasse scolastiche o universitarie e di adottare gli accorgimenti necessari, quali distanze di cortesia, spazi per colloqui riservati, consegna e trasferimento della documentazione in busta chiusa, e di impartire precise istruzioni al personale sanitario per garantire un elevato livello di tutela della riservatezza delle persone (*Provv.* 21 marzo 2007 [doc. *web* n. 1395821]).

4.1.3. *Le strutture sanitarie e la tutela della dignità delle persone*

Anche nel corso del 2007 l'Autorità ha ribadito agli organismi sanitari pubblici e privati la necessaria adozione di idonei accorgimenti per garantire, nell'organizza-

zione delle prestazioni e dei servizi, il rispetto dei diritti, delle libertà fondamentali e della dignità degli interessati, in attuazione delle misure prescritte dal Codice e in conformità allo specifico *provvedimento* generale adottato dal Garante nel 2005 (*Provv.* 9 novembre 2005 [doc. *web* n. 1191411]).

In particolare, è stato ricordato ad alcune strutture sanitarie che esse, nell'erogare prestazioni sanitarie o nell'espletare adempimenti amministrativi che richiedono un periodo di attesa, sono tenute ad adottare soluzioni che prevedano un ordine di precedenza e di chiamata degli interessati diverso dalla loro individuazione nominativa (*ad es.* attribuendo loro un codice numerico o alfanumerico fornito al momento della prenotazione o dell'accettazione), nonché a predisporre apposite distanze di cortesia, in tutti i casi in cui si effettua il trattamento di dati sanitari (*ad es.* operazioni di sportello, acquisizione di informazioni sullo stato di salute); ciò, nel rispetto dei canoni di confidenzialità e della riservatezza dell'interessato, sensibilizzando in questa prospettiva gli utenti con idonei inviti, segnali o cartelli (*Nota* 8 maggio 2007).

Sotto altro profilo, sulla base di segnalazioni in cui si lamentava la mancanza di riservatezza nell'effettuare ecografie e particolari visite mediche, l'Ufficio ha richiamato l'attenzione di un centro diagnostico sulla necessità che la prestazione medica e ogni operazione di trattamento dei dati personali avvenga nel pieno rispetto della dignità dell'interessato e sul particolare riguardo che, in tal senso, deve essere prestato nei confronti di pazienti sottoposti a trattamenti medici invasivi (*Note* 12 giugno 2007 e 9 ottobre 2007).

La segnalazione di un paziente ha fornito l'occasione per riaffermare che il Codice incentiva le strutture sanitarie a prevedere, in conformità agli ordinamenti interni, le modalità per fornire ai terzi legittimati informazioni circa la dislocazione dei degenti nei reparti, ove si debba ad esempio rispondere a richieste di familiari e parenti, conoscenti e personale del volontariato. In tale circostanza, è stato altresì ribadito che l'interessato cosciente e capace deve essere, anche in questo caso, informato e posto in condizione (*ad es.* all'atto del ricovero) di dare indicazioni circa i soggetti che possono venire a conoscenza del ricovero e del reparto di degenza. Informazioni sullo stato di salute possono essere fornite a soggetti diversi dall'interessato quando sia stato manifestato un consenso specifico e distinto al riguardo, consenso che, in caso di impossibilità fisica, incapacità di agire o incapacità di intendere o di volere dell'interessato, può essere anche espresso da un altro soggetto legittimato.

È stato inoltre fatto presente che, fermi restando in quanto applicabili gli obblighi in materia di segreto d'ufficio, al pari del personale medico e infermieristico già tenuto al segreto professionale, gli altri soggetti non tenuti per legge al segreto professionale (*ad es.*, personale tecnico e ausiliario) devono essere sottoposti a regole di condotta analoghe e l'organismo sanitario, anche avvalendosi di iniziative di formazione del personale designato, deve adottare le necessarie misure organizzative, con riferimento, tra l'altro, ai rischi di accesso non autorizzato ai dati sanitari (*Nota* 26 luglio 2007).

L'Ufficio è anche intervenuto per richiamare le garanzie previste dalla legge a tutela della dignità e della riservatezza delle persone in occasione dei colloqui con i parenti dei pazienti, facendo presente che è doveroso adottare idonee cautele in tali circostanze, specie quando si conferisce con il personale sanitario, per evitare che le informazioni sulla salute dell'interessato possano essere conosciute da terzi (*Nota* 12 febbraio 2008).

Consegna di referti per il *test* Hiv

Si segnala infine che un ospedale, a seguito dell'intervento dell'Ufficio, ha modificato le procedure relative alla consegna dei referti relativi al *test* per l'Hiv sostituendo il registro nominativo da far sottoscrivere agli interessati all'atto del ritiro del referto con una scheda individuale da utilizzare per ciascun paziente (*Nota* 19 marzo 2008).

5 I dati genetici

Si è riferito nella *Relazione* 2006 (*p.* 64) dell'*autorizzazione generale* al trattamento di dati genetici rilasciata il 22 febbraio 2007 (in *G.U.* 19 marzo 2007, n. 65 [doc. *web* n. 1389918]).

La particolare delicatezza della materia, oggetto anche dei lavori della 29° Conferenza internazionale delle autorità garanti svoltasi a Montreal dal 25 al 28 settembre 2008 (*v. par.* 21.4.) e la rilevanza delle sue implicazioni richiedono, però, un'aggiornata sintesi del quadro normativo e un'attenta valutazione della casistica.

In tal senso si è già dato conto (*v. par.* 1) della segnalazione rivolta al Parlamento e al Governo relativa ad iniziative legislative per la creazione di banche dati del Dna a fini di giustizia [doc. *web* n. 1456163], nonché del parere alla Presidenza del Consiglio dei ministri relativo all'istituzione di una banca dati nazionale del Dna [doc. *web* n. 1448799].

Da questi atti emerge la costante attenzione dell'Autorità volta a contemperare l'esigenza di potenziare le tecniche di indagine ai fini di giustizia e di cooperazione sul piano internazionale con la tutela dei diritti e delle libertà fondamentali delle persone.

In particolare, anche in relazione a quanto previsto dal Trattato di Prüm, un accordo internazionale sulla cooperazione di polizia firmato da Belgio, Germania, Spagna, Francia, Lussemburgo, Paesi Bassi e Austria il 27 maggio 2005, diventato ora parte del quadro legislativo dell'Unione europea, il Garante ha individuato alcuni profili tematici che una normativa adeguata dovrebbe prendere in esame: tra gli altri, l'individuazione delle finalità da perseguire e il rispetto delle competenze istituzionali; l'individuazione dei presupposti per la registrazione delle informazioni sul Dna, nonché le modalità e i tempi di conservazione di profili e campioni biologici; la rigorosa regolamentazione degli accessi degli operatori alla banca dati, delle misure di sicurezza e delle garanzie in caso di prelievi del Dna obbligatori per legge (*cfr.* in particolare [doc. *web* n. 1456163]).

Nel corso dell'anno è stato oggetto di accertamenti del Garante presso il Ris di Parma il trattamento di dati genetici acquisiti nel corso di indagini di polizia e sul loro successivo utilizzo a fini giudiziari (*v. par.* 7.2.).

Si segnala inoltre la decisione di inammissibilità di un ricorso nella quale l'Autorità ha ritenuto che la richiesta avanzata dalla ricorrente a un ospedale di Roma avente ad oggetto il prelievo e la consegna di un campione biologico del padre non fosse nel caso di specie relativa ad un dato personale di tipo genetico dell'interessata (*Provv.* 21 giugno 2007 [doc. *web* n. 1433975]; *v. par.* 17). La decisione è in linea con gli orientamenti del Gruppo art. 29 in base ai quali non costituisce, di per sé, dato personale il campione biologico dal quale si estraggono dati biometrici (*v. par.* 20.1.).

6 La ricerca statistica, storica e scientifica

6.1. *La ricerca statistica e storica*

Il Garante, su richiesta dell'Istituto nazionale di statistica, ha espresso nel mese di novembre il proprio parere sul Programma statistico nazionale (Psn) 2008-2010 (*Parere* 15 novembre 2007 [doc. *web* n. 1464806]). In tale occasione l'Istituto ha ribadito il proprio impegno ad attuare la normativa sulla protezione dei dati personali nell'ambito del Sistema statistico nazionale, sottolineando di aver modificato il Programma statistico per gli anni 2007-2009 in conformità alle indicazioni fornite dal Garante con il precedente parere.

Per quanto riguarda il Psn 2008-2010, l'Istituto ha evidenziato in particolare di aver intensificato i controlli volti a individuare la natura dei dati trattati e inserito un nuovo paragrafo sulla comunicazione di dati sensibili e giudiziari all'interno del Sistan.

Il Garante, come già espresso in precedenti pareri, ha ribadito che l'obbligo di fornire tutti i dati richiesti per le rilevazioni previste dal Psn non può riguardare i dati sensibili e giudiziari, neppure quando non siano raccolti presso gli interessati. Occorre quindi rispettare in ogni caso l'eventuale volontà dell'interessato di non aderire alla ricerca; ciò, anche attraverso un'idonea informativa al momento della raccolta, specie quando questa sia effettuata originariamente per scopi diversi da quelli statistici, ovvero prima della comunicazione dei dati al titolare della ricerca, con particolare riguardo ai trattamenti volti a costituire registri di patologia (salvo che tale operazione sia prevista da specifiche disposizioni normative).

L'Autorità ha inoltre invitato l'Istituto a utilizzare specifici accorgimenti al momento della raccolta in modo che, in relazione a particolari domande su temi attinenti ad aspetti intimi o comunque strettamente privati (emergano o meno dati sensibili), sia possibile fornire una risposta con modalità che non creino imbarazzo agli interessati.

In alcune schede informative contenute nel Programma sono risultate mancanti le informazioni necessarie per l'espressione del parere; non può al riguardo ritenersi assolto l'obbligo di informativa attraverso l'inclusione del trattamento nel Psn (art. 6, comma 2, del codice di deontologia e buona condotta per i trattamenti di dati a scopi statistici e di ricerca scientifica effettuati nell'ambito del Sistema statistico nazionale, Allegato A.3. al Codice [doc. *web* n. 488371]); l'informativa dovrà pertanto essere resa con altre idonee modalità e i trattamenti di dati sensibili e giudiziari potranno essere eventualmente effettuati solo dopo l'acquisizione del parere del Garante sulle schede, che è condizione di liceità e correttezza del trattamento.

Il Garante ha inoltre richiamato l'esigenza di definire correttamente le tipologie dei dati trattati nella compilazione delle schede informative, soprattutto per quanto riguarda quelli sensibili e giudiziari.

Gran parte dei progetti contenuti nel Programma continuano a derogare agli obblighi generali di rendere anonimi i dati dopo la raccolta e di individuare precise cautele per l'eventuale conservazione di dati identificativi. L'Autorità ha quindi evidenziato che, per alcune rilevazioni, i dati personali devono essere resi anonimi subito dopo la raccolta.

In relazione a una specifica richiesta dell'Istat, ha altresì ribadito che gli eventuali trattamenti di dati personali indicati all'art. 37, comma 1, del Codice, devono essere

notificati al Garante anteriormente all'inizio del trattamento, pena l'applicazione della prevista sanzione amministrativa.

Il programma statistico regionale

In relazione ai trattamenti effettuati per scopi di ricerca statistica da parte delle Regioni, il Garante ha espresso il parere sul Programma statistico regionale (Psr) 2006-2008 della Regione Toscana, (*Parere* del 25 luglio 2007 [doc. *web* n. 1428057]) dopo aver acquisito anche le valutazioni di competenza della Commissione per la garanzia dell'informazione statistica istituita ai sensi dell'art. 12 del d. lg. 6 settembre 1989, n. 322.

Va ricordato al riguardo che gli uffici di statistica delle regioni, quali soggetti appartenenti al Sistema statistico nazionale, possono trattare dati sensibili e giudiziari per scopi statistici in conformità al Programma statistico regionale (*Provv.* 13 aprile 2006 [doc. *web* n. 1272225]). Tale Programma, o un altro documento regionale programmatico, da adottarsi sentito il Garante, deve individuare i tipi di dati sensibili o giudiziari trattati, le rilevazioni per le quali i predetti dati sono trattati e le modalità di trattamento.

La Regione Toscana ha dichiarato di aver preso in considerazione le osservazioni e le indicazioni contenute nel parere espresso dal Garante sul Programma statistico nazionale (Psn) 2007-2009.

Il Garante ha osservato che il parere è espresso esclusivamente sui trattamenti di dati sensibili e giudiziari specificamente contemplati, non compresi nel Psn 2007-2009. Inoltre, affinché sia applicabile il codice deontologico per i trattamenti di dati personali a scopi statistici e di ricerca scientifica effettuati nell'ambito del Sistema statistico nazionale, è necessario che tutte le rilevazioni ed elaborazioni contenute nel Programma siano effettuate dall'Ufficio di statistica.

L'Autorità ha richiesto alla Regione che i soggetti, responsabili e incaricati, cui sono affidate le fasi di rilevazione ed elaborazione possiedano i requisiti di esperienza, capacità ed affidabilità necessari a garantire il pieno rispetto della normativa in materia di protezione di dati personali in ambito statistico.

Per la liceità dei trattamenti è in ogni caso necessario assicurare in concreto il rispetto dell'eventuale volontà dell'interessato di non aderire alla ricerca statistica, anche quando i dati siano raccolti presso terzi, ovvero per scopi in origine diversi; ciò, anche attraverso un'idonea informativa da rendere al momento della raccolta dei dati presso l'interessato, ovvero prima dell'utilizzo dei dati nell'ambito della ricerca statistica. L'Autorità ha infine richiesto che nelle schede di rilevazione, nel rispetto del principio di indispensabilità di cui all'art. 22 del Codice vengano indicate, se del caso, le comprovate esigenze da cui emerga l'impossibilità di rendere anonimi i dati dopo la raccolta.

L'Osservatorio sullo sfruttamento e abuso sessuale dei minori

L'Autorità ha proseguito la collaborazione con gli uffici del Ministro delle politiche della famiglia con riferimento all'Osservatorio per il contrasto della pedofilia e della pornografia minorile istituito presso la Presidenza del Consiglio dei ministri, al fine di garantire il puntuale rispetto della normativa in materia di dati personali nel monitoraggio del fenomeno, riducendo al minimo il trattamento di dati personali volto al raggiungimento delle finalità affidate dalla legge all'Osservatorio (*Parere* 25 luglio 2007 [doc. *web* n. 1436237]).

Ricerca storica - Archivi di Bad Arolsen

Nel 2007 si è consolidato il processo di apertura a fini di ricerca degli archivi di Bad Arolsen (Repubblica federale tedesca) che contengono documentazione relativa ai deportati nei campi di concentramento nazionalsocialisti, disponibile, in base ai Protocolli del 2006 di modifica degli Accordi internazionali di Bonn del 1955, anche per scopi di ricerca (mentre in precedenza era accessibile solo ai parenti delle persone deportate e detenute [*v. Relazione* 2006, *p.* 69]).

L'accesso per fini di ricerca è disciplinato dal regolamento approvato ad Amsterdam il 14 e il 15 maggio 2007 nella riunione annuale della Commissione

internazionale per il Servizio internazionale delle ricerche (Ic Its) composta dagli undici Stati firmatari (Belgio, Francia, Germania, Grecia, Israele, Italia, Lussemburgo, Polonia, Olanda, Regno Unito, Stati Uniti d'America oltre al Comitato Internazionale della Croce Rossa), cui ha partecipato, nell'ambito della delegazione italiana, anche l'Autorità, in ragione dell'estrema delicatezza delle informazioni raccolte negli archivi e contenute in milioni di documenti.

Il regolamento rappresenta un riferimento, ai fini della disciplina dell'accesso, per gli Stati firmatari che intendono acquisire nel loro territorio le copie digitali dell'archivio (tra i quali rientra l'Italia).

Il documento richiama in modo inequivocabile il rispetto della protezione dei dati personali, anche con riferimento alla divulgazione nell'ambito dell'impegnativa (parte integrante del regolamento) che i ricercatori dovranno firmare al momento della consultazione.

I Protocolli sono entrati in vigore nel febbraio 2008, al completamento delle procedure di recepimento da parte di tutti gli Stati membri della suddetta Commissione internazionale; da questa data è possibile per ciascuno Stato firmatario ottenere copia dei documenti, per la parte già digitalizzata, ed è operativo il regolamento sull'accesso.

Nella riunione di Amsterdam del 2007 era stata anche avviata la riflessione sul futuro del Centro per il Servizio internazionale delle ricerche (Its) sito a Bad Arolsen, a seguito dell'entrata in vigore dei Protocolli e del progressivo esaurirsi del suo mandato umanitario di ricerca. La questione è stata affrontata nella riunione plenaria del maggio 2008 a Varsavia, sotto la presidenza polacca, ove è stata formalizzata la decisione di istituire un apposito Gruppo di lavoro, stante la particolare complessità degli aspetti giuridici e organizzativi da esaminare (fra cui la natura dell'istituzione e la proprietà della documentazione).

6.2. *La ricerca scientifica*

Ricerca medica, biomedica ed epidemiologica Sperimentazioni cliniche dei medicinali

Nel 2007 l'Autorità ha elaborato un testo di base per le "Linee-guida per i trattamenti di dati nell'ambito delle sperimentazioni cliniche di medicinali", su cui ha avviato una consultazione pubblica (*deliberazione* n. 62 del 29 novembre 2007 [doc. *web* n. 1468981]). Il testo sarà definitivamente adottato dopo aver valutato le osservazioni e i commenti acquisiti.

Il documento è stato redatto considerando le difficoltà di applicazione della disciplina sul trattamento dei dati personali emerse in occasione degli accertamenti e delle ispezioni svolti presso società farmaceutiche e altri enti coinvolti nelle sperimentazioni.

Dopo aver ricostruito i flussi di dati tra *sponsor* (casa farmaceutica), centri di sperimentazione e altri soggetti quali i *cd. "monitor"*, i laboratori di analisi o le organizzazioni di ricerca che si occupano del monitoraggio e dell'analisi statistica dei dati, il documento affronta i più delicati aspetti del trattamento dei dati nelle sperimentazioni, nonché i profili relativi alla custodia e alla sicurezza dei dati.

In particolare, a differenza di quanto ritenuto in una prima fase dalle case farmaceutiche, il Garante ha constatato che le informazioni relative alla sperimentazione collegate con il codice identificativo dei pazienti consentono di risalire all'identità degli interessati. Si tratta dunque di "dati personali" sulla salute (artt. 2, al. 1, lett. *a*) e 8 dir. 95/46/Ce; art. 4, comma 1, lett. *b*) e *d*), del Codice) anziché di dati "anonimi". Il loro trattamento deve avvenire nel rispetto della pertinente disciplina del Codice (art. 26, *autorizzazione* n. 2/2007 [doc. *web* n. 1429775]) e, ove applicabile,

dell'*autorizzazione* del Garante al trattamento dei dati genetici (*Provv.* 22 febbraio 2007 [doc. *web* n. 1389918]) ed essere accompagnato da precise garanzie per i pazienti interessati.

Le case farmaceutiche, aventi in genere responsabilità distinte rispetto ai centri di sperimentazione, si configurano quali autonomi titolari, ovvero contitolari del trattamento (art. 28 del Codice); esse sono tenute a designare quali "incaricati" o "responsabili del trattamento" i soggetti con i quali collaborano, impartendo loro idonee istruzioni (artt. 29 e 30 del Codice). Particolare attenzione deve essere prestata nella designazione degli addetti al monitoraggio, che possono accedere presso i centri di sperimentazione a documenti sanitari e identificativi dei pazienti interessati. I *monitor* vanno sottoposti a regole di condotta assimilabili al segreto professionale e specificamente formati e istruiti sulle precauzioni da utilizzare per tutelare la riservatezza e la confidenzialità delle informazioni, anche nei riguardi dello stesso *sponsor*.

Le case farmaceutiche devono informare con maggiore trasparenza i pazienti (art. 13 del Codice) indicando chiaramente tutti i soggetti che possono venire comunque a conoscenza dei loro dati, la circostanza che queste informazioni possano essere trasmesse all'estero, nonché i diritti di accesso, rettifica e correzione dei dati. Occorre anche consentire ai pazienti di esprimere consapevolmente la loro volontà sui trattamenti effettuati, anche nell'ambito di eventuali ulteriori ricerche, presso la società farmaceutica *sponsor* e gli altri soggetti che partecipano alla sperimentazione (artt. 23 e 26 del Codice). Senza una corretta manifestazione del consenso i dati della sperimentazione non sono, infatti, utilizzabili lecitamente (art. 11, comma 2, del Codice).

Infine, anche in relazione al fatto che le case farmaceutiche *sponsor* sono spesso multinazionali e hanno necessità di trasferire dati in Paesi anche non appartenenti all'Unione europea, il Garante ha individuato una articolata serie di specifiche misure di sicurezza a protezione dei dati (art. 31 del Codice). Risultano in particolare necessarie procedure di autenticazione forte per l'accesso ai dati, sistemi di cifratura per la memorizzazione e l'archiviazione e, soprattutto, protocolli di comunicazione sicuri per la trasmissione elettronica dei dati dai centri di sperimentazione al *database* della società farmaceutica e ai soggetti incaricati della loro validazione ed elaborazione statistica.

A conclusione dell'istruttoria l'Autorità impartirà specifiche prescrizioni a garanzia dei pazienti interessati indicando un termine entro il quale le società farmaceutiche *sponsor* e gli altri soggetti che partecipano alle sperimentazioni dei medicinali dovranno conformarsi ad esse.

Comunicazioni *ex* art. 39 del Codice

Tra le comunicazioni riguardanti progetti di ricerca in campo medico, biomedico ed epidemiologico (art. 39, comma 1, lett. *b*), del Codice) si segnala quella del Ministero della salute sulla sperimentazione di un sistema di sorveglianza circa i progressi delle aziende sanitarie per la salute in Italia (Passi), incluso in un programma di ricerca sanitaria di cui all'art. 12-*bis* del d.lg. 30 dicembre 1992, n. 502 (art. 110 del Codice). A seguito di alcuni approfondimenti istruttori (*Nota* 29 ottobre 2007), l'Ufficio ha fornito al Ministero indicazioni in merito all'effettiva natura dei dati da trasmettere alle regioni e all'Istituto di sanità a cura delle aziende sanitarie, all'esaustività dell'informativa da fornire agli interessati e alla previsione di modalità -altrettanto agevoli rispetto a quelle per il conferimento dei dati- tramite le quali consentire agli interessati sia di opporsi all'utilizzo dei loro dati personali per l'estrazione del campione, sia di esprimere le proprie preferenze riguardo alle modalità del contatto telefonico, sia di non rispondere a singole domande del questionario (artt. 7 e 10, comma 1, del Codice).

È stato inoltre precisato che l'inserimento stabile dell'attività di sorveglianza nel Nuovo sistema informativo sanitario potrà avvenire solo nel rispetto della distinta disciplina che regola il trattamento dei dati sensibili da parte dei soggetti pubblici, in quanto risponda a finalità di rilevante interesse pubblico individuate per legge e venga effettuato applicando il principio di indispensabilità (artt. 20, 22 e 85 del Codice). Analogamente, per inserire l'iniziativa nell'ambito delle rilevazioni del Sistema statistico nazionale dovrà farsi riferimento alla specifica disciplina di settore (art. 108 del Codice; d.lg. 6 settembre 1989, n. 322; codice di deontologia e buona condotta per i trattamenti di dati personali a scopi statistici e di ricerca scientifica nell'ambito del Sistema statistico nazionale, Allegato A.3. al Codice [doc. *web* n. 488371]).

Ricerca sociologica in ambito sanitario

Un'azienda ospedaliera ha interpellato il Garante per realizzare con un'università una ricerca sociologica sulla percezione del danno in ambito sanitario e del rischio connesso ad un'eventuale situazione di malattia. Al riguardo è stato sottolineato che i dati anagrafici dei pazienti che l'azienda intendeva trasmettere all'Università, pur non integrando un riferimento puntuale alla tipologia del danno denunciato dagli interessati, in considerazione del contesto da cui l'evento era originato, sono idonei a rivelare il loro stato di salute e devono essere trattati con le cautele previste dal Codice per i dati sensibili (*Nota* 16 marzo 2007).

Poiché la ricerca in questione non risultava essere prevista dalla legge, né rientrava in uno dei programmi di ricerca biomedica o sanitaria, l'Ufficio ha inoltre precisato che l'azienda e gli altri enti ospedalieri coinvolti non avrebbero potuto mettere a disposizione dell'Università i dati richiesti senza acquisire previamente il consenso informato delle persone interessate (art. 13, 76 e 78, comma 5, del Codice). Qualora il questionario previsto dalla ricerca fosse stato sottoposto per telefono a coloro che avessero deciso di parteciparvi, sarebbe stato altresì opportuno chiedere previamente anche un recapito telefonico al quale ricevere l'intervista, al fine di scongiurare il rischio che soggetti diversi dall'interessato potessero venire indebitamente a conoscenza delle loro vicende sanitarie.

L'Università avrebbe potuto trattare i dati personali così acquisti secondo le modalità previste dal Codice per i trattamenti a fini di ricerca (artt. 104 *ss.*) e nel rispetto delle previsioni del codice deontologico per i trattamenti di dati personali per scopi statistici e scientifici (Allegato A.4 del Codice, *G.U.* n. 190 del 14 agosto 2004 [doc. *web* n. 1038384]).

Acquisizioni di dati sulla disabilità

Era stato segnalato all'Autorità un progetto sulle disabilità promosso da un istituto di ricerca, che prevedeva di acquisire i dati nominativi degli invalidi civili presso alcune aziende sanitarie; l'Ufficio, informato dallo stesso istituto in conformità agli artt. 39 e 110 del Codice, ha portato a compimento gli accertamenti avviati a seguito della segnalazione (*Nota* 16 luglio 2007).

Alla luce degli elementi acquisiti presso il Ministero della salute, il progetto è risultato assimilabile alle attività di ricerca finalizzata incluse in un programma previsto in base alla legge (art. 12-*bis* d.lg. 30 dicembre 1992, n. 502). L'Ufficio, ha pertanto confermato la possibilità per l'istituto di avvalersi della disciplina prevista dall'art. 110 comma 1, del Codice per i trattamenti effettuati per scopi di ricerca medica, biomedica ed epidemiologica; ha precisato, altresì, che l'accesso ai dati nominativi degli invalidi civili presso le aziende sanitarie avrebbe potuto essere effettuato lecitamente dall'istituto, anche in assenza del consenso degli interessati e tramite modalità telematiche, a condizione che fosse limitato alle sole informazioni effettivamente necessarie per la selezione di un campione sufficientemente rappresentativo per la ricerca (artt. 3, 11, 22 del Codice).

L'Ufficio ha inoltre sottolineato la necessità di informare le persone selezionate nel campione anche sulle condizioni alle quali i loro dati personali erano stati cono-

sciuti dall'istituto, in assenza del loro consenso, garantendone la tempestiva cancellazione nell'eventualità in cui l'interessato non volesse aderire alla ricerca. In relazione all'esigenza, emersa in una fase avanzata del progetto, di integrare il campione selezionato con i dati delle liste degli invalidi civili detenute dall'Inps, anche quest'ultimo è stato sollecitato a rendere una specifica informativa agli interessati, fatta salva ogni valutazione sulla necessità di sottoporre all'assenso del Ministero della salute tale variazione al progetto, in conformità alle pertinenti disposizioni di settore (art. 56 l. 27 dicembre 2002, n. 289; d.P.C.M. 7 aprile 2003; convenzione tra il Ministero e l'Istituto n. PS/03/1 del 19 luglio 2004).

7 Attività di polizia

7.1. *Il controllo sul Ced del Dipartimento di pubblica sicurezza*

Si è riferito nella *Relazione* 2006, all'esito di accertamenti presso gli archivi del Centro elaborazione dati (Ced) del Dipartimento della pubblica sicurezza del Ministero dell'interno, del *provvedimento* dell'11 ottobre 2006 con cui sono state prescritte alcune misure finalizzate a rafforzare il livello di protezione delle informazioni registrate nel Ced.

Il successivo riscontro ha consentito di rilevare che, nonostante l'impegno delle strutture interessate, alcune misure non sono state attuate stante la necessità, rappresentata dal Dipartimento, che ritiene di non poter prescindere dalla definizione delle procedure di riordino dell'organizzazione del Dipartimento stesso, dal trasferimento fisico di sedi dell'ufficio e dall'approvazione di modifiche al d.P.R. 3 maggio 1982, n. 378.

L'Autorità, nel rappresentare al Ministro dell'interno l'importanza delle prescrizioni non ancora adempiute, ha rinnovato la richiesta di una sollecita definizione delle menzionate procedure (*Nota* 27 novembre 2007).

Un secondo *provvedimento*, adottato dal Garante l'8 maggio 2007, ha avuto per oggetto gli altri profili esaminati nel secondo ciclo di accertamenti, svolto nel 2006 e dedicato all'approfondimento delle modalità e della complessiva organizzazione del trattamento dei dati personali presso il Ced.

Con detto *provvedimento* l'Autorità ha prescritto ai sensi degli artt. 154 e 160 del Codice al Ministero dell'interno-Dipartimento della pubblica sicurezza le modificazioni e integrazioni da apportare al trattamento dei dati personali svolti presso il Centro, per dare attuazione agli obblighi stabiliti dal Codice e dai princìpi posti nella Raccomandazione n. R(87)15 del Consiglio d'Europa, con riferimento, in particolare, alla pertinenza e aggiornamento dei dati, alle informazioni acquisite da attività amministrative, ai tempi di conservazione dei dati, alla connessione con altre banche dati e all'esercizio dei diritti da parte degli interessati.

Il Garante ha, altresì, rappresentato al Ministro dell'interno la necessità di accelerare l'adozione del regolamento previsto dall'art. 57 del Codice, nonché di individuare i trattamenti non occasionali di cui al comma 1 dell'art. 53 del medesimo Codice effettuati con strumenti elettronici, e i relativi titolari.

A seguito di segnalazioni ricevute, l'Autorità ha inoltre assicurato il riscontro da parte del Dipartimento della pubblica sicurezza e di uffici periferici della polizia di Stato alle richieste degli interessati sia di accesso e comunicazione dei dati conservati presso il Ced, sia di eventuale rettifica dei dati medesimi, nel rispetto delle disposizioni poste dall'art. 10 della legge n. 121/1981, come modificato dall'art. 175 del Codice.

7.2. Altri interventi in relazione a ulteriori attività di forze di polizia

Conservazione ed utilizzazione di dati genetici a fini di indagine giudiziaria

Nella *Relazione* 2006 si è dato conto dell'istruttoria relativa alla raccolta in un archivio informatico, da parte del Reparto investigazioni scientifiche di Parma dell'Arma dei carabinieri (Ris), di dati genetici acquisiti nel corso di attività di polizia giudiziaria, nonché alla loro utilizzazione nell'ambito di successive indagini giudiziarie. L'Autorità, nel corso del 2007, ha acquisito dal Ris dettagliati elementi di valutazione, con particolare riferimento alla base giuridica della conservazione e dell'utilizzo, a fini di accertamento penale, di campioni biologici e di dati genetici acquisiti nell'ambito di procedimenti penali precedenti. Sono stati acquisiti documenti e informazioni anche in ordine al numero di campioni biologici e di profili genetici detenuti, alla tipologia di soggetti cui i medesimi si riferiscono e alle misure di sicurezza adottate per la loro custodia.

All'esito dell'istruttoria e con *provvedimento* del 19 luglio 2007 il Garante, ai sensi degli artt. 143, 144, 154 e 160 del Codice, ha prescritto all'Arma dei carabinieri-Reparto investigazioni scientifiche di Parma che l'ulteriore utilizzo dei campioni biologici e dei profili genetici, anche con riferimento all'attività di comparazione tra i profili genetici, venga effettuata in conformità a quanto disposto dalle competenti autorità giudiziarie e alle condizioni e nei limiti previsti dal codice di procedura penale.

L'Autorità ha altresì impartito una serie di prescrizioni per rafforzare il livello di protezione dei profili genetici e dei campioni biologici conservati presso il Reparto. Tali prescrizioni riguardano l'adozione di sistemi di autenticazione, basati anche sull'uso di dispositivi biometrici, per l'accesso sia al *database* contenente i profili, sia ai locali ove sono collocati i campioni, e il tracciamento di tutti gli accessi e delle operazioni effettuate concernenti i profili, i campioni e il *server* che gestisce il sistema. L'Autorità ha infine prescritto l'adozione di idonee modalità di conservazione dei dati di *log* relativi agli accessi, la cui consultazione deve essere consentita ai soli soggetti dotati di profili di autorizzazione preventivamente individuati.

Il Garante, preso positivamente atto dell'adozione delle misure prescritte, che l'Arma dei carabinieri ha esteso anche ai Reparti investigazioni scientifiche di Roma, Messina e Cagliari, ha accolto la richiesta dell'Arma limitata a dilazionare il solo termine originariamente assegnato per la realizzazione delle misure concernenti l'accesso ai contenitori ove sono custoditi i campioni biologici, motivata dall'esigenza di espletare le procedure volte all'individuazione del fornitore del programma informatico destinato a gestire le misure medesime e dalla complessità del progetto, volto alla gestione e al tracciamento di tutti i processi di laboratorio svolti presso i Ris e non solo di quelli relativi all'individuazione dei profili genetici.

Sistema informativo di controllo della velocità *"Tutor"*

Il Dipartimento della pubblica sicurezza-Direzione centrale per la polizia stradale del Ministero dell'interno ha comunicato al Garante l'avvenuta installazione, ad opera della Società Autostrade per l'Italia, di impianti tecnologici, realizzati con l'utilizzo di sensori e di telecamere, per l'accertamento delle infrazioni ai limiti di velocità da parte degli autoveicoli, in tratti di strada limitati, mediante il rilevamento della loro velocità media.

A seguito della richiesta di chiarimenti, relativa al trattamento dei dati personali (targa dei veicoli in transito, data e ora del passaggio) raccolti attraverso tali apparecchiature, il Dipartimento ha comunicato che il trattamento stesso viene effettuato esclusivamente ad opera della polizia stradale per prevenire, controllare e reprimere comportamenti illeciti; ha inoltre riferito che i dati dei veicoli che risultano avere superato i limiti imposti vengono conservati solo per contestare l'infrazione, mentre in mancanza di violazione i dati rilevati vengono immediatamente

cancellati dal sistema; ha anche fornito precisazioni sull'informativa resa agli automobilisti ai sensi dell'art. 4 della legge 1 agosto 2002, n. 168 e sulle modalità di conservazione dei dati raccolti.

Preso atto di tali chiarimenti, l'Autorità ha invitato il Dipartimento della pubblica sicurezza a comunicare tempestivamente eventuali sviluppi o modifiche del progetto o l'assunzione di ulteriori analoghe iniziative.

Videosorveglianza a bordo dei treni

Le società Trenitalia S.p.A. e Ferrovie dello Stato S.p.A. hanno comunicato all'Autorità di aver installato impianti di videosorveglianza a bordo di una nuova tipologia di treni regionali immessi in servizio, denominati "Minuetto" e "Vivalto", indicando la titolarità del relativo trattamento di dati personali in capo al Dipartimento della pubblica sicurezza-Direzione centrale per la polizia ferroviaria del Ministero dell'interno.

L'Autorità ha chiesto al Dipartimento una compiuta relazione e, in particolare, precisazioni circa le linee interessate e le specifiche esigenze che hanno reso indispensabile l'installazione degli impianti, nonché in ordine agli adempimenti posti in essere in attuazione delle pertinenti disposizioni del Codice e del *provvedimento* generale emanato in materia dal Garante (*Provv.* 29 aprile 2004 [doc. *web* n. 1003482]).

Il Dipartimento ha sostenuto che l'installazione dei sistemi di videosorveglianza si è resa necessaria a seguito di ripetuti e consistenti atti vandalici nelle vetture e di episodi di microcriminalità a danno dei passeggeri all'interno di alcuni convogli ferroviari utilizzati in ambito nazionale per il trasporto locale; ha precisato le caratteristiche degli impianti e gli accorgimenti tecnici adottati con riferimento al posizionamento delle telecamere e alla registrazione delle riprese, nonché le modalità dell'eventuale visualizzazione delle immagini esclusivamente ad opera della polizia ferroviaria, i tempi di conservazione delle immagini e le modalità con cui viene resa l'informativa ai passeggeri.

Alla luce di tali informazioni l'Autorità ha chiesto al Dipartimento di voler tempestivamente comunicare eventuali sviluppi o modifiche del progetto o l'assunzione di ulteriori analoghe iniziative.

7.3. *Il controllo sul Sistema di informazione Schengen*

Accertamenti disposti dal Garante

Nell'ambito dell'azione comune avviata dall'Autorità comune di controllo Schengen, di cui si è dato conto nella *Relazione* 2006, il Garante ha deliberato (*Provv.* 8 febbraio 2007 [doc. *web* n. 1388902]) di effettuare, nei modi previsti dall'art. 160 del Codice, gli accertamenti necessari a verificare presso i competenti uffici centrali e periferici del Ministero dell'interno le modalità di inserimento nel sistema delle segnalazioni previste dall'art. 99 della Convenzione di applicazione dell'Accordo di Schengen (*v. par.* 20).

Con il medesimo *provvedimento* l'Autorità ha deliberato di effettuare anche più ampi accertamenti sulla liceità e correttezza dei trattamenti comunque effettuati per l'attuazione della Convenzione. Gli accertamenti sono in fase di prossima definizione.

Accesso diretto

Nel 2007 si è mantenuto sostanzialmente stabile rispetto al 2006 il numero delle richieste degli interessati pervenute direttamente al Garante, in conseguenza delle nuove modalità di esercizio dei diritti introdotte dal Codice, in virtù delle quali l'interessato, relativamente ai dati che lo riguardano registrati nell'N-Sis, può rivolgersi in Italia direttamente all'autorità che ha la competenza centrale per la sezione nazionale del Sis, ossia al Dipartimento della pubblica sicurezza (*cd.* "accesso diretto").

Dall'esame delle istanze che pervengono all'Autorità e delle note inoltrate al Garante, per conoscenza, dalla Divisione N-Sis (come anche dalle questure compe-

tenti), può rilevarsi anche per l'anno 2007 un'accentuata articolazione delle richieste avanzate dagli interessati, personalmente o con l'assistenza di propri legali; tali richieste riguardano non solamente l'accesso ai dati registrati nel sistema e la loro comunicazione, bensì problematiche di maggiore complessità non tutte di competenza dell'Autorità, quali le modalità di richiesta di revoca dell'espulsione, la scadenza dei termini relativi all'espulsione stessa, la prova dell'uscita dal territorio nazionale, il ricongiungimento familiare e l'usurpazione d'identità.

Richieste di accesso ai dati sono pervenute al Garante anche da autorità di controllo di sezioni nazionali del Sis di altri Stati contraenti della Convenzione, interpellate dagli interessati in relazione a segnalazioni inserite nel sistema da autorità di polizia italiane.

Le informazioni sono state comunicate, previa consultazione degli uffici segnalanti, nel rispetto delle disposizioni degli artt. 109 e 114 della Convenzione.

8 Attività giornalistica e tecnologie della comunicazione

Anche il 2007 ha visto il Garante impegnato nel delicato bilanciamento tra libertà di informazione e tutela del diritto alla riservatezza.

Il tema è stato affrontato anche durante la tradizionale Conferenza di primavera dei Garanti europei (Larnaka 11 maggio 2007) da Mauro Paissan, componente del Collegio, che ha illustrato i princìpi che devono guidare tale bilanciamento [doc. *web* n. 1408381]. L'intervento ha evidenziato, fra l'altro, la peculiarità dei poteri del Garante italiano in materia di informazione; ha sottolineato la responsabilità del giornalista, in prima istanza, nel valutare se, nel riferire di una notizia, la diffusione di un dato personale è essenziale per l'interesse pubblico e nel misurare la propria libertà rispetto al dovere di tutelare la dignità delle persone; ha posto altresì l'accento sull'incidenza di Internet e dei motori di ricerca sia sul "diritto all'oblìo", ovvero il diritto "a veder dimenticata una notizia che ci riguarda, passato un ragionevole periodo di tempo", sia sulla possibile circolazione senza controllo di notizie errate e incomplete che possono ledere gravemente l'immagine delle persone.

8.1. *Minori*

Minori e Tv

Il bilanciamento tra libertà di informazione e tutela dei minori costituisce un tema di particolare rilievo per il Garante. Pur nella difficoltà di individuare regole generali, l'Autorità ha fornito alcune indicazioni al Comitato tv e minori sulla tutela della *privacy* dei minori nelle trasmissioni televisive di informazione e di intrattenimento. In particolare, oltre a ribadire alcuni princìpi consolidati –l'obbligo di garantire l'anonimato di minori vittime di violenza, il dovere del giornalista di valutare l'interesse del minore anche prescindendo da eventuali determinazioni dei genitori– l'Autorità ha precisato che le garanzie vigenti (*cfr.* art. 50 del Codice; art. 7 del codice di deontologia dei giornalisti - Allegato A.1. al Codice [doc. *web* n. 487496]; Carta di Treviso, Del. n. 49 del 26/10/2006, in *G.U.* 13 novembre 2006, n. 264 [doc. *web* n. 1357821]) operano certamente anche nei casi di morte dei minori, per suicidio o per azioni lesive compiute ai loro danni. Notizie relative a simili accadimenti possono essere quindi date evitando di indugiare su dettagli quali, ad esempio, quelli relativi alla sfera sessuale o alla salute e, comunque, astenendosi dal diffondere immagini e informazioni lesive della dignità (*Nota* 6 giugno 2007).

Separazioni dei genitori

L'Autorità si è inoltre pronunciata in merito alla pubblicazione da parte di un giornale locale di diversi dati idonei a identificare alcuni minori coinvolti nella travagliata separazione dei loro genitori (città in cui si era svolta la vicenda, nome, età e particolari dettagliati sulla salute di uno dei figli, nome ed età della sorella, nomi ed iniziali del cognome dei genitori, loro professione, luogo di attuale residenza della madre), nonché delicati dettagli sul loro stato di salute. Il Garante ha ribadito che non basta omettere il cognome per tutelare un minore, se poi sono forniti particolari che lo rendono facilmente identificabile, e ha quindi vietato al quotidiano l'ulteriore utilizzo dei dati (*Provv.* 19 settembre 2007 [doc. *web* n. 1445858]).

Minori e procedimenti penali

L'Autorità si è poi occupata della diffusione, da parte di un'emittente televisiva nel corso di un telegiornale nazionale, di immagini idonee a identificare i bambini di una scuola materna di Rignano Flaminio, coinvolti in un procedimento penale per presunti abusi sessuali compiuti ai loro danni. Nel filmato –che riproponeva immagini relative ad una perizia effettuata per conto della Procura di Tivoli– i bambini risultavano identificabili a causa di riprese chiare e ravvicinate. Il Garante ha vietato all'emittente di diffondere ulteriormente tali dati personali (*Provv.* 19 luglio 2007 [doc. *web* n. 1425235]).

Sono state poi esaminate due altre segnalazioni riguardanti la vicenda processuale, come ricostruita in un volume ad essa dedicato. Pur non riscontrando i presupposti per uno specifico *provvedimento*, l'Ufficio ha evidenziato la delicatezza dei dati contenuti nel volume (nel quale venivano riportate descrizioni piuttosto dettagliate sui comportamenti sessuali che i minori sarebbero stati costretti a tenere), attesa la possibile identificabilità di alcuni minori a livello locale (*Nota* 4 febbraio 2008).

Famiglie di personaggi noti

Anche nel 2007 sono pervenute segnalazioni sulla pubblicazione, ad opera di settimanali, di servizi fotografici relativi a personaggi pubblici (che operano nel mondo dello spettacolo, politici, *ecc.*) e loro familiari, anche minori.

In alcuni casi l'Ufficio ha richiamato all'attenzione degli editori la necessità di rispettare il principio dell'essenzialità dell'informazione, che comporta il dovere di evitare riferimenti a congiunti e ad altri soggetti non interessati ai fatti (art. 137, comma 3, del Codice; artt. 5 e 6 del codice di deontologia), ricordando che la notorietà di una persona non può affievolire i diritti dei congiunti e in particolare dei minori (*Note* 9 agosto 2007 e 14 gennaio 2008).

A conferma di quest'orientamento va ricordato un pronunciamento della Corte di appello di Milano (sentenza n. 2397 del 21 giugno 2007), con cui taluni giornalisti sono stati assolti dal reato di illecita diffusione di dati sensibili (art. 25, comma 2, l. 31 dicembre 1996, n. 675, ora art. 167, comma 2, del Codice) precisando che a tale trattamento effettuato per finalità giornalistica non si applica la tutela penale. La Corte di cassazione (sentenza n. 16145 del 5 marzo 2008) ha però annullato con rinvio la sentenza, non condividendo l'interpretazione della corte milanese, che avrebbe di fatto *"«sottratto» l'intera categoria dei giornalisti ad una norma incriminatrice di portata carattere generale"*. La Corte di cassazione ha contestato l'interpretazione del giudice di merito ricavando invece dalla direttiva 95/46/Ce una tutela rigida e incomprimibile dei dati personali concernenti la salute; ha quindi ritenuto che, ai fini della non rilevanza penale del trattamento dei dati predetti, non sia affatto sufficiente che il giornalista persegua le finalità della sua professione, essendo per contro parametri inderogabili nel trattamento dei dati sensibili anche il rispetto del diritto di cronaca e dell'essenzialità dell'informazione.

Sull'ambito di tutela della sfera privata dei personaggi pubblici la Corte di cassazione (sent. n. 42067 del 9 ottobre 2007) ha anche affermato che le vicende private di personaggi impegnati nella vita politica e sociale possono risultare di interesse pubblico quando da esse si possano desumere elementi di valutazione della personalità di chi deve godere della fiducia dei cittadini, e non per soddisfare la semplice curiosità del pubblico.

Adozione

Sono giunte, da parte di genitori interessati, diverse segnalazioni sul tema dei dati idonei a rivelare un rapporto adottivo. Il Garante ha affermato –come già negli anni precedenti (*Relazione* 2006, *p.* 75)– che non si può pubblicare, senza il consenso dei genitori, la notizia che un minore è figlio adottivo; né si può rivelare la sua provenienza geografica. Per tutelare la personalità dell'adottato e della sua famiglia la legge sull'adozione affida infatti ai genitori la scelta sui modi e i termini per informare il minore del suo *status* e sanziona, anche penalmente, la divulgazione illecita

del dato (artt. 28 e 73 l. 4 maggio 1983, n. 184, modificata dalla l. 28 marzo 2001, n. 149; *cfr. Comunicato stampa* 25 marzo 2008).

8.2. *Cronache giudiziarie*

Intercettazioni e altro materiale di indagine

Anche nell'anno di riferimento sono pervenuti numerosi reclami e segnalazioni riguardanti cronache giudiziarie. L'Autorità ha chiarito più volte che la pubblicazione di dati relativi a procedimenti penali (*v.* anche art. 4, comma 1, lett. *e*) del Codice) è ammessa anche senza il consenso dell'interessato, ma nei limiti dell'essenzialità dell'informazione riguardo a fatti di interesse pubblico (art. 137, comma 3, del Codice; artt. 5, 6 e 12 del menzionato codice di deontologia), da valutarsi caso per caso, nel contesto dei fatti narrati e nel rispetto delle disposizioni che tutelano il segreto delle indagini e gli atti processuali (artt. 114 e 329 c.p.p.) (*Provv.* 10 gennaio 2008 [doc. *web* n. 1489978] e *Provv.* 31 gennaio 2008 [doc. *web* n. 1491621]).

Tali princìpi sono stati richiamati dal Garante in relazione alla ripetuta pubblicazione del contenuto di intercettazioni di conversazioni telefoniche disposte nell'ambito di importanti inchieste giudiziarie, di cui hanno riferito ampiamente le cronache nel corso del 2007. Nei casi esaminati le pubblicazioni sono risultate in contrasto con il limite della "essenzialità dell'informazione" sopra ricordato, e con le garanzie poste a tutela dei dati idonei a rivelare abitudini sessuali (*cfr.* art. 11 del codice di deontologia; *Provv.* 15 marzo 2007 [doc. *web* n. 1390923]; *Provv.* 7 giugno 2007 [doc. *web* n. 1421351]; *cfr.* anche *Relazione* 2006, *p.* 76).

Sulla pubblicazione del contenuto audio di intercettazioni telefoniche, l'Autorità ha osservato che la diffusione indifferenziata e a tempo indeterminato delle risultanze audio delle intercettazioni determina uno specifico impatto sulla sfera personale degli interessati e sulla loro dignità, soprattutto quando riguarda un elevato numero di conversazioni.

Pronunciandosi su un ricorso, l'Autorità ha ritenuto che, decorso il tempo strettamente necessario per lo svolgimento della funzione informativa che ne aveva giustificato la pubblicazione, l'ulteriore permanenza massiva di intercettazioni in formato audio sul sito Internet di una testata giornalistica non risultava essenziale per l'informazione, pur legittima e analitica, su fatti di interesse pubblico, tenuto anche conto dell'eccessivo sacrificio di diritti di terzi interessati (*Provv.* 25 ottobre 2007 [doc. *web* n. 1458851]; *Provv.* 5 marzo 2008 [doc. *web* n. 1517832]).

Con numerosi reclami, ricorsi e segnalazioni è stata lamentata l'illiceità della pubblicazione dei nomi delle persone sottoposte a procedimento penale.

Al riguardo è stato ribadito l'orientamento già espresso dal Garante sulla liceità, di regola, di tale pubblicazione (*Relazione* 2006, *p.* 76 *ss.*) salve eventuali cautele necessarie per tutelare l'identità delle vittime degli illeciti (*Nota* 1 ottobre 2007; in precedenza anche *Provv.* 6 maggio 2004 [doc. *web* n. 1007634]).

L'Ufficio ha poi ricordato che nelle notizie concernenti persone che hanno subìto azioni delittuose il limite della "essenzialità dell'informazione" deve essere valutato con particolare rigore, anche considerando gli ulteriori rischi cui la diffusione dei dati personali può esporre l'interessato. È stato quindi ritenuto non rispondente a tale principio un articolo che conteneva i dati identificativi della vittima di un furto, nonché altri dati personali (la professione, l'indirizzo e la fotografia dell'abitazione dell'interessata, l'indirizzo di un altro immobile di sua proprietà) (*Nota* 22 gennaio 2008).

Dati e immagini degli arrestati

La Corte di cassazione, decidendo su un ricorso presentato avverso un *provvedimento* del Garante del 19 marzo 2003 [doc. *web* n. 1053451] ha affermato che "la foto di un imputato in stato di arresto con le manette ai polsi, se ritrae il predetto in una

posa in cui non sono visibili le manette non incontra alcun divieto normativo alla sua pubblicazione" (sentenza n. 7261 del 19 marzo 2008). La Corte ha ritenuto che "la rivelazione dell'immagine di un imputato costituisce certamente un dato personale, è da porsi sotto il medesimo profilo della comunicazione delle generalità dello stesso e, quando è effettuata in relazione ad un fatto di interesse pubblico, quale nel caso di specie l'informazione su eventi delittuosi, va ritenuta essenziale all'espletamento del diritto di cronaca" (*cfr.* in tema anche *Provv.* 8 maggio 2007 [doc. *web* n. 1410586]).

Diffamazione

In numerose segnalazioni veniva lamentato il contenuto diffamatorio di alcune notizie pubblicate; l'Ufficio ha ricordato che per questo specifico profilo non possono essere invocate disposizioni in materia di protezione dei dati personali, bensì altre specifiche forme di tutela (rettifica, risarcimento dei danni, querela) previste dal codice civile, dal codice penale e dalla legge sulla stampa (l. 8 febbraio 1948, n. 47), da far eventualmente valere dinanzi al giudice ordinario (*cfr.* anche Corte di appello di Milano, sent. n. 2397 del 21 giugno 2007).

A una persona che contestava la verità di notizie che la riguardavano, pubblicate su alcune testate *on-line*, l'Ufficio ha poi risposto che il carattere diffamatorio di un articolo non poteva essere comprovato dalla sola richiesta di rinvio a giudizio per diffamazione, riferita a un diverso articolo pubblicato da un altro quotidiano (*Nota* 16 aprile 2008).

8.3. *Diffusione di dati idonei a rivelare lo stato di salute e tutela della dignità della persona*

Informazioni sui decessi

L'essenzialità dell'informazione e la dignità delle persone, a maggior ragione quando queste sono colpite da malattie, costituiscono i princìpi-cardine dell'attività giornalistica che, come il Garante ha più volte precisato, operano anche se si tratta di persone decedute.

Sulla base di tali princìpi il Garante è intervenuto, a seguito di un reclamo, nei confronti di alcuni quotidiani che avevano dato notizia di una donna morta quasi due anni prima per il morbo di Creutzfeldt-Jakob (il *cd.* morbo della "mucca pazza") rivelandone nome, cognome, luogo di nascita e di residenza, professione, oltre a informazioni dettagliate sulla malattia (tra cui sintomi, descrizione degli accertamenti medici svolti, risultati dell'autopsia). Una delle testate aveva pubblicato anche una fotografia ripresa dalla lapide.

I numerosi dati riportati, soprattutto di natura sensibile, secondo quanto precisato dalla reclamante (la figlia della donna deceduta), non erano stati resi noti né dai familiari, né da loro comportamenti tenuti in pubblico.

L'Autorità ha quindi accolto il reclamo, ricordando che il giornalista, nel far riferimento allo stato di salute di una persona, deve rispettarne la dignità, il diritto alla riservatezza e il decoro personale, specie nei casi di malattie gravi o terminali, e deve altresì astenersi dal pubblicare "dati analitici di interesse strettamente clinico" (art. 10 del codice di deontologia). L'Autorità ha pertanto vietato ai quotidiani indicati nel reclamo l'ulteriore diffusione –anche attraverso i loro siti *web*– delle generalità e di altri dati personali della donna defunta (*Provv.* 29 novembre e 6 dicembre 2007 [doc. *web* nn. 1478059 e 1478083]).

Un richiamo alla tutela della dignità delle persone, anche defunte, e all'essenzialità dell'informazione è stato effettuato in occasione dei servizi stampa e televisivi dedicati alla figura di Luciano Pavarotti e alle sue vicende familiari (*Comunicato stampa* 25 ottobre 2007), nonché in relazione alla pubblicazione di dettagli intimi e corrispondenze private inerenti ai rapporti tra i protagonisti del caso di Garlasco (*Comunicato stampa* 14 dicembre 2007).

Nel quadro degli stessi princìpi, il Garante ha altresì avviato un'istruttoria in relazione alla diffusione, da parte di un'emittente televisiva locale, di alcune immagini del cadavere della studentessa inglese trovata uccisa a Perugia il 2 novembre 2007, immagini che erano state raccolte dalla Polizia scientifica durante uno dei sopralluoghi sul luogo dell'omicidio (*Comunicato stampa* 1 aprile 2008). Il divieto della diffusione di tali immagini, risultata non giustificata dal punto di vista dell'*"essenzialità dell'informazione riguardo a fatti di interesse pubblico"* e in grave violazione della dignità della persona, è stato stabilito con *provvedimento* 24 aprile 2008 [doc. *web* n. 1519915].

In linea con questi orientamenti del Garante si pone anche una decisione del Tribunale di Frosinone (n. 760 del 30 novembre 2007) che ha ritenuto fondate le contestazioni mosse nei confronti di un quotidiano il quale, nel dare notizia della morte di un bambino e delle relative esequie, aveva diffuso dati sensibili non essenziali relativi alla situazione familiare e di salute dei congiunti del deceduto. Il Tribunale, tenuto conto delle risultanze testimoniali, ha ritenuto illecita –anche alla luce di quanto previsto dall'art. 5 del codice di deontologia– la pubblicazione di alcune fotografie dei familiari del defunto scattate durante i funerali nonostante il divieto degli interessati "chiaramente e vivacemente manifestato".

Interruzione volontaria della gravidanza

L'Autorità ha inibito l'ulteriore diffusione del nome e cognome della donna protagonista di una vicenda relativa ad una interruzione volontaria della gravidanza, nel mese di febbraio 2008, presso l'Azienda universitaria ospedaliera "Federico II" di Napoli. Alcuni quotidiani (per la gran parte locali) e agenzie di stampa avevano pubblicato il nome e cognome della donna, unitamente a descrizioni particolareggiate delle circostanze e modalità in cui sarebbe avvenuta l'interruzione della gravidanza. Sebbene l'episodio avesse assunto un rilevante interesse pubblico, la diffusione di tali dati personali non era comunque giustificata, anche perché le informazioni sull'interruzione volontaria della gravidanza ricevono una specifica protezione da parte dell'ordinamento (artt. 5, 11 e 21 l. 22 maggio 1978, n. 194). Inoltre, benché i dati identificativi dell'interessata fossero contenuti in atti parlamentari lecitamente conoscibili, non veniva meno il dovere dei giornalisti di valutare autonomamente il rispetto delle garanzie poste a tutela dei diritti fondamentali delle persone (*Provv.* 5 marzo 2008 [doc. *web* n. 1523741]).

Sugli stessi princìpi si basa il richiamo del Garante agli organi di informazione con riferimento alle notizie emergenti sulle indagini in corso a Genova riguardo all'ipotizzata attività illecita di interruzione volontaria della gravidanza e, in particolare, alla tutela dei nomi delle donne coinvolte nella vicenda, anche se indagate (*Comunicato stampa* 14 marzo 2008).

Disagio sociale

L'Autorità, a seguito di alcune segnalazioni, ha invitato televisioni e giornali ad adottare tutte le cautele possibili affinché, nei servizi giornalistici sul disagio sociale e la povertà, non vengano rese riconoscibili le persone oggetto dei servizi (*ad es.*, indugiando sul volto, nei servizi televisivi), senza il loro esplicito consenso. Spesso, infatti, le persone vengono ritratte mentre frugano nei cassonetti o in situazioni che rivelano comunque, anche nello svolgimento di normali attività quotidiane, uno stato di indigenza e sofferenza sociale. L'Autorità ha osservato che è giusto e necessario documentare tali situazioni, ma nel rispetto della dignità della persona (*Comunicato stampa* 4 marzo 2008).

Incidenti

Diversi quesiti e segnalazioni hanno riguardato la pubblicazione di dati personali riferiti a persone che avevano subìto incidenti stradali. La pubblicazione di simili notizie è espressione di un legittimo esercizio del diritto/dovere di cronaca e, in base ai princìpi generali in tema di giornalismo (art. 137 del Codice), il riferimento alle persone coinvolte non costituisce di per sé un illecito. Tuttavia, come più volte precisato dall'Autorità, l'essenzialità dell'informazione va valutata caso per caso, in rap-

porto al complesso di dati personali che integrano la notizia. Talvolta, infatti, gli articoli indugiano sulle condizioni di salute delle persone o sono corredate da immagini che possono risultare lesive della loro dignità.

Tra i casi esaminati, il Garante ha ritenuto fondata la segnalazione avente per oggetto gli articoli di due quotidiani locali che, nel riferire di un incidente stradale, avevano pubblicato diversi dati personali relativi alle persone coinvolte negli incidenti, compresa la circostanza che il segnalante aveva subìto l'amputazione di un arto. Il Garante ha ritenuto che nel caso di specie il dettaglio sulle conseguenze sull'incidente, riferito a una persona identificata, non rispettasse le disposizioni del codice di deontologia (artt. 5 e 10). I dati relativi alla sfera personale dei segnalanti nel loro complesso risultavano eccedenti ai fini della cronaca sull'accaduto; è stata ritenuta parimenti ingiustificata sul piano normativo (art. 25 del Codice e art. 8 del codice di deontologia) la comunicazione e la successiva riproduzione delle foto-tessera dei documenti di riconoscimento dei segnalanti, rinvenuti dalla polizia stradale nell'autovettura incidentata (*Provv.* 2 aprile 2008 [doc. *web* n. 1519908]).

L'Autorità ha invece constatato che ha agito nel quadro del legittimo esercizio di cronaca un quotidiano che, nel pubblicare la notizia di un incidente stradale in cui aveva perso la vita un uomo, aveva definito la persona che era con lui al momento dell'incidente "sua attuale compagna".

La moglie del defunto aveva chiesto al quotidiano di cancellare l'espressione dagli archivi informatici e dal sito Internet perché riteneva che il termine, incompatibile con l'esistenza di un matrimonio e di una stabile convivenza coniugale, ledesse la sua identità personale. Non ottenuta risposta, la donna si era rivolta al Garante che ha però dato ragione al quotidiano. L'Autorità ha rilevato infatti che il termine "compagna" –non di univoca accezione, in particolare nell'ambito giornalistico– non risultava in necessaria contraddizione, dal punto di vista giuridico e semantico, con la circostanza addotta dalla moglie.

Inoltre, il trattamento dei dati effettuato nel servizio giornalistico non risultava illecito, sia in riferimento alla verità della notizia (in quanto la persona era effettivamente presente al momento dell'incidente), sia riguardo alla sua essenzialità, motivata dalla necessità di illustrare in maniera completa le particolari circostanze del fatto (*Provv.* 3 maggio 2007 [doc. *web* n. 1408971]). L'Autorità ha comunque chiarito che il "dato personale" (art. 4, comma 1, lett. *b*), del Codice) oggetto di contestazione, pur riferito a due persone fisiche diverse dalla ricorrente, era riferibile, sia pure indirettamente, anche alla ricorrente medesima, nei cui riguardi l'informazione pubblicata spiegava parimenti effetti (*cfr.* anche Gruppo art. 29 *"Working document on data protection issues related to Rfid technology"*- WP 104 [doc. *web* n. 1497279]).

Informazioni idonee a rivelare abitudini sessuali

Il Tribunale di Bolzano, con decisione n. 231 del 13 febbraio 2007, ha accolto il ricorso in via d'urgenza presentato nei confronti di alcuni quotidiani locali che avevano diffuso la notizia che una donna, cameriera in un locale della zona, avrebbe avuto contatti di natura sessuale con numerosi clienti e dopo la nascita della figlia avrebbe citato in giudizio un numero consistente di possibili responsabili per accertare la paternità. Il Tribunale, in linea con l'orientamento sopra riportato del Garante sulla riconoscibilità degli interessati, ha affermato che gli articoli, pur senza menzionare il nome della donna, tuttavia contenevano una quantità di dati (l'indicazione del paese e dell'esercizio commerciale in cui lavorava, il luogo in cui ha vissuto, le iniziali, l'età, il fatto che le fosse stato attribuito un diminutivo) che, nel loro insieme, rendevano senz'altro identificabile la ricorrente, almeno per una porzione dell'opinione pubblica locale. Secondo il Tribunale, gli articoli contenevano riferimenti alla vita sessuale della donna (dipinta come eccessiva e sregolata), associati anche a immagini ambigue, risultati eccedenti i limiti del diritto di cronaca e lesivi

della sua dignità. Parimenti illeciti sono stati ritenuti i riferimenti indiretti alla figlia minorenne. Il Tribunale ha quindi vietato l'ulteriore diffusione dei dati relativi alla ricorrente e alla minore per violazione degli artt.136 e seguenti del Codice.

8.4. *Libertà e garanzie nella raccolta dei dati*

Strumenti di ripresa audiovisiva

Diverse segnalazioni hanno lamentato la raccolta di dati personali (anche in forma di conversazioni e immagini), attraverso l'uso di strumenti di ripresa audio e visiva all'insaputa degli interessati.

Un primo intervento ha riguardato la pubblicazione su un settimanale di alcune fotografie che avevano ritratto un noto personaggio politico all'interno del parco della sua abitazione privata in compagnia di alcune sue ospiti. Il Garante ha riscontrato che l'acquisizione delle immagini da parte del fotografo era avvenuta con tecniche di ripresa invasive, rilevando come tale condotta abbia violato i generali princìpi di liceità e correttezza del trattamento previsti dal Codice (art. 11), nonché alcuni specifici obblighi di correttezza e trasparenza sussistenti in capo ai giornalisti (artt. 2 e 3 del codice di deontologia). L'Autorità ha pertanto disposto in via temporanea il blocco (*Provv.* 21 aprile 2007 [doc. *web* n. 1400655]) e, successivamente, il definitivo divieto di ulteriore diffusione del servizio fotografico (*Provv.* 8 maggio 2007 [doc. *web* n. 1409488]); ha precisato, inoltre che la violazione si era concretizzata già al momento della raccolta delle immagini, prescindendo da ogni valutazione sulla notorietà o meno degli interessati, sull'interesse pubblico della notizia e sulle modalità espositive utilizzate nella pubblicazione.

La decisione dell'Autorità ha trovato conferma anche presso la Corte di cassazione (sentenza n. 17408 del 22 febbraio 2008) la quale ha affermato che le fotografie in questione costituivano una violazione dell'art. 615 *bis* c.p. e del codice di deontologia relativo al trattamento dei dati personali nell'esercizio dell'attività giornalistica. La Corte ha inoltre precisato che *"non possono farsi rientrare tra gli* «stampati»*"* (per i quali opera il divieto di sequestro: art. 1 rd. lgs. n. 561/1946) *"le fotografie ritraenti atteggiamenti della vita privata ottenute con una condotta costituente reato, mediante intrusione in luoghi di privata dimora con mezzi tecnici particolari, perché esse non attengono alla manifestazione del pensiero, non trasmettono idee."*.

Il Garante ha poi accolto i ricorsi di tre *imam* ai quali si erano rivolti due giornalisti fingendosi coniugi di fede musulmana alla ricerca di un consulto religioso, affermando che un giornalista non può usare "artifici" per svolgere la sua attività e deve rendere nota la sua professione (*Provv.* 5 luglio 2007, [doc. *web* nn. 1436163 e 1435035] e *Newsletter* 16 ottobre 2007 [doc. *web* n. 1448246)].

Dalla ricostruzione dei fatti è emerso che i giornalisti non avevano informato gli *imam* né dell'uso della telecamera, né che le loro dichiarazioni sarebbero state utilizzate per un servizio giornalistico.

È stato ritenuto sussistente l'interesse pubblico a conoscere le opinioni delle guide religiose di alcune delle principali moschee italiane sull'uso del velo da parte delle donne. Il Garante ha però ravvisato, in particolare, la violazione dell'obbligo del giornalista di rendere note le finalità di un colloquio –ossia la raccolta di informazioni per un servizio giornalistico– e di evitare l'uso di "artifici" (art. 2 del codice di deontologia); ha escluso che ricorresse l'ipotesi prevista dal codice deontologico –invocata invece dalla società televisiva– che esime il giornalista dall'obbligo di qualificarsi nel caso in cui *"ciò comporti rischi per la sua incolumità o renda altrimenti impossibile l'esercizio della funzione informativa"* (art. 2 *cit.*). I due giornalisti televisivi, infatti, avevano reso nota, seppure genericamente, la propria professione agli

imam che li avevano comunque ammessi nei loro uffici all'interno delle moschee e avevano continuato a fornire informazioni, anche se gli stessi le annotavano su un taccuino. Non pertinenti e non essenziali all'informazione sono risultate, inoltre, le traduzioni di brani di telefonate ricevute da uno degli *imam* durante i colloqui, riportate nel servizio. L'Autorità ha pertanto ordinato a una televisione via satellite di non trasmettere più il servizio giornalistico e di cancellarlo dal proprio sito Internet. Analogo divieto è stato disposto nei confronti di un quotidiano il quale aveva pubblicato informazioni relative ai due *imam*, in particolare le loro immagini, anticipando in un articolo la messa in onda del servizio (*Provvedimenti* 5 luglio 2007 [doc. *web* nn. 1435035 e 1436163]).

Intervista telefonica

Al quesito di un giornalista sulla liceità della raccolta e della diffusione di una intervista telefonica registrata all'insaputa dell'interessato, l'Ufficio ha risposto che la registrazione di un'intervista non è di per sé illecita in termini generali; l'interessato deve però esserne però in qualche modo consapevole, specie quando si intende dare diffusione della registrazione stessa. Questa accortezza va ovviamente calibrata caso per caso anche in relazione alle qualità soggettive delle persone interpellate (*Nota* 4 febbraio 2008).

Conversazione al ristorante

Il direttore di una rete televisiva aveva lamentato con ricorso al Garante l'illecita diffusione, da parte di un quotidiano, di alcune sue affermazioni sul festival di Sanremo in via di conclusione e sulle prospettive future della manifestazione. Secondo il ricorrente, le citate dichiarazioni non potevano essere diffuse per il loro carattere confidenziale; erano state carpite di nascosto, da un soggetto non riconosciuto e non riconoscibile quale giornalista, nel corso di una conversazione, in un ristorante, tra il ricorrente e un dirigente della rete.

Il Garante ha ritenuto infondato il ricorso, rilevando che le notizie erano state acquisite in un luogo aperto al pubblico (un noto ristorante al centro di Sanremo frequentato da artisti, giornalisti e altri addetti ai lavori) e non risultavano essere state carpite in violazione del dovere di correttezza. Sussisteva poi un interesse pubblico a conoscere le opinioni del ricorrente sullo svolgimento e sulle prospettive future di una delle più rilevanti manifestazioni musicali –già oggetto di ampio dibattito sulla stampa in quei giorni– essendo egli un personaggio pubblico, nonché il direttore della rete che in quei giorni stava trasmettendo la manifestazione canora (*Provv.* 7 giugno 2007 [doc. *web* n. 1419429)].

Diffusione di una telefonata di servizio

Il Garante ha accolto la richiesta di opposizione all'ulteriore trattamento dei dati del ricorrente (comandante dei vigili del fuoco), contenuti in una conversazione telefonica registrata (come ogni altra telefonata) per finalità proprie del servizio dei vigili del fuoco, poi masterizzata e trasmessa da persone ignote a due quotidiani locali che, a loro volta, l'avevano diffusa sui relativi siti *on-line.*

Il Garante ha riscontrato la violazione del Codice, perché l'uso dei dati personali del ricorrente era diverso e incompatibile con quello della finalità della raccolta (art. 11, comma 1, lett. *a*) e *b*) e ha pertanto vietato l'ulteriore diffusione della registrazione (*Provv.* 8 febbraio 2007 [doc. *web* n. 1388922]).

Corrispondenza privata

Il Garante ha ritenuto fondato il ricorso con cui era stata lamentata l'acquisizione e la successiva diffusione, senza il consenso dell'interessato, da parte di un quotidiano a tiratura nazionale, di una *e-mail* a carattere personale inoltrata al ricorrente da una donna sposata dallo stesso con rito islamico e successivamente ripudiata. Il Garante ha rilevato che, seppur attinente a un argomento di interesse pubblico (il matrimonio islamico, il ripudio e i diritti della moglie ripudiata), una simile pubblicazione contrasta sia con le garanzie costituzionali della corrispondenza *"e di ogni altra forma di comunicazione"* (art. 15 Cost.), sia con le disposizioni dettate dalla legge sul diritto d'autore (art. 93, l. 22 aprile 1941, n. 633) (*Provv.* 24 maggio 2007 [doc. *web* n. 1419749]).

Media e sport

Il Garante ha espresso parere favorevole sullo schema di decreto del Ministero delle comunicazioni che recepisce il "codice *media* e sport" di autoregolamentazione dell'informazione sportiva (*Parere* 11 ottobre 2007 [doc. *web* n. 1449705]). L'Autorità ha rivolto in particolare la sua attenzione sull'art. 3, in base al quale emittenti e fornitori di contenuti si impegnano a realizzare misure adatte, quando necessario, a rendere individuabili le persone che si collegano telefonicamente, in audio o in audio-video, alle trasmissioni. Il Garante ha ritenuto questa previsione coerente con le finalità del "codice *media* e sport", sia per la sua valenza dissuasiva (in caso di telefonate che incitino alla violenza), sia per l'aiuto che essa può fornire alle emittenti, alle quali spetta il compito di valutare l'idoneità a partecipare a ulteriori trasmissioni dei soggetti che si sono resi responsabili di violazione del codice di autoregolamentazione. Al codice di autoregolamentazione hanno aderito, tra gli altri, emittenti televisive e radiofoniche, l'Ordine dei giornalisti, l'Unione stampa sportiva italiana, la Federazione nazionale stampa italiana e la Federazione italiana editori giornali.

8.5. *Reti di comunicazione*

8.5.1. *Invio comunicazioni commerciali non sollecitate*

Numerosi sono stati gli interventi dell'Autorità in merito alla ricezione non richiesta di *e-mail*, *fax*, *Sms* o *Mms* per fini pubblicitari o promozionali.

In particolare, con il *provvedimento* del 22 febbraio 2007 [doc. *web* n. 1388590], è stato ribadito che i dati conferiti dall'interessato per l'esecuzione di un contratto non possono essere utilizzati per uno scopo diverso. È infatti necessario garantire agli interessati il diritto di esprimere liberamente un valido consenso informato per i trattamenti finalizzati al *marketing*, con modalità e in un ambito del tutto distinto da quello relativo al conferimento dei dati indispensabili per dare esecuzione al rapporto contrattuale.

L'inserimento tra le condizioni generali di contratto della riserva di inviare tramite posta elettronica comunicazioni pubblicitarie, quindi, viola il principio di finalità (art. 11, comma 1, lett. *b*), del Codice). Il Garante, nel caso specifico, ha pertanto disposto il divieto di proseguire il trattamento risultato illecito.

In diversi provvedimenti sull'invio di *fax* pubblicitari (*Provv.* 4 aprile 2007 [doc. *web* n. 1402646]; *Provv.* 24 maggio 2007 [doc. *web* n. 1418805]; *Provv.* 3 maggio 2007 [doc. *web* n. 1410276]; *Provv.* 28 giugno 2007 [doc. *web* n. 1433896]; *Provv.* 11 luglio 2007 [doc. *web* n. 1433939]) è stato ribadito che la reperibilità dei dati sugli elenchi pubblici e, in particolare, sugli elenchi categorici (Pagine gialle, Pagine utili, *ecc.*) non esime il titolare del trattamento, in ragione della specificità del mezzo considerato, dal chiedere il consenso all'interessato per l'uso pubblicitario e commerciale del *telefax* (art. 130 del Codice).

In tale sede è stata riscontrata un'interpretazione non corretta del *provvedimento* del 14 luglio 2005 [doc. *web* n. 1151640]), che stabilisce un regime speciale per gli elenchi categorici rispetto a quegli alfabetici. Se è vero infatti che in base a tale *provvedimento*, per la formazione degli elenchi categorici si prescinde dal consenso dei soggetti interessati in quanto il trattamento "riguarda dati relativi allo svolgimento di attività economiche" (art. 24, comma 1, lett. *d*), del Codice), il titolare del trattamento è comunque tenuto a chiedere il consenso all'interessato per l'invio di comunicazioni commerciali, trovando applicazione, come detto, l'art. 130 del Codice.

Per quanto riguarda l'invio di comunicazioni commerciali tramite la posta elettronica, l'Autorità ha ribadito il principio che un indirizzo *e-mail*, per il solo fatto

di essere reperibile in rete, non può essere oggetto di un uso indiscriminato. Il tema si è posto, tra l'altro, nell'ambito del *provvedimento* del 14 giugno 2007 [doc. *web* n. 1424068] in cui l'Autorità ha ricordato che occorre ottenere sempre il consenso preventivo del destinatario prima di utilizzare l'indirizzo di posta elettronica per fini di pubblicità e di *marketing*, non comportando la pubblicità di fatto di un dato la sua libera utilizzabilità con il predetto mezzo.

Con il *provvedimento* del 4 ottobre 2007 [doc. *web* n. 1457973], il Garante ha richiamato il principio stabilito all'art. 15 del Codice per cui chiunque cagiona danno ad altri per effetto del trattamento di dati personali è tenuto al risarcimento del danno, anche non patrimoniale, ai sensi dell'art. 2050 c.c.. L'intervento del Garante, infatti, lascia impregiudicata la possibilità per l'interessato di esercitare in sede civile i propri diritti al fine di ottenere il risarcimento del danno subìto.

L'Autorità ha rilevato l'illiceità di alcuni trattamenti anche nel corso dell'attività di indagine relativa a determinati gestori di telefonia mobile con specifico riferimento all'utilizzo di sistemi di invio di messaggi promozionali del tipo *Sms* e/o *Mms*. In particolare, alcuni clienti di un gestore di telefonia mobile hanno segnalato al Garante la reiterata ricezione di messaggi pubblicitari tramite *Sms* e *Mms* pur avendo espressamente revocato il consenso all'uso dei propri dati. Terminati gli accertamenti condotti anche presso la società telefonica, l'Autorità, con il *provvedimento* del 23 gennaio 2008 [doc. *web* n. 1487925], ha vietato al gestore l'uso dei dati personali di tutti gli abbonati ad un servizio telefonico perché trattati in modo illecito e ha prescritto al gestore l'adozione di misure organizzative e tecniche tali da assicurare a coloro che revocano il consenso di non ricevere più messaggi pubblicitari.

In tema di comunicazioni commerciali non sollecitate, si segnala la partecipazione del Garante a una serie di eventi internazionali volti a realizzare una rete di collaborazione tra le autorità e, con il supporto dei soggetti privati, ad arginare il dilagare del fenomeno dello *spam*. In particolare, il Garante ha preso parte a diverse iniziative del Cnsa (*The EU Contact Network Network of Spam Authorities*): all'incontro del 5 giugno 2007 a Bruxelles, al termine del quale è stato proposto di sensibilizzare tutti i Governi al finanziamento delle iniziative di risoluzione del problema e di organizzare una conferenza a livello ministeriale; a quello del 10 e 11 ottobre 2007 a Washington nel corso del quale sono state analizzate le nuove forme di *spam* (*cd. "spim- spam"*, ovvero attraverso programmi di messaggistica istantanea, *"spit -spam"*, cioè inviato usando *Voip*, e *spam* tramite *bluetooth*) e ipotizzate nuove forme di collaborazione; a quello del 26 febbraio 2008 a Bruxelles, conclusosi con la proposta di rafforzare la cooperazione tra i diversi stati contro lo *spam*, estendendo tale iniziativa anche a Paesi *extra* Ue.

Il Garante ha inoltre collaborato con l'autorità inglese per la risoluzione di un caso in cui le comunicazioni commerciali venivano inviate dall'Italia, ma il *database* veniva gestito da un società con sede nel Regno unito.

8.5.2. *Telefonia*

Attivazione di servizi non richiesti e chiamate indesiderate

Nel 2007 il Garante ha proseguito l'attività relativa al trattamento dei dati personali nell'ambito dei *cd.* "servizi telefonici non richiesti", già oggetto del *provvedimento* generale del 16 febbraio 2006 (in *G.U.* 6 marzo 2006, n. 54 [doc. *web* n. 1242592]). Con tale *provvedimento* l'Autorità aveva prescritto ai fornitori di servizi di comunicazione elettronica una serie di misure –da adottare entro il 31 maggio 2006– volte a evitare l'indebita attivazione di contratti, schede o servizi telefonici non richiesti dagli interessati (*cfr. Relazione* 2006, *p.* 87). Decorsi i termini indicati nel *provvedimento*, le segnalazioni nel frattempo pervenute hanno denunciato sia l'attivazione di servizi non richiesti, quali cambi di gestore, attivazioni di linee Internet veloci, servizi

aggiuntivi sulle linee telefoniche, sia l'inoltro di telefonate pubblicitarie. Si è pertanto resa necessaria, a tutela degli utenti telefonici, una vasta operazione di carattere ispettivo che, dal 27 marzo al 3 aprile 2007, ha interessato 15 accertamenti presso *call center*, interni ed esterni, di cui si servono i principali gestori telefonici. Dall'esame delle risultanze e dei documenti acquisiti è emerso che in diversi casi i *call center* non ottemperavano all'obbligo di informare adeguatamente gli utenti sulla provenienza dei dati e sul loro uso e, quando richiesto, di registrare la volontà dell'abbonato di non essere più disturbato. È stata quindi appurata la mancata osservanza delle prescrizioni impartite con il *provvedimento* del 2006, nonché l'inosservanza del Codice con riferimento al consenso specifico ed informato necessario per effettuare chiamate di carattere promozionale e pubblicitario e alle modalità con le quali viene resa l'informativa alle persone contattate. Il Garante ha pertanto adottato cinque provvedimenti nei confronti di alcuni fra i principali gestori telefonici, delle società che operano in qualità di *call center* per conto degli stessi gestori e di altre importanti aziende prescrivendo una serie di misure volte ad assicurare il rispetto dei diritti degli utenti garantiti dalla disciplina in materia di protezione dei dati personali. Società telefoniche e *call center* hanno dovuto interrompere i trattamenti illeciti di dati informando l'Autorità, entro un congruo termine, circa lo stato di adempimento delle misure prescritte (*Provvedimenti* 30 maggio 2007 [doc. *web* nn. 1412626, 1412610, 1412598, 1412557 e 1412586]).

Con l'intento di verificare l'effettivo adeguamento degli stessi soggetti alle prescrizioni impartite, la Guardia di finanza, nel dicembre 2007, ha avviato un attività di carattere ispettivo nell'ambito del *cd.* progetto "*Teleselling*", effettuando 76 ispezioni in contemporanea su tutto il territorio nazionale presso i *contact center* dei principali gestori telefonici.

Nell'anno di riferimento, l'Autorità ha comminato, per illeciti trattamenti di dati personali, circa 75 sanzioni ai principali gestori di telefonia pari ad un ammontare di circa 332 mila euro.

Fatturazione dettagliata

Nel corso del 2007 il Garante ha avviato un'istruttoria volta a verificare l'adozione, da parte dei fornitori di servizi di comunicazione elettronica accessibili al pubblico, delle misure previste dall'art. 124, comma 2, del Codice, che stabilisce che i fornitori stessi debbano abilitare l'utente ad effettuare comunicazioni e a richiedere servizi da qualsiasi terminale, gratuitamente e in modo agevole, avvalendosi –per il pagamento– di modalità alternative alla fatturazione, anche impersonali, quali carte di credito o di debito o carte prepagate. L'adempimento di queste misure da parte dei fornitori ha ripercussioni sulla disciplina della fatturazione dettagliata: il Garante, infatti, una volta accertata l'effettiva disponibilità di tali modalità alternative di pagamento, può autorizzare il fornitore a indicare nella fatturazione i numeri completi delle comunicazioni effettuate (art. 124, comma 5), derogando così alla previsione del comma 4 dell'art. 124 che prevede invece il "mascheramento" delle ultime tre cifre dei numeri chiamati.

Dall'istruttoria effettuata dall'Autorità è emerso che la maggior parte dei fornitori ha reso reperibili proprie modalità alternative di pagamento, anche impersonali, quali carte "a codice" e carte prepagate. È stata attestata in atti la loro fruibilità sul territorio nazionale; è inoltre emerso che, in aggiunta alle modalità alternative di pagamento messe a disposizione direttamente dai fornitori contattati, ve ne sono altre distribuite sul mercato da parte di altri soggetti (*ad es.* Poste Italiane S.p.A.).

L'Autorità ha pertanto ritenuto che, sia per quanto riguarda la possibilità di effettuare comunicazioni, sia per quel che concerne la richiesta di servizi, tutti i fornitori interpellati risultano adempienti all'obbligo sancito all'art. 124, comma 2, del Codice.

Oggetto di considerazione è stata anche la notevole diffusione nella telefonia mobile delle *cd. "sim card* prepagate" che, per loro stessa natura, costituiscono uno strumento che consente di effettuare chiamate o richiedere servizi, senza che questi risultino nella fatturazione. Per quel che concerne, invece, i contratti di telefonia mobile, è stato rilevato che per essi sussistono le medesime garanzie operanti per i contratti di telefonia fissa: è risultato infatti che anche gli utenti di telefonia mobile sono abilitati dai propri fornitori a effettuare comunicazioni e a richiedere servizi tramite modalità alternative di pagamento (proprie o di terzi).

Nel quadro così delineato, il Garante ha pertanto ritenuto che sussistessero le condizioni per adottare il *provvedimento* generale di carattere autorizzativo ai sensi dell'art. 124, comma 5, del Codice (*Provv.* 13 marzo 2008, in *G.U.* 3 aprile 2008, n. 79 [doc. *web* n. 1501106]). A partire dal 1 luglio 2008, quindi, tutti i fornitori di servizi di comunicazione elettronica accessibili al pubblico che abbiano abilitato i propri utenti a effettuare comunicazioni e a richiedere servizi da qualsiasi terminale avvalendosi per il pagamento di modalità alternative alla fatturazione, sono autorizzati a indicare nella fatturazione dettagliata richiesta dagli abbonati i numeri completi delle comunicazioni.

I fornitori, in tal caso, devono fornire a tutti i propri abbonati un'idonea informativa (da inserire all'interno di almeno due fatture e nel proprio sito *web*), relativa alla decisione di avvalersi dell'autorizzazione, specificando che tutti coloro che abbiano chiesto o chiederanno la fatturazione dettagliata la riceveranno automaticamente "in chiaro", salvo che richiedano esplicitamente il mascheramento delle ultime tre cifre. La medesima informativa dovrà anche contenere l'invito, rivolto a tutti gli abbonati che abbiano chiesto o chiederanno la fatturazione dettagliata "in chiaro", a informare coloro che utilizzino l'utenza che saranno indicati per esteso tutti i numeri oggetto di fatturazione.

9 Propaganda politica ed elettorale

Il Garante ha adottato un *provvedimento* generale in prossimità delle elezioni amministrative del 27-28 maggio 2007 (*Provv.* 3 maggio 2007, in *G.U.* 7 giugno 2007, n. 130 [doc. *web* n. 1409206]), e un altro in vista delle elezioni politiche e amministrative del 13-14 aprile 2008 (*Provv.* 28 febbraio 2008, in *G.U.* 8 marzo 2008, n. 58 [doc. *web* n. 1493909]).

In entrambi i casi sono state richiamate integralmente le prescrizioni interessati contenute nel *provvedimento* generale del 7 settembre 2005 (in *G.U.* 12 settembre 2005, n. 212 [doc. *web* n. 1165613]) sul trattamento dei dati senza informativa agli interessati.

In particolare, con il primo *provvedimento* è stato previsto che, decorsa la data del 31 luglio 2007, partiti, movimenti politici, comitati promotori, sostenitori e singoli candidati potevano continuare a trattare temporaneamente (anche mediante mera conservazione) i dati personali lecitamente raccolti secondo le modalità indicate nel predetto provvedimento del 7 settembre 2005, solo dopo aver informato gli interessati entro il 30 settembre 2007, nei modi previsti dal Codice. Con il secondo *provvedimento*, è stato invece stabilito che decorsa la data del 31 luglio 2008, i predetti soggetti debbano informare gli interessati entro il 31 ottobre 2008 per poter continuare a trattare i dati lecitamente raccolti.

Gli ulteriori princìpi affermati nei predetti provvedimenti si possono sintetizzare nei termini seguenti:

- possono essere utilizzati, senza il preventivo consenso degli interessati, i dati contenuti nelle fonti documentali detenute da soggetti pubblici, che in base a una specifica norma siano liberamente accessibili a chiunque senza limitazioni di sorta quali, ad esempio, le liste elettorali e gli altri elenchi e registri in materia di elettorato attivo e passivo;
- i titolari di cariche elettive possono utilizzare le informazioni raccolte nel quadro delle relazioni interpersonali con cittadini ed elettori senza il preventivo consenso degli interessati, ma non sono legittimati ad ottenere dagli uffici dell'amministrazione o dell'ente la comunicazione di intere basi di dati, oppure la formazione di appositi elenchi "dedicati" da utilizzare per attività di propaganda elettorale, così come non sono utilizzabili i dati raccolti nell'esercizio di attività professionali e di impresa;
- nell'ambito di partiti, organismi politici, comitati di promotori e sostenitori, si possono utilizzare, senza un apposito consenso, dati personali relativi a iscritti e aderenti, nonché ad altri soggetti con cui si intrattengono regolari contatti. Altri enti, associazioni ed organismi senza scopo di lucro (associazioni sindacali, professionali, sportive, di categoria, *ecc.*), possono prevedere tra i propri scopi anche le finalità di propaganda elettorale che, se perseguite direttamente dai medesimi enti, organismi o associazioni, non richiedono il consenso;
- i dati estratti dagli elenchi telefonici possono essere invece trattati a fini di propaganda elettorale per l'invio di posta ordinaria o di chiamate telefoniche effettuate da un operatore, a seconda dei simboli apposti sull'elenco. Qualora si ricorra all'invio di *fax*, di messaggi *Sms* e *Mms*, o di *e-mail*, non-

ché a chiamate telefoniche senza l'intervento di un operatore oppure a chiamate a terminali di telefonia mobile, non è possibile svolgere attività di propaganda politica senza un consenso preventivo e specifico dell'interessato, basato su un'informativa che evidenzi chiaramente gli scopi per i quali i dati sono utilizzati;

- l'eventuale acquisizione dei dati personali da un terzo (il quale potrebbe averli raccolti in base ad un consenso riferito ai più diversi scopi, compresi quelli di tipo promozionale o commerciale) non esime il partito, l'organismo politico, il comitato o il candidato dall'onere di verificare, anche con modalità a campione e avvalendosi del mandatario elettorale, che il terzo: *a*) abbia informato gli interessati riguardo all'utilizzo dei dati per finalità di propaganda e abbia ottenuto il loro consenso idoneo ed esplicito; *b*) non abbia violato il principio di finalità nel trattamento dei dati associando informazioni provenienti da più archivi, anche pubblici, aventi finalità incompatibili. Queste cautele vanno adottate anche quando il terzo, oltre a fornire i dati, svolge le funzioni di responsabile del trattamento designato da chi effettua la propaganda.

I predetti provvedimenti hanno avuto applicazione pratica a seguito di talune segnalazioni pervenute all'Autorità.

Un caso particolare ha riguardato un medico che aveva inviato messaggi di propaganda elettorale in occasione delle consultazioni elettorali amministrative del 2007, estraendo i dati dei destinatari dalla lista dei pazienti dello studio medico presso il quale esercita la propria attività professionale.

A tal proposito è stato evidenziato che si possono utilizzare senza richiedere preventivamente il consenso specifico degli interessati a fini di propaganda elettorale (art. 24 del Codice) solo i dati estratti da fonti "pubbliche". Invece, qualora si presti un'attività o un servizio (*ad es.*, presso una struttura sanitaria) o si svolga un'attività associativa *no-profit* a scopo diverso da quello politico, non è lecito utilizzare indirizzari o altri dati personali per propagandare candidati interni alla struttura o da questa sostenuti, senza previamente chiedere il consenso degli interessati (artt. 13 e 23 del Codice). Ciò, in quanto la finalità di propaganda non è riconducibile agli scopi per i quali i dati sono raccolti (*Nota* 19 febbraio 2008).

10 Le attività economiche e i rapporti di lavoro

L'Autorità ha continuato ad estendere il ventaglio delle aree di intervento ai diversi ambiti delle attività economiche e produttive. Tenuto conto dell'elevato numero di segnalazioni e reclami che continuano a pervenire, anche nel corso del 2007 si è preferito, ove possibile, considerare congiuntamente le segnalazioni aventi profili in comune formulando, specie in settori che coinvolgono larghe fasce della popolazione, linee-guida suscettibili di ampia applicazione, fornendo con esse indicazioni agli operatori economici. Tale è stato il caso dei trattamenti relativi al rapporto banca-clientela e quello del trattamento di dati personali nel contesto lavorativo mediante l'uso di risorse elettroniche (*e-mail* e Internet).

In pari tempo, l'Autorità ha fatto ulteriori passi avanti nella ricerca di forme di esonero o semplificazione nell'adempimento degli obblighi connessi alla protezione dei dati personali, individuando misure comunque atte ad assicurare la tutela dei dati personali: a tale proposito possono essere richiamati sinteticamente i provvedimenti correlati all'informativa da rendere nell'ambito della *cd.* "catena assicurativa", in occasione delle operazioni di cartolarizzazione o, ancora, dell'esecuzione di servizi di informazione al pubblico resi telefonicamente. Più in generale, con particolare riferimento alle piccole e medie imprese (comprese le attività artigianali), è stata predisposta una "Guida pratica" per facilitare gli operatori dei vari settori nell'adempimento degli obblighi che la normativa sulla *privacy* impone.

10.1. *Settore bancario*

Tra i settori nei quali più intensa è stata l'attività del Garante nel 2007 deve essere menzionato anche quello bancario: ciò, in relazione sia alla verifica del rispetto della disciplina di protezione dei dati e di decisioni adottate in passato dall'Autorità, sia alla formulazione di "Linee-guida", utili ad orientare l'attività degli operatori bancari e a fornire, rispetto ai profili di protezione dei dati, indicazioni alla clientela; la vicenda Swift (*v. infra*) ha focalizzato l'attenzione dell'Autorità anche in un'area sinora poco esplorata, quella del trattamento dei dati personali nell'abito dei sistemi di pagamento.

Linee-guida per trattamenti dati relativi al rapporto banca-clientela

Le "Linee-guida in materia di trattamento di dati personali della clientela in ambito bancario" (*Provv.* 25 ottobre 2007, in *G.U.* del 23 novembre 2007 n. 273, [doc. *web* n. 1457247]) sono state adottate al fine di fissare le garanzie per il corretto uso dei dati personali dei clienti da parte degli istituti bancari e degli operatori postali (quando operano nell'ambito bancario e finanziario) e introdurre alcune semplificazioni a vantaggio degli operatori (ciò, in particolare, in relazione alla cessione degli sportelli bancari).

Oltre a ribadire la necessità di scrupoloso rispetto dei princìpi fondamentali in materia di protezione dei dati personali della clientela (pertinenza e non eccedenza, necessità e qualità e sicurezza dei dati), sono state evidenziate alcune modalità di trattamento che possono condurre ad accessi o utilizzazioni indebite: si pensi alla mancata adozione di idonee misure di sicurezza o, più semplicemente, all'inosservanza di "distanze di cortesia" nelle filiali bancarie, o, ancora, alla comunicazione di

informazioni bancarie a terzi (compresi i familiari o il coniuge) non autorizzati dall'interessato a venirne a conoscenza.

Non pochi sono invece i casi, previsti dalla legge (che ne determina limiti e modalità) in cui la comunicazione di dati personali relativi a un cliente deve essere effettuata: ad esempio, la comunicazione in applicazione della disciplina in materia di antiriciclaggio o di contrasto al terrorismo, quella a vantaggio della Centrale di allarme interbancaria (Cai) e della Centrale dei rischi della Banca d'Italia e, ancora, la comunicazione al creditore procedente nell'ambito di una procedura esecutiva (ai sensi degli artt. 543 *ss.* c.p.c.).

Permangono numerose le segnalazioni relative all'esercizio del diritto d'accesso da parte della clientela: il diritto previsto dall'art. 7 del Codice consente all'interessato di conoscere tutte le informazioni che lo riguardano detenute dalla banca (quali le operazioni bancarie effettuate), ma non il diritto di conoscere informazioni personali riferite a terzi ancorché coinvolti nell'operazione effettuata.

Anche nelle linee-guida il Garante ha ribadito, data la frequenza con la quale è dato assistere al ricorso indifferenziato ai rimedi previsti dal Codice, i caratteri distintivi tra il diritto di accesso ai dati personali detenuti da istituti di credito, disciplinato dagli artt. 7 *ss.* del Codice, e il diverso diritto di ottenere copia della documentazione bancaria (che può contenere o meno dati personali, peraltro riferiti sia all'interessato, sia a terzi) regolato dall'art. 119 d.lg. 1 settembre 2003, n. 385.

Nell'ambito delle linee-guida ha formato oggetto di trattazione anche la cessione di sportelli bancari, che comporta una comunicazione di dati personali relativi alla clientela (ma anche dei dati personali dei dipendenti degli sportelli ceduti) dalla banca cedente a quella cessionaria: a tale proposito l'Autorità ha dato ulteriore applicazione al principio del bilanciamento di interessi previsto dall'art. 24, comma 1, lett. *g*), del Codice (coerentemente al quadro normativo desumibile dalla disciplina di settore all'art. 58 del d.lg. 1 settembre 1993, n. 385), rendendo così lecita la comunicazione dei dati personali (diversi da quelli sensibili) oggetto della cessione degli sportelli bancari anche in assenza del consenso degli interessati. Con riguardo all'informativa cui sarebbe tenuta la banca cessionaria, sono stati ritenuti sussistenti i requisiti per esonerare dall'obbligo di rendere individualmente l'informativa agli interessati (art. 13, comma 5, lett. *c*), del Codice). Gli elementi indicati all'art. 13 del Codice dovranno pertanto essere resi noti agli interessati mediante la loro pubblicazione nella *Gazzetta Ufficiale* (come previsto, anche se a fini diversi, dal citato art. 58 del Tub) e (conformemente alla previsione contenuta nell'art. 13, comma 5, lett. *c*), del Codice) le banche che acquisiscono sportelli dovranno fornire ai soggetti ceduti l'informativa di cui all'art. 13, commi 1 e 2, del Codice alla prima occasione utile successiva all'avvenuta cessione (in armonia con quanto previsto dalle Istruzioni della Banca d'Italia).

Banche, videosorveglianza e registrazione dell'immagine delle impronte digitali presso istituti bancari

Per verificare il rispetto delle prescrizioni impartite dal Garante nel *provvedimento* generale adottato il 27 ottobre 2005 [doc. *web* n. 1246675] sul trattamento di immagini del volto e delle impronte digitali per accedere all'interno delle filiali (sul tema *v.* più ampiamente la *Relazione* 2005, *p.* 69), la Guardia di finanza, su incarico dell'Autorità, ha effettuato accertamenti nei confronti di sette banche (per complessive 34 filiali dislocate sul territorio nazionale, scelte in parte a campione, in parte a seguito di segnalazioni pervenute).

All'esito degli accertamenti, dai quali è emersa in molti casi una sostanziale legittimità dei trattamenti, il Garante ha adottato quattro provvedimenti contenenti prescrizioni per le banche presso le quali sono stati riscontrati profili di non conformità con la disciplina in materia (*Provv.* 23 gennaio 2008 [doc. *web* nn. 1490533, 1490477, 1490463 e 1490382]).

In particolare, nei confronti di un istituto di credito è emerso un utilizzo generalizzato dei sistemi biometrici (84 filiali su 92 presenti sul territorio nazionale, sono risultate infatti dotate di sistemi di rilevazione) in assenza di specifici elementi che, in base al *provvedimento* del 27 ottobre 2005, evidenziassero una concreta situazione di rischio per la banca (desumibile da alcuni indici, quali l'aver subito precedenti rapine, l'ubicazione in aree ad alta densità criminale o isolate o, comunque, poste nell'immediata prossimità di "vie di fuga"). Il Garante ha quindi prescritto a tale istituto bancario di rivalutare, alla luce della pertinente documentazione eventualmente acquisita presso le competenti autorità di pubblica sicurezza, l'effettiva necessità dei sistemi di rilevazione di impronte digitali e immagini della clientela.

In altri casi le prescrizioni impartite hanno riguardato la necessità di fornire alla clientela un'idonea informativa sulla presenza dei sistemi in parola, nonché di garantire l'accesso agli sportelli mediante modalità alternative (qualora il cliente non voglia o non possa rilasciare le proprie impronte).

Il Garante ha, infine, prescritto ad alcuni istituti bancari interessati dalle verifiche di adottare le misure necessarie, per limitare a una settimana dalla loro registrazione la conservazione delle informazioni raccolte.

Accessi abusivi a informazioni personali da parte di incaricati

Tra i profili oggetto di segnalazione si registra l'asserito accesso abusivo ad informazioni bancarie da parte di incaricati della banca (sovente con comunicazione dei dati a terzi).

L'accertamento può talora essere assai complesso: l'Autorità però ha dato corso a una segnalazione nella quale l'interessato, pur non essendo più cliente di una banca ormai da alcuni anni, era venuto a conoscenza dell'esistenza di accessi relativi al suo nominativo mediante il *cd.* "servizio di prima informazione" reso disponibile presso la Centrale dei rischi della Banca d'Italia e al sistema centralizzato di rilevazione dei rischi di importo contenuto gestito da Sia S.p.A.

In riscontro alla richiesta di informazioni inviata dal Garante, la banca ha ammesso (diversamente da quanto dichiarato in precedenza al segnalante), che dai controlli effettuati erano emersi accessi indebiti da parte di un dipendente per finalità di natura personale. Il Garante, con *provvedimento* dell'8 marzo 2008 [doc. *web* n. 1390872], ha dichiarato illecito il trattamento di dati personali effettuato presso l'istituto di credito e ha prescritto al titolare del trattamento di adottare le misure di sicurezza atte a evitare accessi non autorizzati o trattamenti non conformi alle legittime finalità perseguite dall'istituto di credito; sono state inoltre prescritte misure idonee a consentire controlli più tempestivi ed efficaci sull'effettiva correlazione tra l'accesso ai predetti sistemi informativi e la documentabile necessità di trattare affari che lo giustifichino. Il Garante ha pure invitato la banca ad assicurare un riscontro veritiero e tempestivo agli interessati che presentano richieste di accesso ai propri dati personali ai sensi dell'art. 7 del Codice (circostanza che non si era verificata nel caso di specie), disponendo altresì la trasmissione degli atti e di copia del *provvedimento* all'autorità giudiziaria per le valutazioni di competenza in ordine alla sussistenza di illeciti penalmente rilevanti eventualmente configurabili.

La vicenda Swift

L'Autorità ha continuato a seguire, anche partecipando alle riunioni del sottogruppo stabilito nell'ambito del Gruppo dei Garanti europei, il "caso Swift" (*v. Relazione* 2006, *p.* 162). La vicenda, come noto, si riferisce a un programma di monitoraggio delle transazioni finanziarie che utilizzano il sistema fornito da Swift (Società per le telecomunicazioni finanziarie interbancarie mondiali stabilita in Belgio) da parte delle autorità statunitensi che, nell'ambito delle iniziative adottate per contrastare il terrorismo (*"Terrorism finance tracking programme"*), avrebbero avuto accesso, con tecniche di data *mining*, fin dall'autunno del 2001 ai dati personali di coloro che effettuano transazioni finanziarie internazionali.

Nell'ambito dei negoziati condotti con le autorità Usa dal vice presidente della Commissione europea Franco Frattini per rinvenire una soluzione condivisa dei profili critici sollevati dal caso, le autorità di protezione europee riunite nel Gruppo art. 29 hanno evidenziato la necessità di soluzioni efficaci e non di una mera "legalizzazione" dell'esistente, individuando le garanzie necessarie affinché lo scambio di informazioni con le autorità statunitensi si possa svolgere nel rispetto della disciplina contenuta nella direttiva 95/46/Ce.

In relazione ai profili critici affrontati nel parere del Gruppo (n. 10/2006 del 22 novembre 2006, WP 128) (in particolare riguardo all'inosservanza della disciplina sul flusso transfrontaliero dei dati personali trattati attraverso *SwiftNet* e temporaneamente memorizzati in un *mirror server* situato negli Stati uniti d'America, oltre al mancato rispetto del principio di proporzionalità), la succursale americana di Swift (per rendere legittimo il trasferimento di dati verso gli Usa) ha chiesto e ottenuto dalle autorità statunitensi di poter aderire al *cd. "Safe Harbor"* (*v. Relazione 2002, p. 129*) incrementando in pari tempo la trasparenza delle operazioni di trattamento effettuate grazie alla predisposizione di una informativa per le banche e gli altri organismi clienti.

Inoltre, in una prospettiva di medio termine (entro la fine del 2009), Swift provvederà a modificare l'architettura del proprio sistema, conservando nel *mirror server* situato negli Usa solo le transazioni dirette verso quel Paese e parte delle restanti transazioni (riferite ad altri Paesi che scegliessero di far capo ad esso); il *mirroring* dell'intero *database* sarebbe collocato in un Paese europeo. Nel frattempo le autorità americane potranno continuare ad attingere, con le modalità in uso, all'intero *database*.

Nel contesto nazionale, il Garante –nell'ambito di un'attività concordata con le autorità di protezione degli altri Paesi europei– ha richiesto notizie utili oltre a Swift Italia, anche al Ministero dell'economia e delle finanze, all'Abi e alla Banca d'Italia.

Si è così appurato che le banche si limitano a comunicare a Swift i dati forniti dalla clientela solo per le operazioni bancarie richieste dalla stessa; tramite l'associazione di categoria è stata messa in luce l'estraneità del sistema bancario rispetto alle decisioni assunte da Swift nella localizzazione di un proprio *mirror server* negli Stati uniti. Con particolare riferimento all'informativa da rendersi alla clientela in ordine alla possibilità di un trasferimento dei dati versi gli Stati uniti, con il conseguente rischio di accesso ai medesimi da parte delle autorità statunitensi, Abi ha sottoposto all'Autorità un *fac-simile* di informativa inoltrato successivamente alle banche associate; da primi riscontri è emerso che, con modalità diverse, tale informativa viene resa alla clientela.

L'intera vicenda ha coinvolto anche le banche centrali, sia quella europea, sia quelle nazionali, mettendo in evidenza la necessità di una vigilanza più penetrante su Swift, società che non essendo né un sistema di pagamento, né un intermediario finanziario, non sarebbe allo stato sottoposta a vigilanza, ma a una (meno incisiva) forma di supervisione (*cd. "oversight"*) il cui coordinamento sarebbe rimesso alla Banca centrale del Belgio (*cd. "lead overseer"*). A seguito dell'accaduto, la Banca d'Italia ha rappresentato che le banche centrali del Sebc hanno avviato una riflessione comune, per giungere a un approccio condiviso che tenga conto del ruolo di Swift nel sistema dei pagamenti a livello globale, nonché nell'ambito del nuovo sistema unico europeo dei pagamenti (Sepa), nel quadro della direttiva 2007/64/Ce sui servizi di pagamento, da recepire entro il 1 novembre 2009.

Iban (International banking account number)

Tra le iniziative volte alla realizzazione di un'area europea dei pagamenti (Sepa), l'Associazione bancaria italiana ha interessato l'Autorità sulle misure di aggiornamento "massivo" degli archivi del sistema bancario, al fine di sostituire le "vecchie" coordinate bancarie della clientela con un codice internazionale (*International banking account number - Iban*) che individui in modo univoco i conti correnti.

L'*Iban* (il cui utilizzo per i bonifici transfrontalieri è previsto come obbligatorio dal 2003 già nel Regolamento n. 2560/2001 del Parlamento europeo e del Consiglio) è un codice alfanumerico composto da 27 caratteri: 23 dei quali sono le attuali coordinate bancarie alle quali vengono aggiunti ulteriori 4 caratteri: 2 individuano il codice del Paese presso il quale è detenuto il conto (*ad es.*, IT corrisponde a Italia) e due rappresentano un codice di controllo internazionale.

La procedura che l'Abi ha rappresentato al Garante per realizzare tale progetto prevede l'allineamento degli archivi tra imprese e banche per l'acquisizione delle autorizzazioni all'addebito rilasciate dal correntista e l'allineamento degli archivi tra Ministero dell'economia e finanze e banche (tramite la Banca d'Italia) per il pagamento di stipendi e pensioni domiciliati di dipendenti pubblici sui propri conti correnti bancari tramite bonifico.

All'esito degli approfondimenti svolti, l'Autorità ha ritenuto che la procedura elettronica configurasse un mero aggiornamento delle coordinate bancarie dei correntisti (già detenute dalle banche) e rientrasse quindi nell'ambito dell'esecuzione del rapporto contrattuale già in essere; si è ritenuta perciò sufficiente l'informativa resa già alla clientela prima dell'avvio della procedura, senza che fosse necessario provvedere a reiterarla (*Nota* 10 aprile 2007).

Attuazione dell'art. 53, comma 2-*ter*, del d.lg. 1 settembre 1993, n. 385

Si segnala, infine, la collaborazione con la Banca d'Italia in vista dell'attuazione della disciplina prevista dall'art. 53, comma 2-*ter*, del d.lg. 1 settembre 1993, n. 385 (introdotta dalla l. 23 febbraio 2007, n. 15, di conversione del decreto legge n. 27 dicembre 2006, n. 297, per il recepimento delle direttive 2006/48/Ce e 2006/49/Ce). La disposizione, da attuare con regolamento della Banca d'Italia previo conforme parere dell'Autorità, prevede che i soggetti che rilasciano alle banche valutazioni del rischio di credito o sviluppano modelli per la valutazione dell'adeguatezza patrimoniale, possano conservare, per tale esclusiva finalità (anche in deroga alle altre vigenti disposizioni normative), i dati personali detenuti legittimamente per un periodo di osservazione ulteriore, che sia congruo secondo criteri dettati dalla Banca centrale.

Tale prolungata conservazione dovrà tuttavia avvenire secondo modalità che assicurano la non identificabilità delle informazioni; nonostante la collaborazione con la Banca d'Italia, emerge al riguardo la difficoltà di assicurare l'univocità delle informazioni riferite agli interessati e il necessario, progressivo aggiornamento delle stesse (necessari per dare effettiva attuazione alle previsioni contenute negli accordi di Basilea II) unitamente alla "non identificabilità" prescritta dal legislatore.

10.2. *Settore assicurativo*

L'informativa sul trattamento dei dati personali e la *cd.* "catena assicurativa"

Le compagnie di assicurazione più rappresentative in termini di quote di mercato sono state oggetto di una verifica congiunta a livello europeo relativa al rispetto dei princìpi in materia di protezione dati (*v. par.* 20.1).

A livello nazionale il settore assicurativo, tramite l'Associazione nazionale fra le imprese assicurative (Ania), aveva per altro già richiesto l'individuazione di modalità più snelle per l'adempimento dell'obbligo dell'informativa (ora previsto dall'art. 13 del Codice). In ragione della complessità delle attività connesse alla gestione del contratto assicurativo, con specifico riferimento alla pluralità di soggetti (persone fisiche e giuridiche, operanti in Italia e all'estero) che possono venire a conoscenza delle informazioni relative a una specifica posizione assicurativa, tale problematica, nota con la locuzione di "catena assicurativa", ha infine formato oggetto del *provvedimento* del 26 aprile 2007 [doc. *web* n. 1410057].

Con esso, anche ai sensi dell'art. 13, comma 5, lett. *c*), del Codice, il Garante ha autorizzato le imprese assicurative stipulanti (titolari del trattamento) a rendere l'informativa alla clientela *una tantum*, in sede di conclusione del contratto di assicurazione, anche nell'interesse dei diversi soggetti che, in qualità di autonomi titolari del trattamento, utilizzano dati personali relativi al medesimo rischio assicurato.

L'Ania aveva sottolineato che l'informativa da parte di ciascun titolare del trattamento operante all'interno della catena assicurativa avrebbe comportato modalità complesse di realizzazione, oltre che costi e impegni amministrativi sproporzionati rispetto al diritto tutelato, considerato anche che, il più delle volte, i soggetti che a vario titolo partecipano alla catena assicurativa non hanno alcun contatto diretto con l'interessato e ricevono i dati dall'assicuratore. Anche per la clientela sarebbe stato preferibile conoscere mediante un'informativa fornita in un unico contesto i diversi ambiti di circolazione delle informazioni personali relative al medesimo rischio assicurato.

Di tali aspetti il Garante ha tenuto conto nell'adozione, ai sensi dell'art. 13, commi 3 e 5, del Codice (e tenendo in considerazione la previsione contenuta nell'art. 13 della direttiva 95/46/Ce oltre alle indicazioni formulate dalla Raccomandazione del Consiglio d'Europa R(2002)9, del 18 settembre 2002), del menzionato *provvedimento* del 26 aprile 2007 volto a semplificare, nel rispetto della disciplina di protezione dei dati personali, alcuni adempimenti gravanti sulle imprese del settore assicurativo.

Il Garante ha comunque precisato che l'informativa non deve essere resa da parte dei (numerosi) soggetti che, nelle *cd.* "fasi assuntiva e liquidativa", vengono a operare quali "responsabili del trattamento". Anche alla luce di tale considerazione, le imprese di assicurazione devono però valutare con attenzione la funzione effettivamente svolta dai soggetti che vengono chiamati a cooperare (o ad operare) nell'ambito della catena assicurativa per dare esecuzione alla medesima prestazione.

Infatti, solo in presenza di un reale ed autonomo potere decisionale in ordine alle finalità del trattamento, soggetti appartenenti alla *cd.* "catena assicurativa" opereranno quali "titolari del trattamento" ai sensi degli artt. 4, comma 1, lett. *f*) e 28 del Codice. Diversamente è appropriato ricorrere, con la necessaria designazione di tali ausiliari, a "responsabili del trattamento" (*cfr. Provv.* 19 dicembre 1998 [doc. *web* n. 41941]): si pensi, ad esempio, a soggetti che operano nella fase precontrattuale senza effettiva autonomia decisionale in ordine alle finalità del trattamento, ad esempio produttori o agenti; o, ancora, a soggetti che operano quali ausiliari dell'assicurazione in sede di distribuzione dei prodotti assicurativi o che operano quali *outsourcers* per determinate operazioni (per assicurare taluni servizi informatici, di archiviazione, di liquidazione sinistri, di posta, di manutenzione, di tipografia, *ecc.*).

Come già chiarito in passato, l'informativa dovrà riferirsi a tutte le operazioni necessarie per la corretta esecuzione al rapporto contrattuale, nonché agli altri trattamenti che (talora anche in base a esplicite previsioni di legge) possono essere effettuati lecitamente (*v.* già *Provv.* 28 maggio 1997 [doc. *web* n. 40425]); essa dovrà illustrare i flussi comunicativi e indicare con precisione le finalità in concreto perseguite dalla compagnia di assicurazione, i soggetti o le tipologie di soggetti ai quali i dati possono essere comunicati (in qualità di autonomi titolari del trattamento) o che possono venirne a conoscenza quali "responsabili del trattamento".

Per evitare un impiego di mezzi sproporzionato rispetto al diritto tutelato (*Provv.* 26 novembre 1998 [doc. *web* n. 39624]), con il *provvedimento* in esame il Garante ha individuato modalità semplificate affinché l'assicurazione stipulante possa fornire un'idonea informativa anche nell'interesse degli altri titolari del tratta-

mento (con particolare riferimento ai coassicuratori e ai riassicuratori), in relazione a un medesimo rischio assicurato: questi ultimi, ai sensi del predetto art. 13, comma 5, lett. *c*), sono così esonerati dall'obbligo di fornire un'autonoma informativa sul trattamento già reso noto all'interessato, a condizione che *"i medesimi titolari del trattamento siano già individuati univocamente nell'informativa resa anche nel loro interesse dall'impresa assicuratrice stipulante o siano comunque individuabili presso quest'ultima"* e che *"l'informativa sia formulata in modo da esplicitare univocamente anche le eventuali finalità ulteriori rispetto alla sola gestione del rischio assicurato perseguite da detti titolari del trattamento"*.

Con il *provvedimento* il Garante ha altresì fornito ulteriori precisazioni in ordine alla modulistica, per le ipotesi in cui sia necessario il consenso dell'interessato. Salva infatti l'ipotesi in cui esso non è richiesto –quando i dati sono necessari (per instaurare o) per dare esecuzione a un contratto di assicurazione (art. 24, comma 1, lett. *b*), del Codice), oppure in quanto gli stessi sono trattati sulla base di uno dei presupposti di cui all'art. 24 del Codice nei casi in cui il consenso dell'interessato sia comunque necessario (*ad es.*, per il trattamento dei dati sensibili)– l'impresa assicuratrice stipulante potrà limitare la formula di consenso ai soli trattamenti da essa effettuati, oppure formularla in modo da ricomprendere, nei limiti del medesimo rischio assicurato, anche gli specifici trattamenti ulteriori effettuati da altri "titolari" appartenenti alla catena assicurativa chiaramente individuabili nell'informativa resa.

Da ultimo, in considerazione del particolare ruolo svolto dai riassicuratori –che non instaurano un rapporto contrattuale con i soggetti coinvolti nel contratto di assicurazione– il Garante ha stabilito che l'eventuale comunicazione di dati (ad eccezione dei dati di natura sensibile) da parte della compagnia assicuratrice al riassicuratore rientra nell'ambito di applicazione dell'istituto del bilanciamento degli interessi tenuto conto del legittimo interesse dei titolari del trattamento coinvolti, e non richiede pertanto il consenso dell'interessato (art. 24, comma 1, lett. *g*), del Codice).

Prodotti finanziari emessi da imprese di assicurazione e notificazione del trattamento

Interpellato dall'Ania, il Garante è tornato a occuparsi dell'esonero dall'obbligo di notificazione preventiva ai sensi dell'art. 37 del Codice da parte delle imprese assicuratrici (*Nota* 9 agosto 2007). Con specifico riferimento ai trattamenti di dati personali della clientela che nella fase precontrattuale comportino la profilazione del contraente, necessari in base alla nuova disciplina dell'offerta dei prodotti finanziari per garantire l'adeguatezza dell'offerta dei prodotti assicurativi, l'Autorità ha precisato che per tali trattamenti non è necessaria la notificazione ai sensi dell'art. 37, comma 1, lett. *d*) del Codice (art. 1, comma 1, lett. *w-bis*, 21, comma 1 e 25-*bis* del d.lg. 24 febbraio 1998, n. 58, testo unico delle disposizioni in materia di intermediazione finanziaria).

Con *deliberazione* del Garante del 31 marzo 2004 (doc. *web* n. 852561) l'Autorità aveva infatti stabilito che l'esenzione concerne i trattamenti dei dati personali *"che non siano fondati unicamente su un trattamento automatizzato volto a definire il profilo di un investitore, effettuati esclusivamente per adempiere a specifici obblighi previsti dalla normativa in materia di intermediazione finanziaria"*.

10.3. *Rapporti di lavoro e previdenza*

10.3.1. *Rapporto di lavoro in ambito pubblico*

L'attività dedicata nel 2007 al trattamento di dati personali dei dipendenti da parte dei datori di lavoro pubblici è stata particolarmente intensa. L'esame di un consistente numero di segnalazioni, reclami, quesiti e richieste di parere, spesso di

tenore similare, ha consentito di elaborare un documento di sintesi su problematiche sollevate di frequente da amministrazioni pubbliche, dipendenti e organizzazioni sindacali.

Le Linee-guida del Garante

Con le "Linee-guida in materia di trattamento di dati personali di lavoratori per finalità di gestione del rapporto di lavoro in ambito pubblico" (*Provv.* 14 giugno 2007 [doc. *web* n. 1417809]), nel quadro della tendenziale uniformità dei princìpi applicabili al rapporto di lavoro, sono state evidenziate alcune specificità del trattamento effettuato da soggetti pubblici, in qualità di datori di lavoro, indicando le misure e gli accorgimenti cui essi devono attenersi nel trattamento dei dati personali di lavoratori.

In termini generali il datore di lavoro pubblico può trattare lecitamente i dati personali dei lavoratori necessari per la corretta gestione del rapporto di lavoro, avendo cura di applicare le previsioni che riguardano le proprie funzioni istituzionali o il rapporto di lavoro, contenute in atti normativi o contrattuali, in modo da avvalersi in piena trasparenza di informazioni personali e modalità di trattamento proporzionate ai singoli scopi (artt. 3, 11, 13 e 18 Codice).

L'amministrazione deve adottare particolari cautele nella trasmissione –tra uffici del medesimo ente o verso soggetti esterni preposti al trattamento (artt. 29 e 30 del Codice)– di informazioni personali riferite ai propri dipendenti, selezionando quelle di volta in volta indispensabili, ed evitando, in linea di principio, riferimenti puntuali a particolari condizioni personali, specie se riguardanti la salute (artt. 11 e 22 del Codice). Per prevenire la conoscenza ingiustificata di dati da parte di persone non autorizzate, l'ente pubblico deve inoltre adottare forme di comunicazione con lo stesso dipendente protette e individualizzate: inoltrando le note in busta chiusa, inviandole all'*e-mail* personale o invitandolo a ritirare personalmente la documentazione.

Particolare attenzione deve essere posta nei rapporti con le organizzazioni sindacali, avendo cura che il rispetto degli obblighi di informativa, consultazione, concertazione e contrattazione sia ispirato ai princìpi di necessità e proporzionalità nella comunicazione di informazioni ai sindacati (artt. 3 e 11 del Codice). Salvi casi specifici in cui la normativa contrattuale preveda espressamente la comunicazione alle medesime organizzazioni di dati nominativi, le amministrazioni possono, infatti, fornire solo dati numerici o aggregati e non anche informazioni riferibili a uno o più lavoratori individuabili, per verificare la corretta attuazione di taluni atti organizzativi.

A parte quanto eventualmente previsto per specifiche categorie di atti, le amministrazioni, sulla base di apposite disposizioni normative, possono avvalersi delle potenzialità offerte dalle nuove tecnologie per mettere a disposizione del pubblico atti e documenti contenenti dati personali, purché ne assicurino l'esattezza, l'aggiornamento e la pertinenza, garantendo altresì agli interessati il "diritto all'oblìo" (mediante forme adeguate di selezione delle informazioni che, trascorso un certo periodo dalla pubblicazione, non consentano di rintracciare i loro dati personali tramite motori di ricerca esterni). È in ogni caso vietata la diffusione di informazioni sulla salute di lavoratori o familiari interessati.

Le nuove tecnologie possono facilitare anche le comunicazioni dell'amministrazione con gli interessati, come ad esempio in occasione di concorsi o selezioni pubbliche: in tali casi vanno riportati nelle graduatorie da pubblicare (indipendentemente dal mezzo utilizzato per la diffusione) soltanto dati pertinenti (elenchi nominativi abbinati ai risultati, elenchi di ammessi alle prove scritte o orali, con l'esclusione di altre informazioni quali recapiti telefonici, codice fiscale *ecc.*).

Anche nel pubblico impiego non è consentito un uso generalizzato dei dati biometrici dei dipendenti (impronte digitali, iride) per controllare le presenze o gli

accessi sul luogo di lavoro. Il Garante può autorizzare tali sistemi di rilevazione solo in presenza di esigenze che impongano l'adozione di elevati e specifici livelli di sicurezza (aree adibite alla sicurezza dello Stato, torri di controllo, conservazione di oggetti di particolare valore) e con precise garanzie (verifica preliminare dell'Autorità, notificazione al Garante, esclusione di archivi centralizzati, codice cifrato dell'impronta memorizzato solo nel *badge* del dipendente, informativa specifica agli interessati).

Dati sensibili o giudiziari possono essere utilizzati per attuare la normativa in materia di instaurazione e gestione di rapporti di lavoro, nonché per finalità di formazione o per concedere benefici economici e altre agevolazioni (artt. 95, 68, 112 del Codice). Il loro trattamento va limitato alle sole informazioni e operazioni previste negli atti regolamentari conformi al parere del Garante applicabili a ciascuna amministrazione (artt. 20, 21 e 154 del Codice).

In particolare, nei casi di assenza per malattia, vanno consegnati all'amministrazione certificati medici privi di diagnosi e con la sola indicazione dell'inizio e della durata dell'infermità. Se il lavoratore produce documentazione in cui è presente anche la diagnosi, l'ufficio pubblico deve astenersi dall'utilizzare queste informazioni e deve invitare a non produrre altri certificati con le stesse caratteristiche. Particolari cautele devono essere inoltre adottate dall'ente pubblico che tratti dati sulla salute dei dipendenti nei casi di visite medico legali, denunce di infortunio all'Inail, abilitazioni al porto d'armi e alla guida.

Le linee-guida sul pubblico impiego hanno reso possibile all'Ufficio fornire indicazioni e orientamenti di carattere generale in relazione a specifiche istanze pervenute.

L'Ufficio ha ad esempio interessato diversi organismi sanitari sulle garanzie da osservare nella trasmissione ai datori di lavoro pubblici dei verbali di visita relativi agli accertamenti di idoneità al servizio dei rispettivi dipendenti (*v., ad es., Nota* 18 dicembre 2007). In particolare è stato evidenziato che il datore di lavoro può conoscere non le eventuali patologie accertate, ma la sola valutazione finale circa l'idoneità del dipendente allo svolgimento di date mansioni. I collegi medici devono quindi trasmettere all'amministrazione di appartenenza dell'interessato il verbale relativo all'accertamento con la sola indicazione del giudizio-medico legale di idoneità o inidoneità, anche parziale, al servizio. Il datore di lavoro, inoltre, qualora sia destinatario di atti di accertamento recanti ulteriori informazioni riferite al lavoratore, non può, comunque, utilizzarle ulteriormente (art. 11, comma 2, del Codice).

Pubblicazione di corrispondenza in bacheca

Con riferimento alla casistica individuale, l'Ufficio ha esaminato una segnalazione riguardante l'affissione in bacheca sindacale, senza il consenso degli interessati, di una missiva della rappresentanza sindacale unitaria dal contenuto apparentemente lesivo della riservatezza. Tale trattamento è in termini generali lecito nell'esercizio del diritto riconosciuto ai soggetti sindacali, individuati nel contratto collettivo applicabile, di affiggere "testi e comunicati inerenti a materie di interesse sindacale e del lavoro" negli appositi spazi predisposti dall'amministrazione in luoghi accessibili a tutto il personale all'interno dell'unità operativa (art. 25, l. 20 maggio 1970, n. 300; artt. 3 e 10, ccnq sulle modalità di utilizzo dei distacchi, aspettative e permessi, nonché delle altre prerogative sindacali del 7 agosto 1998).

I trattamenti di dati personali effettuati per tale finalità, rientrano tra quelli volti a concretizzare la libera manifestazione del pensiero (*v.* Cass. 24 maggio 2001, n. 7091; Cass. 22 ottobre 1998, n. 10511; Cass. 22 agosto 1997, n. 7884; Trib. Viterbo 19 dicembre 2005) e sono pertanto consentiti anche in assenza del consenso delle persone interessate, purché nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità degli interessati, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali (artt. 2 e 21 Cost.; artt. 2, 11 e 136 *ss.* del Codice). Secondo la giurisprudenza, inoltre, la qualificazione

di un testo come inerente a "materie di interesse sindacale e del lavoro" deriva dalla circostanza che esso abbia formato oggetto di scelta da parte del sindacato, fermi restando i limiti della provenienza del materiale affisso dai soggetti legittimati, nonché quelli inerenti al rispetto del decoro, della reputazione e dell'onore degli interessati (art. 2 Cost.; Cass. 23 marzo 1994, n. 2808).

Prima di affiggere in bacheca un documento contenente dati personali i soggetti sindacali devono in particolare valutare la necessità, pertinenza e non eccedenza dei dati trattati (artt. 3 e 11 del Codice) rispetto alle finalità perseguite, garantendo agli interessati il "diritto all'oblìo" trascorso un certo periodo di tempo dal verificarsi delle vicende dalle quali è originata l'affissione (*Nota* 23 gennaio 2008).

Comunicazione di dati sensibili tra enti locali

In un altro caso l'Ufficio è stato chiamato a valutare la liceità della comunicazione tra amministrazioni comunali limitrofe di informazioni sanitarie fornite a un comune per attestare la propria inidoneità fisica da un conducente di taxi, il quale, in un concorso successivamente bandito dallo stesso comune, era risultato socio di una società che svolgeva servizio di noleggio con conducente in comuni limitrofi.

Al riguardo è stato evidenziato che, in linea generale, ciascun ente comunale, anche per il tramite della Polizia municipale, è legittimato a verificare i requisiti previsti dalla legge e dal proprio regolamento per il rilascio di licenze e autorizzazioni per i servizi di taxi e noleggio con conducente (artt. 4 e 5 della legge l. 15 gennaio 1992, n. 21 e artt. 2, 16 e 32 del regolamento comunale applicabile). Tuttavia, la normativa in materia di trasporto di persone mediante autoservizi pubblici non di linea prevede che eventuali accertamenti relativi all'esercizio abusivo di tale attività vengano trasmessi soltanto a determinati soggetti tra i quali la Motorizzazione civile e non anche alle altre amministrazioni comunali limitrofe (artt. 4, comma 2, e 6, comma 5, l. 15 gennaio 1992, n. 21; artt. 5, c. 4, lett. *b*) e 12, l. regionale applicabile).

Dal momento che nel caso in esame il trattamento dei dati sanitari dell'interessato non trovava fondamento nella disciplina di settore, né in altra disposizione idonea a legittimarla (art. 20 del Codice, regolamento comunale sul trattamento dei dati sensibili e giudiziari), l'Ufficio ha rilevato che tali dati, ai sensi dell'art. 11, comma 2, del Codice non potevano più essere utilizzati dal comune (*Nota* 27 febbraio 2008). È stato pertanto considerato inibito ogni ulteriore trattamento dei dati riferiti all'interessato con l'eccezione della conservazione, in quanto presupposto essenziale dell'atto con cui era stata precedentemente autorizzata la cessione ad un altro soggetto della sua licenza per il servizio di taxi.

Rete socio-istituzionale di contrasto al lavoro irregolare

A seguito di una comunicazione ai sensi dell'art. 39, comma 1, lett. *a*), del Codice, l'Autorità è stata chiamata a valutare la conformità al Codice dell'iniziativa di una prefettura di costituire una rete socio-istituzionale per contrastare il lavoro irregolare nell'edilizia privata tramite un sistema informatico volto a consentire alle amministrazioni comunali, al comitato paritetico territoriale e agli organi di controllo e di vigilanza di condividere una serie di informazioni relative ai cantieri di lavori di edilizia privata.

Al riguardo, l'Ufficio ha precisato che la prefettura può accedere al sistema informativo e utilizzare i dati ivi registrati con modalità e per finalità definite in autonomia, soltanto ove ravvisi, tra le sue finalità istituzionali, specifici profili di competenza in materia di indirizzo e coordinamento delle attività di contrasto del lavoro irregolare che non potrebbero essere altrimenti realizzati (artt. 3, 18 e 28 del Codice; art. 1 d.lg. 23 aprile 2004, n. 124; art. 13 l. 1 aprile 1981, n. 121). L'amministrazione, infatti, non può avvalersi di tale sistema per perseguire attività che la disciplina di settore conferisce specificamente ad altri soggetti coinvolti nell'iniziativa, ovvero agli organi di polizia (art. 14 l. 1 aprile 1981, n. 121; art. 5, comma 2, d.lg. 23 aprile 2004, n. 124). L'Ufficio non ha, invece, ravvisato alcun

ostacolo in ordine alla possibilità che la prefettura svolga rispetto al sistema informativo le funzioni di amministratore di sistema, in qualità di "responsabile del trattamento" (art. 29 del Codice) (*Nota* 28 febbraio 2008).

Modalità di consegna dei "cedolini" dello stipendio

In seguito a una segnalazione inoltrata da alcune organizzazioni sindacali, un'azienda sanitaria, su sollecitazione dell'Ufficio (*Nota* 12 dicembre 2007), ha provveduto a adottare opportune cautele nelle modalità di consegna ai propri dipendenti dei *cd.* "cedolini" dello stipendio inserendoli in busta chiusa. L'Ufficio ha ricordato che all'atto della consegna tali documenti andrebbero imbustati, ovvero piegati e spillati, o coperti nelle parti che non riportano informazioni di comune conoscenza, per limitare l'immediata accessibilità delle informazioni ivi contenute al solo interessato e agli incaricati del trattamento (*Parere* 31 dicembre 1998 [doc. *web* n. 39324], *Provv.* 31 ottobre 2007 [doc. *web* n. 1459297]).

Regime di pubblicità degli incarichi e dei compensi conferiti dalle amministrazioni pubbliche

Nel riscontrare taluni quesiti sull'applicabilità alle regioni, agli enti, alle agenzie o alle società a partecipazione regionale del regime di pubblicità degli incarichi e dei compensi conferiti dalle amministrazioni pubbliche (art. 1, comma 593, legge 27 dicembre 2006, n. 296), l'Ufficio ha richiamato le specifiche direttive fornite dalla Presidenza del Consiglio dei ministri (*Nota* 28 novembre 2007). In particolare, la Presidenza ha chiarito che sono estranei al campo di applicazione della suddetta disciplina gli enti di autonomia territoriale (per i quali vigono tuttavia gli specifici obblighi di pubblicità di cui all'art. 1, comma 725, della legge finanziaria 2007) e tutti gli enti non riconducibili all'apparato dello Stato, quali le aziende sanitarie locali (dir. P.C.m. del 16 marzo 2007 pubblicata in *G.U.* 3 luglio 2007, n. 152).

Per quanto riguarda richieste di accesso formulate da associazioni sindacali ad atti contenenti le informazioni relative ai predetti incarichi e compensi, è stato evidenziato che la disciplina in materia di protezione dei dati personali non pone ostacoli di fondo all'applicazione delle disposizioni in materia di accesso ai documenti amministrativi (art. 59 del Codice). Spetta a ciascuna amministrazione, destinataria di un'istanza di accesso, verificare, caso per caso, l'interesse e i motivi sottesi alla richiesta, nonché valutare la sussistenza di una delle ragioni per le quali i documenti possano eventualmente essere sottratti in tutto o in parte alla conoscibilità dell'istante, (artt. 22 ss. l. 7 agosto 1990, n. 241; art. 6 d.P.R. 12 aprile 2006, n. 184).

Affissione all'albo di delibere riferite a dipendenti

Nell'istruttoria preliminare di un reclamo, con il quale un dipendente comunale lamentava che l'amministrazione aveva affisso all'albo pretorio una delibera di concessione del patrocinio legale contenente alcune informazioni riguardanti la vicenda giudiziaria nella quale era coinvolto, l'Ufficio ha ribadito quanto precisato in più occasioni dall'Autorità circa l'applicazione delle previsioni normative sulla pubblicità delle deliberazioni degli enti locali (art. 124 d.lg. 18 agosto 2000, n. 267).

Nel ricordare che l'amministrazione deve selezionare le informazioni effettivamente necessarie per perseguire, nei singoli casi, le finalità di trasparenza dei propri organi, specie se si tratti di dati sensibili e giudiziari (artt. 11 e 22, commi 3 e 5, del Codice), l'Ufficio ha sottolineato che vanno rivalutate con estrema attenzione le stesse tecniche di redazione delle deliberazioni e dei loro allegati, menzionando ad esempio tali dati solo negli atti a disposizione degli uffici, adoperando espressioni di carattere generale o utilizzando, eventualmente, codici numerici (*cfr. Provv.* 19 aprile 2007 [doc. *web* n. 1407101]).

A seguito dell'intervento dell'Ufficio (*Nota* 12 ottobre 2007), l'ente locale ha affermato di aver adottato le misure suggerite dall'Autorità.

In un altro reclamo, riguardante la pubblicazione, all'albo di un consorzio, di deliberazioni commissariali relative a provvedimenti disciplinari emessi a carico del reclamante, l'Ufficio non ha invece rilevato generali profili di illiceità del tratta-

mento dei dati dell'interessato effettuato dal consorzio (*Nota* 12 febbraio 2008) alla luce della pertinente disciplina del Codice (artt. 23 e 24, comma 1, lett. *a*)) sulla diffusione di dati comuni da parte di enti pubblici economici, e della vigente normativa in materia di adozione di provvedimenti disciplinari e di doverosa pubblicazione delle delibere degli organi consortili (art. 7 l. 20 maggio 1970, n. 300; art. 22 e art. 1, all. h), ccnl per i dirigenti dei consorzi di bonifica del 29 marzo 2006; art. 60 r.d. 13 febbraio 1933, n. 215; art. 57 dello statuto del consorzio).

Nel caso esaminato, infatti, non è stato ritenuto in contrasto con i princìpi di pertinenza e non eccedenza dei dati trattati la menzione, negli atti pubblicati all'albo, del numero di matricola dell'interessato in luogo dei suoi dati nominativi (art. 11 del Codice; *Provv.* 12 gennaio 2004 [doc. *web* n. 1053395]; *Provv.* 23 novembre 2006 [doc. *web* n. 1364099]).

Forze armate e di polizia

Sono state completate le verifiche tecniche, avviate dalla Guardia di finanza su richiesta dell'Autorità, nell'ambito di un procedimento ai sensi dell'art. 154 del Codice, per accertare se i *test* utilizzati nell'ambito delle diverse procedure di reclutamento contengano riferimenti e informazioni relative a dati sensibili. Alla luce degli elementi acquisiti l'Autorità sta verificando la liceità dei questionari in uso in relazione al divieto di trattare informazioni sensibili nell'ambito di *test* psico-attitudinali volti a definire la personalità dell'interessato di cui all'art. 22, comma 10, del Codice.

A seguito di una segnalazione pervenuta all'Autorità sono state fornite indicazioni a una questura riguardo alla gestione dei certificati medici degli appartenenti alla polizia di stato. È stato precisato in particolare che l'amministrazione, anche nei casi in cui sia autorizzata a raccogliere documentazione medica recante l'indicazione della diagnosi, insieme a quella della prognosi, a giustificazione delle assenze per malattia (art. 61 d.P.R. 28 ottobre 1985, n. 782; decreto del Ministro dell'interno 21 giugno 2006, n. 244), deve rispettare anzitutto i princìpi di necessità e indispensabilità nel trattamento dei dati sulla salute (artt. 3 e 22 del Codice). Il trattamento di dati relativi alla diagnosi contenuti nei certificati medici prodotti dagli interessati va circoscritto ai soli uffici per i quali la conoscenza di tali dati risulti indispensabile e, segnatamente, a quelli sanitari. Gli uffici di appartenenza del dipendente devono astenersi dal raccogliere tali informazioni (*Nota* 4 aprile 2007).

10.3.2. *Rapporto di lavoro in ambito privato*

Tenuto conto delle segnalazioni pervenute negli anni e dei ricorsi presentati nel 2006 con riguardo alla delicata tematica del contemperamento, nel contesto del rapporto di lavoro, dei diritti fondamentali e della dignità dei lavoratori con le legittime prerogative datoriali, l'Autorità, come anticipato nella *Relazione* 2006, ha adottato proprie linee-guida dedicate al trattamento dei dati personali effettuato in corrispondenza dell'utilizzo della posta elettronica e di Internet (*"Linee-guida del Garante per posta elettronica e Internet"*, *Provv.* 1 marzo 2007 [doc. *web* n. 1387522]).

Internet e posta elettronica

Nell'adozione delle *"Linee-guida per posta elettronica ed Internet"* si è tenuto conto di un quadro normativo che rischia talora di dover inseguire le evoluzioni tecnologiche del settore (profilo peraltro emerso nel corso degli incontri tecnici avvenuti con Abi e Confindustria a seguito dell'adozione delle linee-guida), nonché degli orientamenti espressi dal Ministero del lavoro (Parere 6 giugno 2006, relativo all'ammissibilità del controllo mediante l'utilizzo dei dati relativi al traffico telefonico; Parere 28 novembre 2006, relativo all'ammissibilità di controlli a distanza mediante un *computer* palmare); si sono inoltre considerate le decisioni delle mas-

sime giurisdizioni anche sopranazionali (*v.* in particolare Corte europea dei diritti dell'uomo, *Halford v. United Kingdom*, del 25 giugno 1997 e *Copland v. United Kingdom*, del 3 aprile 2007) e, infine, le indicazioni del Gruppo art. 29 (in particolare "Documento di lavoro riguardante la vigilanza sulle comunicazioni elettroniche sul posto di lavoro"del 29 maggio 2002 - WP 55).

Ciò premesso, le linee-guida evidenziano che l'utilizzo della posta elettronica e di Internet rappresenta una potenziale fonte di informazioni anche sensibili di lavoratori o di terzi, non necessariamente legate all'attività lavorativa.

In tale quadro, l'eventuale trattamento di dati personali riferiti ai lavoratori deve rispettare le legislazioni di settore (in particolar modo quella sui controlli a distanza dell'attività lavorativa) e la disciplina di protezione dei dati personali (in particolare, i princìpi di necessità, di correttezza e di pertinenza e non eccedenza, per il perseguimento di finalità determinate, esplicite e legittime).

A tal fine, i datori di lavoro sono tenuti a indicare chiaramente le modalità di utilizzo degli strumenti messi a disposizione dei lavoratori (*ad es.*, i comportamenti eventualmente "tollerati" rispetto alla navigazione in Internet o alla tenuta di *file* nella rete interna, le soluzioni volte a garantire la continuità dell'attività lavorativa in caso di assenza del lavoratore, *ecc.*) e di eventuali controlli (precisando le ragioni che ne giustificherebbero l'espletamento), anche a mezzo di un apposito disciplinare interno.

I lavoratori devono essere informati in ordine alle principali caratteristiche dei trattamenti, ai soggetti presso cui rivolgersi per esercitare i propri diritti, all'eventualità di controlli sull'impiego di Internet e della posta elettronica; il datore di lavoro, al fine di prevenire l'utilizzo indebito di dati, è chiamato ad adottare opportune misure organizzative e tecnologiche (valutando anche l'impatto sui diritti dei lavoratori dell'eventuale installazione di apparecchiature suscettibili di consentire il controllo a distanza).

Vanno inoltre adottate misure tecnologiche per minimizzare l'uso di dati identificativi dei lavoratori, eventualmente differenziate in funzione della tecnologia impiegata (individuazione di categorie di siti considerati correlati o meno con la prestazione lavorativa, configurazione dei sistemi o utilizzo di filtri che prevengano determinate operazioni reputate inconferenti con l'attività lavorativa, trattamento di dati in forma anonima o aggregata, *ecc.*).

Parimenti, per quanto concerne l'utilizzo della posta elettronica, i datori di lavoro devono contemperare le esigenze di ordinato svolgimento dell'attività lavorativa con la prevenzione di inutili intrusioni nella sfera personale dei lavoratori (*ad es.*, indirizzi di posta elettronica condivisi tra più lavoratori, funzionalità di sistema che consentano l'invio di messaggi automatici in caso di assenza, messaggi di risposta contenenti "coordinate", anche elettroniche o telefoniche, di altro soggetto, ovvero altre utili modalità di contatto della struttura, *ecc.*).

I sistemi *software* devono cancellare periodicamente e automaticamente i dati personali relativi agli accessi ad Internet e al traffico telematico, la cui conservazione non sia necessaria. In assenza di particolari esigenze tecniche o di sicurezza, la conservazione temporanea dei dati relativi all'uso degli strumenti elettronici deve essere giustificata da una finalità specifica e comprovata, nonché limitata al tempo necessario a raggiungerla. Un eventuale prolungamento dei tempi di conservazione può aver luogo solo in riferimento a ipotesi specifiche (*ad es.*, in relazione all'esercizio o alla difesa di un diritto in sede giudiziaria, ovvero all'obbligo di custodire o consegnare i dati su specifica richiesta dell'autorità giudiziaria o della polizia giudiziaria). Il trattamento deve essere comunque limitato alle sole informazioni indispensabili ed essere effettuato con logiche strettamente correlate agli obblighi, compiti e finalità già esplicitati.

Eventuali controlli datoriali devono essere effettuati nella misura meno invasiva possibile e nel rispetto delle previste normative di settore (segnatamente, dell'art. 4 della legge 20 maggio 1970, n. 300). Non risulta ad esempio legittimo il trattamento effettuato mediante sistemi *hardware* e *software* preordinati al controllo a distanza dell'attività di lavoratori (lettura e registrazione sistematica dei messaggi di posta elettronica ovvero dei relativi dati esteriori; riproduzione ed eventuale memorizzazione sistematica delle pagine *web* visualizzate dal lavoratore; lettura e registrazione dei caratteri inseriti tramite la tastiera o analogo dispositivo; *ecc.*). Eventuali controlli legittimi, nel rispetto del predetto art. 4, possono essere effettuati evitando interferenze ingiustificate sui diritti e le libertà fondamentali di lavoratori e terzi, nel rispetto dei princìpi di pertinenza e di non eccedenza. Per quanto possibile, devono essere preferiti controlli effettuati su dati aggregati, riferiti all'intera struttura lavorativa o a sue aree; in caso di eventuali anomalie, le stesse potranno essere "formalizzate" in comunicazioni dirette alla generalità dei lavoratori della struttura o dell'area. In mancanza di ulteriori anomalie, eventuali controlli su base individuale non risultano, di regola, giustificati; va in ogni caso esclusa l'ammissibilità di controlli prolungati, costanti o indiscriminati.

Il datore di lavoro, in qualità di titolare del trattamento, è tenuto ad adottare idonee misure di sicurezza per assicurare la disponibilità e l'integrità di sistemi informativi e di dati; lo stesso può ritenere utile la designazione facoltativa di uno o più responsabili del trattamento cui impartire precise istruzioni sul tipo di controlli ammessi e sulle relative modalità. In caso di interventi per esigenze di manutenzione del sistema, va posta opportuna cura nel prevenire l'accesso a dati personali presenti in cartelle o spazi di memoria assegnati a dipendenti. I predetti soggetti, in ogni caso, potranno svolgere le sole operazioni strettamente necessarie al perseguimento delle previste finalità.

Particolare cura andrebbe prestata nella formazione del personale e in particolare, dei soggetti che operano quali amministratori di sistema o figure analoghe, non solo per i profili tecnico-gestionali e di sicurezza delle reti, ma anche in relazione ai princìpi di protezione dei dati personali e correlati al segreto nelle comunicazioni.

L'immediata attività di divulgazione delle indicazioni e degli orientamenti espressi dall'Autorità con tale documento ha consentito di dare risposta, già nell'anno in esame, ad alcune istanze, in particolare in materia di controllo a distanza dell'attività dei lavoratori.

Con riferimento a una segnalazione volta ad ottenere una pronuncia del Garante in relazione alla soppressione, alterazione e falsificazione di corrispondenza telematica, si è specificato che l'accertamento di profili attinenti a eventuali condotte penalmente rilevanti dei datori di lavoro resta demandato all'autorità giudiziaria ordinaria (*Nota* 11 dicembre 2007).

Non illegittima è risultata l'irrogazione di un provvedimento disciplinare a un dipendente che aveva utilizzato la posta elettronica per comunicazioni con altri lavoratori non attinenti all'attività lavorativa. La società era venuta a conoscenza della trasmissione delle predette comunicazioni non già attraverso un controllo a distanza della casella di posta elettronica in uso al segnalante (in violazione, quindi, dell'art. 4 della legge 20 maggio 1970, n. 300), bensì dalle numerose lamentele ricevute dagli stessi destinatari delle comunicazioni. Alla luce delle dichiarazioni rese dalla società –e a prescindere, in ogni caso, dal merito dell'intimata sanzione– non sono dunque emersi, in relazione alla vicenda segnalata, elementi atti a giustificare un intervento da parte dell'Autorità (*Nota* 28 novembre 2007).

Strumenti di localizzazione satellitare dei lavoratori

Alcune segnalazioni hanno riguardato il trattamento effettuato con strumenti di localizzazione dei veicoli dati in dotazione ai lavoratori. Nel fornire un preliminare riscontro agli interessati, in attesa degli ulteriori opportuni approfondimenti, si è fatto in termini generali richiamo, per quanto applicabile, al *provvedimento* generale

del 1 marzo 2007 (Linee-guida in materia di posta elettronica e Internet, *cit.*) e si sono altresì trasmessi due provvedimenti del Ministero del lavoro relativi a strumenti che consentono la localizzazione dei dipendenti –uno specificamente riferito all'utilizzo del *Gps* su autoveicoli– nei quali si è ritenuto applicabile l'art. 4 dello Statuto dei lavoratori (con riguardo alla possibilità di un controllo a distanza dei medesimi). In un caso specifico, inoltre, questa Autorità ha ritenuto legittima l'installazione di un sistema di localizzazione satellitare *Gps* su mezzi aziendali, stante la sussistenza, nel caso di specie, di un provvedimento autorizzatorio appositamente emesso dalla direzione provinciale del lavoro territorialmente competente (*Nota* 27 dicembre 2007).

L'Autorità sta valutando la necessità di adottare anche in questo contesto un proprio provvedimento.

Biometria e luoghi di lavoro

Dalla documentazione trasmessa con segnalazioni, o a seguito di accertamenti preliminari svolti dall'Autorità, è sovente emerso che l'installazione di sistemi di rilevazione di dati biometrici dei lavoratori è legata a finalità di accertamento delle presenze dei dipendenti sui luoghi di lavoro. Sull'argomento, il Garante (*cfr. Provv.* 21 luglio 2005 [doc. *web* n. 1150679]) anche con le anzidette linee-guida in materia di rapporto di lavoro, ha precisato che l'utilizzo di dati biometrici dei lavoratori può essere giustificato solo in casi particolari e, in relazione ai luoghi di lavoro, per presidiare accessi ad "aree sensibili" (processi produttivi pericolosi, locali destinati a custodia di beni, documenti riservati). Non si è ritenuto invece ammissibile il trattamento di dati biometrici per finalità di ordinaria gestione del rapporto di lavoro (accertamento delle presenza, commisurazione dei tempi di lavoro, *ecc.*).

Questa Autorità ha fatto inoltre presente che, ai fini dell'installazione dei predetti sistemi, restano salve le previsioni di cui all'art. 4 della legge 20 maggio 1970, n. 300 in ordine all'eventuale controllo a distanza dell'attività dei lavoratori che ne potrebbe derivare.

Buste paga

Questa Autorità è stata chiamata da alcune segnalazioni a esaminare fattispecie relative al recapito in busta "aperta" di cedolini paga dei dipendenti, con conseguente agevole accessibilità alle informazioni ivi contenute da parte di soggetti diversi dal destinatario.

Al riguardo, si è già avuto modo di chiarire, mediante le linee-guida sopra richiamate, che il datore di lavoro, salvi i casi in cui sia la legge stessa a prevedere specifiche modalità di divulgazione dei dati, è tenuto a utilizzare forme di comunicazione individualizzata con il lavoratore, adottando misure opportune per prevenire un'indebita comunicazione di dati personali a terzi diversi dal destinatario (tale è, appunto, la consegna in busta chiusa del cedolino dello stipendio). Tali cautele risultano ancor più necessarie quando dalle suddette comunicazioni sia possibile desumere vicende personali del lavoratore (*ad es.*, alcune diciture riportate sulle buste paga, come la voce "pignoramento").

Nel richiamare detti princìpi, questa Autorità ha fornito specifiche indicazioni sulla corretta applicazione della disciplina di protezione dei dati in ordine alle vicende segnalate, invitando in un caso il titolare del trattamento a fornire idoneo riscontro circa le misure adottate per conformarsi alle indicazioni rese (*Nota* 30 novembre 2007).

Ferie e permessi

Con riferimento a una fattispecie di divulgazione a mezzo posta elettronica di dati personali dei dipendenti relativi a ferie e permessi non fruiti, questa Autorità ha invitato il titolare del trattamento ad attenersi scrupolosamente alle indicazioni contenute nelle citate linee-guida in materia di rapporto di lavoro, ribadendo che la conoscenza da parte di terzi dei dati personali dei lavoratori, in assenza degli specifici presupposti normativi, è ammessa solo se l'interessato vi acconsente. In propo-

sito, la società interessata ha dichiarato che la vicenda segnalata è stata frutto di un'iniziativa individuale e che sono state comunque adottate soluzioni idonee a evitare il ripetersi di accadimenti simili. L'Autorità ne ha preso atto, rinnovando l'invito alla società a valutare attentamente l'adeguatezza delle istruzioni fornite ai propri incaricati, al fine di garantire modalità di comunicazione con i lavoratori conformi alla disciplina di protezione dei dati (*Nota* 5 febbraio 2008).

Tesserini identificativi dei dipendenti

Nel corso dell'anno sono inoltre pervenute alcune segnalazioni in ordine alla conformità alla disciplina di protezione dei dati personali di normative settoriali che, per finalità di elusione del lavoro sommerso, impongono ai datori di lavoro di far indossare ai propri dipendenti tesserini identificativi contenenti taluni dati personali agli stessi riferiti (in particolare, fotografia e generalità). Tale obbligo di diffusione presenta profili di criticità in relazione a talune figure professionali (e segnatamente, dalle segnalazioni pervenute, le guardie giurate), che si ritengono esposte al rischio di incolumità personale in ragione dell'agevole conoscibilità, da parte di terzi, di informazioni personali alle medesime riconducibili. La problematica segnalata, considerate le rilevanti implicazioni che la diffusione può comportare sul piano della sicurezza e dell'incolumità individuale, è al vaglio dell'Autorità.

Sanzioni disciplinari

Ulteriori ipotesi di diffusione di dati personali dei dipendenti si sono registrate in relazione ad alcune segnalazioni aventi per oggetto la divulgazione di provvedimenti disciplinari. In particolare, una segnalazione lamentava l'affissione nella bacheca aziendale di una delibera contenente il nominativo di un dipendente associato al provvedimento sanzionatorio irrogato, contestando l'illegittimità del trattamento effettuato.

Al riguardo si è già avuto modo di ribadire che, in termini generali, la diffusione di dati personali riferiti ai lavoratori, in assenza di specifiche disposizioni o comunque di altro presupposto ai sensi dell'art. 24 del Codice, può avvenire solo se necessaria per dare esecuzione a obblighi derivanti dal contratto di lavoro (art. 24, comma 1, lett. *b*)). Quindi, non è di regola lecito dare diffusione a informazioni personali riferite a singoli lavoratori, anche attraverso la loro pubblicazione in bacheche aziendali o in comunicazioni interne destinate alla collettività dei lavoratori, specie se non correlate all'esecuzione di obblighi lavorativi. In tali casi, tra l'altro, la diffusione si pone anche in violazione dei princìpi di finalità e pertinenza stabiliti dall'art. 11 del Codice.

Al riguardo, l'associazione interessata, fornendo chiarimenti in ordine alla vicenda segnalata, ha confermato l'accaduto, addebitandolo tuttavia a un episodio isolato e asserendo di voler introdurre opportuni correttivi per adeguarsi alla normativa vigente. L'Autorità ne ha preso atto e ha inoltrato copia del *provvedimento* generale in materia di rapporto di lavoro al fine di consentire alla stessa una più compiuta attuazione della disciplina di protezione dei dati (*Nota* 21 dicembre 2007).

È risultata invece legittima, alla luce della documentazione trasmessa, la diffusione di dati relativi alla sanzione disciplinare riferita a un dipendente operante presso una società di trasporto pubblico locale. Nel caso di specie, considerata la sia pur risalente normativa di settore –che impone al datore di lavoro di portare a conoscenza del personale, tra l'altro, le sanzioni disciplinari irrogate nei confronti dei dipendenti– non sono stati ravvisati profili di violazione della disciplina di protezione dei dati personali.

Assenze per malattia e controlli datoriali

Alcune segnalazioni hanno lamentato l'illegittimità di comportamenti datoriali volti ad acquisire numeri telefonici dei medici curanti al fine di "approfondire" le cause di assenza per malattia dei dipendenti. Nel fornire riscontro agli interessati si è precisato che il datore di lavoro, come già chiarito dalle linee-guida in materia di rapporto di lavoro (*cfr. par.* 6.2.), può conoscere solo la "prognosi" e non la "dia-

gnosi" della patologia denunciata dal lavoratore (fatte salve alcune limitate fattispecie, come in caso di denuncia all'Inail di infortuni sul lavoro o malattie professionali). Si è ricordato, peraltro, che il datore di lavoro può servirsi degli "ordinari" strumenti previsti dall'ordinamento (contestazioni dirette al solo interessato, visite fiscali, denunce di ipotetico reato), ma nel rispetto della disciplina in materia di protezione dei dati personali (per un caso simile, *cfr. Provv.* 24 settembre 2001 [doc. *web* n. 39460]).

In un caso, tra l'altro, si è riscontrato l'invio a terzi (nella fattispecie, i medici curanti), ad opera del datore di lavoro, di comunicazioni contenenti dati personali di una dipendente per finalità di contestazione della prolungata e ininterrotta assenza dal servizio della dipendente medesima. Nell'invitare il titolare del trattamento a conformarsi ai princìpi di protezione dei dati e al *provvedimento* generale in materia di rapporto di lavoro, questa Autorità ha confermato che simili trattamenti non rispondono ai princìpi di pertinenza, non eccedenza e proporzionalità (*Nota* 18 ottobre 2007).

Iscrizioni sindacali

Con specifico riferimento a un'ipotesi di diffusione di dati sensibili dei lavoratori (nella fattispecie, l'iscrizione di alcuni dipendenti a una organizzazione sindacale), questa Autorità ha ricordato al titolare del trattamento che la diffusione di dati sensibili dei dipendenti non è ammissibile, in assenza dei presupposti di equipollenza del consenso legislativamente previsti (art. 26, comma 4, del Codice), senza il consenso scritto degli interessati (art. 26, comma 1, del Codice). Chiamata a fornire chiarimenti la società interessata ha dichiarato, ai sensi e per gli effetti di cui all'art. 168 del Codice, di non aver diffuso dati personali sensibili dei lavoratori, producendo documentazione fotografica comprovante le proprie deduzioni. Preso atto delle dichiarazioni rese, si è nondimeno provveduto a richiamare la società al più rigoroso rispetto delle misure di sicurezza adottate (*Nota* 24 gennaio 2008).

Contratto di somministrazione

In un caso, questa Autorità è stata interpellata sulla conformità alla disciplina di protezione dei dati personali di un contratto di somministrazione stipulato per ragioni sostitutive e che recava il nominativo del lavoratore temporaneamente sostituito. Alla luce delle dichiarazioni rese dall'agenzia di lavoro presso il quale il contratto era stato stipulato –secondo cui le procedure in essere prevederebbero da tempo l'indicazione del solo numero di matricola del dipendente temporaneamente sostituito in luogo del nominativo al medesimo riferito–, si è ritenuto che, allo stato, non sussistessero i presupposti per un intervento da parte del Garante (*Nota* 15 febbraio 2008).

Procedure societarie interne di "segnalazione" di illeciti commessi da propri dipendenti (*cd. "whistleblowing"*)

Di particolare rilevanza, considerata la delicatezza della materia sotto il profilo della protezione dei dati personali, sono alcune segnalazioni pervenute all'Autorità aventi per oggetto l'adozione di procedure societarie interne di "segnalazione" di illeciti commessi da propri dipendenti (*cd.* "*whistleblowing*"). Trattandosi di materia attualmente priva di qualsiasi disciplina legale, questa Autorità, per i profili di propria competenza, sta valutando quali iniziative intraprendere e quali determinazioni adottare.

Accesso ai dati trattati dal datore di lavoro

Nonostante le linee-guida in materia di rapporto di lavoro abbiano fornito significativi chiarimenti in merito (*v.* in particolare il punto 9.5.), diverse segnalazioni hanno avuto per oggetto molteplici tipologie di informazioni e documenti (rilevazione delle presenze, corrispondenza intercorsa, giornate di malattia, schede di valutazione, *ecc.*) trattati dai datori di lavoro.

In proposito, si è ricordato che l'art. 7 del Codice riconosce agli interessati il diritto di accedere alle informazioni personali a sé riferite, ivi comprese quelle di carattere valutativo (alle condizioni e nei limiti di cui all'art. 8, comma 5, del Codice). L'esercizio di tale diritto consente di ottenere, ai sensi dell'art. 10 del Codice, solo la comunicazione dei dati personali relativi al richiedente detenuti dal titolare del trat-

tamento; non permette, invece, di richiedere il diretto e illimitato accesso a documenti e a intere tipologie di atti, ovvero di ottenere, sempre e necessariamente, copia dei documenti detenuti. In altra occasione si è precisato che il titolare del trattamento è tenuto a comunicare i dati richiesti ed effettivamente detenuti, non già a ricercare o raccogliere altri dati che non siano nella sua disponibilità e non siano oggetto, in alcuna forma, di attuale trattamento.

Credenziali biometriche

Uno studio di consulenza ha chiesto di essere autorizzato a adottare, quale credenziale di autenticazione per l'utilizzo del *personal computer* in dotazione, una caratteristica biometrica dei propri dipendenti, onde elevare il livello di sicurezza in ordine agli accessi ai dati personali sensibili ivi contenuti, assicurando espressamente che il sistema non è preordinato alla rilevazione della presenza dei lavoratori e che non verrebbe costituito alcun archivio centralizzato contenente le impronte dei lavoratori. Con specifico riferimento alla fattispecie evidenziata, si è ritenuto che, allo stato degli atti, non fosse necessaria una verifica preliminare da parte dell'Autorità, tenuto conto delle circostanze sopra evidenziate e della circoscritta finalità perseguita in conformità all'Allegato B) al Codice in materia di protezione dei dati personali [doc. *web* n. 488497], che prevede, quale credenziale di autenticazione, anche l'utilizzo di *"una caratteristica biometrica dell'incaricato eventualmente associata a un codice identificativo o a una parola chiave"* (regola 2 dell'All. B) *cit.*; *Nota* 4 gennaio 2008).

Documenti personali in ambiti di pertinenza aziendale

Un segnalante lamentava l'illegittima sottrazione di documenti (tra cui corrispondenza privata e ricette mediche) da un cassetto della scrivania di lavoro assegnatagli. Non sono però emersi elementi atti a giustificare un intervento del Garante, anche in considerazione della riconducibilità al medesimo segnalante dei documenti sottratti e della loro volontaria dislocazione, per scelte personali, in ambiti di pertinenza aziendale (*Nota* 23 gennaio 2008).

Patto di non concorrenza

È pervenuta a questa Autorità una segnalazione avente per oggetto un patto di non concorrenza sottoscritto dalla segnalante con la sua pregressa società di appartenenza. L'interessata, contattata dalla società che chiedeva informazioni in ordine alla sua "nuova" attività professionale al fine di verificare il rispetto di quanto pattiziamente convenuto, chiedeva delucidazioni all'Autorità in ordine a tale richiesta. Dalla documentazione in atti non sono emersi profili di violazione della disciplina di protezione dei dati, considerato che nel patto di non concorrenza stipulato dalla segnalante figurava una clausola con cui la medesima segnalante si impegnava a comunicare alla società le attività svolte durante la vigenza del patto stesso (*Nota* 14 dicembre 2007).

10.3.3. *Previdenza*

Rivisitazione della modulistica Inps

L'Istituto nazionale della previdenza sociale, recependo le valutazioni effettuate a suo tempo dall'Ufficio, nell'ambito dell'istruttoria preliminare di una segnalazione, ha riformulato la modulistica utilizzata per le richieste di astensione obbligatoria e facoltativa per maternità, con particolare riferimento al rispetto dei princìpi di necessità, indispensabilità, pertinenza e non eccedenza dei dati trattati e alla correttezza dell'informativa sul trattamento dei dati personali (artt. 3, 11, 13 e 22 del Codice). È stata eliminata l'indicazione relativa ad alcune informazioni sulla gestazione della lavoratrice, quali la data dell'ultimo ciclo mestruale, quella dei primi movimenti del feto e dei fenomeni connessi alla gravidanza, nonché i rilievi obiettivi per la diagnosi risultanti dall'esame clinico. Nell'informativa, che è stata aggiornata al Codice, sono stati inoltre espunti i riferimenti al consenso al trattamento dei dati da parte delle lavoratrici, in quanto i soggetti pubblici non devono richiedere il consenso dell'interessato (art. 18 del Codice).

Permessi per l'assistenza a familiari disabili

Su impulso dell'Ufficio, al quale è prevenuta una segnalazione circostanziata, l'Inps sta avviando specifici approfondimenti in merito alle istruzioni fornite alle proprie articolazioni organizzative con la circolare n. 90 del 23 maggio 2007. La circolare prevede che i richiedenti i permessi per l'assistenza ai propri familiari disabili (art. 33 legge 5 febbraio 1992, n. 104), che lavorano o risiedono in luoghi distanti da quello del familiare, presentino all'atto della richiesta, un "Programma di assistenza" a firma congiunta del lavoratore e del familiare interessato (*Nota* 15 novembre 2007). All'esito di tali approfondimenti, l'Autorità verificherà il rispetto dei princìpi di pertinenza, non eccedenza e indispensabilità dei dati trattati dall'Istituto –specie se riferiti a terzi non direttamente interessati alle prestazioni da svolgere– in rapporto alle finalità di rilevante interesse pubblico perseguite (artt. 11, 20, 22, commi 3 e 5, 68 e 86, comma 1, lett. *c*), del Codice).

Modalità di rilascio dell'estratto conto contributivo relativo ai lavoratori

A seguito della segnalazione di una lavoratrice, che lamentava che il datore di lavoro aveva ricevuto un plico anonimo contenente il suo estratto conto contributivo, sono state verificate le modalità adottate dall'Inps per il rilascio di tali documenti, con particolare riferimento all'individuazione dei soggetti, diversi dal lavoratore interessato, che possono venire legittimamente a conoscenza dei dati personali, e alle modalità eventualmente adottate per prevenire l'indebita conoscenza di tali dati da parte di terzi non legittimati (artt. 19, 31 e 33 *ss.* del Codice). Sono stati inoltre richiesti specifici elementi riguardo al funzionamento di talune apparecchiature *self-service* per l'emissione degli estratti contributivi che, all'esito dei primi approfondimenti, risultavano essere installate presso alcune sedi dell'istituto e funzionare mediante l'inserimento del tesserino magnetico del codice fiscale non necessariamente appartenente all'interessato (*Note* 5 novembre 2007 e 21 dicembre 2007).

Dagli elementi acquisti all'esito dell'istruttoria preliminare, le modalità adottate dall'istituto non sono state ritenute in contrasto con la disciplina sulla protezione dei dati personali anche in considerazione della circostanza che l'evoluzione tecnologica ha determinato la riduzione dell'uso tali apparecchiature, le quali non risultano attualmente più attive.

10.4. *Attività di* marketing *e fidelizzazione*

Programmi di fidelizzazione

Il fenomeno delle carte e dei programmi di fidelizzazione (nei settori più vari, della grande distribuzione, telefonia, trasporti, viaggi) ha formato oggetto di accertamenti sulla conformità dei trattamenti al *provvedimento* generale in materia di fidelizzazione della clientela adottato il 24 febbraio 2005 [doc. *web n.* 1103045].

È così emerso che le prescrizioni contenute nel *provvedimento* sono state recepite solo in parte dagli operatori. Nel dettaglio, il Garante ha vietato a quattro società l'uso di dati personali trattati in modo illecito: alcune società raccoglievano, oltre ai dati anagrafici e ai recapiti degli interessati (necessari per attribuire *bonus* connessi all'uso della carta), ulteriori informazioni quali il titolo di studio, la professione e il numero dei componenti del nucleo familiare; dati ritenuti nei casi esaminati non pertinenti ed eccedenti dal Garante che ha ordinato ai titolari dei relativi trattamenti di cancellarli o di renderli anonimi (*Provv.* 15 novembre 2007 [doc. *web* nn. 1466930 e 1466898]). Altre irregolarità sono state riscontrate nella scarsa chiarezza o nella mancanza degli elementi indicati nell'art. 13 del Codice con cui vengono fornite le informative (comprese quelle rese *on-line*) ai consumatori e talora anche nella loro incompletezza, nonché nelle modalità di raccolta del consenso degli interessati (*Provv.* 15 novembre 2007 [doc. *web* nn. 1466971 e 1466985]).

L'Autorità ha ribadito la necessità di mettere il consumatore nelle condizione di poter scegliere liberamente se e quali trattamenti di dati autorizzare, chiarendo agli interessati che il consenso per l'utilizzo dei dati per finalità ulteriori rispetto a quelle connesse alla mera consegna dei premi e vantaggi previsti dal programma di fidelizzazione deve essere prestato liberamente: è quindi necessaria l'autonoma decisione del consumatore per l'utilizzo dei dati anche per finalità ulteriori, quale quella di *marketing* e di profilazione della clientela (*Provvedimenti* 15 novembre 2007 [doc. *web* nn. 1466956 e 1466898]).

Infine, in relazione all'uso di dati il cui conferimento era facoltativo a fini statistici, il Garante ha prescritto alle società di adottare opportuni accorgimenti che impediscano di ricondurre i dati all'interessato fin dal momento della raccolta (*Provv.* 15 novembre 2007 [doc. *web* n. 1466956]).

Sondaggi in materia elettorale

Verifiche sono state svolte nell'ambito del trattamento di dati personali (dati anagrafici, recapiti e opinioni espresse dagli interessati) per l'effettuazione di sondaggi telefonici di natura politico-elettorale finalizzati a rilevare il grado di soddisfazione dei residenti in un comune in vista delle consultazioni amministrative del 2006. Nel corso degli accertamenti è emerso che dalle risposte ai quesiti posti agli interessati era possibile risalire alle opinioni politiche degli intervistati (art. 4, comma 1, lett. *d*), del Codice).

Nella vicenda in parola, la disciplina in materia di protezione dei dati personali è stata violata sotto più profili (*Provv.* 13 settembre 2007 [doc. *web* n. 1523633]): non è risultato acquisito, limitatamente ai dati sensibili trattati, il consenso degli interessati in forma scritta (risultando, in base alle attestazioni fornite dalla società, la sua acquisizione solo telefonica); non sono state rispettate le condizioni previste dall'*autorizzazione generale* n. 5 del 21 dicembre 2005 (all'epoca applicabile e ora sostituita dall'analoga *autorizzazione generale* n. 5/2007) in materia di trattamento dei dati sensibili nello svolgimento di sondaggi e ricerche (Capo II); i trattamenti effettuati non erano stati notificati al Garante (art. 37, comma 1, lett. *e*), del Codice, relativo all'obbligo di notificazione di dati sensibili utilizzati per sondaggi d'opinione).

A ciò si aggiunga che i dati personali trattati (in particolare, quelli identificativi) erano sicuramente eccedenti, atteso che, per l'esecuzione del sondaggio, non è necessario registrare e conservare la valutazione espressa dagli interessati unitamente ai dati identificativi degli stessi (come invece avvenuto nel caso di specie).

Inoltre, anche in relazione ai dati diversi da quelli sensibili, il Garante ha ritenuto che, una volta consegnati gli elaborati delle interviste al committente, non sussistessero più le ragioni per la loro ulteriore conservazione presso la società che aveva eseguito il sondaggio (art. 11, comma 1, lett. *e*), del Codice): esaurita l'elaborazione delle informazioni personali consentita nella misura indispensabile, infatti, la società avrebbe dovuto procedere alla cancellazione o anonimizzazione dei dati personali relativi agli interessati.

Il Garante ha dunque prescritto alla società, titolare del trattamento la cancellazione o l'anonimizzazione dei dati personali raccolti illecitamente. È stato altresì prescritto che prima dell'effettuazione dei sondaggi vengano fornite all'interessato, anche ricorrendo a formulazioni sintetiche ma chiare, le informazioni contenute nell'art. 13 del Codice (anzitutto indicando chiaramente la finalità, mentre nel caso di specie si era operato un riferimento generico alla rilevazione della qualità della vita e dell'ambiente nell'area interessata).

Le proposte commerciali nel mercato dell'energia elettrica

Con *deliberazione* del 25 luglio 2007 [doc. *web* n. 1428567], adottata al termine di una procedura di cooperazione con l'Autorità per l'energia elettrica e il gas, il Garante ha fornito una serie di indicazioni sulle offerte commerciali formulate da

soggetti operanti nel mercato libero elettrico, per garantire una corretta informazione degli utenti e un giusto utilizzo dei loro dati.

La disciplina sulla liberalizzazione dell'energia (d.l. 18 giugno 2007, n. 73) prevede infatti che, a partire dal 1 luglio 2007, i clienti domestici possano scegliere un fornitore diverso. L'Autorità per l'energia elettrica e il gas ha quindi rappresentato la necessità che, per un periodo transitorio, le società che vendono energia possano acquisire dai distributori alcune informazioni di base relative agli utenti del mercato energetico per formulare proposte commerciali.

In questa cornice, l'Autorità per l'energia elettrica e il gas ha approvato con la deliberazione del 27 giugno 2007 n. 157 una prima parte della *"Disciplina in materia di accesso ai dati di base per la formulazione di proposte commerciali inerenti la fornitura di energia elettrica e/o di gas naturale"*, e ha interpellato il Garante sul trattamento dei dati personali degli utenti. Al riguardo l'Autorità ha stabilito che le società distributrici dovranno informare la clientela prima di comunicare i dati personali dati (generalità, consumi, potenza impegnata *ecc.*): per agevolare tale compito il Garante ha curato la predisposizione di un modello (allegato alla citata delibera). L'informativa dovrà preferibilmente essere recapitata unitamente alla corrispondenza inviata ordinariamente alla clientela (*ad es.*, con la bolletta) e dovrà essere messa a disposizione anche sul sito Internet delle società o attraverso i servizi di assistenza e informazione al pubblico.

I venditori dovranno utilizzare i dati solo con modalità strettamente correlate all'invio delle proposte cartacee e non dovranno conservare i dati relativi a clienti che, decorso un congruo termine non superiore a sei mesi, non abbiano aderito alla proposta; ciò, ferma restando la possibilità di utilizzare i dati di base ottenuti dai distributori fino al raggiungimento di un adeguato grado di concorrenza dei mercati dell'energia elettrica e del gas naturale sulla base di valutazioni della competente Autorità e, comunque, non oltre il 31 dicembre 2010. Decorso tale termine tutti i dati personali forniti dai distributori in relazione ai quali non si sia instaurato un rapporto di fornitura dovranno essere cancellati.

10.5. *Altre attività imprenditoriali*

Attività di impresa e semplificazioni. La "Guida pratica" per le piccole e medie imprese

Nel corso degli anni è emerso, anche tramite associazioni di categoria, che alcuni adempimenti contenuti nella disciplina di protezione dei dati personali vengono reputati talvolta onerosi per l'ordinaria attività di impresa.

Considerato però che una giusta protezione dei dati personali può rappresentare una risorsa per l'impresa, rendendone più efficiente l'attività e incrementando la fiducia di consumatori e utenti, il Garante ha messo a punto una "Guida pratica" pubblicata nella *Gazzetta Ufficiale* 21 giugno 2007, *n.* 142 [doc. *web* n. 1412271], per facilitare le piccole e medie imprese, ivi compresi gli artigiani, nell'assolvimento degli obblighi imposti dalla normativa sulla protezione dei dati personali.

La *"Guida pratica e misure di semplificazione per le piccole e medie imprese"* fornisce soluzioni semplificate per un corretto trattamento dei dati personali: dall'individuazione del titolare del trattamento e dei suoi obblighi alle verifiche sui soggetti che possono effettuare il trattamento (incaricati e responsabili); all'indicazione dei casi in cui l'imprenditore non è tenuto ad effettuare la notificazione al Garante o a rendere l'informativa agli interessati, o comunque può renderla in forma semplificata (art. 13, commi 2 e 3); chiarimenti sono espressi anche in relazione ai casi nei quali non è necessario richiedere il consenso dell'interessato (si tratta dei casi che comprendono larga parte dei trattamenti effettuati ordinariamente dall'impresa e

che sono indicati nelle lettere *a*)-*d*) dell'art. 24, comma 1, del Codice); ai doveri del titolare per soddisfare le richieste di accesso nel caso di esercizio dei diritti e alla sempre maggiore necessità di trasferire dati personali all'estero.

La Guida è stata integrata con un questionario che dovrebbe agevolare un'immediata verifica da parte degli imprenditori di eventuali criticità rispetto all'osservanza dei princìpi di protezione dei dati.

Cartolarizzazioni

All'inizio del 2007 (*Provv.* 18 gennaio 2007 [doc. *web* n. 1392461]) l'Autorità si è pronunciata in materia di operazioni di cartolarizzazione, regolate dalla l. 30 aprile 1999, n. 130, e di altre operazioni che presentavano caratteristiche omogenee. L'Autorità aveva già individuato modalità alternative (rispetto a quella individuale) per rendere l'informativa ai debitori ceduti da parte del cessionario (da ultimo *Provv.* 4 aprile 2001 [doc. *web* n. 40763]), disponendo che l'informativa fosse resa dal cessionario mediante pubblicazione sulla *Gazzetta Ufficiale* e con annunci pubblicati su almeno due quotidiani nazionali e uno locale.

Nel corso dell'attività di controllo volta ad accertare l'adozione delle menzionate misure da parte di tutte le società cessionarie che nel tempo avevano inviato al Garante apposita istanza di esonero dall'informativa in vista dell'esecuzione di operazioni di cartolarizzazione, sono emerse ampie aree di omessa o inidonea informativa rispetto alle indicazioni contenute nel *provvedimento* del 2001.

L'intervento dell'Autorità in tale settore è stato ritenuto necessario anche alla luce di alcune innovazioni normative contenute nel Codice (entrato in vigore successivamente all'adozione del menzionato *provvedimento* del Garante). In particolare, l'art. 13, comma 5, lett. *c*), del Codice prevede ora espressamente che, in casi determinati, il titolare del trattamento sia esonerato dall'obbligo di fornire l'informativa all'interessato, rimettendo al Garante l'eventuale individuazione di *"misure appropriate"* per consentire comunque adeguata pubblicità al trattamento effettuato. L'art. 2 del Codice, con disposizione assente nel quadro normativo previgente, dispone, tra l'altro, la semplificazione degli adempimenti richiesti dalla disciplina in materia di protezione dei dati personali ai titolari del trattamento, pur assicurando un elevato livello di tutela dei diritti e delle libertà fondamentali dell'interessato nell'ambito di operazioni di trattamento (*cfr.* art. 2, comma 2, del Codice; considerando n. 49 direttiva 95/46/Ce). L'esigenza di un nuovo intervento dell'Autorità nel settore è derivata anche dalla crescente complessità di talune operazioni di cartolarizzazione, attuate mediante la conclusione di "contratti cornice" tra cedente e cessionario del credito funzionali a regolamentare una pluralità di operazioni di cessione di crediti, nonché l'attribuzione di compiti ulteriori, con particolare riferimento alla gestione dei crediti per conto del cessionario (abitualmente denominato "società veicolo" o *special purpose vehicle*), non di rado posta in capo alla stessa società cedente i crediti (*cd. "originator"*).

Pertanto, muovendo anche dalla considerazione che l'informativa effettuata singolarmente a ciascun debitore comporterebbe costi manifestamente sproporzionati rispetto al diritto tutelato, con il nuovo *provvedimento* il Garante ha individuato chiaramente le operazioni di cessione in blocco dei crediti che determinano la comunicazione dal cedente al cessionario di dati personali relativi al debitore ceduto ("interessato"), precisandone l'ambito di applicazione con riguardo sia alle operazioni di cessione in blocco a titolo oneroso di portafogli di crediti pecuniari, anche futuri, di cui alla l. 30 aprile 1999, n. 130 (recante disposizioni sulla cartolarizzazione di crediti) sia alle operazioni di cessione dei crediti disciplinate all'art. 58 del d.lg. 1 settembre 1993, n. 385 (*Testo unico delle leggi in materia bancaria e creditizia*), sia alle operazioni di cessione dei crediti futuri e di crediti in massa, disciplinate dalla l. 21 febbraio 1991, n. 52, in materia di cessione di crediti d'impresa (*cd.* "legge sul *factoring*").

Ai sensi dell'art. 13, comma 5, lett. *c*) del Codice, il Garante ha, dunque, esonerato, in via generale, i cessionari di crediti in blocco rientranti nell'ambito di applicazione del *provvedimento* dall'obbligo di rendere l'informativa, senza che debba essere presentata apposita istanza di autorizzazione al Garante. In applicazione del principio di semplificazione, inoltre, ha disposto la pubblicazione dell'informativa contenente gli elementi previsti dall'art. 13, commi 1 e 2, del Codice sulla sola *Gazzetta Ufficiale*, eliminando alcuni degli adempimenti che, alla luce delle verifiche effettuate, erano risultati inefficaci sotto il profilo della effettiva conoscibilità da parte degli interessati o troppo onerosi per le imprese. In particolare, non è più richiesta la pubblicazione dell'informativa sulle testate giornalistiche, e quella resa mediante l'affissione nei locali della cessionaria.

Si è provveduto comunque a individuare, quale misura appropriata a garanzia degli interessati, l'invio dell'informativa individuale nei confronti del singolo debitore ceduto alla prima occasione utile (*ad es.*, in sede di invio dell'estratto conto o della prima richiesta di pagamento, se del caso anche tramite la società incaricata dei servizi di *servicing*).

Adempimenti semplificati per i servizi telefonici di assistenza e di informazione al pubblico

L'esigenza di semplificazione è emersa anche in relazione ai servizi telefonici di assistenza e di informazione al pubblico utilizzati da numerosi soggetti nello svolgimento della propria attività (pubblica o privata) per una vasta gamma di funzioni: tra le più ricorrenti, possono evidenziarsi quelle di informazione e/o di assistenza alla clientela (*cd. "customer care"*), con riferimento all'instaurazione e all'esecuzione di rapporti contrattuali in vari contesti (quali prenotazione di servizi a sovrapprezzo di tipo sociale-informativo, di assistenza, di consulenza e di intrattenimento), ma anche quelle svolte a vantaggio della collettività da parte di amministrazioni pubbliche.

Tenendo conto delle dimensioni assunte dal fenomeno, e con riguardo anche alle sollecitazioni provenienti da un'associazione di categoria rappresentativa delle società di *call center* operanti in *outsourcing*, l'Autorità ha ritenuto opportuno intervenire in materia con un *provvedimento* generale del 15 novembre 2007 (doc. *web* n. 1462788), soffermandosi in particolare sulle attività prestate in modalità *"inbound"* (ossia a seguito di chiamate degli utenti, effettuate anche attraverso canali completamente automatizzati).

In attuazione del principio di semplificazione contenuto nel Codice (art. 1, comma 2 e più in particolare art. 13, commi 2 e 3) il Garante ha precisato che in molti casi (specie per servizi meramente informativi), non essendo trattati dati personali, la disciplina di protezione dei dati personali (e i correlativi adempimenti) non trova applicazione.

Nei casi in cui l'informativa non sia già stata fornita in precedenza (si pensi ai *cd.* "servizi *post*-vendita resi telefonicamente), può rendersi necessario fornire all'interessato gli elementi previsti all'art. 13 del Codice: anche per questa ipotesi, tuttavia, il Garante ha precisato (al fine di prevenire una scorretta interpretazione della disciplina e l'introduzione di prassi inutilmente burocratiche) che gli operatori qui presi in considerazione possono non fornire "gli elementi già noti" all'interessato (art. 13, comma 2).

Ogni altro ulteriore elemento, in base al principio di cui all'art. 2 del Codice, può essere comunque fornito con formule sintetiche, purché chiare e di immediata comprensione, ad esempio utilizzando messaggi preregistrati nel corso di eventuali tempi di attesa.

Coloro che prestano i servizi in esame sono stati autorizzati (senza rivolgere al Garante alcuna richiesta), dopo aver rappresentato in modo semplificato agli utenti gli eventuali elementi dell'informativa che risulti necessario fornire, a indicare la modalità attraverso la quale l'interessato può prendere conoscenza integrale del-

l'informativa, anche tramite un messaggio ascoltabile digitando una cifra sulla tastiera del telefono. Apposita istanza deve essere invece formulata solo per situazioni meritevoli di specifico esame.

Per quanto riguarda i servizi abilitati in base alla legge a ricevere chiamate d'emergenza (d.m. Min. comunicazioni 27 aprile 2006 sul servizio "112" quale numero unico europeo d'emergenza; *v.* anche *Parere* 6 aprile 2006, [doc. *web* n. 1269343]) il Garante ha stabilito che, attesa la loro peculiare natura, i titolari del trattamento possono rendere l'informativa agli interessati (se dovuta in base al Codice: *cfr.* art. 53) inserendola nei siti *web* di riferimento.

Nel *provvedimento* l'Autorità ha inoltre invitato le società che operano nella gestione dei servizi telefonici a considerare la natura dei dati trattati, che talora possono essere di natura sensibile (si pensi alle informazioni raccolte nell'ambito di servizi prestati da strutture sanitarie); ad assicurare elevati livelli di professionalità nel trattamento dei dati, nonché ad adottare adeguate soluzioni tecnico-organizzative anche in ordine alla sicurezza dei dati e dei sistemi.

In tal senso, il contratto di fornitura del servizio di assistenza telefonica al pubblico deve contenere concrete modalità operative idonee ad assicurare condizioni di trasparente e corretto svolgimento delle relazioni con l'utenza, indicando altresì le misure di sicurezza che dovranno essere adottate, anche al fine di prevenire commistioni tra distinti archivi gestiti dal medesimo responsabile del trattamento.

L'Autorità ha inoltre precisato che le informazioni raccolte devono essere utilizzate solo per scopi determinati, espliciti e legittimi, senza l'utilizzo di dati di abbonati e di utenti non necessari.

I soggetti privati devono di regola sollecitare il consenso informato qualora intendano utilizzare i dati per finalità diverse e compatibili, come nel caso del *marketing* o della creazione di profili relativi all'utenza (artt. 23 e 24 del Codice), mentre i soggetti pubblici devono operare pur sempre per dichiarate finalità istituzionali, nell'osservanza delle pertinenti disposizioni del Codice (*cfr.* artt. 18 *ss.* del Codice).

Infine, eventuali registrazioni legittime del contenuto delle comunicazioni, effettuate con l'operatore o per il tramite di dispositivi automatici, possono essere conservate solo per un periodo di tempo necessario al corretto assolvimento delle operazioni richieste dagli utenti o alle eventuali esigenze di fatturazione, nei casi di servizi a pagamento, salva l'osservanza di specifici obblighi di legge che ne legittimino l'ulteriore conservazione.

10.6. *Attività di impresa e controlli*

Accertamenti in ambito alberghiero

Nell'ambito di verifiche sull'osservanza della disciplina in materia protezione dei dati personali nella compilazione della *cd.* "schede albergo" e di "altri trattamenti dei dati personali dei clienti" è stato ribadito, in particolare, che il trattamento effettuato per finalità diverse da quelle di esecuzione del contratto alberghiero richiede il consenso libero, specifico e informato dell'interessato (art. 23, comma 3, del Codice) (*Nota* 9 agosto 2007). Nel modello di informativa in uso presso la struttura alberghiera interessata dagli accertamenti, il consenso era richiesto con un'unica formula onnicomprensiva. Come già rilevato in passato dal Garante, la capacità di autodeterminazione dell'interessato non è assicurata quando si sollecita il consenso in modo indifferenziato per perseguire anche la finalità di *marketing*, mediante *"l'invio di mailing"* o la *"comunicazione di offerte speciali"* alla clientela (tra i tanti, *Provv.* 24 febbraio 2005, punto 7 [doc. *web* n. 1103045]).

Con riferimento all'enunciazione delle diverse finalità del trattamento (art. 13, comma 1, lett. *a*) del Codice), l'Autorità ha messo in luce l'opportunità che gli elementi individuati all'art. 13 del Codice "*compaiano in un unico messaggio*" (*cfr.*, sul punto, *Provv.* 13 gennaio 2000 [doc. *web* n. 42276]) in modo da risultare agevolmente individuabili, ponendo in distinta e specifica evidenza le caratteristiche dell'eventuale attività di profilazione e/o di *marketing*, come pure l'intenzione di cedere a terzi specificamente individuati i dati per finalità da indicare puntualmente (*cfr. Provv.* 24 febbraio 2005 [doc. *web* n. 1103045]).

Attesa la scarsa chiarezza del modello di informativa attualmente distribuita alla clientela, la società è stata invitata a predisporre un nuovo modello di informativa riformulato, alla luce delle prescrizioni già fornite in via generale dal Garante con i richiamati provvedimenti, al fine di rendere la medesima trasparente e di agevole comprensione per gli interessati e collocando, altresì, le pertinenti informazioni in un'unica sede.

Trattamenti di dati per il servizio garanzia assegni

A seguito di talune alcune segnalazioni pervenute nel tempo, sono stati svolti accertamenti presso alcuni esercizi commerciali sulla conformità alla disciplina in materia di protezione dei dati personali delle operazioni di trattamento poste in essere da una società che acquista *pro-soluto* crediti vantati da parte di esercizi commerciali convenzionati sorti in occasione di vendite pagate con assegni bancari.

Con *provvedimento* del 17 maggio 2007 (doc. *web* n. 1409251) il Garante ha fornito prescrizioni ai sensi dell'art. 154, comma 1, lett. *c*) del Codice e fissato un termine entro il quale la società ha provveduto a rendere il complessivo trattamento dei dati personali strumentale alla gestione del servizio conforme alla disciplina del Codice.

Nel corso dell'attività istruttoria era emerso che, in particolare, dati identificativi del traente (nome, cognome, indirizzo, tipologia e numero del documento di identità, recapito telefonico) e dati idonei a identificare l'assegno (codice Abi e Cab della banca, conto corrente e numero dell'assegno) erano conservati per un periodo "indefinito"; venivano utilizzati per valutare se procedere all'acquisto del credito nei confronti degli esercizi convenzionati; venivano trattati unitamente a dati eventualmente provenienti da archivi pubblici o privati (quali la Centrale d'allarme interbancaria o società esterne che forniscono dati relativi a protesti o pregiudizievoli).

A tale proposito il *provvedimento* ha ribadito la necessità di identificare tempi massimi di conservazione dei dati trattati alla luce delle finalità in concreto perseguite, salva la necessità che i dati personali siano conservati in conformità a puntuali disposizioni normative (*ad es.*, quelle sulle scritture contabili). Le informazioni necessarie alla gestione del servizio possono essere trattate, infatti, per il tempo strettamente necessario allo svolgimento dello stesso e, comunque, non oltre i termini di prescrizione delle azioni eventualmente esercitabili a tutela del credito (art. 11, comma 1, lett. *e*), del Codice).

Il Garante ha poi prescritto alla società, in qualità di titolare del trattamento, di effettuare le verifiche previste dall'art. 30 del Codice impartendo le dovute istruzioni, anche mediante controlli periodici, ancorché a campione, a mezzo di propri incaricati, sull'adempimento da parte del personale operante presso gli esercizi commerciali dell'obbligo di rendere l'informativa ai sensi dell'art. 13 del Codice.

Con il *provvedimento* in esame il Garante ha dichiarato inidonea l'informativa in quanto nel testo predisposto non risultava presente la circostanza che dati personali riferiti all'interessato potessero essere raccolti dalla società anche presso terzi (nel caso di specie, banche dati pubbliche e private), e ha conseguentemente prescritto di integrarla.

Da ultimo, con riferimento alla designazione degli esercizi commerciali convenzionati e/o dei rappresentanti legali dei punti vendita quali "incaricati del trattamento", l'Autorità ha sottolineato che sono tali solo le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile e in quanto operanti *"sotto la diretta autorità"* di questi, in presenza di un atto scritto di designazione e tenuti comunque ad attenersi alle istruzioni dai medesimi impartite (artt. 4, lett. *h*) e 30 del Codice) (*cfr. Provv.* 8 giugno 1999 [doc. *web* n. 42260]). Con riferimento alla designazione del personale addetto alle vendite all'interno dei punti vendita convenzionati come "incaricati", inoltre, il Garante ha osservato che il rapporto di dipendenza o di collaborazione che tali soggetti hanno con l'esercizio commerciale convenzionato appare incompatibile con la qualifica di incaricati della società. Ciò non toglie che tali soggetti possono comunque porre in essere operazioni di trattamento anche a vantaggio della società, ma quali incaricati di tali operazioni di trattamento da parte del proprio datore di lavoro (previamente designato "responsabile del trattamento" dalla società).

L'Autorità ha quindi fissato un termine, correttamente osservato dalla società per l'attuazione delle prescrizioni formulate.

Trattamento di dati personali presso agenzie di intermediazione immobiliare

Nell'ambito del programma di ispezioni nei confronti di alcuni settori e categorie professionali, è emerso che un'agenzia immobiliare raccoglieva, oltre ai dati necessari per adempiere al proprio mandato (dati anagrafici, indirizzo, numero di telefono, *ecc.*), anche i dati sensibili delle persone che la contattavano per la compravendita o la locazione di una casa in quanto alcuni proprietari non avrebbero gradito stipulare contratti di locazione con extracomunitari, omosessuali o con persone di fede religiosa islamica.

Con il *provvedimento* dell'11 gennaio 2007 [doc. *web* n. 1381620], accertata l'illiceità del trattamento, il Garante ha vietato all'agenzia immobiliare di utilizzare tali informazioni personali, in quanto discriminatorie e lesive della dignità delle persone, e in contrasto con quanto stabilito dal Codice e dalle autorizzazioni generali in materia di trattamento di dati sensibili (artt. 2, 11, 26, 40 e 41 del Codice), oltre che in violazione delle norme sulla parità di trattamento tra le persone (art. 29, comma 1, lett. *d*), punto 9 l. n. 39/2002; art. 3, comma 1, lett. *i*) d.lg. n. 215/2003).

Il Garante ha inoltre prescritto all'agenzia di riformulare l'informativa, in particolare quella resa *on-line*, specificando chiaramente le finalità di utilizzo dei dati personali raccolti; si è inoltre rilevato che l'agenzia è tenuta inoltre a fornire indicazioni agli interessati circa la facoltà di rifiutare sin dall'inizio (oltre che in occasione di successive comunicazioni) l'utilizzo dell'indirizzo di posta elettronica per finalità di *marketing* (art. 130, comma 4, del Codice; in merito *v.* pure *Provv.* 3 novembre 2005, punto 3.2. [doc. *web* n. 1195215]).

È stata invece considerata lecita dal Garante la raccolta di informazioni relative ad *handicap* o patologie invalidanti in quanto effettuata dall'agenzia per escludere dalle trattative immobili con barriere architettoniche o privi di ascensore.

Recupero crediti

Nel 2007 il Garante ha avviato e concluso accertamenti sullo svolgimento dell'attività di recupero dei crediti, al fine di verificare l'osservanza delle prescrizioni contenute nel *provvedimento* generale del 30 novembre 2005 [doc. *web* n. 1213644], a suo tempo trasmesso a tutte le società interessate dall'istruttoria.

La maggior parte delle società interessate ha dichiarato nella sostanza di aver adeguato le proprie procedure interne alle prescrizioni del Garante.

Tuttavia, in considerazione di ulteriori segnalazioni pervenute, è emerso che persistevano prassi finalizzate al recupero stragiudiziale dei crediti caratterizzate da modalità di ricerca e di presa di contatto del debitore invasive e, talora, lesive della riservatezza e della dignità personale.

L'Autorità ha così provveduto –anche avvalendosi dell'ausilio della Guardia di finanza– a inviare richieste più analitiche di informazioni ai sensi dell'art. 157 del Codice nei confronti di sette società che, a vario titolo, effettuano il recupero stragiudiziale del credito.

Dalle risultanze ispettive è emerso che, complessivamente, le società operanti nel settore hanno rispettato le prescrizioni del Garante contenute nel *provvedimento* del 30 novembre 2005.

Un profilo di criticità, emerso anche nel corso di un incontro con l'associazione di categoria (Unirec-Unione nazionale imprese recupero crediti e informazioni commerciali), attiene alla qualificazione soggettiva delle società di recupero crediti quando operano quali mandatarie nell'attività di riscossione. In particolare, talvolta esse vengono designate quali "responsabili del trattamento"; talora, invece, appaiono assumere il ruolo di "titolari del trattamento" (pur operando quali mandatarie del creditore o, comunque, nell'ambito dell'appalto di servizi nell'attività di recupero dei crediti e salva ogni ulteriore verifica in ordine al consenso prestato dalla clientela a tale comunicazione a terzi).

Trattamento di dati personali in sede di recupero credito mediante sistemi automatizzati di chiamata

Una società ha chiesto chiarimenti sulla parte del *provvedimento* nella quale si prevede che integri un illecito trattamento il ricorso a comunicazioni telefoniche preregistrate volte a sollecitare i pagamenti dovuti.

Con *Nota* 1 giugno 2007 l'Autorità ha precisato che non deve ritenersi precluso l'utilizzo di comunicazioni telefoniche senza l'intervento di un operatore per sollecitare pagamenti, ma che l'impiego di tale modalità –proprio in considerazione delle specifiche caratteristiche del mezzo usato, oltre che del contenuto del messaggio trasmesso– implica il rischio di comunicare a soggetti diversi dall'interessato, in assenza di sua espressa autorizzazione (art. 4, comma 1, lett. *l*) del Codice), dati personali riferiti al debitore e, in particolare, il suo asserito inadempimento.

Pertanto, in questi casi è necessario che il trattamento delle informazioni riferite ai debitori con le modalità anzidette si svolga nel pieno rispetto della disciplina in materia di protezione dei dati personali e in presenza dei presupposti di liceità del trattamento previsti dal Codice.

A questo riguardo sono state fornite ulteriori indicazioni ricordando che, in generale, la società che intenda avvalersi del meccanismo di chiamate preregistrate, anche senza l'ausilio di un operatore, è tenuta a dotarsi di idonei meccanismi a tutela della riservatezza degli interessati.

A tal fine potrebbe essere fornito al cliente, in sede di conclusione del contratto, un codice identificativo personale (di agevole memorizzazione) da digitare sull'apparecchio telefonico per ascoltare eventuali comunicazioni preregistrate a lui dirette, sì da scongiurare che comunicazione di dati personali riferiti al debitore siano resi noti a terzi che, per le ragioni più varie, utilizzino la medesima utenza telefonica.

Diversamente, ove si adottino modalità di trattamento di dati personali suscettibili di determinare una comunicazione a terzi di dati personali (non necessaria ai fini dell'esecuzione del contratto), è indispensabile, in assenza di altri presupposti di liceità del trattamento (artt. 24 e 25 del Codice), che i committenti, in qualità di titolari del trattamento (artt. 4, comma 1, lett. *f*) e 28 del Codice), acquisiscano uno specifico consenso informato dell'interessato alla comunicazione di dati a terzi (nel caso di specie, da individuarsi nei soggetti che potrebbero far uso dell'utenza telefonica attribuita al debitore) (artt. 13 e 23 del Codice).

Si è infine richiamata l'attenzione sul generale obbligo di informativa, in sede di raccolta delle informazioni personali della clientela: in tale occasione, con riferimento all'attività di recupero crediti, devono essere chiarite le *"modalità del trattamento cui sono destinati i dati"* (art. 13, comma 1, lett. *a*) del Codice), nonché indi-

cati i *"soggetti o le categorie di soggetti ai quali i dati possono essere comunicati"* (art. 13, comma 1, lett. *d*) (nell'ipotesi indicata al punto 4, i soggetti che possono rispondere all'utenza telefonica del debitore) o che *"possono venirne a conoscenza in qualità di responsabili o incaricati e l'ambito di diffusione degli stessi"* (dipendenti, collaboratori, anche società di recupero crediti, se nominate responsabili).

Vivavoce

Per quanto concerne l'impiego di dispositivi atti a consentire l'ascolto di conversazioni a soggetti diversi dagli utenti, è pervenuta all'Autorità una segnalazione con cui si contestava un utilizzo indebito del *cd.* "viva voce" da parte di una società di gestione del credito. L'Autorità, nell'invitare quest'ultima a fornire chiarimenti, ha ricordato che l'art. 131, comma 3, del Codice impone all'utente di informare l'altro utente *"quando, nel corso della conversazione, sono utilizzati dispositivi che consentono l'ascolto della conversazione stessa da parte di altri soggetti"*. Tale obbligo discende direttamente dal più generale principio di lealtà e correttezza che deve informare ogni trattamento di dati personali (art. 11, comma 1, lett. *a*) del Codice). All'esito degli accertamenti preliminari effettuati, nel prendere atto delle dichiarazioni rese dalla società ai sensi e per gli effetti di cui all'art. 168 del Codice non si sono ravvisati elementi per adottare un provvedimento (*Nota* 29 febbraio 2008).

11 Trasferimento di dati personali all'estero

La tematica delle *cd. "Binding corporate rules (Bcr)"* ha formato oggetto di approfondito esame anche nel corso del 2007, considerato che già nel 2006 (*cfr. Relazione* 2006, *p.* 108), erano pervenute numerose richieste provenienti da altre autorità di controllo volte a concordare la scelta della *cd. "lead authority"* nell'ambito di procedure di cooperazione concernenti alcuni progetti di *Bcr* elaborati da vari gruppi societari operanti a livello sopranazionale; in taluni casi sono pervenuti anche *consolidated draft* rispetto a progetti di *Bcr* in fase di più avanzata elaborazione.

Nel 2007 anche un gruppo bancario italiano ha formulato, in relazione al trattamento dei dati relativi ai propri dipendenti, una richiesta volta a instaurare la procedura di coordinamento per l'approvazione di *Bcr* innanzi all'autorità italiana in qualità di *lead authority*; al fine di effettuare una valutazione preliminare del progetto di *Bcr* menzionato hanno avuto luogo alcuni incontri tecnici, finalizzati anche a verificare la sussistenza dei presupposti affinché il Garante possa assumere il ruolo di *lead authority* della relativa procedura (in conformità al documento WP 107 del Gruppo art. 29).

In termini più generali, sussistono dubbi sull'efficacia vincolante dello strumento delle *Bcr* nell'ordinamento italiano (questione sollevata in passato anche da altre autorità di protezione dati) e, quindi, sull'effettiva garanzia per i cittadini interessati in caso di loro inosservanza.

L'attuale incertezza potrebbe indurre il Garante a disconoscere la sussistenza di adeguate garanzie per i diritti degli interessati, che pure siano previste all'interno dei menzionati codici di condotta.

Il Garante, nella consapevolezza dell'importanza che rivestono oggi i flussi di dati personali nello svolgimento di operazioni economiche transfrontaliere (ormai ricorrenti nel mercato globalizzato), ha pertanto segnalato formalmente al Parlamento e al Governo l'opportunità di integrare la disciplina di protezione dei dati personali (come già accaduto in altri ordinamenti nazionali, quali la Francia e la Germania) con una norma che consenta di reputare le regole di condotta osservate all'interno di gruppi di società quale strumento adeguato ai fini del trasferimento dei dati personali al di fuori dell'Ue e dello Spazio economico europeo.

12 Libere professioni

Nel 2007 si è registrato un notevole incremento di attività con riguardo sia a segnalazioni e reclami pervenuti in tema di attività forense, ordini professionali e pubblici servizi, sia ai lavori del codice di deontologia e di buona condotta per il trattamento dei dati personali effettuato per investigazioni difensive o per tutelare un diritto in sede giudiziaria (art. 135 del Codice).

12.1. *Attività forense*

Nel quadro dell'esame degli atti pervenuti all'Autorità in materia di attività forense, è stata dedicata particolare attenzione alle modalità di acquisizione e di utilizzazione delle prove dedotte in giudizio da parte dei legali nell'esercizio delle funzioni di assistenza e difesa.

In particolare, è emersa l'esigenza di richiamare gli operatori del settore ad un più attento rispetto dei princìpi di liceità e di correttezza del trattamento, soprattutto in relazione alle modalità di raccolta e di utilizzo nel processo di dati personali sensibili.

Con specifico riferimento a singoli episodi di trattamento di dati idonei a rivelare lo stato di salute e la vita sessuale, è stato necessario intervenire, in diverse occasioni, nei confronti del titolare, richiamandolo al puntuale rispetto del principio del "pari rango" (*cfr. Provv.* 9 luglio 2003 [doc. *web* n. 29832]).

In ordine all'ammissibilità di prove dedotte in giudizio, l'Autorità, in risposta alle numerose segnalazioni pervenute, ha ribadito la necessità che eventuali eccezioni circa la liceità e l'ammissibilità di prove e di fonti di prova nel processo vengano sollevate innanzi al giudice adito o designato e non davanti al Garante.

Il codice di deontologia e di buona condotta

Il 2007 ha segnato un passaggio importante nell'ambito dell'attività volta alla sottoscrizione del codice di deontologia e di buona condotta per il trattamento dei dati personali effettuato per svolgere investigazioni difensive o per far valere o difendere un diritto in sede giudiziaria (art. 135 del Codice).

I lavori di redazione di tale codice si sono susseguiti con notevole intensità nel corso dell'anno, anche all'interno delle riunioni promosse dall'Autorità con i soggetti interessati.

Per le categorie interessate ai sensi dell'art. 12 del Codice, hanno preso parte ai lavori, in rappresentanza dell'avvocatura: il Cnf (Consiglio nazionale forense), l'Aiga (Associazione italiana giovani avvocati), l'Oua (Organismo unitario dell'avvocatura), l'Ucp (Unione delle camere penali), l'Ucc (Unione delle camere civili), l'Uae (Unione avvocati europei); per il mondo dell'investigazione privata: la Federpol (Federazione italiana istituti privati investigazioni informazioni sicurezza), il Sandip (Sindacato autonomo nazionale degli investigatori privati), il Conipi (Confederazione nazionale investigatori privati), l'Aipros (Associazione italiana professionisti della sicurezza).

Gli incontri, caratterizzati da grande spirito di collaborazione da parte di tutti i partecipanti, hanno reso possibile la definizione, negli ultimi mesi dell'anno, di uno schema preliminare di codice, sottoposto dalle medesime categorie interessate all'esame del Garante per le valutazioni di cui all'art. 6 del regolamento del Garante n. 2/2006.

Lo schema, che, sulla base di una prima verifica, il 20 marzo 2008 è stato ritenuto dall'Autorità conforme alla normativa vigente, è stato sottoposto a consultazione pubblica anche tramite il sito *web* del Garante [doc. *web* n. 1503511], al fine di consentire la raccolta di eventuali osservazioni da parte dei "soggetti interessati", prima della sua formale sottoscrizione (art. 12 del Codice; artt. 5 e 6 del regolamento del Garante n. 2/2006).

Gli aspetti di principale novità introdotti dallo schema di codice sottoposto all'attenzione dell'Autorità riguardano l'ambito di applicazione, i tempi di conservazione delle informazioni, i rapporti con i terzi e con la stampa e le modalità di trattamento dei dati personali per le finalità di difesa di un diritto in sede giudiziaria. Quest'ultimo aspetto, in particolare, ha sollevato l'esigenza di sollecitare i soggetti coinvolti a prestare specifica attenzione con riferimento allo scambio di corrispondenza, specie per via telematica, all'esercizio contiguo di attività autonome all'interno di uno studio, all'utilizzo di dati riportati su particolari dispositivi o supporti, specie se elettronici, come le registrazioni audio/video o i tabulati di flussi telefonici o informatici, e all'acquisizione informale di notizie, dati e documenti connotati da un alto grado di confidenzialità o che possono comportare, comunque, rischi specifici per gli interessati.

12.2. *Ordini professionali*

Con i rappresentanti delle libere professioni sono intercorsi diversi rapporti a livello nazionale e locale. Numerose sono state, in tale senso, le risposte a ordini professionali su quesiti e richieste di parere riguardanti il regime di circolazione dei dati personali degli iscritti agli albi ed elenchi tenuti presso gli ordini medesimi.

In merito, si è ricordato in diverse occasioni che l'art. 61 del Codice, rubricato *"Utilizzazione di dati pubblici"*, non ha modificato la disciplina legislativa relativa al regime di pubblicità degli albi professionali, i quali restano soggetti alle norme (legislative e/o regolamentari di settore) poste a presidio dei rispettivi ordini. La facoltà di comunicare e/o diffondere i dati trattati, deve essere valutata, di volta in volta, dal Consiglio dell'ordine interessato in considerazione delle specifiche forme di pubblicità predisposte dalla normativa di settore, con particolare attenzione a quanto previsto dalle leggi professionali e dai relativi regolamenti di attuazione.

Molto intensa è stata anche l'attività di vigilanza e di intervento a seguito di segnalazioni e di reclami nei confronti di singoli professionisti, ordini e collegi professionali. Nel corso dell'anno sono state evidenziate alcune situazioni di non conformità alla previsioni del Codice, soprattutto in relazione al mancato rispetto dei princìpi di proporzionalità, di necessità, di liceità e di correttezza del trattamento.

Sul punto, si segnala, tra l'altro, il *provvedimento* del 23 gennaio 2008 [doc. *web* n. 1487903], adottato nei confronti del Consiglio dell'ordine degli avvocati di Santa Maria Capua Vetere, in relazione alla raccolta dei dati personali biometrici di alcuni praticanti avvocati, mediante la predisposizione di un sistema di rilevamento delle impronte digitali con finalità di controllo degli accessi e di verifica della frequenza delle lezioni tenute presso la Scuola di formazione forense.

L'Autorità ha fatto presente che, sebbene rientri tra le legittime facoltà del Consiglio dell'Ordine quella di sovrintendere al regolare espletamento dei corsi di formazione dei praticanti iscritti, verificando la loro effettiva partecipazione alle lezioni della Scuola, tale esigenza non legittima di per sé il ricorso a sistemi di raccolta e trattamento di dati biometrici fuori dal quadro di garanzie in materia.

L'utilizzo di dati particolarmente significativi, quali quelli relativi alle impronte digitali, può essere, infatti, giustificato per soddisfare specifiche esigenze relative alla sicurezza di beni e di persone, laddove si evidenzi, sulla base di obiettive e documentate circostanze, una situazione di elevato rischio (*cfr. Provv.* 15 giugno 2006 [doc. *web* nn. 1306551 e 1306530]; *Provv.* 27 ottobre 2005 [doc. *web* n. 1246675]).

Non può, invece, ritenersi lecito l'uso dei dati biometrici per generiche esigenze di sicurezza e di mero ausilio al rispetto delle regole scolastiche e deontologiche, specie laddove esso riguardi la raccolta di dati particolari, come le impronte digitali, per i quali occorre individuare specifici accorgimenti volti a prevenire eventuali utilizzi impropri e possibili abusi (art. 17 del Codice).

Anche in queste ipotesi, il titolare del trattamento deve rispettare i princìpi di necessità e di proporzionalità (artt. 3 e 11), restando impregiudicata la facoltà di adottare altri sistemi di controllo degli accessi che escludano l'utilizzo di dati biometrici, in grado di consentire parimenti un'efficace attività di verifica dell'identità personale degli interessati ma, al tempo stesso, più rispettosi della sfera personale degli individui (quali, ad esempio, l'utilizzo di tesserini magnetici e l'effettuazione di controlli "a vista" dei partecipanti).

13 Concessionari di pubblici servizi

L'attività dell'Autorità in continuità con le azioni intraprese nel 2006, si è concentrata, in particolare, su due filoni di intervento: le *cd. "dichiarazioni stragiudiziali"* e le modalità di trattamento di dati poste in essere dall'Agenzia delle entrate (in qualità di titolare del trattamento) e dalla Rai-Radiotelevisione italiana (quale responsabile del trattamento), mediante il ricorso ad "agenti" privati (comunemente noti come "ispettori Rai") per contrastare il fenomeno del mancato pagamento del canone per i servizi radiotelevisivi.

Dichiarazioni stragiudiziali

Sono giunte diverse segnalazioni sulle *"dichiarazioni stragiudiziali"* che il concessionario del servizio per la riscossione dei tributi può chiedere (ai sensi dell'art. 75-*bis* del d.P.R. n. 602/1973, come modificato dalla legge n. 211/2004, recante la legge finanziaria per il 2005, art. 1, comma 425) anche prima di procedere al pignoramento presso terzi, ai debitori del soggetto iscritto a ruolo, per conoscere le cose e le somme da essi dovute al soggetto medesimo.

In relazione a tale normativa, dalla formulazione piuttosto generica, il Garante aveva previsto l'obbligo dei concessionari suddetti di informare preventivamente il soggetto iscritto a ruolo circa la possibilità, in caso di mancato pagamento, dell'acquisizione presso terzi della dichiarazione medesima (*cfr. Provv.* 25 maggio 2005, [doc. *web* n. 1131826] e *Relazione* 2006, *p.* 115).

A seguito dell'adozione del *provvedimento*, sono pervenute numerose segnalazioni, da parte di cittadini, concernenti prevalentemente violazioni dell'obbligo di rilascio della previa informativa.

Successivamente, la legge n. 286/2006 ha riscritto l'art. 75-*bis* del d.P.R. n. 602/73, stabilendo espressamente che gli agenti della riscossione possono procedere al trattamento dei dati personali acquisiti tramite dichiarazione stragiudiziale senza rendere l'informativa prevista all'art. 13 del Codice in materia di protezione dei dati personali.

L'attività del Garante, in parte ancora in corso, ha tenuto conto di tale ulteriore modifica del quadro normativo e ha peraltro rilevato, in diverse occasioni, il mancato rispetto dei princìpi di pertinenza e di non eccedenza nei trattamenti posti in essere dagli agenti della riscossione.

Agenzia delle entrate e Rai-Radiotelevisione italiana S.p.A.

Il Garante ha definito con *provvedimento* del 5 marzo 2008 [doc. *web* n. 1501024] l'istruttoria condotta nel 2007 sul trattamento di dati personali effettuato dall'Agenzia delle entrate-Sportello abbonamenti TV e presso Rai-Radiotelevisione italiana S.p.A. per finalità di promozione e di recupero del canone radiotelevisivo.

Numerose segnalazioni avevano lamentato comportamenti irrituali da parte di "ispettori" Rai, con toni minacciosi e modalità ritenute "inquisitorie" e "intimidatorie" nella raccolta di dati personali, anche in relazione alla prospettazione di possibili accertamenti intrusivi in caso di mancato conferimento di determinate informazioni.

Il Garante ha, in primo luogo, preso atto che in base alla convenzione in fase di applicazione tra l'Agenzia delle entrate e la Rai, quest'ultima può affidare a persone fisiche lo svolgimento di attività di promozione degli abbonamenti radiotelevisivi, anche attraverso contratti di agenzia, designandole come incaricati del relativo trattamento di dati personali.

Sotto il profilo della correttezza del trattamento, il Garante ha prescritto all'Agenzia delle entrate, per ciò che concerne l'attività svolta per suo conto da Rai, l'adozione entro il 30 aprile 2008 di misure che garantiscano che il trattamento dei dati personali, effettuato a cura degli incaricati suddetti, sia conforme ai princìpi del Codice. Ciò, in particolare, deve avvenire evitando induzioni in errore degli interessati, come pure eventuali artifici, anche per quanto concerne le informazioni che gli agenti forniscono ai medesimi interessati circa la propria attività, le proprie qualità e le proprie effettive funzioni di incaricati del trattamento di dati per finalità di promozione degli abbonamenti radiotelevisivi.

L'informativa sul trattamento dei dati personali fornita preventivamente agli interessati deve recare corrette indicazioni circa la reale obbligatorietà o facoltatività del conferimento di dati.

Nelle sollecitazioni rivolte di persona agli interessati, inoltre, deve essere evitata l'indebita prospettazione di controlli intrusivi in caso di mancato conferimento da parte degli stessi di dati di carattere personale.

L'Autorità si è riservata, nell'ambito di un autonomo procedimento, la verifica della corretta predisposizione delle misure di sicurezza relative al trattamento dei dati personali svolto per il recupero dell'evasione del canone radiotelevisivo.

14 Sicurezza dei dati e dei sistemi

14.1. *Conservazione dei dati di traffico: misure e accorgimenti a garanzia dei cittadini*

Il tema della conservazione dei dati di traffico telefonico e telematico per finalità di accertamento e repressione dei reati è stato al centro dell'attenzione dell'Autorità anche nel 2007.

Consapevole dei rischi per la libertà e la segretezza delle comunicazioni derivanti da banche dati di enormi dimensioni e in cui confluiscono informazioni particolarmente delicate, il Garante ha adottato quattro *provvedimenti* prescrittivi e di divieto nei riguardi dei principali gestori telefonici (Telecom Italia S.p.A., Vodafone Omnitel N.V., Wind telecomunicazioni S.p.A. e H3G S.p.A.), nonché un *provvedimento* di carattere generale ai sensi dell'art. 132 del Codice. Tali decisioni sono state assunte dopo complessi accertamenti ispettivi volti a verificare il rispetto, da parte dei gestori, delle misure e degli accorgimenti in materia di sicurezza prescritti con i *provvedimenti* del 15 dicembre 2005 [doc. *web* n. 1203890] e del 20 settembre 2006 [doc. *web* n. 1341009] nell'esecuzione di intercettazioni telefoniche e telematiche disposte dall'autorità giudiziaria (*cfr.* *Relazione* 2005, *par.* 15.7 e *Relazione* 2006, *par.* 1.1.1). Limitatamente a Telecom Italia S.p.A., la verifica da parte del Garante ha riguardato anche l'adempimento delle prescrizioni fornite con il *provvedimento* del 1 giugno 2006 ([doc. *web* n. 1296533], *v.* *Relazione* 2006, *p.* 3 *ss.*), finalizzato all'adozione di specifiche misure per rendere trasparente e controllato l'accesso ai *database* contenenti i tabulati di traffico (*cfr.* anche il *Provv.* 7 dicembre 2006 [doc. *web* n. 137104], che ha differito di 90 giorni i termini di adozione delle misure impartite).

Provvedimenti adottati nei riguardi dei singoli gestori

L'attività svolta nei confronti di Telecom Italia S.p.A., Vodafone Omnitel N.V., Wind telecomunicazioni S.p.A. e H3G S.p.A. ha fatto emergere alcuni profili critici sul rispetto della normativa e comportato la denuncia all'autorità giudiziaria di due compagnie per mancata adozione di misure minime di sicurezza.

In particolare, il Garante ha prescritto a Telecom, Vodafone e H3G, la cancellazione delle informazioni riguardanti i siti Internet visitati dai relativi abbonati e ha impartito a Vodafone, H3G e Wind l'adozione di specifiche misure tecniche per la messa in sicurezza dei dati personali conservati a fini di giustizia.

I fornitori di accesso alla rete Internet devono infatti conservare esclusivamente i dati di traffico strumentali alla fornitura e alla fatturazione del servizio di connessione e non quei dati apparentemente "esterni" alla comunicazione (pagine *web* visitate o gli indirizzi Ip di destinazione), che possono peraltro, in diversi casi, coincidere di fatto con il "contenuto" della comunicazione, consentendo di ricostruire relazioni personali e sociali, convinzioni religiose, orientamenti politici, abitudini sessuali e stato di salute.

Più precisamente, nei riguardi di Telecom, il Garante ha imposto anche la cancellazione di dati che talvolta comprendevano persino le interrogazioni ai motori di ricerca effettuate dagli utenti. Alla società è stato inoltre vietato l'uso di sistemi informatici (*proxy server*) non necessari né all'instradamento della comunicazione, né alla fatturazione e che, interponendosi tra l'utente e i siti, consentivano un'ingente raccolta di dati relativi alle connessioni effettuate nel corso della navigazione.

Nei confronti di Vodafone, il Garante ha anche impartito una serie di prescrizioni relative al rispetto delle misure di sicurezza previste dal Codice, all'adozione di

sistemi tecnologici richiesti dal ricordato *provvedimento* del Garante del dicembre 2005, e a ulteriori criticità rilevate nel corso delle ispezioni.

Analogamente nei riguardi di H3G, il Garante ha anche prescritto l'adozione di misure di sicurezza e di ulteriori accorgimenti tecnici in relazione ai profili emersi nel corso degli accertamenti ispettivi.

L'Autorità ha infine prescritto a Wind l'adozione di specifiche cautele relative al rispetto delle misure di sicurezza dettate dal Codice e dal *provvedimento* del 2005, nonché ad ulteriori profili di illiceità del trattamento riscontrati.

Conservazione dei dati di traffico: misure e accorgimenti a tutela degli interessati

Prima del recente recepimento in Italia della direttiva 2006/24/Ce in materia di conservazione dei dati di traffico (che prevede un periodo minimo di sei mesi e massimo di due anni), i tempi di conservazione obbligatoria per le finalità di accertamento e repressione dei reati erano di circa 8 anni, per il traffico telefonico, e quasi 4 anni, per quello telematico (*cfr.* d.l. 27 luglio 2005, n. 144, convertito in legge dall'art. 1 della l. 31 luglio 2005, n. 155 e successive modificazioni).

Tale situazione desta preoccupazione in ragione dei pericoli connessi a una così ampia e prolungata conservazione di dati relativi a milioni di persone.

L'intensità dei flussi di comunicazione comporta la formazione di innumerevoli informazioni con una *"accentuata valenza divulgativa di notizie caratterizzanti la personalità dell'autore"* (*cfr.*, fra l'altro, *Corte cost.* 11 marzo 1993, n. 81 e 14 novembre 2006, n. 372) e che consentono di ricostruire nel tempo intere sfere di relazioni personali, professionali, commerciali, e istituzionali.

Eventuali abusi (quali quelli emersi di recente, allorché sono stati constatati gravi e diffusi fenomeni di utilizzo illecito di dati), possono comportare serie ripercussioni sulla riservatezza degli individui o violare segreti attinenti a determinate attività, relazioni e professioni.

Emerge quindi la necessità di assicurare che la conservazione di tali dati da parte dei fornitori, necessaria per prestare un servizio ovvero imposta dalla legge, avvenga nel rispetto dei diritti e delle libertà delle persone.

Per tali ragioni, con il *provvedimento* di carattere generale del 17 gennaio 2008 [doc. *web* n. 1482111], l'Autorità ha prescritto ai fornitori di servizi di comunicazione elettronica l'adozione, entro il 31 ottobre 2008, di dettagliate misure organizzative e di sicurezza, volte a garantire un elevato livello di protezione dei dati di traffico telefonico e telematico conservati sia per finalità di giustizia, sia per le altre finalità ammesse dalla normativa (art. 123 del Codice).

Tale *provvedimento*, adottato all'esito dei complessi accertamenti ispettivi di cui sopra si è accennato, ha tenuto conto anche delle osservazioni e dei commenti pervenuti a seguito di una consultazione pubblica indetta dall'Autorità su un documento preliminare nel quale era stato delineato un primo quadro regolamentare della materia.

Come è noto, per i fornitori di servizi di comunicazione elettronica è previsto l'obbligo di conservare i dati relativi al traffico per finalità di accertamento e repressione di reati nel rispetto di specifiche misure ed accorgimenti a garanzia dell'interessato (*cfr.* artt. 17 e 132 del Codice), la cui individuazione è stata demandata dal legislatore al Garante (art. 132, comma 5 del Codice).

Il *provvedimento* del 17 gennaio 2008 chiarisce l'ambito di applicazione dell'obbligo di conservazione.

Sul piano soggettivo, per *"fornitore"* sul quale incombe l'obbligo deve intendersi chi mette a disposizione del pubblico servizi di comunicazione elettronica su reti pubbliche di comunicazione; per *"servizi di comunicazione elettronica"* devono intendersi quelli consistenti, esclusivamente o prevalentemente, *"nella trasmissione di segnali su reti di comunicazioni elettroniche"*. Sono pertanto esclusi da tale obbligo i

gestori di esercizi pubblici e *Internet café*, i gestori di siti Internet che diffondono contenuti sulla rete (*"content provider"*), i gestori dei motori di ricerca, le aziende o le amministrazioni pubbliche che mettono a disposizione del personale reti telefoniche e informatiche (*ad es.*, centralini aziendali) o che si avvalgono di *server* resi disponibili da altri soggetti.

Quanto all'ambito oggettivo, l'obbligo riguarda i dati relativi al traffico telefonico, inclusi quelli concernenti le chiamate senza risposta, nonché i dati inerenti al traffico telematico, esclusi comunque i contenuti delle comunicazioni. In particolare, sono oggetto di conservazione i soli dati che i fornitori sottopongono a trattamento per la trasmissione della comunicazione o per la relativa fatturazione. Il *provvedimento* richiama pertanto i fornitori a conservare, per esclusive finalità di giustizia, i dati di traffico che risultino nella loro disponibilità in quanto derivanti da attività tecniche strumentali alla resa dei servizi offerti dai medesimi, nonché alla loro fatturazione. Il Garante rinvia poi all'art. 5 della direttiva 2006/24/Ce che contiene un'elencazione delle informazioni da conservare e individua diverse categorie di dati di traffico, a seconda si tratti di traffico telefonico (chiamate telefoniche, servizi supplementari, messaggeria e servizi multimediali) o telematico (accesso alla rete Internet, posta elettronica, *fax* nonché messaggi *Sms* e *Mms* via Internet; telefonia via Internet).

L'Autorità ricorda che i dati conservati per gli scopi di cui all'art. 132 del Codice possono essere utilizzati solo per accertamento e repressione di reati. Pertanto, ad esempio, i fornitori non possono corrispondere a eventuali richieste riguardanti tali dati formulate nell'ambito di una controversia civile, amministrativa e contabile; è tenuto a rispettare questo vincolo di finalità anche l'interessato, che può esercitare i diritti di cui all'art. 7 del Codice solo in riferimento a finalità penali.

Il Garante precisa poi di aver individuato gli accorgimenti ritenuti idonei per la conservazione tenuto conto in particolare dell'esigenza normativa volta a prevedere specifiche misure rapportate alla quantità e qualità dei dati da proteggere; dell'opportunità di individuare misure protettive che siano verificabili anche in sede ispettiva; dei costi derivanti dall'adozione delle misure e degli accorgimenti prescritti, anche in ragione della variegata capacità tecnica ed economica dei soggetti interessati; del contesto europeo di riferimento, specie alla luce dei pareri resi dal Gruppo art. 29 che riunisce i Garanti europei; dello stato di evoluzione tecnologica.

Le cautele prescritte dall'Autorità lasciano ai fornitori la facoltà di scegliere l'architettura informatica più idonea per la conservazione obbligatoria dei dati di traffico e per le ordinarie elaborazioni aziendali. I dati di traffico conservati per un periodo non superiore a sei mesi dalla loro generazione possono essere trattati con i medesimi sistemi di elaborazione e di immagazzinamento utilizzati per la generalità dei trattamenti (fatturazione, commercializzazione, *ecc.*), oppure duplicati per effettuare un trattamento dedicato esclusivamente al perseguimento delle finalità di giustizia. In quest'ultimo caso, le misure e gli accorgimenti prescritti per i dati conservati per esclusive finalità di giustizia si applicano sin dall'inizio del trattamento.

In questo quadro, il trattamento dei dati di traffico telefonico e telematico deve essere consentito solo a specifici incaricati, previo utilizzo di sistemi di autenticazione informatica basati su tecniche di *strong authentication*, consistenti nell'uso contestuale di almeno due differenti tecnologie di autenticazione. Per i dati conservati per esclusive finalità di giustizia (cioè quelli generati da più di sei mesi, oppure la totalità dei dati trattati per queste finalità se conservati separatamente dai dati trattati per le altre finalità fin dalla loro generazione), una di tali tecnologie deve essere, poi, basata su caratteristiche biometriche dell'incaricato. Tali cautele trovano applicazione anche per gli addetti tecnici (amministratori di sistema, di rete, di *database*) che possono esserne esonerati solo in circostanze eccezionali (*ad es.*, guasti, aggior-

namento, *ecc.*). In tali casi, tuttavia, deve essere tenuta preventivamente traccia in un apposito "registro degli accessi" dell'evento, nonché delle motivazioni che lo hanno determinato, con una successiva descrizione sintetica delle operazioni svolte, anche mediante l'utilizzo di sistemi elettronici.

Salvo quanto sarà aventualmente previsto a seguito del recepimento della direttiva i profili di autorizzazione devono differenziare le funzioni di trattamento dei dati di traffico per finalità di ordinaria gestione da quelle per finalità di accertamento e repressione dei reati, distinguendo, tra queste ultime, gli incaricati abilitati al solo trattamento dei dati di cui al primo periodo di conservazione obbligatoria (art. 132, comma 1, del Codice), dagli incaricati abilitati anche al secondo periodo di conservazione obbligatoria (art. 132, comma 2, del Codice) e, infine, dalle funzioni di trattamento dei dati in caso di esercizio dei diritti dell'interessato (art. 7 del Codice). Ciò, ha chiarito il Garante, non determina la moltiplicazione degli addetti ai servizi per scopi di giustizia, potendo lo stesso incaricato ricevere entrambi i profili di autorizzazione.

Con riferimento alle modalità di conservazione, il Garante ha precisato che i dati di traffico trattati per esclusive finalità di giustizia vanno conservati in sistemi informatici distinti fisicamente da quelli utilizzati per gestire dati di traffico anche per altre finalità. Le relative attrezzature informatiche devono essere collocate all'interno di aree ad accesso selezionato e munite di dispositivi elettronici di controllo o di procedure di vigilanza. Nel caso di trattamenti relativi a dati di traffico telefonico, il controllo degli accessi deve comprendere una procedura di riconoscimento biometrico.

Quanto ai controlli, l'Autorità ha prescritto che ogni operazione compiuta dagli incaricati o dagli amministratori di sistema sia tracciata e registrata in appositi *audit log*. Devono essere, poi, effettuati controlli periodici sulla legittimità degli accessi ai dati da parte degli incaricati, sul rispetto delle norme di legge e delle misure organizzative tecniche e di sicurezza prescritte, nonché sull'effettiva cancellazione dei dati una volta decorsi i termini di conservazione.

Infine, contro rischi di acquisizione indebita, anche fortuita, delle informazioni registrate da parte di incaricati di mansioni tecniche (amministratori di sistema, amministratori di *database*, manutentori *hardware* e *software*), il Garante ha prescritto che i dati di traffico trattati per esclusive finalità di giustizia siano protetti con tecniche crittografiche.

L'Autorità ha da ultimo esteso l'applicazione di alcune misure e accorgimenti anche ai *database* contenenti dati di traffico conservati per finalità diverse e, segnatamente, per scopi di fatturazione, di commercializzazione di servizi, di statistica, *ecc.* (art. 123 del Codice). Ciò, al fine di favorire un quadro più ampio di sicurezza di dati e sistemi (*strong authentication*, separazione rigida delle funzioni tecniche di assegnazione di credenziali di autenticazione e di individuazione dei profili di autorizzazione rispetto a quelle di gestione tecnica dei sistemi e delle basi di dati; procedure di cancellazione dei dati allo scadere dei termini previsti dalle disposizioni vigenti; controlli sulle attività poste in essere dagli incaricati; documentazione dei sistemi informativi secondo i princìpi dell'ingegneria del *software*).

Monitoraggio delle reti *peer to peer*: caso Peppermint

Nel corso del 2007 numerosi utenti italiani che utilizzano sistemi di *file sharing* si sono visti recapitare, dopo che l'autorità giudiziaria aveva imposto ad alcuni gestori telefonici la comunicazione dei loro dati identificativi, note raccomandate da parte della casa discografica Peppermint contenenti richieste di risarcimento del danno per violazione del diritto d'autore.

Al riguardo sono pervenuti all'Autorità numerosi reclami e segnalazioni, relativi ad asserite violazioni della normativa sulla protezione dei dati personali commesse da tre società (Peppermint Jam Records GmbH, casa discografica con sede in

Germania; Techland sp. z. o.o., società che elabora e commercializza giochi elettronici con sede in Polonia; Logistep AG, con sede in Svizzera che ha svolto un'attività di monitoraggio delle reti *peer to peer* tramite un *software* proprietario). Data l'importanza della questione, il Garante ha ravvisato l'esigenza di costituirsi in alcuni giudizi instaurati presso il Tribunale di Roma con i quali le società Peppermint e Techland sp. z. o.o. intendevano ottenere da taluni fornitori di servizi di comunicazione elettronica la comunicazione delle generalità di soggetti ritenuti responsabili di avere scambiato *file* protetti dal diritto d'autore tramite reti *peer to peer*. I ricorsi si basavano sull'attività svolta per conto e su autorizzazione delle predette società da Logistep AG, che aveva individuato numerosi indirizzi Ip i cui titolari erano stati considerati responsabili della predetta condotta.

Dopo alcune iniziali pronunce favorevoli alle società ricorrenti, il Tribunale di Roma, anche a seguito della costituzione in giudizio del Garante, ha respinto i ricorsi (ordinanza 14 luglio 2007, in causa Peppermint e Techland c/ Wind Telecomunicazioni S.p.A.; ordinanza 14 luglio 2007, in causa Peppermint e Techland c/ Telecom Italia S.p.A.; ordinanza 26 ottobre 2007, in causa Peppermint c/ Wind Telecomunicazioni S.p.A.).

Il Tribunale, pronunciandosi in tema di interpretazione e applicazione dell'art. 156-*bis* della legge n. 633/1941 (introdotto dall'art. 3 del d.lg. n. 140/2006), ha statuito, come richiesto dall'Autorità, che i fornitori di servizi di comunicazione elettronica, allo stato della legislazione vigente, non possono comunicare in sede giurisdizionale civile ai soggetti titolari del diritto d'autore i nominativi degli interessati ritenuti responsabili di violazioni del diritto d'autore in rete. Ciò, stante la specifica disciplina della conservazione dei dati di traffico, prevista solo per finalità di accertamento e repressione dei reati dall'art. 132 del Codice (*v.* anche artt. 5 e 15 della direttiva 2002/58/Ce), ritenuto costituzionalmente legittimo nella parte in cui opera il bilanciamento fra il diritto alla riservatezza e le esigenze di tutela di beni della collettività prevalenti minacciati da gravi illeciti penali (*Corte cost.* n. 372/2006).

Il Garante ha quindi avviato una specifica istruttoria per verificare la liceità e la correttezza dei trattamenti di dati personali posti in essere dalle predette società.

All'esito di tale istruttoria, l'Autorità, con *provvedimento* del 28 febbraio 2008 [doc. *web* n. 1495246], richiamando anche la decisione dell'omologa autorità svizzera (*cfr. www.edoeb.admin.ch*), ha ritenuto illecito il monitoraggio sistematico delle reti *peer to peer* (P2p) svolto per individuare gli utenti che si scambiano illegalmente contenuti protetti dal diritto d'autore (nel caso di specie, *file* musicali e giochi).

Il Garante ha ricordato anzitutto che la direttiva europea sulle comunicazioni elettroniche vieta ai privati di effettuare monitoraggi, ossia trattamenti di dati massivi, capillari e prolungati nei riguardi di un numero elevato di soggetti.

L'Autorità ha, inoltre, ritenuto violato anche il principio di finalità, essendo le *cd.* "reti P2p" finalizzate allo scambio tra utenti di dati e *file* per scopi personali. L'utilizzo dei dati dell'utente può dunque avvenire soltanto per queste finalità e non per scopi ulteriori quali quelli perseguiti dalle società Peppermint e Techland (cioè, il monitoraggio e la ricerca di dati per la richiesta di un risarcimento del danno); ha infine ritenuto non rispettati i princìpi di trasparenza e correttezza, perché i dati erano stati raccolti ad insaputa sia degli interessati, sia di abbonati non necessariamente coinvolti nello scambio di *file*.

Il Garante ha pertanto vietato l'ulteriore trattamento dei dati personali relativo a soggetti ritenuti responsabili di aver scambiato *file* protetti dal diritto d'autore tramite reti *peer to peer* e ne ha disposto la cancellazione entro il termine del 31 marzo 2008.

Occorre sottolineare su una questione per molti aspetti simile alla vicenda italiana si è pronunciata la Corte di giustizia delle Comunità europee (sentenza 29 gennaio 2008, causa C-275/06 Promusicae c/ Telefónica de España Sau).

In tale sede la Corte ha confermato che il diritto comunitario consente agli Stati membri di circoscrivere all'ambito delle indagini penali o della tutela della pubblica sicurezza e della difesa nazionale –ad esclusione, quindi, dei processi civili– il dovere di conservare e mettere a disposizione i dati sulle connessioni e il traffico generati dalle comunicazioni. La Corte ha rilevato che anche i dati di traffico conservati per finalità di fatturazione non possono essere utilizzati in *"controversie diverse da quelle insorgenti tra i fornitori e gli utilizzatori, relative ai motivi della memorizzazione dei dati avvenuta per attività previste dalle disposizioni dell' art. 6 della direttiva 2002/58/Ce"* (*cfr.* art. 123 del Codice); ha, pertanto, escluso la possibilità che tali dati potessero essere messi a disposizione per controversie civili relative ai diritti di proprietà intellettuale (*cfr.* punto 48 della sentenza; artt. 15, n. 2, e 18 della direttiva 2000/31/Ce relativa a taluni aspetti giuridici dei servizi della società dell'informazione, in particolare il commercio elettronico, nel mercato interno; artt. 8, n. 1 e 2 direttiva 2001/29/Ce sull'armonizzazione di taluni aspetti del diritto d'autore e dei diritti connessi nella società dell'informazione; art. 8 direttiva 2004/48/Ce sul rispetto dei diritti di proprietà intellettuale; artt. 17, n. 2 e 47 Carta dei diritti fondamentali dell'Unione europea).

Pubblicazione di dati personali in Internet

Sul delicato tema della pubblicazione di dati personali in Internet meritano menzione in particolare due decisioni.

La prima (*Nota* 16 maggio 2007) è stata adottata a seguito di un reclamo proposto da un deputato che lamentava la pubblicazione su una pagina *web* del sito Internet *http://italy.indymedia.org* di una lista di parlamentari che sarebbero risultati positivi al *cd. "test drug-wipe"* (effettuato con modalità che questa Autorità ha ritenuto illecita) nella quale appariva anche il suo nome. L'interessato riconduceva la diffusione di questi dati al *test* effettuato da alcuni inviati della trasmissione televisiva "Le Iene" e lamentava la non veridicità dei dati diffusi, sulla base del presupposto che egli non era *"mai stato oggetto delle inchieste e delle interviste effettuate dagli inviati della trasmissione Le Iene"*.

Dagli accertamenti compiuti dall'Ufficio era emerso che tali informazioni risultavano essere state inserite in rete antecedentemente al *provvedimento* inibitorio del Garante adottato nei confronti della società editrice del predetto programma televisivo. Al *provvedimento* di blocco adottato in via d'urgenza dall'Autorità in data 10 ottobre 2006 [doc. *web* n. 1345622] aveva fatto seguito un ulteriore *provvedimento* (adottato il 14 dicembre 2006 [doc. *web* n. 1370781]) che, sulla base di un compiuto esame del merito, aveva accertato la mancanza di liceità e correttezza nel trattamento (*v. Relazione* 2006, *p.* 79 *ss.*). Nella pagina *web* diffusa non risultava inoltre specificato che le informazioni ivi pubblicate erano state acquisite utilizzando i *test* effettuati dagli inviati della trasmissione "Le Iene". Ancora, dalle informazioni disponibili risultava che la pagina *web* era stata inserita in un *forum* di discussione (*cd. "newswire"*, ossia *"uno spazio informativo a pubblicazione aperta"*) presente su un sito Internet (*www.indymedia.org*), già in passato oggetto di un provvedimento da parte dell'autorità giudiziaria, i cui *server* risultavano ubicati negli Stati uniti d'America e il cui nome a dominio risultava registrato da un soggetto residente in Brasile. Infine, il trattamento contestato non risultava riconducibile a persone fisiche individuabili, essendo stati utilizzati alcuni *alias*. Tuttavia, non si poteva escludere che tali persone fossero stabilite sul territorio dello Stato italiano, in ragione di alcuni elementi fra i quali la lingua utilizzata, il fatto che la sezione del *forum* fosse stata dedicata specificamente al pubblico italiano (*Italy Indymedia*) e a questioni attinenti alla vita politica e sociale italiana.

Il Garante ha pertanto rilevato che solo laddove fosse pienamente comprovato questo presupposto, poteva essere configurabile un intervento dell'Autorità nei confronti delle predette persone (*cfr.* art. 5 del Codice); non emergevano, invece, allo stato degli atti, i presupposti giuridici per consentire un intervento diretto nei riguardi del gestore del sito. L'Autorità ha quindi prospettato al reclamante, ferma restando la possibilità di adire anche l'autorità giudiziaria ordinaria per eventuali profili di carattere penale, di rivolgersi direttamente al gestore del sito Internet, richiedendo la rimozione immediata dei contenuti ritenuti illeciti. Ciò, anche in relazione a una prassi nota come *"notice and take down"*, applicata in altri ambiti normativi per proteggere i titolari di diritti d'autore e introdotta negli Stati uniti dal *Digital Millenium Copyright Act* nonché, in ambito comunitario, dalla direttiva 2000/31/Ce (relativa a taluni aspetti giuridici dei servizi della società dell'informazione nel mercato interno, con particolare riferimento al commercio elettronico, e recepita in Italia con il d.lg. n. 70/2003).

La seconda decisione (*Nota* 16 maggio 2007) è stata, invece, adottata a seguito di una segnalazione che lamentava la diffusione via Internet di notizie considerate inesatte e diffamatorie.

In tale occasione il Garante ha ricordato i contatti avviati con la società Google Inc., con sede negli Stati uniti, per individuare soluzioni volte a garantire i diritti della persona interessata, anche quando il titolare del trattamento effettuato sia stabilito fuori dell'Unione europea e non sia pertanto soggetto all'applicazione del Codice. Il Garante, in particolare, ha ricevuto formali assicurazioni circa la disponibilità della società statunitense a rendere più agevole e tempestiva la cancellazione delle pagine *cache* (copie delle pagine originali) e dei relativi "titoli" e "sommarietti" reperibili con il motore di ricerca, quando, però, le pagine originali non sono più presenti presso i siti *web* "sorgente", ossia i siti dai quali sono estratte le copie *cache* (*cfr. Comunicato stampa* 30 maggio 2006). L'Autorità ha, pertanto, sollecitato il segnalante, relativamente agli articoli pubblicati in Italia, a esercitare i diritti di rettifica di dati erronei o di aggiornamento e integrazione nei riguardi dell'editore titolare del trattamento ai sensi dell'art. 7 del Codice. In particolare, ha suggerito di chiedere (art. 7, comma 1, lett. *c*) del Codice), l'attestazione che le operazioni di cui sopra siano state portate a conoscenza, anche per quanto riguarda il loro contenuto, di coloro ai quali i dati sono stati comunicati o diffusi (ossia, nel caso di specie, Google Inc.). A tale riguardo, ha inoltre ricordato che il *webmaster* del sito "sorgente" può anche utilizzare alcuni meccanismi di rimozione di "contenuti obsoleti" messi a sua disposizione da Google.

14.2. *Prescrizioni sulla sicurezza dei dati negli uffici giudiziari*

Come riferito nella *Relazione* 2006, il Garante ha preso in esame anche l'applicazione delle misure di sicurezza nei trattamenti dei dati personali cartacei e automatizzati, di tipo amministrativo e per ragioni di giustizia, effettuati presso gli uffici giudiziari, nella convinzione che l'introduzione di livelli elevati di sicurezza in tali trattamenti contribuisce anche al buon funzionamento delle strutture giudiziarie.

In tale ambito, l'Autorità ha deliberato di effettuare una prima serie di accertamenti in relazione ai trattamenti di dati personali svolti, per motivi di giustizia (art. 47, comma 2, del Codice), presso il Tribunale ordinario di Roma, limitatamente, in una prima fase, al settore civile (*Provv.* 1 febbraio 2007, [doc. *web* n. 1385301]). Gli accertamenti, intrapresi nei modi previsti dalla legge, con la presenza di un componente del Garante da questo designato e con l'assistenza di personale specializzato

(art. 160 del Codice), si sono protratti nell'arco del 2007 mediante l'acquisizione di informazioni e documentazione e attraverso numerose verifiche e sopralluoghi svolti, con la piena collaborazione della magistratura e del personale amministrativo, presso tutte le sezioni civili e il settore informatico del Tribunale.

Le risultanze degli accertamenti costituiscono parte integrante della motivazione del *provvedimento* del 15 novembre 2007 con il quale il Garante, ravvisata l'esigenza di rafforzamento del livello di protezione dei dati, ha indicato al Tribunale ordinario di Roma la necessità di apportare alcune modificazioni e integrazioni alle misure di sicurezza concernenti il trattamento dei dati gestiti con strumenti elettronici e contenuti nei fascicoli processuali.

L'Autorità ha disposto di inviare copia del provvedimento al Ministero della giustizia con riferimento alle pertinenti competenze in tema di organizzazione e funzionamento dei servizi relativi alla giustizia, e al Consiglio superiore della magistratura, per ogni opportuna conoscenza in relazione alle relative attribuzioni.

15 La videosorveglianza e la biometria

15.1. *Videosorveglianza in ambito privato*

Verifiche preliminari

Nonostante i ripetuti interventi del Garante, a distanza di circa quattro anni dall'adozione del *provvedimento* generale del 29 aprile 2004 [doc. *web* n. 1003482] sono continuate a giungere diverse richieste di verifiche preliminari sull'installazione di impianti di videosorveglianza da parte di soggetti privati.

Al riguardo, in più circostanze è stato ribadito che devono essere sottoposti a esame preventivo dell'Autorità solo i trattamenti connessi ad alcuni sistemi (specificamente individuati al punto 3.2 del menzionato *provvedimento*) quali i sistemi di videosorveglianza *cd.* "dinamico-preventiva", ovvero quelli che prevedono una raccolta delle immagini collegata e/o incrociata e/o con altri particolari dati personali. Pertanto, gli impianti installati in conformità alla disciplina di protezione dei dati personali e alle prescrizioni contenute nel citato *provvedimento* non devono essere oggetto di alcuna verifica preliminare da parte dell'Autorità.

Tale profilo è stato oggetto di approfondimento anche in occasione di un incontro presso la sede dell'Autorità tenutosi con la Federazione nazionale imprese elettrotecniche ed elettroniche (Anie), in rappresentanza dei principali produttori ed installatori di sistemi di videosorveglianza. Le questioni ivi sollevate, allo stato oggetto di analisi e studio da parte dell'Autorità, concernono principalmente i casi in cui risulta necessario procedere a una richiesta di verifica preliminare *ex* art. 17 del Codice in ragione di alcune specifiche caratteristiche tecniche degli impianti di videosorveglianza attualmente in commercio (quali la digitalizzazione/indicizzazione delle immagini), nonché dei profili connessi alle misure di sicurezza e all'attestazione di conformità dei sistemi (regola 19 Allegato B del Codice). A quest'ultimo proposito l'Associazione ha rappresentato l'opportunità di predisporre, anche a seguito di un'attività collaborativa con l'Autorità, una modellistica utilizzabile dalla pluralità di soggetti che possono intervenire nelle fasi di produzione, progettazione, e installazione del sistema di videosorveglianza.

Ulteriore aspetto oggetto di riflessione da parte dell'Autorità, anche alla luce di talune segnalazioni pervenute, è poi quello legato all'identificazione di tempi congrui di conservazione dei dati registrati, al di là dei limiti temporali indicati, in assenza di una disciplina di settore che regoli il delicatissimo settore della videosorveglianza negli spazi pubblici, nel già citato *provvedimento* generale del 2004.

Vigilanza negli spogliatoi

A seguito della denuncia di un furto avvenuto all'interno degli spogliatoi di una piscina, i Carabinieri hanno acquisito la videocassetta delle riprese effettuate da un sistema di videosorveglianza che si avvaleva di due coppie di telecamere, entrambe visibili, e ne hanno dato notizia al Garante. È emerso in particolare che le telecamere, oltre a controllare la zona adibita a guardaroba, riprendevano direttamente le persone anche mentre si cambiavano gli indumenti.

Nonostante la presenza delle telecamere fosse segnalata, l'Autorità ha ravvisato la violazione della riservatezza e della dignità delle persone (art. 2 del Codice) in quanto, pur essendo lecito l'utilizzo di sistemi di videosorveglianza per tutelarsi da eventuali danni o furti, non erano stati adottati accorgimenti volti a evitare riprese indebite di persone negli spogliatoi.

Il Garante ha quindi disposto il divieto di installare telecamere con le modalità indicate e ha bloccato il trattamento dei dati già raccolti, nelle more di eventuali altre attività di accertamento da parte delle competenti autorità; ha poi prescritto al titolare del trattamento il rispetto dei princìpi generali in materia di sistemi di videosorveglianza e protezione dei dati stabiliti nel *provvedimento* del 29 aprile 2004 [doc. *web* n. 1003482], sottolineando in particolare l'obbligo di adottare tutte le misure necessarie per evitare la ripresa delle persone negli spogliatoi e per assicurare un'adeguata informativa ai clienti sulla presenza di telecamere (*Provv.* 8 marzo 2007 [doc. *web* n. 1391803]).

Videosorveglianza sui luoghi di lavoro

In relazione ad alcune generiche segnalazioni sull'installazione di impianti di videosorveglianza in violazione dello Statuto dei lavoratori (art. 4 l. n. 300/1970), il Garante ha ricordato, in base alla specifica normativa di settore (fatta peraltro salva dall' art. 114 del Codice), la competenza delle direzioni provinciali del lavoro.

Sotto altro profilo, non sono stati ravvisati elementi per un intervento da parte dell'Autorità in ordine ad un impianto di videosorveglianza installato presso alcune zone di transito e d'ingresso agli uffici di una società di trasporto pubblico locale. All'esito dei preliminari accertamenti effettuati dal Garante, infatti, la società ha dichiarato, ai sensi e per gli effetti di cui all' art. 168 del Codice, che il sistema informativo e il relativo programma informatico erano stati conformati in modo tale da non utilizzare dati relativi a persone identificate o identificabili (con esclusione, pertanto, della possibilità di ingrandire le immagini) (*Nota* 23 gennaio 2008).

La videosorveglianza nei condomìni

Il trattamento connesso all'installazione di sistemi di ripresa nelle aree comuni di edifici condominiali e loro pertinenze è oggetto di ulteriori approfondimenti da parte del Garante, in considerazione delle ampie fasce di popolazione coinvolta e della necessità di tutelare il diritto alla riservatezza e le libertà personali in prossimità dei luoghi adibiti a privata dimora.

In particolare, le questioni sollevate, solo in parte oggetto di intervento da parte del Garante con il *provvedimento* del 29 aprile 2004 [doc. *web* n. 1003482] e non chiaramente risolte dal codice civile, riguardano soprattutto le operazioni di trattamento conseguenti all'installazione di sistemi di videosorveglianza da parte dell'intera compagine condominiale all'interno di aree comuni quali, portoni d'ingresso, androni, cortili, scale, aree comuni di accesso ai parcheggi, al fine di preservare la sicurezza di persone e la tutela di beni comuni (*ad es.*, contro aggressioni o danneggiamenti e furti).

Finalità esclusivamente personali

È stato inoltre chiarito che la disciplina di protezione dei dati non trova applicazione in caso di trattamenti effettuati per fini esclusivamente personali, purché le immagini registrate non siano oggetto di successiva comunicazione sistematica o diffusione (*cfr.* art. 5, comma 3 del Codice). Peraltro, considerato che numerose segnalazioni avevano ad oggetto l'installazione di impianti di videosorveglianza in ambito condominiale, questa Autorità ha provveduto a puntualizzare che, onde evitare di incorrere nel reato di interferenze illecite nella vita privata (art. 615-*bis* c.p.), l'angolo visuale delle riprese deve essere limitato ai soli spazi di esclusiva pertinenza del singolo condomino (*ad es.* antistanti l'accesso alla propria abitazione), escludendo ogni forma di ripresa, anche senza registrazione, di immagini relative ad aree comuni (cortili, pianerottoli, scale, garage comuni) o riferite ad aree antistanti l'abitazione di altri condomini. Una specifica segnalazione è stata da ultimo inoltrata al Parlamento e al Governo.

15.2. *Biometria in ambito pubblico*

Nel 2007 è stata completata l'ampia istruttoria sull'utilizzo, da parte di soggetti pubblici, di sistemi di riconoscimento delle impronte digitali dei dipendenti per il controllo degli accessi sui luoghi di lavoro.

Le conclusioni di tale attività sono confluite nel *provvedimento* generale sul trattamento di dati personali di lavoratori per finalità di gestione del rapporto di lavoro in ambito pubblico (*Provv.* 14 giugno 2007 [doc. *web* n. 1417809]).

In particolare, il citato *provvedimento* evidenzia che l'utilizzo generalizzato di sistemi di rilevazione automatica delle presenze dei dipendenti mediante la raccolta di dati biometrici ricavati dalle impronte digitali non è consentito ove siano attivabili misure "convenzionali" non lesive dei diritti della persona. Inoltre non può desumersi alcuna approvazione implicita dal semplice inoltro al Garante di note relative a progetti di installazione di impianti di rilevazione di impronte digitali, cui eventualmente non segua un esplicito riscontro dell'Autorità.

Tali chiarimenti sono stati forniti ai diversi segnalanti che si erano rivolti all'Autorità e alle numerose amministrazioni pubbliche che avevano inoltrato specifiche richieste di parere al riguardo (*Note* 11 luglio 2007, 18 luglio 2007, 20 luglio 2007, 26 luglio 2007, 30 luglio 2007, 1 agosto 2007, 9 ottobre 2007, 7 dicembre 2007, 10 dicembre 2007 e 18 dicembre 2007).

Un ente locale ha posto un quesito su un sistema di riconoscimento biometrico dell'impronta digitale per l'utilizzo di *personal computer* dei dipendenti abilitati ad accedere ai dati sensibili presenti nelle banche dati. L'impronta sarebbe stata memorizzata e verificata non come immagine dattiloscopica, ma in forma sintetizzata e complessa (*template*), e poi registrata in una *smart card* nell'esclusiva disponibilità del dipendente. Attraverso tale progetto si sarebbe inteso attivare una credenziale di autenticazione in conformità alla regola n. 2 del Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B al Codice).

Come in analoghe circostanze, nel caso di specie, non è risultato necessario prescrivere misure o accorgimenti, tenuto conto della sola finalità perseguita di autenticazione informatica. L'adozione di un sistema di autenticazione informatica, mediante il quale gli incaricati dotati di apposite credenziali possono effettuare specifici trattamenti di dati personali, se conforme ai requisiti tecnici indicati dal Codice (*cfr.* regole da 1 a 11 dell'Allegato B al Codice), costituisce infatti una misura minima di sicurezza che il titolare, il responsabile (ove designato) e l'incaricato sono tenuti a utilizzare. Tali credenziali di autenticazione possono consistere anche in una caratteristica biometrica dell'incaricato, eventualmente associata a un codice identificativo o a una parola chiave (*cfr. Relazione* 2005, *p.* 113; *Relazione* 2006, *p.* 121; *Nota* 1 giugno 2007).

Una soprintendenza archeologica aveva chiesto che fosse oggetto di verifica preliminare ai sensi dell'art. 17 del Codice un sistema di riconoscimento biometrico basato sul rilevamento delle caratteristiche geometriche della mano per consentire a un numero limitato di dipendenti l'accesso a un'area riservata particolarmente sensibile, al fine di identificarli in modo certo e garantire così *standard* di sicurezza specifici ed elevati, richiesti dalla natura delle attività svolte nell'area riservata.

Il sistema prevedeva l'associazione alle caratteristiche geometriche della mano di un algoritmo crittografico poi archiviato nella memoria interna del dispositivo biometrico. Tale dispositivo non era collegato in rete e poteva essere attivato per effettuare l'accesso solo attraverso una parola chiave numerica scelta dal dipendente.

Il trattamento dei dati in questione è stato ritenuto dall'Autorità lecito e proporzionato allo scopo. Da una parte, l'attività di identificazione rientrava nelle finalità istituzionali della soprintendenza, la quale, dovendo garantire nel caso di specie ele-

vati *standard* di sicurezza, aveva necessità di un rigoroso accertamento dell'identità dei dipendenti. Dall'altra, è stato rilevato che le caratteristiche geometriche della mano di un individuo, a differenza delle impronte digitali utilizzabili anche in altri contesti con effetti sugli interessati, non sono descrittive al punto tale da risultare uniche; possono eventualmente non garantire l'identificazione univoca e certa di una persona, ma sono sufficientemente dettagliate per essere impiegate in circoscritti ambiti ai fini della verifica di identità. La geometria della mano appartiene a quella categoria di dati biometrici che non lasciano tracce suscettibili di essere utilizzate per scopi diversi da quelli perseguiti da chi le raccoglie ed usa.

Nell'autorizzare l'uso del sistema, il Garante ha comunque prescritto di integrare l'informativa ai dipendenti, specificando le modalità alternative di accesso per coloro che non avessero voluto o potuto avvalersi del sistema di rilevazione delle caratteristiche della mano (*Provv.* 8 novembre 2007 [doc. *web* n. 1461908]).

Da ultimo, l'Ufficio (*Nota* 11 marzo 2008) ha fornito alcune indicazioni preliminari su un sistema di distribuzione automatica di tabacchi basato sul riconoscimento dell'impronta digitale.

In un quesito, l'Amministrazione autonoma dei monopoli dello Stato, per evitare l'acquisto di tabacchi lavorati nei distributori automatici da parte di minori infrasedicenni, in specifiche fasce orarie notturne aveva ipotizzato un sistema basato su *smart card* non nominative che memorizzerebbero in forma cifrata l'impronta digitale delle persone che la richiedano, senza identificarle direttamente.

Il quesito non chiariva tutti i dettagli necessari, e perciò nella risposta sono state considerate diverse ipotesi.

Qualora il rivenditore si limitasse a verificare genericamente l'età della persona che richiede la *smart card* (essendo evidente che non si tratti di minore, sulla base di conoscenza personale o della mera esibizione di un documento di identità), il dato relativo all'impronta memorizzata sulla *smart card* avrebbe pur sempre carattere personale, ma non sarebbe necessario sottoporre formalmente il sistema al vaglio preliminare del Garante ai sensi dell' art. 17 del Codice ai fini della prescrizione di particolari misure e accorgimenti a garanzia degli interessati.

In tal caso, quindi, il rivenditore non tratterrebbe alcun dato personale identificativo dei richiedenti (generalità, copie di documenti di identità), apparendo sufficiente che la *smart card* sia in concreto utilizzabile solo dalla persona legittimata (non identificata) che l'ha richiesta. Si dovrebbe allora prevedere (a parte una sintetica informativa agli interessati) che nella *smart card* sia registrato in forma cifrata il solo *template* (forma sintetizzata e complessa) dell'impronta, anziché l'immagine fotografica cifrata dell'impronta stessa, e che si chiariscano i profili relativi all'eventuale tracciamento delle operazioni svolte dalle singole *smart card* e all'eventuale conservazione temporanea dei dati corrispondenti.

Invece, nel caso in cui presso il rivenditore o altrove restasse traccia nominativa dei richiedenti, sarebbe necessario avviare un formale procedimento di verifica preliminare ai sensi del predetto art. 17.

15.3. *Videosorveglianza in ambito pubblico*

Anche nel 2007 numerose segnalazioni pervenute al Garante hanno confermato l'attualità delle problematiche relative all'impiego dei sistemi di videosorveglianza da parte dei soggetti pubblici.

Si è reso pertanto necessario fornire talune precisazioni in relazione alle indicazioni contenute nel *provvedimento* generale del 29 aprile 2004 [doc. *web* n. 1003482].

In particolare, in ambito sanitario, a seguito della richiesta di un sindacato, il Garante ha sottolineato che nell'uso di videocamere all'interno di un'azienda sanitaria per finalità di sicurezza si deve evitare accuratamente il rischio di diffondere immagini di persone malate su *monitor* collocati in locali liberamente accessibili al pubblico. L'eventuale controllo di ambienti sanitari deve essere limitato ai casi di stretta indispensabilità, circoscrivendo le riprese solo a determinati locali e a precise fasce orarie e l'accesso alle immagini ai soggetti specificamente autorizzati (*ad es.*, personale medico ed infermieristico) (*Nota* 16 aprile 2007).

In relazione a un quesito di un'azienda sanitaria circa la possibilità di installare un dispositivo di videosorveglianza a circuito chiuso nei servizi igienici del laboratorio di patologia clinica e tossicologica dell'azienda medesima, al fine di evitare che il campione urinario da prelevare potesse essere oggetto di falsificazione da parte del soggetto sottoposto al controllo tossicologico, è stata richiamata l'esigenza di rispettare il principio generale di proporzionalità tra i mezzi impiegati e le finalità perseguite.

Più in particolare, l'Ufficio, nel ricordare che il trattamento di dati personali non deve comportare un'ingerenza ingiustificata nei diritti e nelle libertà fondamentali dei soggetti ripresi, ha evidenziato che l'installazione di una telecamera nei servizi igienici può configurarsi come lesiva della dignità degli individui sottoposti ai controlli e ha richiamato le vigenti norme dell'ordinamento civile e penale in materia di interferenze illecite nella vita privata, di tutela della dignità, dell'immagine, del domicilio e degli altri luoghi cui è riconosciuta analoga tutela (*toilette*, stanze d'albergo, cabine, spogliatoi, *ecc.*) (*Nota* 17 gennaio 2008).

Analoga questione ha riguardato un'altra azienda sanitaria che ha formulato un quesito relativo all'istallazione di sistemi di videosorveglianza con registrazione presso il locale di distribuzione del metadone, al fine di monitorare l'effettiva assunzione del farmaco da parte dell'assistito (*Nota* 26 luglio 2007).

Nel diverso ambito degli istituti scolastici, l'Ufficio ha ribadito la necessità di garantire il rispetto del diritto alla riservatezza dello studente, e ha evidenziato che l'installazione di sistemi di videosorveglianza in ambienti scolastici, potendo comportare la raccolta di dati riguardanti anche minori, deve essere limitata ai casi di stretta indispensabilità. In caso di reale necessità, tali sistemi, in conformità al principio di proporzionalità, devono essere comunque circoscritti alle sole aree interessate ed attivati nell'orario di chiusura dell'istituto (*Nota* 5 luglio 2007).

A un ente locale che intendeva utilizzare *webcam* per finalità turistiche, è stato precisato che, in linea generale, non viola le disposizioni in materia di protezione dei dati personali l'impiego per fini promozionali, turistici o pubblicitari, di *webcam* o *camera on-line* che non consentano di individuare i tratti somatici delle persone riprese (*cfr. Provv.* 29 aprile 2004, già cit. e *Provv.* 14 giugno 2001 [doc. *web* n. 41782]).

In tale occasione il Garante ha avuto anche modo di ricordare che l'installazione di sistemi di videosorveglianza non deve essere sottoposta all'esame preventivo dell'Autorità; non può, pertanto, desumersi alcuna approvazione implicita dalla semplice trasmissione al Garante di comunicazioni o di progetti relativi all'installazione di sistemi di videosorveglianza. Non è infatti stabilito alcun termine decorso il quale i progetti sottoposti alla verifica dell'Autorità possano ritenersi autorizzati, non applicandosi al riguardo il principio del silenzio-assenso (*Nota* 1 agosto 2007).

L'Autorità, nuovamente interpellata da alcune amministrazioni in ordine alla necessità di sottoporre taluni trattamenti di dati personali alla verifica preliminare, ha ricordato che il *provvedimento* del 29 aprile 2004 individua espressamente le ipotesi in cui i sistemi di videosorveglianza da attivare devono essere sottoposti alla verifica preliminare del Garante. Spetta, quindi, all'amministrazione richiedente valu-

tare se, nell'ambito di una attività di videosorveglianza, vi siano trattamenti rientranti in quelle ipotesi, da sottoporre all'esame preventivo dell'Autorità.

Ad esempio, il normale esercizio di un impianto di videosorveglianza digitale, in cui le immagini vengono riprese da telecamere digitali dotate delle ordinarie funzioni di ricerca, non comporta rischi specifici per gli interessati, essendo funzionalmente analogo alla videosorveglianza tradizionale con registrazione analogica delle immagini su supporti magnetici. Pertanto, l'adozione di sistemi digitali di questo tipo non implica la richiesta di verifica di cui all' *art.* 17 del Codice, necessaria, invece, in caso di utilizzo di tecniche avanzate di indicizzazione e ricerca, miranti al riconoscimento o alla classificazione sulla base di caratteristiche morfologiche e comportamentali degli interessati (*Nota* 2 gennaio 2008).

Da ultimo si menziona la segnalazione di un cittadino che lamentava la presenza di telecamere installate dal comune in grado di effettuare riprese ravvicinate all'interno del suo appartamento.

Le telecamere, come dichiarato dallo stesso comune, erano state posizionate, oltre che per monitorare il traffico, anche per esigenze di maggiore sicurezza dei cittadini, tutela del patrimonio e controllo di determinate aree.

Dagli accertamenti disposti dal Garante è emerso tuttavia che il tipo di telecamera installata permetteva *zoom*, brandeggio e identificazione dei tratti somatici delle persone riprese e che il sistema consentiva a qualsiasi operatore che avesse accesso diretto al *server* di spostare le telecamere nelle diverse direzioni operando così un'ingiustificata intromissione nella vita privata degli interessati.

Valutati questi elementi il Garante ha stabilito che, per utilizzare lecitamente il sistema di videosorveglianza, il comune avrebbe dovuto adottare ogni accorgimento volto ad evitare la ripresa di persone in abitazioni private, delimitando la dislocazione, l'uso dello *zoom* e l'angolo visuale delle telecamere in modo da escludere ogni forma di ripresa, anche in assenza di registrazione, di spazi interni, attraverso eventuali sistemi di "settaggio" e oscuramento automatico, non modificabili dall'operatore. È stato inoltre prescritto di integrare il modello di informativa fornita dal comune indicando, oltre al monitoraggio del traffico, le finalità di sicurezza e di controllo di competenza (*Provv.* 4 ottobre 2007 [doc. *web* n. 1457505]).

16 Il registro dei trattamenti

Il Garante ha il compito di tenere il registro dei trattamenti, formato sulla base delle notificazioni ricevute (art. 154, comma 1, lett. *l*)) e liberamente consultabile da chiunque attraverso la connessione al sito *web* dell'Autorità.

La notificazione, disciplinata dagli artt. 37 e 38 del Codice, consiste in una dichiarazione formale compilata direttamente sul *computer* dell'utente, con la quale vengono comunicati al Garante i trattamenti di dati suscettibili di recare particolare pregiudizio ai diritti e alle libertà dell'interessato, in ragione delle relative modalità o della natura dei dati personali. Nell'ottica della semplificazione amministrativa, i casi di notificazione sono stati ridotti dal Garante che ha la facoltà di individuare, nell'ambito dei trattamenti indicati nello stesso art. 37, quelli non suscettibili di recare pregiudizio ai diritti e alle libertà dell'interessato (*Provv.* 31 marzo 2004 [doc. *web* n. 852561]).

La notificazione riguarda solo informazioni essenziali che rendono comunque possibile effettuare ampi controlli, estrazioni di dati ed elaborazioni statistiche. Il registro viene infatti utilizzato dall'Autorità a fini di monitoraggio, controllo e orientamento delle attività ispettive in determinati settori.

La procedura della notificazione che –ad esclusione dell'apposizione della firma digitale sulla dichiarazione– avviene tramite connessione telematica via Internet sul *server* del Garante, presenta diversi vantaggi per l'utente: non vi sono orari vincolanti; la procedura può essere sospesa illimitatamente; numerosi avvertimenti inseriti direttamente nei campi di compilazione facilitano la comprensione; è possibile chiedere assistenza inviando *e-mail* o lasciando un messaggio durante la fase di sospensione della compilazione; il pagamento dei diritti di segreteria può essere effettuato anche *on-line* con carta di credito. Il costante monitoraggio della procedura da parte del personale del dipartimento (anche per le notificazioni non ancora concluse) assicura celeri risposte e la soluzione di eventuali problemi (spesso relativi alla fase di apposizione della firma digitale e comunque di lieve entità).

La procedura di notificazione ha continuato a fornire esiti particolarmente positivi in termini di efficienza, affidabilità e soddisfazione del pubblico. Gli obiettivi posti col sistema di notificazione (contenimento delle informazioni da chiedere ai titolari, massima semplificazione dell'*iter*, pubblicità completa del registro dei trattamenti) possono ritenersi interamente raggiunti e prevedono, tra l'altro, la possibilità di ulteriori applicazioni. È quanto avvenuto ad esempio nel caso della procedura di verifica preliminare *on-line* relativa ai dati biometrici utilizzati dalle banche.

Anche dal punto di vista della sicurezza, il sistema si è rivelato pienamente affidabile e l'impiego di un codice segreto (Cun, codice univoco del notificante), permette al titolare di apportare modifiche alle precedenti notificazioni o di dichiararne la cessazione.

In relazione poi alla possibilità di semplificare ulteriormente la fase di apposizione della firma digitale, è ancora in corso la collaborazione con il Cnipa per la sperimentazione di soluzioni alternative rispetto all'attuale procedura.

Chi non fosse in possesso della firma digitale può farla apporre da altri soggetti (avvocati, commercialisti, notai, conoscenti, *ecc.*) o da intermediari convenzionati con il Garante che assicurano una capillare presenza di uffici sul territorio e un servizio a prezzi contenuti (Poste italiane S.p.A., Unappa, Alar).

Numerosi sono stati i controlli effettuati tramite il registro circa l'obbligo di notificazione da parte dei titolari dei trattamenti. Ad esempio, l'accertamento di diverse violazioni di tale obbligo da parte di laboratori di analisi, pubblici e privati è avvenuto utilizzando i dati contenuti nel registro e confrontandoli con gli elenchi forniti dai vari assessorati regionali alla sanità.

In tal senso il registro si è rivelato un prezioso ausilio per orientare le attività ispettive del Garante.

Nell'anno 2007 è stata riscontrata una notevole flessione del numero delle notificazioni ricevute (fenomeno sulle cui motivazioni è ancora difficile formulare ipotesi attendibili): complessivamente, ne sono pervenute circa 1.400 rispetto alle 2.400 circa dell'anno precedente. Tali numeri si riferiscono alle prime notificazioni (la prima volta che si effettua la dichiarazione), alle modifiche (mutamenti dei contenuti della precedente dichiarazione) e alle cessazioni (nel caso in cui il trattamento denunciato non venga più effettuato).

L'incasso derivante dai diritti di segreteria è diminuito conseguentemente ma risulta comunque sufficiente a coprire i costi di mantenimento del registro.

17 La trattazione dei ricorsi

17.1. Considerazioni generali

Una lettura superficiale dei dati relativi al numero dei ricorsi pervenuti nel 2007 potrebbe portare a ravvisare una "crisi" del ricorso, ovvero una diminuita fiducia dei cittadini in questo strumento di tutela, specie se ci si limitasse al mero confronto delle cifre riepilogative.

In effetti, è proseguita anche nell'anno 2007 la diminuzione dei ricorsi proposti all'Autorità; ne sono stati decisi, infatti, 316 rispetto ai 435 esaminati nel 2006, che aveva già visto una diminuzione dei procedimenti avviati ai sensi degli artt. 145 ss. del Codice.

L'esame delle singole fattispecie sottoposte al vaglio dell'Autorità permette però di cogliere alcune linee di tendenza significative.

È senza dubbio diminuita la presentazione dei ricorsi di tipo "seriale", specie con riguardo al trattamento di dati personali conservati negli archivi dei *cd.* "sistemi di informazioni creditizie". Si tratta di quell'ambito di trattamenti che, a partire dal 2002, aveva fatto aumentare in maniera esponenziale il numero dei ricorsi, impegnando l'Autorità nel complesso esame di trattamenti di dati che non trovavano, allora, alcuna regolamentazione nell'ordinamento: situazioni che implicano necessariamente complessi rapporti tra i soggetti richiedenti il credito, le istituzioni finanziarie e, appunto, le *cd.* "centrali rischi private" (ora denominate sistemi di informazioni creditizie, *cd.* "sic") sorte per monitorare e censire le posizioni creditizie, con particolare riguardo all'ambito del credito al consumo.

La riflessione iniziata allora (specie su profili quali l'informativa, il consenso e la sua eventuale revoca, la qualità dei dati conservati, i tempi di registrazione e conservazione dei dati nel sistema, *ecc.*) ha portato, come noto, all'emanazione nel 2004 (*Provv.* 16 novembre 2004, in *G.U.* 23 dicembre 2004, n. 300 [doc. *web* n. 1070713]) del *"Codice di deontologia e di buona condotta per i sistemi informativi gestiti da soggetti privati in tema di crediti al consumo, affidabilità e puntualità nei pagamenti"* che ha regolamentato, per la prima volta, la materia, contribuendo a dare certezza di comportamento agli operatori del settore e, soprattutto, permettendo ai milioni di clienti censiti di essere informati in maniera chiara su un meccanismo che ha un impatto decisivo sulla possibilità di accesso al credito.

Dal 2005 è stato così possibile riscontrare, al tempo stesso, una diminuzione e una specializzazione del contenzioso in materia, finalizzato all'esame e all'eventuale contestazione di specifiche posizioni creditizie e non più genericamente volto all'ottenimento della cancellazione di tutti i dati personali di un ricorrente presenti negli archivi di un sic.

Questa linea di tendenza si è confermata nel corso del 2007 anche in relazione ad altri ambiti tematici. Il notevole numero di provvedimenti di carattere generale e di linee-guida adottati dal Garante negli ultimi anni ha infatti avuto evidenti ricadute sul tipo e sulle caratteristiche dei ricorsi. I numerosi temi affrontati (dalle problematiche relative al rapporto di lavoro, ai trattamenti di dati in ambito bancario, a quelli relativi al settore delle telecomunicazioni, *ecc.*) hanno infatti richiamato l'at-

tenzione su specifiche tipologie di trattamento (mostrando le infinite potenzialità applicative della disciplina sui dati personali e "stimolando" in alcuni casi il relativo contenzioso), ma hanno anche contribuito a "incanalare" le controversie entro le corrette categorie normative precisate appunto nei provvedimenti generali.

In quest'ottica lo strumento del ricorso acquista e consolida sfaccettature sempre nuove confermandosi, comunque, come utile indicatore del reale grado di percezione e di applicazione della disciplina sulla protezione dei dati. Da questo particolare punto di vista, se viene confermata l'impressione che la *privacy* (o meglio le implicazioni giuridiche della sua tutela) abbia fatto breccia nella vasta platea dei professionisti legali, è altrettanto vero che esistono ancora incertezze diffuse sul reale ambito di applicazione della disciplina e sulla stessa nomenclatura di base (concetti di dato personale, trattamento, titolare, *ecc.*) sicché, talora, il rigore delle categorie giuridiche lascia spazio a nozioni importate dalla cronaca giornalistica o dalla riflessione sociologica. Di tutto ciò è testimonianza il numero, che permane elevato, di ricorsi dichiarati inammissibili o infondati, perché spesso proposti in relazione a situazioni che esulano dal corretto ambito di applicazione del Codice.

Nell'ultimo anno si è poi consolidata un'altra linea di tendenza: quella che vede nel ricorso non solo lo strumento di tutela degli specifici e puntuali diritti elencati nell'art. 7 del Codice, ma anche il mezzo (incastonato nel quadro delle diverse tutele apprestate dall'ordinamento) atto a creare le condizioni per proporre, integrare, avvalorare l'esercizio di altre azioni in giudizio. Gli esempi non mancano: dall'accesso ai dati personali detenuti da un istituto di credito al fine di acquisire le necessarie informazioni per contestare la liceità di determinate clausole contrattuali o per intraprendere (in quanto erede) una causa di tipo successorio, alla raccolta di informazioni e di dati personali (sensibili e non) relativi al rapporto di lavoro finalizzata a ottenere tutela in ordine a controversie relative a progressioni di carriera o a denunciare azioni di *mobbing*, *ecc.*

Naturalmente, però, i rapporti fra i diversi strumenti giuridici impiegati (e i diversi fori implicati) pongono questioni complesse anche in riferimento ad alcune disposizioni del Codice, al centro, non a caso, di discussioni anche a livello dottrinale. Va ricordato anzitutto il disposto dell'art. 145, comma 2, del Codice in base al quale *"il ricorso al Garante non può essere proposto se, per il medesimo oggetto e tra le stesse parti, è stata già adita l'autorità giudiziaria"*. La disposizione è stata oggetto, anche recentemente, di interpretazione da parte dell'Autorità (*Provv.* 25 marzo 2008 [doc. *web* n. 1519557]) che, in ordine al caso di specie –nel confronto fra le richieste formulate con il ricorso e quelle precedentemente proposte nel corso di un procedimento civile– ha rilevato che dalle stesse emergeva un caso di sostanziale litispendenza, ravvisandosi appunto una situazione di continenza tra l'oggetto delle istanze rivolte all'Autorità con quelle formulate dinanzi al tribunale in riferimento a una delicata vicenda familiare.

Non meno rilevante, nella concreta dinamica fra le diverse forme di tutela, è il ruolo dell'art. 8, comma 2, lett. *e*), del Codice che pone un limite all'esercizio dei diritti di cui all'art. 7 quando *"potrebbe derivarne un pregiudizio effettivo e concreto per lo svolgimento delle investigazioni difensive o per l'esercizio di un diritto in sede giudiziaria"*.

Spesso il Garante, in sede di decisione sui ricorsi, è stato chiamato al non facile compito di valutare la sussistenza dei requisiti per il citato differimento, al fine di contemperare le richieste ispirate dall'esigenza di tutela dei dati personali con la non meno rilevante necessità di assicurare la tutela del diritto di difesa costituzionalmente garantito dall'art. 24 Cost. (*cfr. Provvedimenti* 10 dicembre 2007 [doc. *web* n. 1497600] e 21 dicembre 2007 [doc. *web* n. 1490154]).

Va infine ricordata, a conclusione di questi brevi cenni sulle interrelazioni fra i diversi tipi di procedimenti, la disposizione di "raccordo" di cui all'art. 160, comma 6, del Codice che *"rimette alle pertinenti disposizioni processuali nella materia civile e penale"* il giudizio su *"validità, efficacia e inutilizzabilità di atti (...) basati sul trattamento di dati personali non conforme a disposizioni di legge o regolamento"*.

17.2. *Ampiezza della nozione di dato personale*

Anche nello scorso anno alcuni ricorsi hanno permesso al Garante di riflettere sulla nozione di dato personale, ampliandone ulteriormente la latitudine, attesa l'ampia definizione che, sulla falsariga della direttiva comunitaria 95/46/Ce, è stata accolta dall'art. 4, comma 1, lett. *b*), del Codice.

Due vicende hanno riguardato trattamenti svolti in ambito giornalistico e hanno comportato l'accoglimento di due ricorsi relativi a interessati che, pur non nominativamente individuati, risultavano però "identificabili" dal contesto. Nel primo, (*Provv.* 8 marzo 2007 [doc. *web* n. 1396630]), la contestuale combinazione di diversi elementi identificativi (attività professionale, limitata estensione del centro abitato cui erano riferite le cronache, nominativi dei ricorrenti facilmente e liberamente disponibili presso altre fonti informative) poteva consentire – seppur non alla generalità degli utenti, ad un numero comunque significativo di persone– di identificare con precisione i ricorrenti.

In altra vicenda (*Provv.* 19 settembre 2007 [doc. *web* n. 1445858]) la contestuale diffusione di alcune informazioni (età e nome di battesimo di un minore, nomi, iniziali dei cognomi, professioni dei genitori, città ove si è svolto il fatto) determinava l'identificabilità dell'adolescente di cui veniva tratteggiata in un articolo la controversa vicenda familiare.

Nella decisione del 3 maggio 2007 [doc. *web* n. 1408971] nei confronti dell'editore di un quotidiano, un dato personale pubblicato con specifico riferimento a due persone diverse dalla ricorrente, è stato considerato quale dato personale riferibile, sia pure indirettamente, anche a quest'ultima, dal momento che l'informazione in questione spiegava parimenti effetti che la interessavano (in particolare, era stata riportata la notizia della morte del marito della ricorrente in un incidente stradale ed era stato detto che lo stesso era accompagnato dalla sua *"attuale compagna"*).

Non è stata invece considerata quale valida istanza di accesso *ex* art. 7 del Codice la richiesta di un erede di aver accesso a materiale organico (ipoteticamente detenuto da un ospedale) che avrebbe potuto contenere tracce biologiche di un ascendente defunto. Ciò in quanto la richiesta era relativa, come dovuto, non a "dati personali", ma all'acquisizione di tessuti che solo a seguito di specifici procedimenti di estrazione ed esame avrebbero potuto eventualmente portare all'individuazione di informazioni di tipo genetico (*Provv.* 21 giugno 2007 [doc. *web* n. 1433975]).

17.3. *Dato personale e valutazioni*

Un altro tema ricorrente nella trattazione dei ricorsi, trasversale a molti ambiti e settori, è quello connesso alle delicate ipotesi di trattamento di dati di tipo valutativo (giudizi, opinioni, note caratteristiche, valutazioni annuali di dipendenti e collaboratori, *ecc.*).

È un tema strettamente connesso alla sempre più ampia diffusione di procedure articolate e personalizzate di valutazione del personale dipendente da parte dei

datori di lavoro, ma non è limitato a tale ambito. Ne è testimonianza anche il diffuso contenzioso connesso alle richieste di accesso ai dati personali contenuti nelle perizie medico-legali in campo assicurativo che contengono, per definizione, delicate informazioni di questa natura.

Peraltro, nel caso dei dati valutativi raccolti in riferimento all'ordinaria gestione del rapporto di lavoro, le richieste di accesso a tali dati personali (ferma restando l'impossibilità di chiederne la rettificazione o l'integrazione) sono nella maggioranza dei casi legittimamente esperibili.

Diversa la situazione in ordine alle perizie effettuate per ragioni di difesa e di tutela delle compagnie di assicurazione e rispetto alle quali, per tale motivo, è opponibile la disposizione (art. 8, comma 2, lett. *e*), del Codice) che prevede la possibilità di un differimento del diritto di accesso quando l'ostensione dei dati personali richiesti determinerebbe un pregiudizio effettivo e concreto per lo svolgimento delle investigazioni difensive o per l'esercizio del diritto in sede giudiziaria da parte del titolare del trattamento (*Provv.* 10 dicembre 2007 [doc. *web* n. 1497600]).

Negli ultimi mesi, però, si sono moltiplicati i casi nei quali i dati valutativi oggetto di contenzioso sono riferiti non a persone fisiche, bensì a persone giuridiche, in particolare a operatori economici. Il tema coinvolge primariamente il ruolo e le modalità di azione dei soggetti che operano nel settore delle *cd.* "informazioni commerciali". Si tratta di soggetti che offrono *dossier* sempre più approfonditi sulla vita, lo sviluppo, le potenzialità delle imprese e delle persone fisiche preposte alla loro guida. Ciò, attraverso il ricorso non solo alla divulgazione dei dati provenienti dalla consultazione delle fonti pubbliche disponibili (camere di commercio, archivi delle *ex* conservatorie dei registri immobiliari, registri presso i tribunali, *ecc.*), ma anche alla rielaborazione originale del complesso delle informazioni disponibili.

Tali operazioni determinano così la creazione di "indici", "giudizi di affidabilità", "schede persona" che, anche attraverso il ricorso a punteggi e codici, valutano la "consistenza" degli operatori economici e il grado di sicurezza delle eventuali transazioni concluse con gli stessi, attraverso il controllo, ad esempio, degli "eventi pregiudizievoli" o il grado di "rilevanza storica dei fenomeni di insolvibilità" (*Provv.* 8 marzo 2008 [doc. *web* n. 1396584]).

È evidente il peso e l'influenza che tali valutazioni possono avere sull'attività di un'impresa, condizionandone pesantemente l'operatività e le prospettive di sviluppo: da qui l'emergere di un diffuso contenzioso al riguardo (*v. Provv.* 31 ottobre 2007 [doc. *web* n. 1458863] e 23 gennaio 2008, [doc. *web* n. 1490183]) imperniato sul rispetto dei princìpi di liceità e correttezza con particolare riguardo alla completezza di tali informazioni, alla loro capacità di offrire un'informazione corretta su un certo operatore economico, alla liceità dell'associazione di dati negativi risalenti nel tempo (*ad es.*, essere stato socio non amministratore di una società poi fallita) al profilo attuale di un imprenditore.

La delicatezza del tema (portato all'attenzione dell'Autorità anche da numerose segnalazioni) ha spinto il Garante ad avviare un approfondimento organico della problematica, per la quale l'art. 118 del Codice prevede l'adozione di un apposito codice di deontologia e di buona condotta.

17.4. *Trattamento dei dati e* cd. *"furto d'identità"*

Il moltiplicarsi delle forme anche automatizzate di trattamento delle informazioni personali e la proliferazione di archivi e sistemi di centralizzazione dei rischi, specie nel campo creditizio, ha moltiplicato i rischi di sottrazione fraudolenta delle

informazioni, diffondendo anche nel nostro Paese il fenomeno del *cd.* "furto d'identità", che è venuto in evidenza anche nella trattazione di alcuni ricorsi (*v. Provv.* 5 marzo 2008 [doc. *web* n. 1501621]). Settore particolarmente esposto è appunto quello del credito al consumo, dove richieste di finanziamento effettuate utilizzando dati identificativi (veri o parzialmente veri) di soggetti ignari portano spesso all'instaurazione di rapporti contrattuali mirati a fini di truffa, forieri peraltro di rilevanti conseguenze negative non solo per l'ente finanziatore, ma anche per il cittadino i cui dati vengono illecitamente utilizzati (e che finiscono per essere censiti incolpevolmente negli archivi dei sic).

17.5. *Appunti di tipo procedurale*

Più volte nel corso dell'anno 2007 sono emerse questioni relative alla corretta interpretazione delle disposizioni di legge relative ai procedimenti sui ricorsi.

Va anzitutto ricordato l'art. 5, comma 3, del Codice, per il quale non sono soggetti all'applicazione delle disposizioni di cui agli artt. 7 e 145 i trattamenti di dati personali effettuati da persone fisiche per fini esclusivamente personali. Ciò, determina la conseguente inammissibilità di quei ricorsi (che restano ancora numerosi) aventi ad oggetto, ad esempio, le controversie fra vicini di casa determinate dall'utilizzo di impianti di videosorveglianza. Naturalmente, tali situazioni possono trovare tutela sulla base di altre disposizioni previste dall'ordinamento giuridico (*ad es.*, l'art. 615 *bis* c.p.).

Resta poi in diversi casi confuso o inappropriato l'utilizzo di quel nutrito catalogo di posizioni giuridiche tutelate dall'art. 7 del Codice (le sole rispetto alle quali, come noto, può poi essere proposto il ricorso all'Autorità). Troppe volte gli interessati richiamano nella sua totalità tale elenco senza cogliere lo specifico di alcune particolari posizioni giuridiche.

Questo porta a generiche richieste di cancellazione dei dati (che non indicano la violazione di legge che legittimerebbe tale istanza), oppure a confusione fra l'opposizione al trattamento a fini di invio di materiale pubblicitario e la più complessa (e di più ampio respiro) opposizione per motivi legittimi al trattamento di dati.

Parimenti diffusa (nonostante i frequenti richiami contenuti nelle motivazioni dei provvedimenti) è, poi, la sovrapposizione fra il concetto di accesso ai dati personali e il diverso diritto di accesso alla documentazione amministrativa (legge n. 241/1990) o a quella bancaria (tutelato dall'art. 119 del *cd.* "testo unico bancario"). Ciò conferma l'impressione, già rilevata, per la quale la legge sulla protezione dei dati sembra, a volte, essere invocata quale rimedio onnicomprensivo adatto alle più diverse situazioni.

17.6. *Brevi cenni sulla casistica*

In questo paragrafo si pongono in evidenza solo alcuni degli ambiti tematici rispetto ai quali sono stati presentati i ricorsi decisi nell'anno 2007 sottolineando alcune delle decisioni più significative.

Trattamenti svolti presso i sic (sistemi di informazioni creditizie)

È il settore che ha fatto registrare ancora una volta il maggior numero di decisioni. Come già accennato nelle premesse di questo capitolo, l'attenzione è stata rivolta essenzialmente al corretto adempimento delle prescrizioni di cui al codice deontologico di settore. Da questo punto di vista è risultata confermata la centralità della disposizione di cui all'art. 4, comma 7, di tale codice di deontologia e di buona

condotta che prevede l'inoltro all'interessato, al verificarsi di ritardi nei pagamenti delle rate di un finanziamento, di un preavviso volto a informare il debitore medesimo che il protrarsi dell'inadempimento porterà alla registrazione dei suoi dati personali fra le *cd.* "posizioni negative" conservate negli archivi dei sic.

È una disposizione che adempie a evidenti ragioni di correttezza e trasparenza (oltre ad avere un significativo valore deterrente nei confronti dei contraenti "ritardatari") il cui mancato rispetto da parte degli enti finanziatori ha portato all'accoglimento nell'ultimo anno di alcuni ricorsi: ciò, in un caso recente, anche in relazione alla posizione del coobbligato rispetto ad un finanziamento erogato ad un terzo (*Provv.* 13 marzo 2008 [doc. *web* n. 1502131]). Anche nei confronti di tale soggetto incombe infatti l'obbligo, a carico dell'ente finanziatore, di provvedere all'inoltro del citato preavviso di inserimento nei sic.

Negli ultimi mesi, peraltro, diversi provvedimenti hanno riguardato non l'archivio del sic propriamente detto, ma quegli ulteriori e distinti archivi dove gli operatori del settore conservano altri tipi di informazioni, quali le banche dati contenenti le informazioni ricavate dai tribunali e dai registri immobiliari. Si tratta di dati tratti da pubblici registri che, in via generale, possono essere utilizzati senza il consenso degli interessati. Sono informazioni cui non si applica il codice di deontologia previsto per il settore del credito al consumo, avendo la legge previsto la redazione dello specifico codice deontologico di cui all'art. 61 del Codice.

Nei casi sottoposti all'esame dell'Autorità sono emersi, in particolare, profili connessi alla completezza ed esattezza delle informazioni rese disponibili. Ciò, con particolare riferimento all'utilizzo di espressioni (quali *"atto colpito da annotamento"*) che, in presenza dell'intervenuta cancellazione di un'ipoteca, risultavano equivoche e fuorvianti (*v.*, fra gli altri, *Provv.* 21 febbraio 2008 [doc. *web* n. 1501246]). L'attenzione alla qualità dei dati ha, del resto, un ruolo fondamentale nella realtà economica contemporanea atteso che le informazioni inesatte o incomplete possono rappresentare in maniera distorta l'identità e, in particolare, il profilo imprenditoriale degli interessati.

Alcune vicende hanno portato anche quest'anno all'attenzione del Garante il trattamento dei dati svolti presso l'archivio informatizzato degli assegni bancari e postali e delle carte di pagamento (Centrale d'allarme interbancaria-Cai).

Si tratta di un ambito puntualmente regolamentato dalla legge n. 386/1990 e dalle relative norme di attuazione. Al rispetto di tale disciplina si richiamano le decisioni del Garante che verifica normalmente la regolarità della procedura (sotto il profilo del corretto trattamento dei dati personali nella stessa implicati) presso l'ente segnalante, intervenendo con provvedimenti di accoglimento (invero rari) solamente qualora risultino irregolarità nella stessa (*v. Provv.* 28 febbraio 2008 [doc. *web* n. 1500676]).

Trattamento dei dati personali dei lavoratori

Quello dei dati personali dei lavoratori è un ambito che –con particolare riferimento al settore privato nel quale non è possibile utilizzare altri strumenti conoscitivi quali il diritto di accesso ai documenti amministrativi tutelato dalla legge n. 241/1990– registra un costante flusso di istanze e di ricorsi. In tutte le fattispecie rimane centrale l'esercizio del diritto di accesso ai dati personali che acquista sempre più spesso i contorni della ricostruzione di un'intera vicenda professionale, intrecciandosi sia con le patologie del rapporto (licenziamento, comunicazioni di sanzioni disciplinari), sia con momenti comunque delicati dello stesso (selezioni, procedure di valutazione, ricostruzione di percorsi professionali in occasione di trasferimenti, cessioni di ramo d'azienda, pensionamenti, *ecc.*). I diversi casi esaminati (*v.*, tra gli altri, *Provv.* 4 ottobre 2007 [doc. *web* n. 1449401]) hanno evidenziato ancora una difficoltà e una ritrosia sia dei piccoli imprenditori, sia delle società di maggiori dimensioni a soddisfare integralmente e tempestivamente le richieste dei dipendenti.

Emerge la difficoltà di raggruppare e rendere disponibili complessi di informazioni conservati ancora largamente in forma cartacea e archiviati in banche dati spesso disperse sul territorio. In alcuni casi si è segnalata la difficoltà di collegare e considerare unitariamente le informazioni più tipicamente proprie del rapporto di lavoro (dati su orari, presenze, malattie, stipendi, *ecc.*) e i dati personali, specie valutativi, trattati in riferimento alle progressioni di carriera. Difficoltà che si acuiscono quando il dipendente occupa posizioni di rilievo o è stato impiegato in molteplici dipendenze dell'azienda e ha pertanto ampiamente "disseminato" i propri dati che, difficilmente, possono trovare completa e indifferenziata collocazione nel tradizionale fascicolo personale.

Trattamenti svolti da investigatori privati

In connessione con il segnalato, sempre più frequente, intreccio fra disciplina di protezione dei dati e attività finalizzate alla tutela di un diritto in giudizio, si collocano le decisioni adottate in relazione all'attività svolta dagli investigatori privati.

Si tratta di vicende (*Provv.* 21 dicembre 2007 [doc. *web* n. 1490154] e 25 marzo 2008 [doc. *web* n. 1519557]) nelle quali, non a caso, le società di investigazione sono state chiamate in causa unitamente ai titolari del trattamento nel cui interesse operavano e ai legali che, nell'esercizio del loro mandato, avevano commissionato appunto le attività investigative private.

I casi esaminati hanno permesso di mettere a fuoco temi delicati quali, ad esempio, i limiti dell'azione degli investigatori, le corrette modalità del loro operare e i profili legati ai tempi di conservazione delle informazioni raccolte.

Ciò, in un contesto (quale quello delle due vicende citate) nel quale la potenziale invasività delle forme di controllo veniva esaltata dalle tecnologie impiegate e, in un caso, dallo stesso tentativo di acquisire, ad insaputa dell'interessato, informazioni di tipo genetico. Le situazioni esaminate sono state un indubbio banco di prova anche per verificare la "tenuta" delle prescrizioni contenute nelle autorizzazioni generali al trattamento dei dati sensibili rilasciate con riferimento a questo ambito professionale e per acquisire utili elementi di riflessione in vista del completamento della disciplina di riferimento, con particolare riguardo alla redazione del codice di deontologia e di buona condotta per il trattamento dei dati finalizzati appunto alle investigazioni difensive e alla difesa di un diritto in sede giudiziaria (codice di cui è prossimo l'esame definitivo dello schema preliminare aperto alla consultazione pubblica [doc. *web* n. 1503511]).

Trattamenti per finalità giornalistiche

Rispetto agli anni passati, il 2007 ha visto la presentazione di un significativo numero di ricorsi in materia giornalistica. La rapidità del procedimento e la possibilità di proporre l'atto in via d'urgenza, invocando anche la tutela cautelare di cui all'art. 150, comma 1, del Codice, hanno sicuramente indotto gli interessati all'utilizzo di questo strumento al fine di ottenere una tutela quanto più immediata possibile ed evitare del tutto, o ridurre al minimo, la risonanza mediatica di vicende spesso delicate. Non a caso, molti dei casi esaminati hanno riguardato l'utilizzo del mezzo radiotelevisivo o (quando la divulgazione è avvenuta a mezzo di pubblicazioni a stampa) erano riferiti a persone che, dal mezzo televisivo, avevano ricevuto quella notorietà che ha indotto anche altri mezzi di comunicazione a dare spazio a determinate notizie. Ne è esempio la decisione del 7 giugno 2007 [doc. *web* n. 1419429] che trae spunto da uno *scoop* giornalistico (originato dall'ascolto –avvenuto in modo non scorretto– di alcune conversazioni in un ristorante) incentrato sulla futura conduzione della più importante rassegna canora nazionale. Così come, in un altro caso, la tempestiva presentazione del ricorso (*Provv.* 22 novembre 2007 [doc. *web* n. 1470697]) ha permesso di bloccare la messa in onda, nell'ambito di una delle più seguite trasmissioni televisive, delle immagini di una persona che era stata ritratta e "intervistata" senza consenso.

Anche nel settore giornalistico, peraltro, le problematiche più interessanti sono emerse in relazione all'utilizzo delle nuove tecnologie che hanno proposto fattispecie inedite sia in riferimento alla fase di raccolta, sia in ordine alla successiva diffusione delle informazioni acquisite. Vanno così ricordate le decisioni del 24 maggio 2007 [doc. *web* n. 1419749] e del 5 luglio 2007 [doc. *web* n. 1436163] che hanno posto all'attenzione del Garante, in un caso, l'acquisizione e il successivo utilizzo, senza il consenso dell'interessato, in un articolo di cronaca giornalistica, di un messaggio di posta elettronica a carattere personale e pertanto soggetto anche alla disposizione di cui all'art. 93 della legge sulla protezione del diritto d'autore; nell'altro, l'utilizzo, ritenuto scorretto, di immagini e brani di conversazioni acquisite all'insaputa dell'interessato da due persone che avevano peraltro celato la loro vera identità.

Devono infine essere ricordate le decisioni che hanno portato all'accoglimento di ricorsi concernenti la diffusione via Internet, tramite i siti delle testate giornalistiche, di *file* audio contenenti registrazioni di telefonate. In un caso (*Provv.* 8 febbraio 2007 [doc. *web* n. 1388922]) la registrazione, fatta pervenire ad un quotidiano locale, risultava illegittimamente acquisita. In un altro (*Provv.* 25 ottobre 2007 [doc. *web* n. 1458851]) –pur riconoscendo la legittimità dell'acquisizione dei dati relativi a intercettazioni telefoniche avvenute nell'ambito di un procedimento penale e la rilevanza della loro divulgazione, in un primo momento, anche in forma audio– il Garante ha però ritenuto che la diffusione indifferenziata e a tempo indeterminato di tali risultanze audio determinava un ulteriore, specifico impatto sulla sfera personale degli interessati e sulla loro dignità. Ciò, in una misura che rendeva eccedente tale forma di diffusione rispetto alle esigenze di giustificata informazione su vicende di interesse pubblico e imponeva pertanto l'interruzione di tale particolare trattamento di dati.

18 Il contenzioso giurisdizionale

18.1. *Considerazioni generali*

Nel 2007 si è avuta un'importante conferma del sempre maggiore favore che incontra presso gli interessati il procedimento introdotto dall'art. 152 del Codice, volto alla tutela giurisdizionale del diritto alla protezione dei dati personali, attraverso una procedura snella e specifica, alternativa al ricorso presentato in sede amministrativa al Garante.

A fronte dei cinquantanove ricorsi del 2006, nel corso del 2007 sono stati notificati all'Autorità ben centotrentaquattro ricorsi, non coinvolgenti direttamente pronunce del Garante, con un aumento di oltre il 125%.

Tale incremento accresce il rilievo degli strumenti messi a disposizione del Garante in ordine alla conoscenza e alla gestione del contenzioso in materia di protezione dei dati, costituiti dall'obbligo di notifica all'Autorità di tutti i ricorsi presentati all'autorità giudiziaria ordinaria concernenti l'applicazione del Codice (art. 152, comma 7) e, per le cancellerie, dall'obbligo di trasmettere al Garante copia dei provvedimenti emessi in relazione a quanto previsto dal Codice o in materia di criminalità informatica (art. 154, comma 6). Oltre a fornire un'informazione ampia sull'evoluzione della giurisprudenza in materia, tali strumenti permettono all'Autorità di intervenire nelle controversie in cui, pur non essendo direttamente coinvolta, sono in discussione profili di carattere generale sulla protezione dei dati.

18.2. *I profili procedurali*

L'art. 152 prevede infatti che tutte le controversie riguardanti l'applicazione del Codice sono devolute all'autorità giudiziaria ordinaria (comma 1), con ricorso da depositare nella cancelleria del tribunale del luogo ove risiede il titolare del trattamento (comma 2).

Anche nel 2007, tuttavia, il giudice amministrativo si è dovuto pronunciare su di un ricorso in materia di protezione di dati personali.

Si è rivolta al Tribunale amministrativo regionale del Lazio una società operante nel settore del *direct marketing* chiedendo l'annullamento, previa sospensione, del *provvedimento* del Garante del 15 luglio 2004 [doc. *web* n. 1032381] concernente l'individuazione delle modalità di inserimento e di successivo utilizzo dei dati personali relativi agli abbonati negli elenchi telefonici cartacei o elettronici. Costituitasi in giudizio, l'Autorità ha eccepito il difetto di giurisdizione del giudice amministrativo, alla luce della ricordata chiara dizione normativa.

Dopo avere respinto la domanda di sospensione presentata dalla ricorrente (ordinanza del 25 maggio 2005) il Tribunale, con sentenza n. 2664 del 27 marzo 2007, ha dichiarato inammissibile il ricorso in quanto la controversia rientra appunto nella giurisdizione dell'autorità giudiziaria ordinaria.

Con sentenza n. 5091 del 2 ottobre 2007 il Consiglio di Stato ha confermato tale decisione.

In tema di competenza territoriale assume particolare interesse la decisione della Corte di cassazione concernente una fattispecie nella quale l'interessato ha proposto

opposizione avverso un *provvedimento* emesso dal Garante nei confronti di più titolari del trattamento i quali risiedono in luoghi situati nel circondario di tribunali diversi. Adita dall'interessato con regolamento di competenza, la Suprema Corte ha rilevato che con la disposizione del comma 2 dell'art. 152 il legislatore ha istituito una competenza territoriale assoluta e inderogabile, con conseguente inapplicabilità sia del disposto dell'art. 33 c.p.c. in materia di cumulo soggettivo, che può determinare lo spostamento di competenza territoriale solo ove questa abbia carattere relativo e derogabile, sia del foro erariale di cui all'art. 25 c.p.c., norma generale sulla quale prevale la disposizione speciale posta dall'art. 152 del Codice.

Ne consegue, ha concluso la Cassazione, che avendo il ricorrente attribuito a tutte le società convenute la titolarità di più trattamenti lesivi, egli deve impugnare il *provvedimento* del Garante e proporre separate domande avanti a ciascuno dei giudici nel cui territorio hanno sede le convenute. Ogni giudice possiede quindi competenza in ordine alla controversia inerente al *provvedimento* dell'Autorità per la parte in cui il *provvedimento* stesso riguarda il titolare che in quel circondario ha attratto la competenza (Cass. civ., sez. III, ord. n. 23280 del 25 settembre 2007).

Anche nel 2007 è stato proposto un ricorso straordinario al Presidente della Repubblica nei confronti di un provvedimento del Garante. Come riferito nella *Relazione* 2006, con parere n. 2265/2005, emesso nell'ambito di un analogo procedimento, il Consiglio di Stato ha ritenuto ammissibile tale ricorso anche nei confronti dei provvedimenti delle autorità indipendenti in quanto rimedio amministrativo previsto, ai sensi dell'art. 8, comma 1, d.P.R. 1199/1971, nei confronti di tutti gli atti amministrativi definitivi, a prescindere dall'attribuzione di una materia ad una determinata giurisdizione.

18.3. *I profili di merito*

Un aspetto che caratterizza le controversie concernenti la protezione dei dati personali attiene alla individuazione e liquidazione dei danni conseguenti ai trattamenti illeciti.

L'art. 15 del Codice sancisce l'obbligo a carico di ogni soggetto che effettua un trattamento di dati personali di risarcire ai sensi dell'art. 2050 c.c. il danno, anche non patrimoniale, cagionato per effetto del trattamento stesso.

Il Codice non attribuisce al Garante alcuna competenza in questa materia, riservata alla competenza esclusiva dell'autorità giudiziaria ordinaria (art. 152, comma 12) la quale nel corso del 2007, si è pronunciata più volte sulle richieste di risarcimento proposte dagli interessati con decisioni emesse in fattispecie in cui non erano in discussione provvedimenti adottati dall'Autorità.

L'esame di tali decisioni permette di rilevare che, mentre vi è uniformità di giudizio in ordine alla necessità che l'interessato assolva in maniera rigorosa all'onere della prova della sussistenza del danno patrimoniale di cui chieda il ristoro al fine della concessione del relativo risarcimento, altrettanta uniformità non si riscontra relativamente alla sussistenza della prova del danno non patrimoniale.

Premesso che il richiamo operato dall'art. 15 del Codice all'art. 2050 c.c. attiene alla dimostrazione della responsabilità e non del danno subìto, alcune pronunce attribuiscono il risarcimento per il solo fatto dell'esistenza della violazione della normativa in materia di protezione dei dati, ritenendo quindi –seppur implicitamente– che tale violazione sia di per sé produttiva di danno, anche a prescindere dalla sua concreta dimostrazione e, per quanto può evincersi dalla lettura delle decisioni,

in presenza della sola generica allegazione da parte dell'interessato di alcuni profili atti astrattamente ad integrarlo, solitamente indicati nella lesione all'onore e alla reputazione o, più genericamente, alla riservatezza.

In altre decisioni, di minor numero, il difetto dell'allegazione di elementi probatori relativi all'esistenza del danno non patrimoniale ha invece condotto al rigetto della relativa domanda; ulteriori pronunce hanno liquidato tale voce di danno proprio in presenza di elementi di prova, in genere identificati in documentate alterazioni dello stato di salute dell'interessato.

Relativamente, infine, al profilo relativo alla liquidazione del danno non patrimoniale, le pronunce in esame hanno adottato concordemente il criterio equitativo, basato su parametri individuati, a seconda dei casi, nella quantità dei dati oggetto di trattamento, nell'arco di tempo nel quale questo si è protratto, nelle modalità utilizzate dall'agente, specie in casi di diffusione illecita delle informazioni personali, nel contesto generale nel quale si è concretata la condotta illecita e il suo grado di offensività.

18.4. *Le opposizioni ai provvedimenti del Garante*

Nel corso del 2007 sono state proposte diciotto opposizioni ad altrettanti provvedimenti del Garante, di cui nove nei confronti di decisioni assunte a seguito di ricorso, mentre tre hanno riguardato provvedimenti adottati su segnalazione degli interessati.

La casistica indica che quattro opposizioni sono state proposte nei confronti di provvedimenti assunti d'ufficio dal Garante all'esito di attività istruttorie svolte nell'ambito della verifica, compiuta anche attraverso l'espletamento di accertamenti ispettivi, della liceità dei trattamenti dei dati effettuati nei più vari settori di attività.

Due, infine, sono state le opposizioni proposte nei confronti di ordinanze ingiunzioni concernenti il pagamento di sanzioni amministrative comminate dall'Autorità sulla base dell'accertamento della violazione delle rispettive disposizioni del Codice.

Nel corso del 2007 sono intervenute undici decisioni dell'autorità giudiziaria relative a opposizioni a provvedimenti del Garante, che in tali giudizi si è sempre costituito.

Due opposizioni sono state proposte da società titolari del trattamento aventi sede in luoghi situati nel circondario di tribunali diversi, nei confronti del medesimo *provvedimento* del 9 febbraio 2005 [doc. *web* n. 1142194] con il quale il Garante ha ordinato alle due società, che gestiscono per finalità di informazione commerciale banche dati contenenti informazioni desunte dai pubblici registri immobiliari tenuti dalle agenzie del territorio, di cancellare i dati dell'interessato relativi a un pignoramento iscritto a proprio carico, di cui era stata successivamente annotata la cancellazione. Il Garante ha assunto tale decisione a seguito all'entrata in vigore della legge n. 311/2004 il cui art. 1, al comma 367, ha disposto il divieto di riutilizzazione commerciale di tali dati.

Le due opposizioni hanno trovato accoglimento.

Con la prima decisione il Tribunale di Roma, con sentenza n. 6546 del 27 marzo 2007, pur riconoscendo corretto l'esame del ricorso da parte del Garante alla luce della disposizione entrata in vigore nelle more del procedimento, ha tuttavia ritenuto che la conservazione delle informazioni da parte delle società non potesse ritenersi illegittima, in quanto la norma non prevede un divieto assoluto di riutilizzazione, che è invece ammesso seppur subordinato alla stipula di specifiche convenzioni con l'Agenzia del territorio.

Nell'accogliere la seconda opposizione il Tribunale di Monza ha osservato che l'interessato non aveva posto a base della richiesta di cancellazione la disposizione di legge applicata dal Garante; ha quindi ritenuto che non potesse applicarsi nella specie il diritto all'oblìo invocato dal ricorrente e che non potesse trovare accoglimento la richiesta di cancellazione del dato relativo al pignoramento immobiliare e dell'annotazione della sua cancellazione (sentenza n. 151 del 15 gennaio 2007).

Deve peraltro rilevarsi che in un caso di opposizione proposta avverso un analogo provvedimento l'ordine di cancellazione dei dati adottato del Garante (*Provv.* 17 febbraio 2005 [doc. *web* n. 1148378]) è stato invece confermato dal Tribunale di Roma che, con sentenza n. 22621 del 6 febbraio 2007, ha modificato la pronuncia dell'Autorità nel solo capo concernente la determinazioni sulle spese, che sono state compensate, con la motivazione che il Garante avrebbe dovuto tenere conto della legittimità del trattamento dei dati operato dalla società resistente sino alla data di entrata in vigore della normativa che ne ha successivamente vietato il riutilizzo.

È stata respinta (Tribunale di Roma, sentenza n. 15454 del 28 giugno 2007) l'opposizione proposta nei confronti del provvedimento adottato dal Garante il 17 febbraio 2005 [doc. *web* n. 1148335] con il quale, ai sensi dell'art. 8 del Codice, è stata ribadita l'inammissibilità di un ricorso proposto nei confronti della Banca d'Italia.

Nel settore del trattamento dei dati nello svolgimento dell'attività giornalistica è stato respinto il ricorso proposto da una società editrice di una trasmissione televisiva avverso il *provvedimento* del 12 gennaio 2006 [doc. *web* n. 1213631] con il quale l'Autorità ha vietato l'ulteriore diffusione di dati personali sensibili, idonei a rivelare informazioni sulla sfera sessuale, relativi a un noto personaggio pubblico in quanto ritenuta esorbitante dal legittimo esercizio del diritto di cronaca e lesiva dei diritti della personalità dell'interessato. Il Tribunale di Roma, con sentenza n. 10455 del 15 maggio 2007, ha in particolare ritenuto che, fermo restando che la pubblicazione di notizie relative alle abitudini sessuali di una persona può essere lecita se questa riveste una posizione di particolare rilevanza sociale o pubblica (art. 11, comma 2 del codice di deontologia del settore), nel caso in esame il servizio giornalistico non presentasse alcuna attinenza con le ragioni della notorietà del personaggio.

Ancora, in materia di trattamento dei dati in ambito giornalistico ha trovato conferma la pronuncia del 5 ottobre 2006 [doc. *web* n. 1356268] con cui il Garante ha ritenuto lecita la pubblicazione su di un quotidiano di un articolo contenente ampi stralci di un verbale di interrogatorio reso dall'interessata all'autorità giudiziaria quale persona informata sui fatti, nonché di talune intercettazioni telefoniche acquisite nell'ambito di una nota vicenda giudiziaria. Nella specie il Tribunale di Roma, con sentenza n. 8174 del 19 aprile 2007, ha respinto l'opposizione proposta dalla società editrice, ritenendo che la pubblicazione dell'articolo fosse espressione del legittimo esercizio del diritto di cronaca, riportando notizie pertinenti e non più coperte dal segreto istruttorio.

È stata infine proposta opposizione anche avverso due *provvedimenti* di divieto del trattamento del 14 dicembre 2006 [doc. *web.* n. 1370954] adottati dal Garante in sostituzione dei *provvedimenti* provvisori di blocco assunti nei confronti di una società concessionaria di reti televisive (*Provvedimenti* 10 ottobre 2006 e 19 ottobre 2006 [doc. *web* nn. 1345622 e 1350853], *v. Relazione* 2006). Il Tribunale ha dichiarato la cessazione della materia del contendere in relazione alle opposizioni proposte nei confronti dei provvedimenti di blocco, sostituiti e pertanto non più efficaci. I giudizi relativi alle opposizioni avverso i provvedimenti di divieto sono in corso.

Si è definitivamente concluso il giudizio avente per oggetto l'opposizione proposta da un'associazione senza scopo di lucro nei confronti di una contestazione di violazione amministrativa elevata dal Garante in relazione all'omessa notifica, ai sensi dell'art. 37 del Codice, del trattamento dei dati sensibili relativi agli associati. Con sentenza

n. 25097 del 5 dicembre 2006 il Tribunale di Roma, nel confermare l'ordinanza di rigetto dell'istanza di sospensione dell'efficacia esecutiva della contestazione (ordinanza del 13 luglio 2006, *v. Relazione* 2006), ha dichiarato inammissibile il ricorso, in quanto il giudizio di opposizione disciplinato dagli artt. 22 e 23 della legge n. 689/81 va instaurato contro il provvedimento che applica la sanzione amministrativa e non avverso il verbale di accertamento della violazione, che non è di per sé lesivo di situazioni giuridiche soggettive e costituisce solo un atto di natura procedimentale.

Il Tribunale di Milano (sentenza n. 835 del 23 gennaio 2007) ha confermato il provvedimento del 18 maggio 2006 [doc. *web* n. 1299100] con il quale il Garante ha ritenuto legittime sia la segnalazione effettuata alla Centrale rischi della Banca d'Italia da una società di intermediazione finanziaria abilitata all'esercizio di attività di cartolarizzazione dei crediti, in quanto soggetta al potere di vigilanza della Banca e destinataria dell'obbligo di segnalazione, sia la cessione del credito ad altra società in virtù di informativa semplificata, ammessa in caso di cessione in blocco di crediti. Il Tribunale ha, altresì, rilevato che i dati oggetto delle segnalazioni alla Centrale rischi non possono ritenersi inclusi nell'ambito dei dati sensibili, come definiti dall'art. 4, comma 1, lett. *d*), del Codice.

È stata respinta (Tribunale di Milano, sentenza n. 1207 del 31 gennaio 2007) l'opposizione al provvedimento del 24 maggio 2006 [doc. *web* n. 1298784] con il quale il Garante ha dichiarato l'illiceità del trattamento dei dati personali effettuato da una società operante nel settore dell'arredamento in occasione del rilascio di carte di fidelizzazione della clientela. In particolare, il Tribunale ha confermato i rilievi mossi dall'Autorità in ordine all'inidoneità dell'informativa resa alla clientela e alla conseguente mancata acquisizione di un autonomo, libero e specifico consenso per lo svolgimento dei distinti trattamenti di *marketing* e di quelli connessi alla definizione dei profili individuali dei clienti. La decisione ha sottolineato la particolare pertinenza del richiamo, nel provvedimento del Garante impugnato, alle regole di correttezza e di buona fede che devono disciplinare la formulazione dell'informativa e che impongono il ricorso a modalità chiare e inequivoche.

È stato, infine, confermato dall'autorità giudiziaria (Tribunale di Milano, sentenza n. 13671 del 13 novembre 2007) anche il *provvedimento* del 5 ottobre 2006 [doc. *web* n. 1357375] con il quale l'Autorità ha ritenuto lecito il trattamento di dati personali di un dipendente, effettuato da un istituto di credito al fine di esercitare il proprio potere di controllo sul corretto svolgimento delle mansioni affidate. È stata in particolare confermata la legittimità dell'utilizzo da parte della banca, al fine di verificare la complessiva correttezza dell'operato del dipendente, anche di informazioni relative a rapporti personali da questi intrattenuti con l'istituto in qualità di correntista, alla luce del particolare ambito lavorativo considerato e dell'importanza e delicatezza del ruolo ricoperto nella banca dall'interessato.

18.5. *L'intervento del Garante nei giudizi relativi all'applicazione del Codice*

Conformemente agli indirizzi giurisprudenziali e al parere espresso dall'Avvocatura generale dello Stato –che si è pronunciata in termini favorevoli alla costituzione in giudizio del Garante, ritenendo essenziale che l'Autorità possa far valere le proprie ragioni, a tutela unicamente dell'interesse pubblico, tenendo conto delle sue specifiche e caratteristiche funzioni– il Garante ha limitato la propria attiva presenza, nei giudizi che non coinvolgono direttamente pronunce dell'Autorità, ai soli casi in cui sorge, o può sorgere, la necessità di difendere o comunque far valere particolari questioni di diritto.

In questo quadro, l'Autorità ha comunque seguito con attenzione tutti i contenziosi nei quali non ha ritenuto opportuno intervenire, chiedendo alle avvocature distrettuali dello Stato di essere informata sullo svolgimento delle vicende processuali e di riceverne comunicazione in merito agli esiti.

Per la novità e la rilevanza della questione, che investiva un aspetto generale concernente la corretta applicazione del Codice in ordine alle modalità di acquisizione in Internet e utilizzazione in giudizio di dati di traffico telematico, il Garante (*v. par.* 14.1), si è costituito presso il Tribunale di Roma nei sopra menzionati giudizi con i quali alcune società intendevano ottenere da taluni fornitori di servizi di comunicazione elettronica le generalità di soggetti ritenuti responsabili di avere scambiato file protetti dal diritto d'autore tramite reti *peer to peer*. Il Tribunale ha accolto quanto prospettato dal Garante.

19 L'attività ispettiva e le sanzioni

19.1. *La programmazione dell'attività ispettiva*

L'Autorità ha proseguito, anche nell'anno 2007, il processo di sviluppo dell'attività ispettiva, già avviato nell'anno 2006. L'attività di controllo è stata essenzialmente volta a:

- incrementare il numero delle verifiche;
- sviluppare nuove metodologie di controllo attraverso l'integrazione, nei *team* ispettivi, di competenze tecniche specialistiche per l'esecuzione di accessi ai sistemi informatici e alle banche dati elettroniche;
- sperimentare controlli per categorie omogenee di titolari del trattamento secondo una metodologia predefinita denominata "a progetto".

Sotto il primo profilo, nell'anno 2007 si è registrato un ulteriore importante incremento delle attività (+30% rispetto al 2006) in linea con la tendenza generale di aumento dell'attività di controllo, già evidenziata negli anni precedenti.

Anno	2002	2003	2004	2005	2006	2007
Ispezioni	40	69	100	230	350	452

Delle quattrocentocinquantadue attività ispettive effettuate, trecentosettanta riguardano l'attuazione di programmi ispettivi semestrali disposti dall'Autorità e ottantadue esigenze istruttorie connesse a reclami, segnalazioni e ricorsi presentati dai cittadini.

Grande importanza riveste l'attività di prevenzione effettuata attraverso accertamenti *cd.* "di iniziativa", avviati d'ufficio dall'Autorità (anche in assenza di specifici atti di impulso da parte dei cittadini quali segnalazioni, reclami o ricorsi), che ha costituito la parte più consistente dell'attività di controllo (oltre l'80%).

Il Collegio determina, con cadenza semestrale, le linee di indirizzo dell'attività ispettiva di iniziativa dell'Ufficio attraverso deliberazioni di programmazione che indicano gli ambiti del controllo e gli obiettivi numerici da conseguire per il semestre e, sulla base di tali indirizzi, l'Ufficio individua i titolari dei trattamenti da sottoporre a controllo. Le linee generali della programmazione dell'attività ispettiva vengono rese pubbliche.

Questa impostazione consente, attraverso verifiche nei confronti di più soggetti operanti nello stesso settore o che effettuano tipologie omogenee di trattamento, di acquisire importanti elementi di valutazione in ordine:

- al grado di adeguamento alla legge da parte degli operatori appartenenti a un determinato settore o che utilizzano i dati personali per particolari finalità;
- a fenomeni di ampia portata che possono costituire presupposto per l'adozione di provvedimenti generali (diretti, cioè, ad un insieme indeterminato di operatori);
- alla verifica dell'impatto dei provvedimenti adottati.

Ne deriva così una valorizzazione dell'attività di controllo come strumento di governo del sistema in un'ottica non solo repressiva, ma anche conoscitiva e di indirizzo.

Nell'anno 2007 il programma relativo al primo semestre (gennaio-giugno) ha previsto che l'attività ispettiva curata dall'Ufficio del Garante, anche per mezzo della Guardia di finanza, fosse indirizzata ad accertamenti su profili di interesse generale per categorie di interessati nell'ambito di:

- trattamenti di dati personali effettuati da *call center* per conto di operatori telefonici;
- trattamenti di dati personali effettuati da società farmaceutiche, in relazione alla somministrazione di farmaci e prestazioni sanitarie e alla sponsorizzazione di attività di cura o di ricerca, con particolare riguardo all'informativa agli interessati e al consenso eventualmente necessario;
- trattamenti di dati personali effettuati da compagnie telefoniche con riferimento ai *cd.* "dati di traffico".

Con riferimento, invece, al periodo luglio-dicembre 2007, l'attività ispettiva di iniziativa è stata finalizzata ad accertamenti nell'ambito di:

- soggetti pubblici che utilizzano i sistemi informativi della fiscalità mediante "anagrafe tributaria";
- istituti di credito, con riferimento alla gestione dei servizi di *e-banking*;
- trattamenti di dati personali effettuati da strutture sanitarie, in relazione alla somministrazione di farmaci e prestazioni sanitarie e alla sponsorizzazione di attività di cura o di ricerca.

Oltre ai temi di controllo sopra delineati, nei due semestri, sono state anche effettuate:

- verifiche sull'adozione delle misure minime di sicurezza da parte di soggetti, pubblici e privati, che effettuano trattamenti di dati sensibili;
- altre verifiche di iniziativa concernenti, in particolare, l'adempimento dell'obbligo di notificazione nei confronti di soggetti, pubblici e privati, individuati mediante raffronto con il registro generale dei trattamenti;
- verifiche sulla liceità e correttezza dei trattamenti di dati personali con particolare riferimento al rispetto dell'obbligo di informativa, alla pertinenza e non eccedenza nel trattamento, alla libertà e validità del consenso, nei casi in cui questo è necessario, nonché alla durata della conservazione dei dati nei confronti di soggetti, pubblici o privati, appartenenti a categorie omogenee. Ciò, prestando anche specifica attenzione a profili sostanziali del trattamento che spiegano significativi effetti sulle persone da esso interessate.

19.2. *La collaborazione con la Guardia di finanza*

Anche nel 2007 è risultato determinante, nel settore ispettivo, il rapporto con la Guardia di finanza che ha consentito all'Autorità di poter disporre di altre risorse qualificate per espletare l'attività di controllo prevista dalla legge.

Il Protocollo di intesa siglato nel 2005 consente al Garante di avvalersi del Corpo attraverso:

- la partecipazione di proprio personale agli accessi alle banche dati, ispezioni, verifiche e alle altre rilevazioni nei luoghi ove si svolge il trattamento;
- l'assistenza nei rapporti con l'autorità giudiziaria;
- lo sviluppo di attività ispettive delegate o sub-delegate per l'accertamento delle violazioni;
- la contestazione delle sanzioni amministrative rilevate nell'ambito delle attività delegate;
- l'esecuzione di indagini conoscitive sullo stato di attuazione della legge in

determinati settori;

- la segnalazione all'Autorità di situazioni rilevanti, ai fini dell'applicazione della legge, acquisite anche nell'esecuzione di altri compiti di istituto.

L'Autorià, quando ritiene necessario avvalersi della collaborazione del Corpo, attiva il Nucleo speciale funzione pubblica e *privacy* con sede a Roma che, disponendo di personale specializzato, provvede direttamente ad effettuare gli accertamenti, utilizzando anche, ove necessario, reparti del Corpo territorialmente competenti.

Le informazioni e i documenti acquisiti nell'ambito degli accertamenti vengono trasmessi all'Autorità per le successive verifiche in ordine alla liceità del trattamento e al rispetto dei princìpi previsti dalla legge. Quando nell'ambito dell'ispezione emergono violazioni penali o amministrative la Guardia di finanza procede direttamente alla segnalazione della notizia di reato all'autorità giudiziaria e alla contestazione della sanzione amministrativa.

Sono proseguite, anche nel 2007, le attività tese a realizzare un maggior coinvolgimento nell'attività di controllo della componente territoriale della Guardia di finanza (nuclei di polizia tributaria, compagnie e tenenze).

L'obiettivo è fruire di un dispositivo di controllo flessibile e articolato che consenta, in funzione della complessità degli accertamenti, di effettuarli direttamente a cura del dipartimento ispettivo dell'Ufficio, ovvero attraverso il Nucleo speciale, oppure, nel caso di accertamenti di non elevata complessità che concernono ad esempio la verifica di singoli adempimenti, delegando i reparti territoriali della Guardia di finanza.

In questo ambito è stata effettuata, in via sperimentale, una prima attività di controllo denominata "a progetto". Si tratta di un'attività complessa di carattere operativo che rientra nell'attuazione di linee strategiche definite di concerto con il Comando generale della Guardia di finanza e che comporta l'esecuzione di compiti correlati tra loro da parte di unità organizzative della componente speciale e di quella territoriale del Corpo, con obiettivi, tempi e assorbimento di risorse definiti.

Questa particolare tipologia di controllo è stata effettuata sulla base dell'elaborazione congiunta da parte dell'Ufficio e del Nucleo speciale di una guida per l'accertamento nell'ambito della quale sono stati definiti, in modo estremamente analitico, i passi che i *team* di ispettori avrebbero dovuto compiere successivamente e le liste dei controlli da eseguire *in loco.*

In esecuzione della prima di queste attività denominata "progetto *teleselling*" gli accertamenti sono stati indirizzati alla verifica del rispetto delle disposizioni previste dal Codice in relazione anche ai provvedimenti già adottati dall'Autorità nel settore dei *call center.* Sono stati sottoposti a controllo 76 *call center* operanti per le maggiori compagnie telefoniche (Telecom Italia S.p.A., Vodafone Omnitel NV, Wind telecomunicazioni S.p.A. e H3G S.p.A.) e gli esiti di tale attività sono tuttora all'esame dell'Autorità.

19.3. *I settori oggetto dei controlli e i casi più rilevanti*

Nel 2007 sono state effettuate, suddivise per settore, le seguenti attività ispettive:

- centodieci controlli nei confronti di operatori telefonici con riferimento ai trattamenti effettuati tramite *call center* ;
- quaranta controlli nei confronti di enti previdenziali, istituti sanitari (pubblici e privati) e imprese/società che trattano dati sensibili, con riferimento

all'adozione delle misure minime di sicurezza;
- quaranta controlli nei confronti di istituti di credito per verificare, in particolare, il rispetto dell'obbligo di informativa con riferimento all'impiego di sistemi di rilevazione biometria e di videosorveglianza;
- quaranta controlli nei confronti di società che effettuano trattamenti per i quali è prevista la notificazione al Garante;
- trenta controlli nei confronti di soggetti pubblici e privati che utilizzano sistemi di videosorveglianza, per verificare la liceità del trattamento e il rispetto del relativo provvedimento generale del Garante;
- venti controlli nei confronti di dentisti, per verificare le modalità di trattamento dei dati, anche sensibili, dei clienti;
- venti controlli nei confronti di oculisti, per verificare le modalità di trattamento dei dati, anche sensibili, dei clienti;
- venti controlli nei confronti di istituti di preparazione privatistica agli esami, per verificare le modalità del trattamento dei dati degli studenti;
- venti controlli nei confronti di alberghi con centri benessere, per verificare le modalità di trattamento dei dati, anche sensibili, dei clienti;
- venti controlli nei confronti di imprese di trasporti, per verificare la correttezza dei trattamenti dei dati dei clienti e il rispetto degli adempimenti relativi all'informativa;
- venti controlli nei confronti di società che si avvalgono del servizio garanzia degli assegni fornito da *Centax* S.p.A.;
- quindici controlli nei confronti di società che hanno effettuato ricerche di personale a mezzo di annunci pubblicati sul giornale, per verificare le modalità di trattamento dei *curricula* raccolti e l'assolvimento degli adempimenti di legge;
- dieci controlli nei confronti di agenzie matrimoniali, per verificare la correttezza dei trattamenti dei dati dei clienti e il rispetto degli adempimenti relativi all'informativa e al consenso;
- dieci controlli nei confronti di autoscuole, per verificare la correttezza dei trattamenti dei dati dei clienti e il rispetto degli adempimenti relativi all'informativa e al consenso;
- dieci controlli nei confronti di società che effettuano vendita di strumenti elettronici di rilevazione ambientale, per verificare la correttezza dei trattamenti dei dati dei clienti ed il rispetto degli adempimenti relativi all'informativa ed al consenso;
- dieci controlli nei confronti di notai, per verificare le modalità di trattamento dei dati, anche sensibili, dei clienti;
- cinque controlli nei confronti di società per verificare il trattamento dei dati personali nell'ambito di un sondaggio politico elettorale;
- quattro controlli nei confronti di società farmaceutiche, in relazione alla somministrazione di farmaci e prestazioni sanitarie e alla sponsorizzazione di attività di cura o di ricerca, con particolare riguardo all'informativa agli interessati e al consenso eventualmente necessario;
- quattro controlli nei confronti di soggetti pubblici che utilizzano i sistemi informativi della fiscalità mediante "anagrafe tributaria";
- tre controlli nei confronti di compagnie telefoniche con riferimento ai *cd.* "dati di traffico";
- un controllo nei confronti di un istituto di credito, con riferimento alla gestione dei servizi di *e-banking*.

In relazione a quanto emerso dagli accertamenti sono state effettuate circa novanta proposte di adozione di provvedimenti inibitori e/o di prescrizioni per conformare il trattamento alla legge a fronte delle quali l'Autorità ha adottato alcuni provvedimenti di particolare rilievo per le garanzie nei confronti dei cittadini.

In particolare si segnalano:

- il provvedimento nei confronti di un'agenzia di intermediazione immobiliare in relazione al trattamento dei dati idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, lo stato di salute e/o lo stato di disabilità, nonché la vita sessuale (*Provv.* 11 gennaio 2007 [doc. *web* n. 1381620]);
- il provvedimento nei confronti di un istituto di credito, in relazione alla consultazione di informazioni sulla solvibilità e affidabilità dei clienti (*Provv.* 8 marzo 2007 [doc. *web* n. 1390872]);
- il provvedimento nei confronti di una società, in relazione al servizio denominato "garanzia assegni" (*Provv.* 17 maggio 2007 [doc. *web* n. 1409251]);
- i provvedimenti nei confronti di gestori di compagnie telefoniche, in relazione all'attività di *call center* svolta anche attraverso società esterne (*Provvedimenti* 30 maggio 2007 [doc. *web* nn. 1412586, 1412557, 1412598, 1412610 e 1412626]);
- i provvedimenti nei confronti di diverse società, in relazione all'invio di comunicazioni commerciali mediante *telefax* (*Provv.* 28 giugno 2007 [doc. *web* n. 1433896]; *Provv.* 11 luglio 2007 [doc. *web* n. 1433939]; *Provv.* 4 ottobre 2007 [doc. *web* n. 1457973]; *Provv.* 31 gennaio 2008 [doc. *web* nn. 1489843 e 1488781]);
- il provvedimento nei confronti di un ente pubblico, in relazione al trattamento dei dati personali effettuato attraverso un sistema di videosorveglianza (*Provv.* 4 ottobre 2007 [doc. *web* n. 1457505]);
- i provvedimenti nei confronti di società operanti nel settore della grande distribuzione, in relazione al trattamento dei dati personali raccolti per il rilascio alla clientela di "carte di fedeltà" e utilizzati illecitamente anche a fini di *marketing* (*Provvedimenti* 15 novembre 2007 [doc. *web* nn. 1466898, 1466930, 1466971, 1466956 e 1466985]);
- il provvedimento generale nei confronti di gestori di compagnie telefoniche, in relazione alla sicurezza dei dati di traffico telefonici e telematici (*Provv.* 17 gennaio 2008 [doc. *web* n. 1482111]);
- i provvedimenti nei confronti di istituti di credito, in relazione al trattamento di dati biometrici (*Provvedimenti* 23 gennaio 2008 [doc. *web* nn. 1490382, 1490477 e 1490533]);
- il provvedimento nei confronti di una catena alberghiera, in relazione al trattamento dei dati personali dei clienti (*Provv.* 31 gennaio 2008 [doc. *web* n. 1490553]).

Riguardo all'attività ispettiva svolta dall'Ufficio nei confronti di gestori di compagnie telefoniche in relazione alla conservazione dei dati di traffico telefonico e telematico e di società farmaceutiche con riferimento alla sperimentazione dei farmaci, l'Autorità, attese le criticità emerse nell'ambito degli accertamenti e la rilevanza del pregiudizio per un'ampia platea di interessati, dopo aver definito alcune linee-guida, ha avviato una consultazione pubblica tesa a definire regole più precise e rigorose per tutti i soggetti che effettuano tali trattamenti di dati personali (*Provv.* 19 settembre 2007 [doc. *web* n. 1442463] e *Provv.* 29 novembre 2007 [doc. *web* n. 1468981]).

19.4. *L'attività sanzionatoria del Garante*

In conseguenza delle ispezioni effettuate, sono state inviate all'autorità giudiziaria quindici informative (di cui tredici a cura del Dipartimento attività ispettive e sanzioni dell'Ufficio e due da parte della Guardia di finanza) e avviati duecentoventotto procedimenti sanzionatori amministrativi (di cui centododici istruiti dal Dipartimento e centosedici della Guardia di finanza).

Per quanto riguarda le violazioni penali, esse hanno riguardato: mancata adozione delle misure minime di sicurezza (10), mancato adempimento di una deliberazione del Garante (2), trattamento illecito dei dati (2) e falsità nelle dichiarazioni e notificazioni al Garante (1).

Otto sono stati i procedimenti connessi al *cd.* "ravvedimento operoso" in materia di misure minime di sicurezza, previsto dall'art. 169, comma 2, del Codice.

Tale disposizione prevede infatti che, nel caso in cui venga rilevata una violazione di una o più delle misure minime di sicurezza specificatamente previste dal Disciplinare tecnico sulle misure minime di sicurezza (Allegato B al Codice) il Garante, a seguito di una prescrizione da impartire alla persona individuata come responsabile della predetta violazione, verificato il rispetto della prescrizione stessa, possa ammettere i destinatari della prescrizione al pagamento pari a un quarto del massimo della sanzione prevista. L'adempimento alla prescrizione e il pagamento della somma vengono comunicati all'autorità giudiziaria competente per le valutazioni in ordine all'estinzione del reato.

L'attività in questione ha riguardato quindici persone (in qualità di titolari/responsabili dei trattamenti), per un totale di sanzioni applicate pari a 185.329 euro.

Come evidenziano i dati di seguito riportati, anche per quanto attiene l'attività sanzionatoria, nell'anno 2007, si è registrato un notevole incremento.

Anno	2002	2003	2004	2005	2006	2007
Violazioni contestate	46	27	27	84	158	228

Le sanzioni amministrative contestate, per un totale compreso tra un minimo di 725.000 euro e un massimo di 4.355.000 euro, hanno riguardato:

- omessa o inidonea informativa (duecentosedici);
- omessa notificazione (sei);
- omessa risposta alle richieste del Garante (quattro)
- codice del consumo (due).

A fronte delle contestazioni notificate sono stati riscossi 814.625 euro a titolo di definizione in via breve.

L'incidenza delle violazioni penali e amministrative riscontrate è stata pari a circa il 51% sul totale delle ispezioni.

È risultata più sanzionata la violazione dell'obbligo di fornire all'interessato tutte le informazioni riguardanti il trattamento dei dati al fine di rendere lo stesso interessato pienamente consapevole dell'effettivo utilizzo dei dati personali che lo riguardano.

Occorre evidenziare che tale violazione assume particolare rilevanza nei casi in cui la legge impone al titolare del trattamento di acquisire anche il consenso dell'interessato per specifiche finalità (ad esempio, per l'utilizzo dei dati per finalità di *marketing*, o per la comunicazione di dati a terzi). In questi casi, l'omessa o inidonea informativa produce effetti anche sulla validità del consenso eventualmente acquisito che, sulla

base di quanto previsto dall'art. 23, comma 3 del Codice, può ritenersi valido solo se sono state fornite all'interessato le informazioni di cui all'art. 13 del Codice.

Nel numero delle contestazioni effettuate per l'omessa o inidonea informativa, si segnala che circa il 35% sono da riferirsi a segnalazioni relative a trattamenti effettuati, attraverso *call center*, da compagnie telefoniche in relazione all'attivazione di servizi non richiesti; ciò, a riprova dello straordinario sforzo compiuto nel 2007 dall'Autorità per contrastare tale fenomeno.

20 Le relazioni internazionali

Conferenze tra autorità di protezione dei dati a livello europeo

La Conferenza annuale delle autorità europee di protezione dati che si è tenuta nel 2008 a Roma il 17 ed il 18 aprile, con la partecipazione di 38 delegazioni di oltre 30 Paesi europei, si è articolata in sei sessioni; le prime tre, relative a sicurezza, imprese e nuove tecnologie, sono state introdotte da un contributo video affidato rispettivamente a una personalità del mondo delle istituzioni, del diritto e della ricerca. Gli interventi miravano a stimolare la discussione su alcune questioni di fondo: come garantire la *privacy* in un contesto globalizzato, caratterizzato da un crescente impiego di nuove tecnologie e alle prese con seri problemi di sicurezza; quali siano le prospettive per una efficace protezione dei dati personali riguardo ai flussi transfrontalieri di dati e all'uso di informazioni commerciali a fini di perseguimento dei reati; come addivenire a regole globali per governare lo sviluppo della rete; come si configurano gli scenari presenti e futuri per l'attività delle autorità di protezione dei dati personali.

La seconda giornata è stata invece dedicata alle tematiche legate alla collaborazione giudiziaria e di polizia e all'attività del Gruppo delle autorità europee su Polizia e Giustizia (*Working Party on Police e Justice, v. infra*), presieduto da Francesco Pizzetti, nonché alle relazioni di alcuni gruppi di lavoro (*Case Handling Workshop*, Gruppo di Berlino sulla protezione dei dati nel settore delle telecomunicazioni) che riferiscono tradizionalmente alla Conferenza.

In conclusione è stata adottata una dichiarazione sulle misure di controllo delle frontiere e della circolazione di tutti i viaggiatori, in arrivo o in partenza dall'Europa, per invitare con forza tutte le istituzioni interessate a valutare l'effettiva necessità di adottare tali misure e a individuare criteri di controllo proporzionati rispetto agli obiettivi da raggiungere (*v.* anche *par.* 20.2.). Con tale dichiarazione è stato sottolineato, inoltre, che l'esigenza di controlli efficaci per garantire le frontiere deve essere conforme all'idea di un'Europa "aperta al mondo", uno degli obiettivi perseguiti in questi anni dall'Unione europea. La dichiarazione è stata inviata a tutte le istituzioni europee (Parlamento, Consiglio, Commissione).

Nel 2007 la Conferenza di Primavera è stata ospitata dal *Data Protection Commissioner* di Cipro (10-11 maggio 2007). Le oltre trenta delegazioni presenti hanno approvato tre documenti rivolti a tutte le istituzioni europee, per sottolineare la necessità sia di tutelare i diritti fondamentali dei cittadini europei nell'ambito della cooperazione giudiziaria e nelle attività di polizia, sia di rispondere con maggiore rapidità e incisività ai rischi derivanti dalla sempre più massiccia raccolta di dati personali a fini di sicurezza. Le autorità hanno convenuto sull'esigenza di un approccio uniforme europeo per garantire il rispetto dei princìpi fondamentali della protezione dei dati, attraverso strumenti utili e efficaci e una riflessione ampia e condivisa che coinvolga più direttamente i Parlamenti nazionali e le opinioni pubbliche degli Stati europei.

Sono state approvate una decisione e due dichiarazioni, queste ultime, rispettivamente, sulla proposta di decisione quadro del Consiglio Ue sulla protezione dei dati personali trattati nell'ambito del *cd.* "Terzo pilastro" (cooperazione giudiziaria e di polizia) e sul principio di disponibilità sancito dal "Programma de L'Aja" (ossia sull'obbligo per gli Stati membri di rendere reciprocamente disponibili i dati raccolti a livello nazionale per finalità di giustizia e polizia).

Nella prima dichiarazione, i Garanti ribadiscono che la decisione quadro del Consiglio Ue, limitando la protezione ai soli dati oggetto di scambio fra gli Stati (nell'ottica della "disponibilità" suddetta), e non estendendola anche ai trattamenti effettuati a livello nazionale, rischia di introdurre "due velocità" nell'ambito del *cd.* "Terzo pilastro". Viceversa, occorre garantire uniformità di tutela a livello nazionale e sopranazionale nel trattamento dei dati raccolti per finalità di giustizia e polizia.

La seconda dichiarazione contiene indicazioni utili a valutare se, e in quale misura, strumenti normativi proposti (a livello europeo o nazionale) per facilitare lo scambio di dati siano compatibili con i princìpi di protezione dei dati. L'obiettivo è potenziare le libertà civili ampliando, al tempo stesso, le possibilità di utilizzo di informazioni da parte di forze dell'ordine e autorità giudiziarie.

Con la decisione è stato conferito al menzionato Gruppo di lavoro per le questioni di Terzo pilastro un mandato più ampio, per una risposta rapida ed efficace ai rischi derivanti dal crescente uso di banche dati a fini di sicurezza. La Conferenza ha riconosciuto che tale obiettivo potrà essere meglio raggiunto attraverso un'articolazione permanente e strutturata del *Working Party*. Il Presidente dell'Autorità italiana è stato nominato Presidente del gruppo, ridenominato *"Working Party on Police and Justice"*.

Conferenze delle autorità su scala internazionale

La 29ma Conferenza mondiale delle autorità garanti svoltasi a Montreal dal 25 al 28 settembre 2007 ha affrontato temi relativi alle nuove frontiere della protezione dei dati personali, come evidenziato dal titolo *"Terra Incognita - Gli orizzonti della protezione dei dati"*.

Il programma, particolarmente denso, ha riguardato tra l'altro la sicurezza e la globalizzazione, i rischi e le potenzialità della rete, le nuove tecnologie e il tracciamento delle persone, i dati genetici e le bio-banche.

Sono state adottate tre importanti risoluzioni.

La prima sottolinea l'urgenza di pervenire a criteri globalmente condivisi per tutelare i dati dei passeggeri, oggetto di pressioni sempre più forti da parte dei Governi di molti Paesi del mondo.

I Garanti hanno chiesto collaborazione a soggetti pubblici e privati, organizzazioni non governative e autorità di protezione dati, per garantire alcuni princìpi basilari nella raccolta e nell'utilizzazione di questi dati, sottolineando la necessità di conciliare le esigenze connesse alla lotta al terrorismo con la tutela dei diritti dei cittadini e delle imprese coinvolte. I princìpi riguardano la trasparenza nelle finalità della raccolta dei dati; la loro utilizzazione quando siano realmente indispensabili; il rispetto di criteri di proporzionalità nella raccolta; i limiti al numero dei soggetti ai quali possono essere comunicati; l'accuratezza delle informazioni; le garanzie per i cittadini che intendano esercitare diritti di accesso o rettifica dei dati stessi, a cominciare da un'adeguata informativa sulle caratteristiche del trattamento.

La seconda risoluzione riguarda la definizione di *standard* universali in materia di *privacy* in collaborazione con l'Iso (*International Organization for Standardization*). Essa evidenzia che il tentativo di tradurre i princìpi di protezione dati in regole tecnologicamente efficaci merita sostegno, benché in ambito Iso trovino appoggio soprattutto le tematiche della sicurezza dei sistemi informativi. La conferenza ha invitato tutte le autorità di protezione dati a partecipare attivamente al processo di definizione di tali *standard*, anche attraverso un migliore coordinamento delle iniziative nazionali e il coinvolgimento diffuso del mondo scientifico e della ricerca.

La terza risoluzione è stata dedicata all'esigenza di potenziare la cooperazione con gli organismi (quali l'Ocse, il Consiglio d'Europa, l'Apec) che, in maniera diversa, stanno sviluppando strumenti a sostegno della protezione dei dati e della *privacy*, nel

solco delle indicazioni fornite dalla Conferenza internazionale delle autorità tenutasi nel 2006 a Londra (*cfr. Relazione* 2006, *p.* 150).

Il presidente dell'autorità italiana ha presieduto una sessione plenaria specificamente dedicata alla protezione dei minori su Internet; nel suo intervento, ha espresso preoccupazione per la scarsa attenzione dimostrata dai giovani alla protezione della loro *privacy* nel contesto tecnologico in cui si muovono. In particolare, ha evidenziato che la comunicazione elettronica e le tecnologie dell'informazione tendono a trasformare ogni relazione interpersonale in un flusso di dati e che, pertanto, la tutela dei dati personali su Internet significa innanzitutto proteggere i rapporti tra gli individui e la loro stessa libertà. Nella società "smaterializzata" i giovani sono più esposti al rischio di manipolazioni della loro sfera privata. La diffusione di immagini su Internet, le fotografie scattate senza consapevolezza o i video girati per uso personale possono finire sulla rete generando pregiudizievoli conseguenze sui bambini. Allo stesso modo, l'utilizzo delle *chat* e lo scambio di *e-mail* senza l'adeguata consapevolezza dei rischi possono esporre i più giovani a situazioni pericolose.

20.1. *La cooperazione tra autorità garanti nell'Ue: il Gruppo art. 29*

Il Gruppo art. 29 (che riunisce i rappresentanti delle autorità per la protezione dei dati europee, ed è stato istituito ai sensi dell'art. 29 della direttiva 95/46/Ce) per rendere più effettiva la sua funzione di consulenza "indipendente" verso le istituzioni comunitarie, e *in primis* verso la Commissione, ha stabilito di definire un programma biennale di attività e di rivedere le modalità con cui promuovere la trasparenza sulle attività svolte. Il Programma di lavoro del Gruppo per gli anni 2008-2009 (WP 146) è piuttosto ambizioso e intende concentrare le attività, fatte salve le richieste di parere su iniziative legislative della Commissione, su quattro temi strategici. Il primo, relativo al miglioramento dell'applicazione della direttiva 95/46/Ce, prevede interventi volti a chiarire l'interpretazione di alcuni aspetti chiave: oltre al lavoro già svolto in relazione alla nozione di dato personale, il Gruppo intende chiarire i concetti di responsabile e di incaricato del trattamento, il diritto applicabile, la limitazione delle finalità ed i presupposti per il trattamento. Il secondo è rivolto alla necessità di garantire la protezione dei dati nei trasferimenti internazionali, in particolare in relazione all'uso di strumenti quali le *binding corporate rule* e del *Safe Harbor*; il terzo mira a garantire la protezione dei dati in relazione alle nuove tecnologie (oltre al parere adottato sui motori di ricerca, il Gruppo si occuperà di reti sociali *on-line*, di profilazione, di radiodiffusione digitale, l'uso della biometria e dell'*Rfid*). Il quarto tema, più interno, riguarda il miglioramento dell'efficacia del lavoro del Gruppo e prevede diverse azioni, alcune delle quali esposte in un recente documento sulla trasparenza (WP 135). Il programma di lavoro tiene anche conto delle ulteriori sfide cui occorre prepararsi, in particolare dell'impatto del trattato di Lisbona.

Il concetto di dato personale (WP 136)

I Garanti europei, per chiarire meglio la nozione di "dato personale", hanno approvato il parere4/2007 [doc. *web* n. 1496512], fornendo alcune indicazioni sull'applicazione della direttiva 95/46/Ce ai trattamenti effettuati con le nuove tecnologie (quali l'*Rfid*) o in contesti altamente tecnologici (*e-Government*, cartelle cliniche elettroniche, *ecc.*).

La definizione di dato personale contenuta nella direttiva (*"qualsiasi informazione concernente una persona fisica identificata o identificabile"*) è stata analizzata con esempi tratti dai casi affrontati dalle diverse autorità di protezione dei dati. Dall'analisi è emersa, anzitutto, l'ampiezza del concetto di dato personale (*"qualsiasi informazione"*),

in linea con la giurisprudenza della Corte europea dei diritti umani e della Corte europea di giustizia nei casi concernenti possibili violazioni del diritto alla vita privata. La riflessione ha consentito di proporre un'interpretazione equilibrata in base alla quale, ad esempio, rientrano nella definizione di dato personale sia le istruzioni impartite dal cliente alla propria banca e registrate, sia le immagini filmate da un impianto di videosorveglianza, nella misura in cui i singoli individui siano riconoscibili. Un dato biometrico (l'impronta digitale) è un dato personale perché identifica una persona, ma i campioni di tessuto dai quali si estraggono i dati biometrici non sono di per sé dati personali (anche se le operazioni effettuate per estrarre tali informazioni biometriche configurano un trattamento di dati personali). Un'informazione, inoltre, può "riguardare" una persona fisica identificata o identificabile sotto vari aspetti: perché oggetto dell'informazione è chiaramente una persona fisica, oppure la finalità del dato raccolto è, alla luce delle circostanze specifiche, quella di "incidere" in qualche modo su una persona specifica; oppure, perché l'informazione, se trattata, è suscettibile di effetti sui diritti e gli interessi di una determinata persona.

L'"identificabilità", secondo la direttiva, può essere "diretta" o, valutando tutte le circostanze del caso specifico, "indiretta": notizie di stampa su un vecchio procedimento penale di grande risonanza possono costituire un dato personale poiché è possibile ricostruire l'identità di una persona consultando vecchi numeri del giornale; informazioni apparentemente frammentarie e prive di riferimenti diretti all'identità di una persona (il nome) costituiscono dato personale se il titolare intende utilizzarle per identificare una determinata persona e possiede presumibilmente i mezzi per ricostruire tale identità (si pensi alla videosorveglianza diretta a favorire l'eventuale identificazione di determinati soggetti, o agli indirizzi Ip raccolti per individuare presunte violazioni del *copyright*).

Infine, la direttiva si riferisce a informazioni concernenti una *"persona fisica"*, ma, almeno in determinate circostanze, può essere rilevante anche il trattamento di dati relativi a defunti in quanto la legge nazionale lo ammette, oppure perché onore e immagine sono tutelati anche dopo la morte della persona. Della stessa tutela possono godere anche le persone giuridiche come ha chiarito la Corte europea di giustizia, in base alla quale *"nulla impedisce che uno Stato membro estenda la portata della normativa nazionale di attuazione della direttiva 95/46/Ce a settori non compresi nell'ambito di applicazione di quest'ultima, purché non vi osti alcun altra disposizione del diritto comunitario"* (Corte di giustizia delle Comunità europee, 6 novembre 2003, C-101/01).

Indagine sulle società assicurative

Nel 2007 il Gruppo art. 29 ha realizzato per la prima volta una verifica congiunta, sull'osservanza nei Paesi dell'Unione europea dei princìpi di protezione dati da parte delle società che offrono polizze di assistenza sanitaria integrativa. L'analisi ha preso le mosse da un questionario distribuito in tutti gli Stati membri alle compagnie di assicurazione più rappresentative in termini di quote di mercato. Dall'indagine (WP 137, rapporto n. 1/2007) è emerso il sostanziale rispetto delle norme in materia, soprattutto per quanto concerne l'informativa agli assicurati e la raccolta del necessario consenso. Tuttavia, sono state evidenziate carenze in alcuni ambiti, in particolare relativamente alla circolazione delle informazioni con riguardo ai terzi, eventuali beneficiari delle polizze assicurative e all'adozione di adeguate misure organizzative per garantire l'accuratezza, l'aggiornamento e la correzione dei dati personali.

Parere sul nuovo accordo Pnr con gli Stati Uniti d'America

Il Gruppo articolo 29 ha pubblicato il 17 agosto 2007 un parere molto critico sul nuovo accordo stipulato fra l'Ue e l'Amministrazione statunitense in materia di dati relativi ai passeggeri (*Passenger Name Record*, Pnr) (parere 5/2007, WP 138). L'accordo, che apparentemente riduce da 34 a 19 le categorie di dati oggetto di tra-

sferimento, in realtà accorpa alcuni dati in categorie più ampie; in base ad esso, inoltre, continueranno a essere trasferiti i dati sensibili, e il loro "filtraggio" sarà effettuato ancora dalle autorità americane (in particolare, il *Department for Homeland Security, Dhs*), punto sul quale il WP 29 si era dichiarato più volte contrario; il periodo di conservazione dei dati trasferiti è aumentato da 3 anni e mezzo a 7 anni e i dati possono restare accessibili (in casi specifici) per ulteriori 8 anni (l'accordo utilizza l'espressione *"in stato di sonno"* per indicare tali dati). È previsto l'"impegno" delle autorità Usa a mettere in atto il sistema *cd. "push"* (invio dei dati da parte delle compagnie aeree) anziché *"pull"* (accesso diretto ai *database* delle compagnie aeree da parte delle autorità Usa), ma a una serie di condizioni che necessitano di ulteriori precisazioni.

In tale materia, il sottogruppo che nell'ambito delle attività del Gruppo art. 29 si occupa di Pnr ha anche predisposto una bozza di risoluzione (*Resolution on the urgent need for global standards for safeguarding passenger data to be used by governments for law enforcement and border security purposes*) approvata dalla *World Conference* di Montreal (*cfr. supra, par.* 20).

Pareri sul Sistema di cooperazione per la tutela dei consumatori e sul Sistema di informazione del mercato interno (Imi)

I pareri del Gruppo art. 29 n. 6/2007 (WP 139) e n. 7/2007 (WP 140) sono stati richiesti dalla Commissione europea su due proposte presentate per la creazione, rispettivamente, di una base di dati per lo scambio di informazioni tra le autorità nazionali responsabili dell'applicazione delle disposizioni in materia di tutela dei consumatori e la Commissione stessa (Cpcs-*Consumer Protection Cooperation System*), e di un *database* centralizzato per lo scambio di informazioni relative alle professioni regolamentate (Imi-*Internal Market Information System*). Quanto al Cpcs, il Gruppo ha condiviso sostanzialmente le osservazioni critiche del Garante europeo della protezione dei dati, soprattutto sulla necessità di assicurare il rispetto dei princìpi di finalità (nell'utilizzo dei dati contenuti nella costituenda banca dati, che deve servire esclusivamente alla tutela dei consumatori), pertinenza e non eccedenza dei dati, nonché sull'eccessiva durata del periodo di conservazione previsto per le informazioni contenute in tale *database* (5 anni). Per l'Imi il Gruppo ha invece segnalato l'opportunità di una decisione specifica della Commissione a corredo delle direttive che prevedono la costituzione del sistema, anche ai fini della creazione di una base giuridica solida che ne renda legittimo l'utilizzo.

Livello di protezione dati a Jersey e nelle Isole Fær Øer

Il parere di adeguatezza del Gruppo art. 29 è necessario affinché la Commissione europea possa adottare una decisione formale ai sensi della direttiva 95/46/Ce sul trasferimento di dati personali in un Paese terzo senza alcuna limitazione. Con riguardo all'Isola di Jersey e al territorio delle Isole Fær Øer (pareri 8 e 9 del 2007, WP 141-142) le autorità europee si sono pronunciate favorevolmente, pur evidenziando alcune ambiguità nella legislazione emanata nel Bailato di Jersey, soprattutto con riguardo ai poteri dell'autorità di controllo.

Ottava direttiva concernente gli *"Statutory Audit"*

Con il parere 10/2007 (WP 143) il Gruppo si è occupato della comunicazione di dati relativi alle attività di *audit* finanziario e contabile fra le autorità pubbliche europee competenti in materia (in Italia la Consob) e quelle di Paesi terzi. Il parere verte, in particolare, sull'art. 47 della direttiva 2006/43/Ce, ossia sulla trasmissibilità –da parte delle autorità pubbliche competenti per la vigilanza sui controlli contabili nei Paesi Ue alle omologhe autorità dei Paesi terzi– dei dati personali inseriti nella documentazione da fornire (nominativi dei revisori, nominativi di altri soggetti interessati, eventualmente dipendenti dell'azienda, *ecc.*). La direttiva prevede due scenari, cosiddetti di "breve periodo" (trasmissione dei dati in caso di indagini specifiche su casi di presunte irregolarità) e di "medio periodo" (invio dei dati alle autorità pubbliche competenti nel Paese terzo in riferimento ai controlli contabili *standard*). In base al parere il trasferimento può essere giustificato, nel primo caso,

attraverso la deroga al divieto di trasferimento di dati verso Paesi terzi basata sull'art. 26, comma 1, lett. *d*), della direttiva 95/46/Ce (sussistenza di un interesse pubblico rilevante quale giustificazione del trasferimento). Tuttavia, tale disposizione, come già ricordato dal Gruppo nel documento del 25 novembre 2005 relativo all'interpretazione dell'art. 26(1) della direttiva 95/46/Ce (WP114), deve essere applicata e interpretata dagli Stati membri in modo restrittivo anche con riguardo alla necessità dei dati dei quali si chiede o si prevede il trasferimento. Per quanto concerne la situazione di "medio periodo", occorre garantire che negli accordi di reciprocità previsti fra le autorità competenti Ue e quelle di Paesi terzi siano soddisfatte tutte le condizioni di adeguatezza indicate nell'articolo 47(3) della direttiva 2006/43/Ce. Infine, il "regime speciale" di cui all'articolo 47(4) (trasferimento diretto da parte dei revisori contabili stabiliti in un Paese Ue alle autorità competenti del Paese terzo), per il suo carattere eccezionale e derogatorio rispetto alla norma generale, deve essere meglio definito dalla Commissione con il necessario ausilio del Gruppo art. 29.

Proposta di decisione-quadro sull'uso dei dati Pnr nelle attività di contrasto del terrorismo

Il Gruppo art. 29 e il *Working Party on Police and Justice* (*cfr. par.* 20.2) hanno adottato un parere congiunto per richiamare l'attenzione del Consiglio Ue e della Commissione sugli aspetti ritenuti contrari ai princìpi fondamentali in materia di tutela dei dati personali nella proposta di decisione-quadro del Consiglio che istituirebbe il cosiddetto "Pnr europeo", presentata dalla Commissione il 6 novembre 2007 (WP 145/WPPJ 01/07).

Attraverso tale decisione verrebbe introdotto in Europa l'obbligo di comunicare alle "autorità competenti" i dati dei passeggeri aerei diretti verso i Paesi dell'Ue, come già avviene per gli Usa.

I Garanti ritengono che la proposta comporti una grave compressione dei diritti fondamentali dei cittadini europei, che non risulta pienamente giustificata né assolutamente indispensabile "in una società democratica", come già esposto nei numerosi pareri concernenti il trasferimento dei dati Pnr negli Usa (*v. Relazione* 2006, *p.* 159).

In questo caso, non sono dimostrate né la necessità, né la proporzionalità del trattamento previsto nel progetto di decisione-quadro. Soprattutto, non ha trovato ancora piena attuazione in tutti gli Stati membri la direttiva 2004/82/Ce che prevede l'obbligo per i vettori aerei europei di raccogliere e rendere disponibile, a richiesta, i dati Api (*Advance Passenger Information*), che corrispondono in sostanza alle informazioni personali utilizzate per il *check-in*. Appare quindi quanto meno eccessivo introdurre un obbligo ulteriore per finalità di sicurezza quando non si è ancora verificata l'efficacia del sistema istituito per vigilare sulle frontiere europee.

Numerosi altri aspetti della proposta sono stati giudicati problematici: le categorie di informazione oggetto di trasferimento risultano addirittura più numerose di quelle previste nell'Accordo sul Pnr-Usa; il periodo di conservazione dei dati da parte delle autorità competenti è eccessivo (tredici anni); non vi è chiarezza sulla necessità di prevedere esclusivamente un sistema del tipo *"push"*, e non *"pull"* (*v. supra*), come già indicato nei pareri sul Pnr-Usa; l'eliminazione dei dati sensibili eventualmente raccolti (il cui trattamento è riservato solo ad alcuni specifici soggetti) deve essere effettuata dai singoli vettori aerei, e non dalle autorità riceventi; troppo ampia risulta infine la discrezionalità degli Stati membri nell'attuare la decisione, soprattutto per quanto riguarda l'ambito di circolazione delle informazioni fornite dai vettori aerei.

Le autorità europee per la *privacy* hanno quindi chiesto un serio dibattito sul tema, con tutte le parti in causa.

Protezione dei dati personali dei minori

Il Gruppo art. 29 si è pronunciato sul tema della protezione dei dati relativi ai minori con il documento di lavoro del 18 febbraio 2008 (WP 147). Il documento, suddiviso in due sezioni principali, individua nella prima parte i princìpi fondamen-

tali sulla protezione del minore, anche con riferimento alla tutela dei dati; nella seconda, fornisce indicazioni per l'attuazione dei princìpi di data *protection* nel settore scolastico. I destinatari principali sono coloro che a vario titolo trattano i dati relativi ai minori, in particolare insegnanti e autorità scolastiche.

Dopo aver richiamato i princìpi fondamentali sulla protezione del minore previsti dalle convenzioni internazionali in materia, viene prestata particolare attenzione al principio dell'interesse primario del minore (*cd. "best interest of the child"*), elemento fondamentale per la risoluzione di eventuali conflitti, anche tra i minori e i loro rappresentanti. Ampio spazio è inoltre dedicato ai princìpi di qualità dei dati (correttezza, proporzionalità, sicurezza) e al principio di rappresentanza (da parte dei genitori o di chi abbia titolo), nonché alla necessità di accrescere la consapevolezza del minore con un'adeguata informativa e di coinvolgerlo nelle scelte che lo riguardano, in base al suo grado di maturità.

Nella parte generale viene anche menzionato il diritto all'oblìo, particolarmente significativo perché le informazioni relative al minore possono rapidamente divenire obsolete ed eccedenti rispetto all'originario scopo della raccolta.

Il documento affronta inoltre il tema dell'esercizio dei diritti del minore, normalmente esercitati dai rappresentanti del minore, ma che possono essere esercitati dal minore stesso a seconda della sua maturità.

La seconda parte del documento riguarda il contesto scolastico e affronta temi quali il trattamento dei dati nei *curricula* e l'impiego delle nuove tecnologie, con particolare riguardo alla videosorveglianza, all'accesso ai locali della scuola attraverso dispositivi biometrici, ai siti *web* scolastici e all'uso di videofonini in aula; sottolinea inoltre il ruolo delle scuole nella sensibilizzazione dei minori sui rischi derivanti dal trattamento dei dati che li riguardano e sull'esercizio dei loro diritti.

Si richiamano altresì i compiti delle autorità per la protezione dei dati nel promuovere la consapevolezza anche dei *policy maker* sull'importanza della protezione dei dati relativi ai minori e nel rendere i titolari del trattamento consapevoli dei loro obblighi.

Nella parte conclusiva viene segnalata l'opportunità di accordi tra le autorità per la protezione dei dati, i Ministri dell'istruzione e altre autorità competenti per rafforzare la protezione dei dati nell'ambito dei diritti fondamentali.

Protezione dei dati e attività dei motori di ricerca

Con il parere del 4 aprile 2008 (WP148) il Gruppo art. 29 ha svolto un'analisi delle principali questioni di protezione dei dati con specifico riferimento ai motori di ricerca che operano sulla rete. Il documento definisce l'insieme delle responsabilità in capo ai motori di ricerca, i quali effettuano la raccolta di dati personali in quanto fornitori di servizi (ove a*d es.*, raccolgano indirizzi Ip degli utenti, informazioni necessarie per accedere a servizi personalizzati attraverso *userID* e *password, ecc.*), o di contenuti (qualora memorizzino, attraverso la *cd.* "copia *cache*", i risultati di ricerche su Internet contenenti informazioni personali, ovvero forniscano profili personali o comunque informazioni organizzate relative ad un determinato soggetto).

Il parere valuta le legittime esigenze (di natura commerciale) dei motori di ricerca alla luce della necessità di garantire la tutela dei dati personali. Le autorità europee ribadiscono che la direttiva 95/46/Ce si applica pienamente anche ai trattamenti di dati personali effettuati da motori di ricerca situati al di fuori del territorio Ue e dello Spazio economico europeo, alla luce delle disposizioni contenute nell'articolo 4(1), lettera *c*), della direttiva stessa, nella misura in cui essi utilizzino per il trattamento dispositivi situati sul territorio degli Stati membri (*ad es.*, i *cookie*). Per contro, è da escludere l'applicabilità ai motori di ricerca sia della direttiva 2002/58/Ce (*cd.* "direttiva *e-Privacy*"), sia della direttiva 2006/24/Ce (*cd.* "direttiva *data retention*"). Entrambe, infatti, non riguardano i *"servizi della*

società dell'informazione" quali i motori di ricerca, esclusi espressamente dall'ambito di applicazione della direttiva *e-Privacy* (e, quindi, della direttiva sulla *"data retention"*) dall'articolo 2, lettera *c*), della direttiva-quadro sui servizi di comunicazione elettronica (2002/21/Ce).

Il parere sottolinea inoltre che i motori di ricerca sono tenuti a valutare attentamente la natura delle operazioni o dei servizi che essi gestiscono, in particolare per la conservazione dei dati personali raccolti, che devono essere distrutti o resi anonimi (con procedure realmente efficaci) se non necessari agli scopi del trattamento. I Garanti ribadiscono inoltre la necessità che i motori di ricerca incorporino i requisiti fondamentali in materia di protezione dati nei propri meccanismi operativi (*cd. "privacy by design"*). A tale scopo, viene formulata una serie di indicazioni e raccomandazioni: fornire un'adeguata informativa agli utenti (specificando il soggetto titolare del trattamento, la natura dei dati raccolti, gli scopi del trattamento); ottenere il consenso degli utenti per l'attività di profilazione o comunque per raffronti con altre informazioni in possesso del motore di ricerca stesso; effettuare la cancellazione (o l'anonimizzazione) dei dati non più necessari per le specifiche finalità per le quali sono stati raccolti. Il Gruppo sottolinea infine che spetta ai motori di ricerca giustificare la conservazione prolungata (in linea di principio, non superiore a 6 mesi) dei dati personali eventualmente in loro possesso. In tal senso, deve essere garantito il diritto all'oblìo delle persone i cui dati siano memorizzati nella *cd.* copia *"cache"*, evitando che permangano in rete informazioni superate e con ciò garantendo agli interessati l'esercizio effettivo dei diritti di accesso, rettifica e cancellazione previsti dalla direttiva 95/46/Ce.

Il Gruppo, in sintonia con quanto fatto dal Garante europeo, ha posto all'ordine del giorno un parere sulla proposta presentata dalla Commissione nel novembre 2007 di modifica del quadro normativo in materia di comunicazioni elettroniche, che include anche limitate proposte di modifica alla direttiva 2002/58/Ce. Nella proposta l'impianto generale della direttiva resta sostanzialmente immutato, mentre si precisano alcuni obblighi in materia di sicurezza.

20.2. *La cooperazione delle autorità di protezione dei dati nel settore libertà, giustizia e affari interni*

Nel 2007 si è cercato di ricostituire e rendere più efficace l'attività di cooperazione tra le autorità europee di protezione dei dati personali. La Conferenza di primavera delle Autorità ha deliberato infatti più incisive competenze e un nuovo nome per il *Working Party on Police and Justice* ed ha chiamato a presiederlo il Presidente del Garante. La nuova composizione e articolazione del *Working Party* e la maggior autonomia consentiranno di intervenire in modo più tempestivo e mirato, per far conoscere le valutazioni delle autorità di protezione dei dati sulle misure comunitarie suscettibili di avere un impatto sulla protezione dei dati personali.

In tal modo (*v. par.* 20.1), pur in assenza di un quadro normativo adeguato, le autorità di protezione dei dati hanno trovato la possibilità di sviluppare azioni congiunte con il Gruppo dei Garanti europei su temi che, a livello europeo, sono trattati separatamente, quali la conservazione e utilizzo a fini di polizia dei dati raccolti da privati (vettori aerei, gestori e fornitori di servizi di comunicazione elettronica e di sistemi di pagamento, *ecc.*) per fornire servizi commerciali, o i controlli alle frontiere e le politiche di ingresso e soggiorno. Il WPPJ mantiene tuttavia il suo carattere volontario e ufficioso; ciò, se da un lato non rende obbligatorio per il legislatore europeo richiedere il parere del gruppo sulle iniziative legislative, facilita, dall'altro,

la visibilità delle autorità di protezione dei dati a livello europeo in un settore in cui non esiste ancora –anche per la distinzione in pilastri delle competenze ora prevista dal Trattato– un quadro comune e condiviso di princìpi che regoli le condizioni di liceità del trattamento dei dati personali.

A tal proposito occorre peraltro ricordare che l'approvazione del Trattato di Lisbona, abolendo tendenzialmente l'attuale articolazione in pilastri, favorisce in prospettiva una disciplina il più possibile unitaria della protezione dei dati personali, anche rendendo cogente il contenuto dell'articolo 8 della Carta dei diritti fondamentali.

Nonostante l'avvicinarsi di tale scadenza, il legislatore comunitario ha continuato a presentare proposte e a sollecitare l'adozione di quelle *in itinere.* Si deve peraltro registrare un certo ritardo per l'entrata in vigore di importanti sistemi informativi, quali il sistema informativo visti e la seconda generazione del Sis (Sis II). Il Trattato di Prüm, trasformato in iniziativa legislativa dell'Unione europea, ha ricevuto un generale accordo, che tuttavia subisce anch'esso rallentamenti nella definizione degli aspetti applicativi dello scambio dei dati.

Parte del "ritardo" è dovuta alla mancata adozione di princìpi per il trattamento dei dati personali nel Terzo pilastro, elemento richiamato dal programma dell'Aja come necessario quadro di riferimento per la cooperazione tra forze di polizia e magistratura nella prevenzione e repressione dei reati. Tali princìpi, presentati dalla Commissione europea nella forma di una proposta di decisione-quadro, sono stati resi sempre più vaghi e generici nel corso dell'esame da parte del Consiglio. Nonostante le forti critiche espresse dai garanti della protezione dei dati e dal Parlamento europeo, la presidenza del Consiglio è riuscita ad ottenere, nel novembre 2007, un accordo politico sul testo. Questo deve essere però nuovamente sottoposto al parere del Parlamento europeo e quindi si spera in qualche margine di manovra per riequilibrare la proposta.

Le autorità di protezione dei dati hanno segnalato con preoccupazione sempre maggiore il progressivo venir meno di "momenti istituzionali" (presso il Consiglio e, in parte, presso la Commissione) per la valutazione dell'impatto delle misure adottate sui diritti fondamentali e, più specificamente, sulla tutela dei dati personali. Nel Terzo pilastro, gli unici organismi che, per gli aspetti di specifica competenza attribuiti dalle Convenzioni cui si riferiscono, svolgono attività di supervisione e controllo sulla legittimità dei trattamenti dei dati sono le Autorità comuni di controllo Schengen, Europol e Dogane, oltre all'autorità comune Eurojust, nella cui composizione non è pero presente il Garante. La supervisione sui trattamenti effettuati nell'unità centrale è passata dall'Autorità comune di controllo Eurodac al Garante europeo recentemente istituito.

Questo modello di supervisione sarà applicato, una volta entrati in funzione, anche per il Vis (sistema informativo visti) e per il Sis II.

Europol: l'attività dell'Autorità di controllo comune e i casi di contenzioso

L'attività dell'Autorità di controllo comune (Acc) nel periodo considerato si è concentrata in particolare sulla proposta di decisione per l'integrazione di Europol tra le strutture dell'Unione europea e la definizione del quadro generale di riferimento per lo svolgimento della sua attività.

L'Acc ha espresso un parere molto articolato sul testo, formulando specifiche raccomandazioni, in particolare riguardo alla divergenza introdotta nel nuovo testo tra obiettivi di Europol e le più ridotte competenze attribuite all'organismo, nonché ai nuovi compiti di Europol di elaborazione di informazioni fornite non più solo dagli Stati membri, ma anche da Paesi terzi e da entità pubbliche e private. Poiché questo determina un notevole incremento dei dati raccolti ed analizzati, l'Acc ha richiamato l'attenzione sulla necessità di prevedere chiaramente se e come Europol potrà aver accesso ai dati e quali le responsabilità.

Il testo attualmente in discussione presso il Consiglio ha tenuto nella giusta considerazione le osservazioni formulate dall'Acc, in particolare per quanto concerne le garanzie per l'accesso ai dati da parte degli interessati e l'esercizio effettivo dei diritti conferiti. Complessivamente gli aspetti relativi al trattamento dei dati personali da parte di Europol sono sostanzialmente immutati rispetto alle previsioni contenute nella Convenzione Europol.

L'attività ispettiva, condotta annualmente, di regola a marzo, si conferma come uno dei più incisivi strumenti posti a disposizione dell'Acc per il suo ruolo di supervisione e controllo sulla liceità dei trattamenti di dati da parte di Europol.

Nel corso dell'ultima ispezione gli esperti partecipanti hanno focalizzato le verifiche sul sistema di informazione Europol, sui seguiti dati alle raccomandazioni formulate in precedenti ispezioni, sul contenuto dei *file* di analisi e sul rispetto delle prescrizioni che l'Acc ha impartito accettando la richiesta di Europol di un approccio diverso e, più in generale, per l'apertura di *file* di analisi aventi per oggetto lo sfruttamento dell'immigrazione illegale.

L'Acc ha riconosciuto l'alto grado di adeguamento alle raccomandazioni formulate da parte di Europol, anche se ha reiterato alcune preoccupazioni, che in parte non sono ascrivibili alla sola Europol, ma anche al modo con cui gli Stati membri svolgono le attività richieste dalla Convenzione. L'Acc pertanto, in relazione a queste ultime, ha richiesto alle autorità nazionali che la compongono di effettuare verifiche rispetto alle azioni che gli Stati debbono assicurare. Il Garante, come autorità nazionale di controllo, ha effettuato le verifiche richieste e ha richiesto la correzione/cancellazione dei dati inesatti.

L'Acc si è inoltre occupata della creazione del sistema *"check the web"*, portale che Europol intende utilizzare per mettere a disposizione degli Stati partecipanti le informazioni e i *link* ai siti *web* che possono considerarsi utili ai fini della lotta alla criminalità. Europol prevede anche un servizio di traduzione per rendere tali informazioni più accessibili alle forze di polizia dei diversi Paesi.

Parte dell'attività è stata anche dedicata alla decisione e preparazione di una conferenza, da tenersi a Bruxelles, per celebrare i dieci anni di attività dell'Acc, valutando i risultati finora raggiunti e le sfide future (*v.* la relazione di attività in *http://europoljsb.consilium.europa.eu*).

Il Sistema informativo doganale: l'attività dell'Autorità di controllo comune

Il sistema informativo doganale (Sid) consiste in una base di dati centrale cui si può accedere tramite terminali situati in ogni Stato membro. La Commissione europea provvede alla gestione tecnica dell'infrastruttura del Sid.

La vigilanza sul corretto funzionamento del Sid è affidata a una autorità comune di controllo, composta di due rappresentanti per ciascun Paese delle autorità nazionali di protezione dei dati.

L'Acc Dogane ha completato il lavoro di verifica del rispetto delle condizioni per la raccolta e trattamento dei dati personali iniziato lo scorso anno, svolto sia con un *audit* sulla congruità delle misure di sicurezza adottate presso l'unità centrale, sia con la raccolta di informazioni a livello nazionale delle misure esistenti sulla scorta di un questionario comune.

Il sistema risulta peraltro molto poco utilizzato dai potenziali utenti, che come base per gli scambi di informazioni in materia preferiscono utilizzare accordi bilaterali o multilaterali.

L'Acc potrebbe comunque decidere di intraprendere un'azione comune finalizzata a verificare la liceità dei trattamenti di dati personali in tutti gli Stati che applicano la Convenzione.

Schengen

L'attività dell'Acc Schengen ha continuato a essere prevalentemente legata agli sviluppi del Sis e al funzionamento dell'attuale sistema.

Occorre ricordare che i regolamenti per l'istituzione del Sis II relativamente alle segnalazioni degli stranieri non ammissibili e per l'accesso ai dati dei veicoli sono stati adottati e pubblicati nella *Gazzetta Ufficiale* nel mese di dicembre 2006, mentre la decisione relativa alla parte del sistema che contiene le segnalazioni ai fini di esecuzione dei mandati di arresto europei, di sorveglianza discreta e di rintraccio persone (finalizzata alla cooperazione giudiziaria e di polizia) è stata pubblicata diversi mesi dopo.

Si prevede che il sistema potrà essere in funzione non prima della metà del 2009: occorre infatti che sia completata l'infrastruttura tecnica e che gli Stati –inclusi quelli entrati più di recente nell'Unione– predispongano il quadro legale e tecnico necessario.

La Commissione europea, che avrà la responsabilità della gestione tecnica del Sis II, sta lavorando alla preparazione di una campagna informativa per i cittadini senza tuttavia aver coinvolto nella predisposizione dei testi l'Acc Schengen, che pure ha preparato le precedenti campagne informative svolte nei Paesi aderenti. Le autorità nazionali di protezione dei dati sono state interpellate singolarmente.

È stata inoltre completata l'azione comune per verificare in ciascuno dei Paesi partecipanti la regolarità delle segnalazioni inserite nel sistema con riferimento all'articolo 99 della Convenzione (sorveglianza discreta e controllo specifico).

Le verifiche sono state svolte seguendo uno schema unico, elaborato in forma di questionario, seguito da controlli *in situ*. Il segretariato, come nella precedente azione comune svolta per verificare la legittimità delle segnalazioni inserite nel sistema ai fini della non ammissione (in base all'articolo 96 della Convenzione), ha redatto un documento complessivo adottato dall'Acc nel dicembre 2007. Il documento sarà tradotto nelle lingue nazionali per favorirne la diffusione e l'utilizzo da parte delle Autorità.

Il Garante ha preso spunto dall'accertamento deliberato dall'Acc per definire in modo più ampio le modalità della verifica da effettuare. La parte nazionale dell'accertamento è previsto che si concluda nel primo semestre del 2008.

Eurodac

Per quanto concerne Eurodac, la base di dati europei che contiene le impronte digitali dei richiedenti asilo e delle persone fermate dalla autorità di frontiere in posizione irregolare, l'attività di coordinamento effettuata dal Garante europeo per la protezione dei dati personali si è conclusa con l'adozione di un rapporto che fa stato delle attività di accertamento svolte in ciascun Paese e di quelle svolte dallo stesso Garante europeo sull'unità centrale (*v.* per il rapporto *www.edps.europa.eu)*.

Molte delle raccomandazioni formulate sono state riprese dal Garante italiano, che ha esteso gli accertamenti alla liceità del trattamento dei dati finalizzato non solo all'inserimento nel sistema Eurodac, ma anche alla procedura di applicazione della Convenzione di Dublino, che prevede la possibilità di rinvio del richiedente asilo ad altro Paese laddove risulti esistente una segnalazione di questo Paese.

Nel corso degli accertamenti il Garante è intervenuto, in particolare, per verificare l'uso delle *cd.* "ricerche speciali", ovvero le richieste di accesso ai dati, previste dal regolamento Eurodac (Regolamento (Ce) n. 2725/2000 del Consiglio, dell'11 dicembre 2000), funzionali all'esercizio dei diritti riconosciuti alla persona interessata. In taluni casi e per alcuni Paesi tra cui l'Italia, gli accessi ai sensi dell'articolo 18 risultano infatti piuttosto numerosi e non sembrano avvenire per le ragioni indicate nel regolamento. Gli accertamenti hanno inoltre riguardato l'adeguatezza delle misure adottate per garantire la sicurezza nel trattamento dei dati nelle diverse operazioni compiute.

La chiusura degli accertamenti del Garante è programmata per il primo semestre del 2008.

Nel corso delle riunioni di coordinamento è stato adottato il regolamento interno e predisposto il programma di lavoro per l'anno in corso.

La Commissione europea ha presentato il rapporto annuale in cui fa stato delle sue attività in relazione alla gestione della banca dati Eurodac, con riferimento ai risultati raggiunti e ai problemi rilevati (*v.* per il rapporto *http://ec.europa.eu/justice_home*).

Un punto particolarmente delicato, esposto dalla Commissione, è quello relativo alla possibilità di una modifica del regolamento Eurodac per rendere possibile l'accesso, a certe condizioni, alle forze di polizia per l'espletamento dei compiti loro assegnati. La Commissione ha precisato che la richiesta è stata formulata dal Consiglio e che essa stessa ritiene utile tale ampliamento. Riguardo a tale ipotesi, le autorità di protezione dei dati hanno espresso viva preoccupazione, rappresentando il cambiamento di finalità che ne consegue e il *Working Party on Police and Justice* ha adottato un parere fortemente critico.

Working Party on Police and Justice

Il *Working Party on Police and Justice* (WPPJ), sotto la Presidenza italiana, si è riunito tre volte nel corso del 2007 (27 giugno, 17 ottobre, 18 dicembre), mentre una quarta riunione si è tenuta all'inizio del 2008 (27 marzo), in previsione della "Conferenza di Primavera" di Roma (*v. par.* 20). Oltre ad adottare il regolamento interno, successivamente sottoposto all'approvazione formale della Conferenza di Roma, il *Working Party* ha monitorato diverse iniziative, non sempre coordinate, relative ai trattamenti di dati personali nel settore della cooperazione giudiziaria e di polizia.

Nel maggio 2007 è stato approvato un *"Position Paper"* critico rispetto all'iniziativa di alcuni Paesi Ue finalizzata ad adottare una decisione del Consiglio sul potenziamento della cooperazione transfrontaliera, con particolare riguardo al contrasto del terrorismo e della criminalità transnazionale ("progetto di decisione del Consiglio sul Trattato di Prüm"). La decisione (poi adottata dal Consiglio giustizia e affari interni con minime modifiche nel mese di giugno 2007), reca disposizioni in materia di scambio di informazioni fra autorità giudiziarie e di polizia, con particolare riguardo al Dna, ai dati dattiloscopici e alle informazioni di immatricolazione, e consente alle suddette autorità di accedere alle banche dati nazionali. Il Gruppo ha ricordato l'assenza di disposizioni armonizzate a livello europeo, e ha sottolineato l'opportunità di definire prioritariamente tale quadro armonizzato, attraverso la decisione-quadro del Consiglio sulla protezione dati nel Terzo pilastro, ad oggi ancora in via di definizione. Il documento è stato inviato al Consiglio Ue e ha ricevuto pubblicità anche attraverso i contatti fra le autorità nazionali di controllo e le autorità governative.

Successivamente (dicembre 2007-marzo 2008), il WPPJ si è occupato della proposta di Decisione del Consiglio che dà attuazione alla Decisione del Consiglio che recepisce il Trattato di Prüm sopra menzionata. È stato elaborato, in particolare, un *"Position Paper"* contenente osservazioni critiche e raccomandazioni sulle disposizioni contenute nell'"Allegato Tecnico" alla suddetta proposta di decisione, preceduto da un breve testo in cui sono sinteticamente rinnovate le osservazioni che il WPPJ aveva già svolto sulla Decisione adottata nel mese di giugno 2007. L'Allegato tecnico fissa gli *standard* riferiti allo scambio di informazioni e alla comparazione dei dati forniti; il WPPJ ha chiesto maggiori garanzie con riguardo alla tracciabilità degli accessi al sistema, alla proporzionalità dei trattamenti effettuati, alle misure di sicurezza e all'accuratezza dei criteri di comparazione. Su questo testo si era pronunciato in modo molto critico (il 19 dicembre 2007) anche il Garante europeo per la protezione dei dati. Il documento è stato approvato nel mese di aprile 2008 e inviato alle istituzioni europee competenti.

Nella riunione di ottobre 2007 si è richiamata l'attenzione delle istituzioni comunitarie, in particolare, sulla necessità di assicurare nella decisione-quadro in materia di protezione dei dati nel Terzo pilastro un livello di tutela non inferiore a quello previsto nella Convenzione n. 108/1981 del Consiglio d'Europa. Il testo è stato inviato anche ai Ministri italiani competenti (interno e giustizia) per sollecitarne l'interessamento nel Consiglio giustizia e affari interni del mese di novembre. Il Presidente del WPPJ è stato invitato dal Parlamento europeo, Commissione "Libertà pubbliche" a partecipare alla seduta pubblica dedicata alla valutazione del testo su cui il Consiglio Gai aveva raggiunto un accordo politico (dicembre 2007).

Sul punto il WPPJ ha mantenuto alta l'attenzione, continuando a sollecitare l'interessamento delle competenti autorità nazionali in sede di Consiglio Ue nei mesi successivi, anche in vista della riconsultazione del Parlamento europeo dopo le modifiche apportate al testo della proposta di Decisione.

Sulla proposta di consentire l'accesso all'archivio Eurodac a soggetti non incaricati delle politiche in materia di asilo (forze di polizia, autorità giudiziarie) il Gruppo, con una lettera del novembre 2007 al vicepresidente della Commissione europea, Frattini, alla presidenza del Consiglio Ue e alla Commissione Libe del Parlamento europeo ha manifestato contrarietà, rispetto allo "sviamento" di finalità che la proposta comporta, tenuto conto che il *database* Eurodac contiene impronte digitali di soggetti richiedenti asilo. Il WPPJ ha deciso di lavorare anche in prospettiva di azioni future (ad esempio, accogliendo la proposta della futura presidenza francese dell'Ue di far parte del gruppo di "Amici della Presidenza" incaricato di lavorare su questo tema).

Nella riunione di dicembre 2007, con riguardo alla proposta di decisione-quadro della Commissione (pubblicata il 6 novembre 2007) sull'obbligo per i vettori aerei in Europa di raccogliere i dati Pnr dei passeggeri in transito da o verso Paesi terzi (il cosiddetto "Pnr europeo") è stato adottato il parere congiunto con il Gruppo art. 29 (*v. par* 20.1.).

Il Gruppo ha richiesto alla Commissione chiarimenti sul cosiddetto "pacchetto Frattini", comprendente tre diverse Comunicazioni presentate ufficialmente nel mese di marzo 2008 in materia di iniziative per la gestione delle frontiere, creazione di un Sistema europeo di sorveglianza delle frontiere, e valutazione del funzionamento della Frontex, l'agenzia incaricata di coordinare la cooperazione in materia di gestione delle frontiere esterne. Il WPPJ ha sottolineato, in particolare, che non appare verificata l'effettiva necessità di tali proposte, né risultano adeguatamente esaminati gli aspetti di *privacy* soprattutto alla luce del parere adottato dalla Conferenza di primavera tenutasi a Cipro nel 2007, relativo alle applicazioni del "principio di disponibilità" previsto dal Programma de L'Aja. Altro elemento di preoccupazione è dato dalla previsione di un massiccio ricorso alle tecnologie biometriche senza soluzioni (di *cd. "fallback"*) che prescindano dall'uso di tali tecnologie.

I risultati di un questionario interno sui poteri effettivi di indagine e controllo delle autorità nazionali di protezione dati nei confronti di autorità di polizia e giudiziarie, presentati nella riunione di marzo 2008, hanno permesso di individuare alcuni settori bisognosi di approfondimento e ulteriori chiarimenti. Infine, il WPPJ ha elaborato la dichiarazione poi adottata dalla Conferenza di Primavera di Roma nel mese di aprile 2008, critica sulla strategia europea di sorveglianza generalizzata dei viaggiatori (*v. par.* 20).

20.3. *La partecipazione ad altri comitati e gruppi di lavoro*

Case Handling Workshop

Il sedicesimo e diciassettesimo incontro del gruppo di lavoro denominato *"Case Handling Workshop"* si sono tenuti rispettivamente a Lisbona (19-20 novembre 2007) e Lubiana (31 marzo-1 aprile 2008); si tratta di seminari di discussione su casi e tematiche di interesse comune, anche per individuare prassi nazionali condivisibili a livello europeo.

L'incontro di Lisbona, dedicato principalmente alla "referenziazione creditizia" (nell'ambito dei trattamenti di dati personali relativi a soggetti che accedono a finanziamenti), si è articolato in quattro sessioni parallele: valutazione del rischio (A), *blacklist* settoriali (B), flussi di dati e profilazione (C), ricorsi e attività di controllo da parte delle autorità per la protezione dei dati (D).

Nella sessione A, dedicata al *"Risk Assessment"* è stato sottolineato da più parti l'affinamento progressivo delle tecniche di valutazione del rischio attraverso strumenti automatizzati sempre più diffusi. A tal proposito, è stato messo in evidenza che l'autorità francese sta curando, con il Ministero dell'economia, la definizione di una serie di criteri che consentano l'emanazione di una sorta di "autorizzazione generale" per i sistemi di *scoring* automatico, anche alla luce delle regole di Basilea-II e al cosiddetto *McDonough Ratio*, ossia la definizione del coefficiente di rischio bancario legato alla solvibilità della clientela. Nella sessione dedicata alle *"blacklist"* (dei *cd.* "cattivi pagatori") in settori diversi dalla referenziazione creditizia (B), molte Autorità hanno concordato sulla necessità che leggi specifiche consentano tali tipi di trattamento, tenuto conto dei rischi che essi possono produrre per gli interessati. Tuttavia, nella (quasi generalizzata) assenza di disposizioni normative occorre comunque individuare idonee garanzie per gli interessati, possibilmente sulla base di un *prior checking*, specie in ordine ai criteri per l'inserimento nelle liste, ai tempi di conservazione, a dovuti preavvisi e informative e al necessario e rigoroso rispetto dei princìpi di proporzionalità e finalità. Nella sessione C numerosi interventi hanno evidenziato la tendenza delle agenzie di referenziazione, nonché del sistema bancario e finanziario ad accrescere le informazioni disponibili. È stata sottolineata la sostanziale uniformità delle strategie adottate dalle autorità per la protezione dei dati per farvi fronte, strategie per lo più fondate sul richiamo al rispetto del principio di necessità, proporzionalità, finalità, e tempi di conservazione non eccedenti. Infine, nella sessione dedicata a casi specifici ed alle attività ispettive (D) è stata riferita l'esperienza italiana riguardo agli accertamenti presso sistemi di informazione creditizia, mentre altre autorità hanno illustrato le difficoltà riscontrate nella gestione dei reclami connessi a tale tipo di trattamenti.

Nella seconda giornata, tra l'altro, l'autorità olandese ha presentato un interessante documento sulla pubblicazione di dati personali in Internet, pubblicato ufficialmente l'11 dicembre 2007 (*v. infra*) previa consultazione pubblica. Significativo anche un caso presentato dall'autorità spagnola, sulla persistenza (nella *cd. "cache"*) di informazioni obsolete o inesatte rispetto al sito originale, e sui numerosi contatti al riguardo intercorsi con vari motori di ricerca (compreso Google).

L'incontro di Lubiana è stato dedicato alla discussione di due temi, biometria e trattamento di dati personali su Internet.

Nel corso della prima sessione, il prof. W.J.M. Voermans, docente nella facoltà di legge dell'Università di Leiden, ha esaminato il rapporto tra diritto alla protezione dei dati personali e diritto di accesso ai documenti pubblici, così come riconosciuti nell'ambito del diritto dell'Unione europea e del sistema del Consiglio d'Europa. L'argomento è di interesse soprattutto per le diverse autorità di protezione dei dati competenti anche in materia di *"right of information"* (tra esse, la stessa autorità slo-

vena, quella greca, quella portoghese) e attuale alla luce dei lavori preparatori per l'adozione, nel contesto del Consiglio d'Europa, di una Convenzione europea sull'accesso ai documenti pubblici.

Le sessioni successive della prima giornata di lavoro sono state dedicate interamente al trattamento dei dati biometrici, che poche legislazioni (Francia, Lussemburgo, Slovenia) disciplinano in modo specifico, richiedendo, la maggior parte delle altre, la notificazione alle autorità di protezione dei dati e spesso anche il *prior checking*. Nel corso della discussione sono state manifestate perplessità sulla necessità del consenso dell'interessato per l'utilizzo di tali dati in ambito lavorativo e sul possibile riconoscimento, in taluni, specifici casi, del legittimo interesse del datore di lavoro al loro trattamento e alla conseguente applicazione dell'istituto del bilanciamento di interessi. L'autorità portoghese ha prospettato che con l'utilizzo dei dati biometrici può aumentare il livello di sicurezza nel trattamento dei dati effettuato presso ospedali, consentendo l'accesso differenziato alle informazioni raccolte nelle cartelle cliniche dei pazienti da parte dei diversi operatori sanitari (medici, infermieri, farmacia ospedaliera, *ecc.*), in modo da tenere traccia degli accessi alle informazioni stesse e favorire la prestazione corretta ed efficace del servizio sanitario.

Nella seconda giornata di lavori diverse autorità hanno presentato le proprie linee-guida in materia di trattamento di dati personali su Internet e, in particolare, attraverso le *cd.* "reti sociali" (*"social networking site"*, quali i noti *Facebook* e *Myspace*). Tra queste, le già citate linee-guida dell'autorità olandese dell'11 dicembre 2007, volte a fornire indicazioni sia ai titolari del trattamento (il divieto di raccogliere dati sensibili in rete, la necessaria previsione di spazi condivisi solo da alcuni utenti e non indicizzati dai motori di ricerca, mezzi celeri e facili per la cancellazione dei dati da parte degli utenti medesimi, *ecc.*), sia agli utilizzatori della rete (per i quali l'Autorità ha messo a disposizione sul proprio sito informazioni e modelli di lettere relativi a trattamenti effettuati in rete). L'autorità olandese, infine, nel richiamare il *memorandum* adottato a Roma dal Gruppo di Berlino in materia di *"social networking site"* (*v. infra*), ha proposto l'adozione di un documento del Gruppo art. 29 in materia, suggerendo un maggiore scambio di informazioni e più approfondite forme di collaborazione tra le autorità di protezione dei dati.

L'autorità britannica, nel novembre 2007, ha creato un sito rivolto ai giovani (*www.ico.gov.uk/youth.aspx*) e predisposto un sondaggio (una serie di domande poste a 2000 ragazzi tra i 14 e i 21 anni) in relazione al trattamento dei dati effettuato da siti di *social networking*. L'esito del sondaggio (che ha dimostrato una diffusa mancanza di consapevolezza da parte dei giovani in merito agli effetti che tali tipologie di trattamento potranno avere sulla loro vita futura) ha attirato l'attenzione di tutta la stampa britannica che ha pubblicato articoli e dedicato programmi televisivi e radiofonici al tema. Per la sensibilizzazione dei minori si sono impegnate con successo l'autorità norvegese (con la campagna *"You decide"* volta a richiamare l'attenzione sulle conseguenze che la diffusione su Internet di dati relativi a minori può avere sulla loro vita di ogni giorno) e quella portoghese (con il programma *"Dadus"* che prevede la creazione di uno spazio *ad hoc* nel sito Internet dell'autorità – *http://dadus.cnpd.pt*– con *forum* di discussioni e *chat* per i minori e materiale didattico messo direttamente a disposizione degli insegnanti per avviare progetti nelle scuole).

IWGDPT

Il "Gruppo di Berlino" (*International Working Group on Data Protection in Telecommunication*) si è riunito a Guernsey (12-13 aprile 2007) ed a Berlino (4-5 settembre 2007); nel marzo 2008 (3-4 marzo) si è tenuto il 43mo incontro ospitato dall'autorità italiana a Roma.

Come di consueto, oltre a fare il punto sui principali sviluppi nazionali, gli incontri del Gruppo di Berlino hanno consentito di affrontare le problematiche

connesse agli sviluppi tecnologici più recenti in chiave di garanzie e rischi per la protezione dei dati personali. Il Seminario pubblico organizzato l'11 aprile 2007 in occasione dell'incontro di Guernsey (*Respecting Privacy in Global Networks*) ha permesso di analizzare problematiche connesse alla *cybersociety* e alla missione cui sono chiamate le autorità di protezione dati, garantire un equivalente livello di protezione fra realtà *off-line* e realtà *on-line* alla luce dei rischi più significativi posti dalle comunicazioni elettroniche (conservazione dei dati di traffico, identificazione, perdita dell'anonimato).

I lavori dei due seminari tenuti nel 2007 hanno condotto all'adozione di un documento dedicato al tema *"Privacy and cross-border marketing"*, da tempo oggetto di discussione, nonché di due ulteriori documenti relativi alla televisione digitale e all'*e-ticketing* (tematiche, queste, peraltro già affrontate in passato dal Garante). In essi il Gruppo ha inteso fornire alcune indicazioni operative a titolari e interessati soprattutto per garantire (come nel caso del *cross-border marketing*) il rispetto dei princìpi di correttezza e trasparenza nel trattamento dei dati personali.

I delegati hanno affrontato anche i temi connessi alle attività dei motori di ricerca (con particolare riguardo alla conservazione delle informazioni contenute nelle stringhe di ricerca e ai rischi di una profilazione occulta), nonché agli sviluppi legati al *cd. "social networking"*, considerato il sempre maggiore favore di cui godono i siti che offrono spazi di incontro ed altri servizi destinati soprattutto agli utenti più giovani. In particolare, ciò ha condotto all'elaborazione di un documento discusso durante l'incontro di Roma e successivamente adottato con procedura scritta. Si tratta di un *memorandum* in cui sono analizzati i rischi connessi ai trattamenti di dati personali effettuati sui siti di *social network* e vengono formulate una serie di raccomandazioni rivolte ai gestori di tali siti, alle autorità di regolazione ed agli utenti.

Fra gli altri temi di cui si è occupato il Gruppo di Berlino nel corso del 2007 e nei primi mesi del 2008 ricordiamo anche il trattamento di dati personali connesso alle iniziative che mirano a garantire una maggiore sicurezza del traffico veicolare (nell'ambito della *"European road safety policy"*) e le implicazioni in termini di protezione dati legate all'applicazione della Convenzione del Consiglio d'Europa sulla criminalità informatica (Convenzione di Budapest del 2001). Su quest'ultimo punto il Gruppo ha adottato a Roma un documento contenente una serie di raccomandazioni rivolte agli Stati membri del Consiglio d'Europa per quanto concerne le misure nazionali di attuazione delle disposizioni della Convenzione, elaborato sulla scorta di una proposta presentata dall'autorità italiana.

Consiglio d'Europa

Nel 2007 l'autorità italiana ha seguito i lavori del Comitato consultivo (T-Pd) della Convenzione del Consiglio d'Europa n. 108/1981 sul trattamento automatizzato di dati di carattere personale, ed è entrata a far parte del *bureau* che si riunisce ogni 4 mesi. Nella riunione del marzo 2007 è stato eletto il *Data Protection Commissioner* del Consiglio d'Europa (Karel Neuwirt, della Repubblica ceca), per un periodo di tre anni. Fra i temi affrontati di maggiore rilevanza vi è un parere sul trattamento automatizzato e titolare del trattamento nel contesto delle reti mondiali di telecomunicazioni.

Il parere del T-Pd sottolinea che la raccolta dei dati, sebbene non inclusa esplicitamente nella definizione data dalla Convenzione 108, deve essere ricompresa nel concetto di trattamento automatizzato, prescindendo dalle modalità di raccolta dei dati stessi; specifica inoltre che la semplice navigazione su Internet non costituisce un trattamento di dati se non è possibile condurre operazioni relative ai dati personali contenuti nelle pagine *web*. Inoltre, in linea con la sentenza Bodil Lindqvist della Corte di giustizia delle Comunità europee (6 novembre 2003, C-101-01), si

ribadisce che rendere disponibili dati su Internet rientra nella definizione di trattamento automatizzato prevista dall'art. 2.c della Convenzione 108. In tale definizione, con riferimento alla videosorveglianza, non rientrano invece i sistemi che non registrano dati e che non danno la possibilità di conservare o svolgere altri trattamenti ricompresi nel concetto stesso di trattamento automatizzato.

Il parere sottolinea inoltre come, in qualunque contesto, l'obbligo di informare gli interessati sulle modalità dell'esercizio di accesso e rettifica rimanga in capo al titolare del trattamento, giuridicamente responsabile anche quando possa poi rivalersi su un responsabile o su un contitolare. Laddove più soggetti pongano in essere il trattamento, spetta a ciascuno di essi determinare i propri compiti e le proprie responsabilità rispetto al trattamento, al fine di evitare di essere ritenuto congiuntamente responsabile con gli altri in caso di danno.

Profilazione

È stato inoltre pubblicato il rapporto commissionato dal T-Pd sull'applicazione della Convenzione 108 al meccanismo della *cd.* "profilazione", quella tecnica di trattamento, cioè, che permette di desumere informazioni relative a una persona a partire da tutti i dati (anonimizzati o meno) relativi ad un gruppo di individui al quale l'interessato appartiene o si suppone appartenga (TP-(2008)01). In base a tale parere, la profilazione nel suo complesso ricade nell'ambito di applicazione della normativa sulla protezione dei dati, anche se alcune operazioni di profilazione, in quanto prive di riferimento a dati riconducibili ad una persona identificata o identificabile, potrebbero non essere soggette all'applicazione della Convenzione n. 108/1981. Lo studio evidenzia l'opportunità di elaborare uno strumento giuridico, in particolare una raccomandazione, che fornisca garanzie rafforzate sull'informativa, sul diritto di opposizione, su un eventuale divieto di profilazione basata sull'impiego di dati sensibili, sull'obbligo di conservare traccia delle inferenze statistiche (ossia, degli elementi utilizzati per costruire il profilo) e sulla necessità di realizzare un bilanciamento degli interessi coinvolti. Sottolinea inoltre la particolare delicatezza del tema con riguardo all'utilizzo di procedure automatiche, che non prevedono l'intervento dell'intelligenza umana.

Agenzia Mondiale Anti-Doping (ADAMS)

Il *Monitoring Group* della Convenzione del Consiglio d'Europa Anti-Doping (T-Do) ha chiesto un parere al T-Pd sulla compatibilità del *database* ADAMS (sviluppato dal *World Anti-doping Agency*-WADA) con i princìpi di protezione dati contenuti nella Convenzione n. 108/1981. WADA è una fondazione di diritto privato situata in Svizzera, mentre la banca dati ADAMS è localizzata in Canada. Appare centrale il problema della base giuridica dell'inserimento dei dati nella banca dati centralizzata; secondo il gruppo né il Codice mondiale anti-doping, né il consenso degli atleti rappresentano una base giuridica adeguata. Il primo, infatti, non contiene disposizioni specifiche che tengano conto della normativa in materia di protezione dati, e in particolare dei princìpi contenuti negli artt. 5-8 della Convenzione n. 108/1981. Né, d'altra parte, può dirsi valido il consenso, posto che, dipendendo dal rifiuto conseguenze negative per gli atleti, esso non risulta libero, espresso e informato. È stato inoltre rilevato che nel *database* risultano presenti anche dati personali non relativi agli atleti (accompagnatori e medici sportivi), senza che venga fornita ai soggetti interessati alcuna informativa, benché si tratti di dati sensibili. Il parere si sofferma poi sulla necessità che l'informativa sia precisa e completa, soprattutto in merito alle finalità del trattamento, al titolare, alle categorie di dati trattati e la loro origine, al periodo di conservazione e le categorie di destinatari, ai diritti degli interessati e alle responsabilità dei differenti titolari e responsabili del trattamento, alle misure di sicurezza. Vengono infine espressi dubbi sia sull'opportunità di includere nei modelli di raccolta dei dati personali categorie aperte come "altre informazioni" o "commenti", di prevedere (come avviene attual-

mente) un periodo di conservazione di 8 anni, che non appare necessario per tutte le categorie di dati raccolti, sia sulla mancanza di meccanismi riparatori in caso di responsabilità per danni derivanti dal trattamento dei dati. Viene ancora sottolineata la necessità di prevedere garanzie appropriate, *ad es.*, attraverso il ricorso alle clausole contrattuali, per i trasferimenti di dati verso Paesi che non assicurino un livello adeguato di protezione dati.

È inoltre proseguita la discussione sia sull'opportunità di elaborare un protocollo addizionale alla Cedu per inserire nel catalogo dei diritti fondamentali il diritto alla protezione dati, sui poteri delle autorità indipendenti e sul regolamento di procedura interna.

Ocse

Il *Working Party on Information Security and Privacy* (Wpisp) ha esaminato nel 2007 temi e documenti relativi alla Conferenza Ministeriale di Seul del giugno 2008, dedicata al tema "Il futuro di Internet". Obiettivo centrale della Conferenza è dimostrare che Internet è un'infrastruttura fondamentale per lo sviluppo economico (crescita, innovazione, produttività, lavoro) e sociale (istruzione, ambiente, salute). In particolare vengono affrontati tre temi: la promozione della creatività al fine di stimolare il ruolo della rete come fonte e strumento di innovazione e crescita; la necessità di far crescere la fiducia in Internet in quanto infrastruttura affidabile per sviluppare attività economiche e sociali; il tentativo di massimizzare i benefici della convergenza di piattaforme prima distinte (tv, telefonia, reti).

La Conferenza stabilirà le linee di azione prioritaria dei gruppi di lavoro in seno all'Ocse, e potrebbe rappresentare il punto di partenza per un ripensamento delle linee-guida del 1980 in tema di *privacy* alla luce dell'utilizzo crescente delle nuove tecnologie; è prevista l'adozione di un documento (*Seoul Ministerial Declaration*), accompagnato da un *Policy Framework* che conterrà le raccomandazioni per i differenti settori.

È stata approvata definitivamente dal Consiglio dell'Ocse il 12 giugno 2007 la Raccomandazione sulla cooperazione transfrontaliera nell'applicazione delle legislazioni in materia di *privacy*, che pur essendo uno strumento di *soft law*, impegna gli Stati membri e può essere condivisa anche da Paesi non membri dell'Ocse. La Raccomandazione si propone di migliorare la cooperazione nell'attuazione delle normative, soprattutto con riferimento all'aumento dei flussi transfrontalieri di dati e dei rischi connessi in termini di garanzie, e di facilitarla, attraverso l'istituzione di una rete di *contact point* nazionali per gli scambi di informazioni fra i soggetti interessati, e di un modulo condiviso per fornire gli elementi chiave nelle richieste di informazioni e collaborazione.

Nella stessa data è stata adottata dal Consiglio la Raccomandazione sull'autenticazione elettronica, sul ruolo fondamentale dell'autenticazione elettronica per la crescita di fiducia nello svolgimento di attività *on-line* e per lo sviluppo dell'economia digitale, in particolare ai fini del commercio elettronico, dello sviluppo dell'amministrazione digitale e più in generale della protezione dei sistemi informativi.

Il Gruppo si è inoltre occupato del tema della *Digital Identity*, con particolare riguardo ai rapporti tra personalità e identità digitale nella società dell'informazione. Il concetto di identità digitale non può prescindere dai princìpi fondamentali in materia di protezione dati, soprattutto con riferimento al controllo delle informazioni sull'identità e, quindi, alla responsabilità nel porre in essere azioni ricollegabili all'individuazione di un soggetto preciso. Solo la possibilità di determinare con certezza l'identità consente di avere fiducia e di garantire un ordine sociale all'interno di una società democratica, mentre una minore protezione dati facilita la profilazione e quindi la perdita di rilevanza della personalità. Per tali ragioni il Wpisp ha deciso di continuare a riflettere sugli elementi costitutivi dell'identità dig-

itale, sulla pluralità di approcci (*user-centric vs. service provider centric vs. network-centric*), e sul ruolo dei Governi; questi ultimi, infatti, possono essere allo stesso tempo "fornitori" di identità digitali, "utilizzatori" di identità digitali e giocare un ruolo importante come "protettori di un bene comune", garantendo diritti fondamentali come la *privacy* e definendo i requisiti minimi di sicurezza per garantirne l'affidabilità.

Un documento del Gruppo si propone inoltre di fornire una panoramica dettagliata sui rischi connessi all'impiego della tecnologia *Rfid* (che si prospetta crescente), aggravati nei casi di convergenza con altre tecnologie, come i sensori o Internet. Gli aspetti più problematici sono legati all'invisibilità della raccolta dei dati, al tracciamento inconsapevole e alla possibile sorveglianza nei casi di interconnessione attraverso Internet. Il *report* non dà indicazioni rispetto a *best practice* o politiche di attuazione: queste ultime sono state inserite in un altro documento, *Draft Policy Principles on Rfid* preparato in vista della Conferenza ministeriale.

Nel 2007 è stata presentata la proposta di creare uno spazio *web* comune dedicato alla *privacy*, alla tutela dei consumatori e allo *spam*. La proposta è nata dalla constatazione che i problemi che incontrano gli utenti *on-line* sono in crescita e spesso hanno ambiti di sovrapposizione: furti di identità, *spyware, malware, spam, ecc.* Una piattaforma *web* condivisa fra i diversi settori consentirebbe agli utilizzatori di comprendere più facilmente a quali strumenti di tutela ricorrere.

Cooperazione bilaterale

La visita di una delegazione dell'autorità macedone di protezione dati, svoltasi nel corso della prima settimana del mese di luglio 2007, ha offerto l'occasione per uno scambio di informazioni sul funzionamento e le competenze dell'autorità italiana e di quella macedone. È stato siglato un accordo di collaborazione che prevede la possibilità di contatti regolari fra le due autorità anche al fine di approfondire singoli aspetti normativi.

Taiex – Incontro con le autorità serbe (Belgrado, 22 ottobre)

Nell'ambito del Programma Taiex, finanziato dalla Commissione europea per i Paesi candidati all'ingresso nell'Unione europea, sono stati organizzati incontri con i rappresentanti dei ministeri e delle autorità competenti della Serbia per discutere del progetto di legge in materia di protezione dei dati, che intende recepire la direttiva 95/46/Ce nel quadro del progetto di riforma nazionale del sistema giudiziario. Il testo è apparso bisognoso di consistenti modifiche per allinearlo ai requisiti comunitari.

21 Le attività di comunicazione, studio e ricerca

21.1 *La comunicazione del Garante: profili generali*

Il concreto rischio di muoversi sempre più velocemente verso una società della sorveglianza e della classificazione; una ancora inadeguata cultura della protezione dei dati; il ricorso massiccio a tecnologie di raccolta e conservazione dei dati sempre più sofisticate; i problemi della sicurezza collettiva nazionale ed internazionale; il potenziale uso indiscriminato anche delle più delicate informazioni sulle persone: sono questi i fattori che hanno spinto il Garante, nel corso del 2007, a intensificare l'azione volta alla crescita di una forte consapevolezza da parte di cittadini, istituzioni e mondo dell'impresa sul ruolo centrale svolto nella nostra società dalla protezione dei dati personali.

L'Autorità ha cercato di mantenere un alto livello di informazione riguardo all'intero spettro delle tematiche sulle quali si è concentrato il suo impegno, in particolare sui grandi temi legati alla protezione dei dati: la messa in sicurezza delle grandi banche dati, pubbliche e private; il ricorso sproporzionato o generalizzato a tecniche di raccolta di dati biometrici; l'uso dei dati genetici; i rapporti tra diritti della persona e diritto di cronaca tutelando in particolare i soggetti deboli, a partire dai minori; la protezione delle reti di telecomunicazione e comunicazione elettronica; i sistemi di videosorveglianza.

Un medesimo impegno è stato posto anche riguardo a questioni di più immediato interesse sociale quali, ad esempio, la limitazione del *marketing* aggressivo, con una decisa azione indirizzata a stroncare il fenomeno delle telefonate pubblicitarie indesiderate e l'attivazione di servizi non richiesti; la tutela della riservatezza negli alberghi; la profilazione dei gusti e delle abitudini consumatori e le cosiddette "carte di fedeltà"; il rispetto della dignità delle persone nelle strutture sanitarie; la protezione dei dati dei passeggeri aerei; la tutela dei minori su Internet.

L'attenzione del Garante è stata rivolta ancora al mondo del lavoro a salvaguardia dei diritti dei lavoratori, in particolare per quanto riguarda l'uso della posta elettronica, la navigazione in Rete, la videosorveglianza, il rilevamento biometrico delle presenze.

In questi settori, l'Autorità ha cercato di assicurare ai cittadini, alle imprese e alle istituzioni, insieme con un'accurata e costante informazione, contributi esplicativi ed indicazioni operative per l'attuazione corretta delle norme fornendo allo stesso tempo

Alcune cifre

La presenza sui *media* delle tematiche riguardanti la protezione dei dati personali e, in particolare, l'attività del Garante, ha registrato un notevole balzo in avanti, di oltre il settanta per cento, rispetto al 2006. Nel periodo dal 1 gennaio al 31 dicembre 2007 sono stati selezionati dal Servizio relazioni con i mezzi di informazione oltre 22.948 articoli di interesse dell'Autorità.

Sulla base della rassegna stampa prodotta, le pagine dei maggiori quotidiani e periodici nazionali e internazionali, dei maggiori quotidiani locali e dei media online, che hanno offerto spazio alle questioni legate generalmente alla *privacy*, sono state oltre 7.384, delle quali 2.100 dedicate specificamente all'attività del Garante. Le prime pagine dedicate ai temi della protezione dei dati personali sono state

circa 732 (di cui 399 riguardanti la sola Autorità). Numerose sono state le interviste pubblicate, gli interventi e le dichiarazioni sulla carta stampata (364), su tv e radio nazionali e locali (266) e anche su pubblicazioni *on-line.*

21.2. *I prodotti informativi*

L'Autorità, nel 2007, ha diffuso 47 comunicati stampa e 14 *Newsletter.*

La *Newsletter*, giunta al suo nono anno di pubblicazione (per un totale complessivo di 298 numeri), privilegia una approfondita informazione nazionale ed internazionale ed è divenuta, ormai, un consolidato strumento dell'attività di comunicazione del Garante. L'obiettivo è quello di coniugare l'illustrazione in chiave giornalistica dei provvedimenti e dell'attività del Garante con l'esigenza di un'informazione di tipo più ampio ed approfondito. La possibilità di una consultazione *on-line* e l'invio telematico ad un numero sempre crescente di abbonati (istituzioni, pubbliche amministrazioni, imprese, liberi professionisti, privati cittadini) ha facilitato e ampliato la diffusione della *Newsletter* contribuendo all'apprezzamento crescente del pubblico.

Il *Cd-rom* del Garante "Il Garante e la protezione dei dati personali" –giunto alla XVII edizione– si apre con una presentazione multimediale sull'attività, le funzioni e l'organizzazione dell'Autorità e sui temi di maggiore interesse affrontati nel corso della sua attività. Al suo interno, in forma integrale e nell'originale veste editoriale, sono disponibili i provvedimenti del Garante, la documentazione relativa alla normativa nazionale e internazionale di riferimento e le pubblicazioni realizzate. L'area tematica dedicata all'informazione permette di accedere alla raccolta completa delle *newsletter* e dei comunicati stampa. I documenti sono stati rimpaginati per una migliore consultazione video. L'archivio digitale ipertestuale, realizzato in formato *pdf*, consente la consultazione con funzioni di ricerca *"full-text"*. Il *Cd-rom* rappresenta uno strumento ormai conosciuto, costantemente richiesto da amministrazioni pubbliche, imprese, liberi professionisti e cittadini.

Il costante impegno per una comunicazione semplice e diretta in primo luogo verso il cittadino trova concreta attuazione nella realizzazione di *depliant* divulgativi in grado di illustrare i diversi temi connessi alla protezione dei dati personali. Il più recente, realizzato nel 2007. La protezione dei dati personali: dalla parte del paziente affronta il tema della tutela e della dignità della persona in ambito sanitario. Uno strumento semplice pensato per il cittadino "paziente"e per gli operatori sanitari che indica una serie di misure da adottare per un uso consapevole e lecito di informazioni delicate quali sono quelle sanitarie.

21.3. *I prodotti editoriali*

Il notiziario bimestrale "GarantePrivacy.it" è giunto al suo quinto anno di pubblicazione e al trentesimo numero. Il bimestrale, destinato a personalità del mondo istituzionale e imprenditoriale, è caratterizzato da una comunicazione mirata ed essenziale, in grado di sottolineare l'attività dell'Autorità nei diversi settori di intervento, con particolare attenzione anche al panorama internazionale. Ciascun numero del bimestrale si apre con un editoriale, su temi all'ordine del giorno, a firma di uno dei quattro componenti del Garante.

Allo scopo di contribuire all'approfondimento dei temi legati alla *privacy* e ai princìpi posti dalla normativa nazionale e comunitaria, il Garante ha da alcuni anni

dato vita alla collana editoriale "Contributi". La raccolta è oggi composta da sette volumi. Nel corso del 2007 è stato pubblicato il "Massimario 2003" che contiene una sintesi dei princìpi affermati dal Garante nel corso dell'anno 2003 e conserva il collaudato schema di classificazione dei volumi che l'hanno preceduto, relativi agli anni 1997/2001 e 2002.

21.4. *Gli incontri internazionali*

Nel corso del 2007 numerosi incontri internazionali hanno registrato la presenza dell'Autorità italiana.

L'intero collegio del Garante ed il segretario generale hanno partecipato all' annuale "Conferenza di primavera delle Autorità europee per la protezione dei dati personali" (*Spring conference*) svoltasi a Larnaka, sull'isola di Cipro, dal 10 all'11 maggio. Al tradizionale appuntamento, presenti oltre trenta paesi europei, molto spazio è stato dedicato alle tematiche della sicurezza e delle attività giudiziaria e di polizia attraverso una riflessione sul ruolo che le Autorità di protezione dati sono chiamate a svolgere, con sempre maggiore frequenza e incisività, in queste materie. Il presidente Francesco Pizzetti è intervenuto nella sessione dedicata a questo tema. Sul delicato e spesso difficile rapporto tra media e riservatezza delle persone, essenzialità dell'informazione e diritto di cronaca, è intervenuto Mauro Paissan, componente dell'Autorità, nell'ambito della sessione dedicata a "*media* e protezione dei dati personali". Nel corso della Conferenza, il Presidente dell'Autorità italiana è stato nominato presidente del gruppo costituito dalle Autorità europee per affrontare le problematiche connesse all'attività di collaborazione giudiziaria e di polizia (*"Working Party on Police and Justice"*).

A settembre dal 25 al 28 l'Autorità ha partecipato alla 29ma Conferenza internazionale delle autorità garanti, svoltasi a Montreal (Canada) (di cui si è riferito *supra*, nel *par.* 20).

A Vilnius, dal 13 al 14 novembre, il presidente Pizzetti ha partecipato alla Conferenza per il decennale dell'autorità lituana.

A Parigi, dal 18 al 19 febbraio, la Cnil –l'autorità per la protezione dei dati personali francese– ha organizzato un incontro di lavoro dedicato ai problemi della comunicazione al quale ha preso parte anche il Garante.

Il segretario generale Buttarelli è intervenuto, tra le varie iniziative di rilievo internazionale, alla 20ma Conferenza internazionale-Leggi sulla *privacy* e le imprese. L'informazione sulla protezione dei dati personali nel mondo, svoltasi a Cambridge (UK) dal 2 al 4 luglio, nonché alla Conferenza organizzata dalla Commissione europea il 20 novembre 2007 a Bruxelles (*Conference on Public Security, Privacy and Technology*).

21.5. Le relazioni con il pubblico

Profili di carattere generale

L'Ufficio relazioni con il pubblico si pone come struttura di raccordo tra il cittadino e l'Autorità, anche alla luce della legge 7 giugno 2000, n. 150 che, portando a compimento l'evoluzione normativa avviata con le riforme degli anni '90, individua nell'Urp uno dei pilastri del sistema della comunicazione e dell'informazione delle pubbliche amministrazioni.

In base alla legge, gli Urp devono curare funzioni di informazione sulle disposizioni normative, su temi di rilevante interesse pubblico e sociale, sulle attività e i ser-

vizi dell'Autorità; ascolto e misurazione della qualità dei servizi; comunicazione interistituzionale, attraverso l'istituzione di flussi informativi tra gli uffici per le relazioni con il pubblico delle varie amministrazioni; svolgere, più specificamente, un servizio di comunicazione che valorizzi il diritto dei cittadini a essere informati e ascoltati e permettere la più ampia diffusione della conoscenza tra il pubblico della disciplina rilevante in materia di trattamento di dati personali e delle relative finalità, per assicurare la trasparenza e la possibilità di scelta delle forme di tutela attivabili davanti all'Autorità.

La soddisfazione degli utenti dell'Ufficio relazioni con il pubblico del Garante è legata anzitutto alla continuità del servizio, nonché alla celerità e completezza delle informazioni fornite. Infatti, i dati raccolti permettono di confermare una stretta correlazione tra "qualità erogata" e "qualità percepita".

L'attività dell'Ufficio relazioni con il pubblico

L'attività dell'Urp dell'Ufficio è stata quindi recentemente valorizzata e rafforzata dal regolamento n. 1/2007 del 14 dicembre 2007 (*G.U.* n. 7 del 9 gennaio 2008 [doc. *web* n. 1477480]) che demanda all'Urp alcuni compiti in materia di quesiti e richieste di parere pervenute al Garante.

Si conferma, anche per il 2007, l'interesse della pubblica opinione per le tematiche legate alla *privacy*, rilevabile dal crescente numero dei contatti registrati nel corso dell'anno. Specie in occasione di fatti ed inchieste condotte dall'autorità giudiziaria che hanno suscitato grande rilievo sui mezzi di informazione (in quanto hanno riguardato aspetti personali e di grande delicatezza) sono pervenute numerose richieste di informazioni da parte dei cittadini, anche semplicemente mossi dal desiderio di esprimere le proprie posizioni o rimostranze. I presunti abusi sui minori della scuola di Rignano Flaminio; le inchieste di Potenza, Perugia e Garlasco; le intercettazioni che hanno riguardato noti esponenti della vita politica italiana, sono solo taluni episodi tra i più rappresentativi che hanno visto impegnato anche l'Urp nella sua funzione di acquisizione anche informale delle diverse istanze rappresentate dai cittadini.

I contatti registrati nel periodo di riferimento, 41.569, risultano aumentati rispetto al 2006 (39.300), seppure diversamente distribuiti; così, mentre rimane sostanzialmente invariato il numero dei visitatori, 1.550, si registra una diminuzione dei contatti telefonici, 15.600, a favore di un significativo incremento delle *e-mail*, 24.419. A questi dati vanno aggiunti 689 fascicoli trattati nel corso del 2007 a fronte dei 520 relativi all'anno 2006.

L'attivazione del servizio di relazioni con il pubblico rappresenta un percorso di cambiamento organizzativo che richiede un'attenta progettazione, sia in fase strategica, sia in fase operativa. Affinché il servizio sia effettivamente in grado di rispondere alle esigenze di semplificazione e miglioramento delle relazioni tra l'amministrazione e cittadini, infatti, l'Ufficio relazioni con il pubblico del Garante è stato pensato e realizzato in funzione delle specificità che caratterizzano il contesto di riferimento. Il pacchetto di servizi, gli strumenti operativi, i processi di lavoro, le professionalità impiegate e persino la logistica sono incardinate all'interno di un progetto organizzativo complessivo in cui i singoli elementi contribuiscono in modo sinergico all'assolvimento di funzioni definite e obiettivi organizzativi prestabiliti.

Tematiche di interesse

Come negli anni precedenti, anche il 2007 è stato caratterizzato dall'analisi di alcune specifiche tematiche. In particolare è stata riscontrata una notevole affluenza del pubblico presso la sede dell'Ufficio in prossimità di scadenze correlate agli adempimenti previsti dal Codice. Al riguardo in concomitanza della scadenza annuale dei termini relativi alle nuove misure minime di sicurezza si continua a registrare un rilevante incremento di quesiti specifici e richieste di chiarimenti.

Continuano a pervenire numerosi quesiti dagli enti locali in materia di accesso agli atti amministrativi ed in particolare di accesso da parte dei consiglieri comunali.

Nella seconda metà dell'anno sono state affrontate, tra le numerose altre, le tematiche correlate all'attività di *marketing* anche in relazione alla nuova disciplina sugli elenchi telefonici. Il Garante è infatti intervenuto in più occasioni sulle problematiche legate al disturbo arrecato dal ricevimento delle telefonate a carattere promozionale, adottando alcuni provvedimenti. Numerose, infatti, sono state le proteste dei cittadini pervenute all'Urp auspicando ulteriori interventi dell'Autorità.

Tra le tematiche che maggiormente hanno suscitato l'interesse degli utenti nel corso dell'anno di riferimento vanno senz'altro annoverate quelle in materia di trattamento dei dati personali di lavoratori per finalità di gestione del rapporto di lavoro (sia ambito sia pubblico sia privato) e il trattamento dei dati personali della clientela in ambito bancario; a tale riguardo, numerose sono le richieste di informazioni sulle questioni connesse all'accesso alla documentazione bancaria. Rilevante è, inoltre, il numero delle segnalazioni pervenute sulle cosiddette truffe telefoniche, sul fenomeno del *phishing* e in occasione del provvedimento sul caso Peppermint, concernente la liceità e correttezza del trattamento di dati personali relativi a utenti identificabili operanti su reti *peer to peer.*

Si segnala, infine, la delicata problematica relativa alle intercettazioni e divulgazioni di comunicazioni che hanno impegnato in più occasioni l'Autorità per i profili di competenza. In numerose occasioni il Garante ha richiamato i mezzi di informazione al rispetto dei princìpi di essenzialità e proporzionalità dell'informazione, con particolare riguardo alla tutela della dignità e dell'immagine, personale e professionale delle persone terze citate nelle conversazioni telefoniche.

21.6. *Manifestazioni e conferenze*

L'attività dell'Autorità collegata a seminari, convegni e altre iniziative a scopo divulgativo ha visto, nel corso del 2007, la conferma di un grande interesse da parte del pubblico. Il Garante ha assicurato la sua presenza a importanti manifestazioni con il proprio *stand* completamente rinnovato e con la partecipazione dei suoi rappresentati a dibattiti e convegni.

Nell'ambito della XVIII edizione del *Forum Pa,* la manifestazione fieristica e congressuale interamente dedicata alla pubblica amministrazione, svoltasi a Roma dal 21 al 25 maggio, l'Autorità ha affrontato temi quali: la protezione dei dati personali come fattore di sviluppo per l'innovazione tecnologica e la riorganizzazione di un'amministrazione pubblica più efficiente e in linea con le aspettative dei cittadini; le grandi banche pubbliche e la loro sicurezza; le nuove tecnologie; la sanità elettronica e le implicazioni per la tutela della *privacy*; il miglioramento della qualità della vita sul posto di lavoro partendo dalla persona; la protezione dei dati personali nella p.a. dopo dieci anni di normativa. Il presidente Pizzetti ha partecipato al convegno *"La* privacy *come fattore di sviluppo della p.a."* (23 maggio); il vice presidente Chiaravalloti è intervenuto al convegno *"Innovazione e salute"* (21 maggio) mentre l'avv. Fortunato ha preso parte all'incontro *"Settima giornata degli innovatori: andare a lavorare con piacere"* (22 maggio). Il 21 maggio, inoltre, il segretario generale Buttarelli ha tenuto una lezione a un *Master* dal titolo *"La protezione dei dati personali nella p.a.: quali novità dopo dieci anni di normativa sulla* privacy*"*. Nei cinque giorni della manifestazione si è registrato un afflusso di circa 45.000 visitatori; 95.000 visitatori virtuali; come lo scorso anno un significativo numero di cittadini ed operatori –stimato in una media giornaliera di 600/700 utenti– ha visitato lo *stand* dell'Autorità.

A Bologna, dal 6 all'8 novembre, l'Autorità è stata presente al Com-Pa, Salone

europeo della Comunicazione pubblica, dedicato al tema *"La pubblica amministrazione dei cittadini"*. Il vicepresidente Chiaravalloti ha partecipato al convegno *"Educazione civica, crescita etica"* (6 novembre) affrontando il tema della protezione dei dati quale diritto centrale per una nuova cultura della cittadinanza, con particolare riguardo ai giovani. L'avv. Giuseppe Fortunato è intervenuto al convegno *"La nuova p.a.: organizzazione e persone"* (7 novembre), trattando il tema della *privacy* come strumento di sviluppo della persona essenziale per una organizzazione che rispetti e valorizzi il ruolo dei dipendenti pubblici. Il 7 novembre, al presidente Pizzetti è stato assegnato il *"Premio Comunicazione pubblica"*. Il Premio, istituito lo scorso anno, è un riconoscimento per quelle personalità del mondo delle istituzioni, della politica, della cultura e dell'economia la cui attività professionale e il cui impegno culturale hanno favorito l'affermazione e la crescita della comunicazione pubblica nel nostro Paese.

Sulla base dei dati forniti dagli organizzatori, anche quest'anno la manifestazione ha registrato una grande affluenza di pubblico: 29.750 visitatori. Lo *stand* del Garante nei tre giorni della manifestazione è stato visitato da circa 1.500 ospiti.

Il 29 gennaio, presente l'intero Collegio del Garante e il segretario generale, si è svolta a Roma la *"Prima giornata della protezione dei dati personali"* celebrata contemporaneamente in tutta Europa. L'iniziativa, promossa dal Consiglio d'Europa con il sostegno della Commissione europea e di tutte le Autorità europee per la protezione dei dati personali, è nata con l'obiettivo di sensibilizzare i cittadini sui diritti legati alla tutela della vita privata e delle libertà fondamentali. Per questo primo appuntamento tutto dedicato alla *privacy*, il Garante italiano ha deciso di puntare sui giovani, perché sono i più esposti a un uso illecito dei loro dati personali e, spesso, meno consapevoli dei pericoli che si corrono nell'uso delle nuove tecnologie, ricche di opportunità, ma dense di nuovi rischi e pericoli, siano esse Internet o i videofonini. Il Garante ha invitato presso la propria sede gli studenti di alcune scuole superiori per stimolare un confronto sui temi della protezione dei dati e ha distribuito *gadget*, dedicati alla protezione dei dati personali, realizzati appositamente per la celebrazione della Giornata.

21.7. *Studi, documentazione e biblioteca*

La redazione della *Relazione* annuale

Anche nel corso del 2007 il Servizio studi ha curato il testo della *Relazione* annuale del Garante, svolgendo un'ampia attività di sistemazione, redazione, omogeneizzazione e selezione dei complessi materiali. L'attività di redazione, coordinata dal Servizio studi con la collaborazione preziosa della Redazione *web*, ha peraltro consentito di rendere disponibile una più larga selezione di materiali italiani e comunitari in allegato alla *Relazione* 2007, nonché di favorire un collegamento diretto ipertestuale tra il testo della *Relazione* e il materiale documentale pubblicato sul sito.

La funzione di studio e di supporto giuridico

Nel periodo di riferimento, inoltre, il Servizio studi ha continuato a curare, di propria iniziativa, ovvero su impulso del Collegio o del segretario generale, alcuni studi e ricerche preliminari su fenomeni emergenti suscettibili di assumere particolare rilevanza per le attività dell'Autorità e per il loro impatto sull'applicazione della normativa in materia di protezione dei dati.

In particolare, per la rilevanza dei temi affrontati, si segnalano gli approfondimenti svolti in relazione a: l'applicazione dell'art. 20 del Codice nei confronti degli organismi di collaborazione tra enti locali per la gestione di funzioni e servizi, nonché delle *cd.* "autorità d'ambito territoriale"; la convenzione internazionale per la protezione di tutte le persone dalle sparizioni forzate; il bilanciamento tra riserva-

tezza e esigenze di accertamento penale; gli accertamenti ispettivi da svolgersi in un'abitazione o in un altro luogo di privata dimora o nelle relative appartenenze; i poteri prescrittivi/inibitori del Garante e reato di "inosservanza dei provvedimenti"; i criteri di applicazione della definizione di "dati di traffico" di cui all'art. 4 del Codice; la definizione di *"unsuccessfull call attempts"* nella direttiva 2006/24/Ce; il furto di identità; il *Foreign Intelligence Surveillance Act* statunitense.

Il Servizio studi e documentazione ha inoltre svolto, come di consueto, altri approfondimenti e analisi su tematiche di interesse dell'Autorità anche ai fini dell'eventuale predisposizione da parte del Garante di specifici provvedimenti. La scelta delle tematiche oggetto di approfondimento è avvenuta, sia su indicazione di componenti il Collegio, sia su iniziativa dello stesso Servizio studi, sia, con modalità informali, su richiesta di altri dipartimenti al fine di approfondimento tempestivo di tematiche di rilevante interesse per il Garante.

Il Servizio studi è stato altresì chiamato a svolgere altra attività di supporto in merito a questioni emergenti nel corso dell'attività istituzionale del Garante; nel quadro di tale attività ha predisposto frequentemente note di sintesi, nonché tabelle e analisi riepilogative a seguito di analitiche indagini giuridiche anche di tipo comparatistico.

I servizi interni di documentazione

L'attività di selezione, acquisizione e distribuzione periodica della documentazione è proseguita nella consapevolezza della necessità di un adeguato bagaglio conoscitivo rispetto alle costanti sollecitazioni provenienti dall'esterno, sia per l'attività svolta dal Garante in base a ricorsi, reclami o segnalazioni provenienti dai cittadini, sia in riferimento alle iniziative intraprese d'ufficio dell'Autorità.

In tale prospettiva il Servizio continua a svolgere un monitoraggio costante delle fonti italiane ed internazionali normative, giurisprudenziali, amministrative e dottrinali, allo scopo di poter rispondere tempestivamente alle esigenze del Garante e degli uffici interni, anche avvalendosi dell'acquisizione di primarie banche dati italiane ed internazionali, in collaborazione con la Biblioteca.

La documentazione e l'aggiornamento del personale sono stati posti al centro dell'attenzione del servizio valorizzando *standard* e procedure improntate all'efficienza, efficacia ed economicità della gestione documentale, al fine di garantire rigore ed attendibilità delle fonti selezionate, nonché tempestività di circolazione e completezza dei materiali raccolti.

La diffusione interna del "Repertorio di documentazione su diritti, libertà fondamentali e dignità della persona", denominato *"Osservatorio* Privacy", che raccoglie novità normative, dottrinali e giurisprudenziali in merito alle tematiche legate alla protezione dei dati e, più in generale, dei diritti delle persone, è divenuta di regola trimestrale per armonizzare la distribuzione con la periodicità di pubblicazione delle principali riviste giuridiche e garantire adeguatezza e differenziazione dell'offerta documentale. La documentazione diffusa è stata ripartita in base alle materie specifiche oggetto dei diversi documenti, individuando una "parte generale" e ulteriori partizioni tematiche coincidenti con le attribuzioni dei dipartimenti giuridici operativi. All'interno delle partizioni rispettive, i documenti sono collegati attraverso il riferimento ad una rubrica tematica che ne faciliti la reperibilità. Distribuito via posta elettronica, l'Osservatorio potrà inoltre essere consultato anche sulla nuova *intranet*.

Il materiale raccolto è stato distribuito nell'ambito della *cd.* funzione di *"aggiornamento continuo a frequenza ravvicinata"* che il Servizio studi svolge attraverso l'inoltro di specifici *alerts* denominati *"Servizio studi* news" con cadenza mensile, in modo da permettere una selezione più completa dei temi di attualità di maggiore interesse (sentenze, orientamenti amministrativi, legislazione straniera), i cui documenti rappresentativi vengono presentati corredati da un'ampia scheda di commento e sintesi.

Nel periodo 2005-2007, con le innovazioni nell'offerta dei servizi di documentazione, il Servizio ha messo complessivamente a disposizione degli utenti interni oltre 1.600 documenti di interesse, indicizzati per materia, tematica e autore.

Nel 2007 la Biblioteca ha curato funzionalità e servizi con lo scopo di soddisfare le richieste di una utenza interna ed esterna in continuo aumento e con profili specialistici differenziati.

La Biblioteca è stata incrementata anche mediante nuove forme di integrazione tecnologica, con un programma di aggiornamento e di integrazione delle collezioni e dei fondi attraverso la selezione di aree tematiche di rilevanza particolare. Ciò, è stato reso possibile anche sulla base di una razionalizzazione delle voci di spesa e di una politica di accrescimento del patrimonio librario che ha potenziato gli scambi e beneficiato di donazioni anche per quanto riguarda la produzione editoriale corrente secondo le materie presenti in catalogo.

La Biblioteca, presso la segreteria generale, risponde in primo luogo alle esigenze di informazione, di studio e di ricerca del personale del Garante ma consente un accesso selezionato a eventuali utenti esterni. La Biblioteca ha provveduto alla:

- raccolta, ordinamento, classificazione e catalogazione in formato elettronico dei materiali acquisiti e prodotti dall'Autorità, nonché di quelli prodotti dalle autorità di protezione dei dati europee e internazionali;
- acquisizione, ordinamento, classificazione e catalogazione in formato elettronico della letteratura giuridica italiana e straniera attinente alla protezione dei dati personali;
- acquisizione, ordinamento, classificazione e catalogazione in formato elettronico della letteratura italiana e straniera sull'incidenza delle trasformazioni della società tecnologica avanzata nel campo della protezione dei dati personali.

Il 2007 ha anche registrato la frequentazione della Biblioteca da parte di studiosi stranieri impegnati in progetti di ricerca.

Il patrimonio cartaceo della Biblioteca consiste attualmente di circa dodicimila titoli monografici (circa seimila titoli in lingua italiana) e di circa quattrocento testate periodiche (circa centodieci periodici correnti e, di questi, circa novanta in lingua italiana).

Si è fatto a volte ricorso anche al mercato antiquario, in primo luogo americano, al fine di costruire un catalogo retrospettivo, scientificamente valido e completo, di titoli sulla *privacy*. Il patrimonio della Biblioteca è stato accresciuto anche da alcune donazioni: si segnala il completamento dell'inventariazione del fondo donato nel 2006 dal prof. Valerio Onida, Presidente emerito della Corte costituzionale, e la nuova donazione da parte del prof. Stefano Rodotà, presidente dell'Autorità dal 1997 al 2005, di circa mille materiali monografici rari e di pregio a incremento del fondo costituito nel 2006.

La Biblioteca, d'intesa con il Servizio studi e documentazione, ha predisposto l'indicizzazione cumulativa e analitica in formato elettronico della raccolta completa dei settanta numeri del "Repertorio di documentazione su diritti, libertà fondamentali e dignità della persona" (denominato *"Osservatorio* Privacy") che raccoglie con periodicità mensile le novità normative, dottrinali e giurisprudenziali, italiane e internazionali, nel campo della protezione dei dati e dei diritti delle persona.

La Biblioteca, con il supporto del Dipartimento per le risorse tecnologiche, ha curato:

- la predisposizione grafica e l'aggiornamento del sito *web* della *Digital Library* consultabile sulla rete *Intranet* dell'Ufficio;
- l'aggiornamento e l'incremento del catalogo Opac (per un totale di

oltre 40.000 notizie bibliografiche) consultabile sul sito;
- la predisposizione di un sistema integrato di accesso con *password* alle risorse bibliografiche elettroniche catalogate sul sito (banche dati giuridiche *on-line* e banche dati giuridiche su *Cd-rom* e *Dvd* italiane e internazionali).

Nel 2007 la Biblioteca ha riscontrato circa duemilanovecento richieste di titoli in lettura da parte di utenti interni (+ 16% rispetto al 2006); circa duecentoventi domande di accesso (+ 22 %) e circa milleottocento richieste di titoli in lettura da parte di utenti esterni (+ 20%); circa quattromila contatti sul catalogo Opac (+ 40%) e circa millecinquecento ore di consultazione di banche dati da parte degli utenti interni ed esterni (+ 50%).

21.8. *Altre iniziative di comunicazione e ricerca*

21.8.1. *Il Laboratorio* Privacy *Sviluppo*

Il Laboratorio *Privacy* Sviluppo

Dal novembre 2006, l'avv. Giuseppe Fortunato, accanto all'ordinaria attività istituzionale dell'Autorità, coordina, con il favore del Collegio, il Laboratorio *Privacy* Sviluppo.

Tale iniziativa si occupa della libera costruzione della propria sfera privata e il pieno esercizio della "sovranità su di sé", mirando all'estrinsecazione totale di ogni potenzialità della persona umana secondo gli obiettivi da ciascuno liberamente determinati. Il Laboratorio è un "luogo" di studio e ricerca al quale ciascuno può dare il proprio contributo per approfondire le modalità di sviluppo della propria identità personale, attraverso le proprie risorse.

Sulla base dei numerosi contributi pervenuti, il testo dal titolo "La svolta. Dal desiderio alla realtà", con il quale hanno avuto inizio i lavori, è stato snellito nelle forme, arricchito nei contenuti e reso di più agevole consultazione. Il testo è stato efficacemente illustrato in un dvd multimediale.

Hanno dato un contributo all'iniziativa le autorità per la protezione dei dati personali di Spagna, Irlanda, Islanda, Malta, Israele, Polonia, Repubblica Ceca, Tailandia, Nuova Zelanda, Catalogna, Cipro, Croazia, Lettonia, Ungheria, Macedonia, Romania, Slovenia, alle quali, nell'anno di riferimento, si sono aggiunte le autorità di Slovacchia, Bulgaria, Grecia, Madrid, Lituania ed Estonia.

Nell'anno 2007 numerosi sono stati gli incontri in cui è stata presentata o richiamata l'iniziativa: presso l'Università cattolica del Sacro Cuore (Milano, 14 marzo e 16 maggio 2007), il Centro universitario Collalto (Roma, 28 aprile 2007), l'annuale appuntamento della "Conferenza di primavera" delle Autorità europee di protezione dei dati personali (Cipro, 13 maggio 2007), il *Forum Pa* (Roma, 22 maggio 2007), i convegni tenutisi presso il Maschio Angioino di Napoli (15 giugno 2007), l'Unione degli industriali (Napoli, 26 giugno 2007), in occasione della presentazione della Relazione annuale dell'Autorità presso il Senato della Repubblica (Roma, 12 luglio 2007), presso la sede italiana dell'Università di Washington (Roma, 5 settembre 2007), in occasione della 29ma Conferenza internazionale sulla protezione dei dati personali (Montreal, 25 settembre 2007), presso l'Università La Sapienza (Roma, 6 ottobre 2007), il *Com-Pa* (Bologna, 7 novembre 2007), l'Università Lum (Bari, 20 novembre 2007), il IV *Seminar on Data Protection Best Practices in European Public Services* (Madrid, 11 dicembre 2007).

Continuando il percorso già avviato nel 2006, il Laboratorio, attraverso incontri di studio, ha coinvolto giovani di numerosi istituti di secondo grado, mentre in alcuni atenei italiani diversi studenti hanno discusso la tesi di laurea e di *master* sui temi che il Laboratorio ha approfondito anche attraverso il coinvolgimento di asso-

ciazioni professionali o comunque dedite alla tutela della persona.

Fra le tantissime Associazioni (oltre 4.000) che stanno partecipando attivamente alle attività del Laboratorio, le venti che garantiscono i maggiori *standard* di impegno fanno permanentemente parte del Comitato-Guida del Laboratorio, che sta approfondendo come l'idea "La svolta" (con il messaggio di "cittadino protagonista"), è presupposto di una democrazia compiuta (Civicrazia) e di una sempre migliore tutela dei diritti (con l'istituzione anche in Italia, unica Nazione europea che ne è priva, dell'*Ombudsman* nazionale).

Con la partecipazione dell'avv. Fortunato alla trasmissione televisiva "10 minuti di ..." su Rai 1 (Roma, 17 dicembre 2007), sono stati illustrati il Laboratorio, la sua attività e il tema centrale della nuova dignità del concetto di *privacy*, intesa non più e non solo come "libertà da", ma anche come "libertà per" lo sviluppo della propria personalità, quale condizione essenziale per l'esercizio delle altre libertà fondamentali.

Il Laboratorio ha accolto nel suo ambito anche la Conferenza nazionale dei garanti delle persone detenute ed *ex* detenute per favorirne il recupero e il reinserimento sociale; la Conferenza ha inserito nel suo Statuto la partecipazione al Laboratorio.

Sempre nell'anno di riferimento sono stati intrapresi accordi con la Scuola Superiore della pubblica amministrazione locale al fine di instaurare un rapporto di collaborazione per attività di studio e ricerca e integrare l'offerta didattica e formativa della Scuola con l'approfondimento dell'idea "La svolta".

L'iniziativa, anche tramite il proprio sito *web www.laboratorioprivacysviluppo.it*, continua a raccogliere i numerosi contributi di quanti ne condividono il messaggio e desiderano aderirvi.

L'Ufficio del Garante

III - L'Ufficio del Garante

22 La gestione amministrativa dell'Ufficio

22.1. *Il bilancio, gli impegni di spesa e l'attività contrattuale*

La gestione amministrativa dell'Ufficio è stata improntata al rispetto dei canoni di trasparenza delle procedure e della flessibilità ed efficienza dell'azione amministrativa.

Le risorse finanziarie sono state destinate a soddisfare le esigenze rappresentate nel documento programmatico approvato in sede di adozione del bilancio di previsione dell'esercizio e al perseguimento dei relativi obiettivi nel rispetto delle procedure previste dalla legge e dai regolamenti che disciplinano la materia.

Nell'esercizio 2007 le entrate complessivamente riscosse ammontano a circa 20,7 milioni di euro. Il contributo dello Stato, pari ad euro 18,7 milioni, si è assestato su valori inferiori di circa 1 milione di euro rispetto al precedente esercizio, mentre le riscossioni di altra natura sono cresciute in misura tale da compensare parzialmente la riduzione del contributo statale e consentire, pertanto, all'Autorità di acquisire somme complessivamente di poco inferiori al 2006.

Un particolare rilievo ha assunto nell'esercizio la riduzione del contributo statale inizialmente previsto dalla legge finanziaria 2007. Per effetto della disposizione contenuta nell'art. 1, comma 507, della stessa legge, infatti, il Ministero dell'economia e delle finanze ha determinato l'entità della riduzione del finanziamento del Garante.

Sotto il versante delle spese effettivamente sostenute per il funzionamento dell'Ufficio, si registra nel complesso un incremento poco significativo rispetto all'anno precedente, pari a circa 100.000 euro. Ciò, sebbene si sia registrato, nel periodo in esame, un incremento di taluni costi connessi all'immissione in servizio di nuovo personale in seguito all'espletamento di apposite procedure concorsuali (*cfr. par.* 2). Emerge pertanto un quadro complessivo di sensibile contenimento della spesa in linea con le stringenti prescrizioni delle recenti leggi finanziarie.

L'attività amministrativa non ha subìto ridimensionamenti significativi in quanto si è avuta la possibilità di sopperire alla carenza dei flussi finanziari attraverso l'utilizzo di una parte delle economie realizzate negli anni pregressi.

L'esercizio 2007 è stato caratterizzato dal contenimento di talune spese per beni e servizi per effetto dell'applicazione di alcune disposizioni legislative che hanno trovato applicazione anche per l'Autorità.

La tabella allegata alla presente *Relazione* (*par.* 25.1., *tab.* 22) riassume sinteticamente per gli anni dal 1997 al 2007 le risorse finanziarie che lo Stato ha trasferito all'Autorità, nonché le somme complessivamente riscosse e quelle realmente pagate per ciascun anno.

La gestione amministrativa, pur nel rispetto dei vincoli di bilancio dettati dalle disposizioni legislative emanate sulla materia, è stata indirizzata a un generale miglioramento delle funzionalità operative dell'Ufficio e a un potenziamento di alcuni settori strategici dell'Autorità quali quello della vigilanza e controllo, da un lato, e degli affari giuridici, legali e normativi, dall'altro lato. Ai settori giuridico-normativi, da ultimo menzionati, sono state destinate risorse in misura proporzionalmente maggiore rispetto al precedente esercizio.

Nello svolgimento dell'attività di controllo la struttura ha continuato ad avvalersi di personale dipendente dal corpo della Guardia di finanza in servizio presso l'Ufficio del Garante.

È proseguita, inoltre, la collaborazione con il Nucleo speciale funzione pubblica e *privacy*, operativo presso la stessa Guardia di finanza, il cui personale specializzato procede direttamente all'esecuzione delle attività ispettive.

Con specifico riferimento alle entrate connesse alla predetta attività di controllo e alle sanzioni irrogate, va segnalato che le stesse non assumono un valore significativo rispetto all'entità complessiva delle risorse che affluiscono al bilancio dell'Autorità. Ciò, anche perché le funzioni ispettive rispondono all'esigenza prioritaria di assicurare il rispetto della legge in materia di tutela della *privacy*.

Va evidenziato, inoltre, che le risorse destinate al bilancio del Garante per effetto delle sanzioni applicate in sede ispettiva scontano rallentamenti procedurali, indipendenti dagli adempimenti posti in essere dall'Ufficio, che hanno determinato in più occasioni l'impossibilità di recuperare integralmente la quota parte delle somme teoricamente spettanti. Infatti, le somme pagate a titolo di sanzione affluiscono direttamente all'Erario mediante versamento da parte del debitore in favore della Tesoreria dello Stato e soltanto successivamente possono essere recuperate dall'Autorità, nella misura spettante del 50 per cento, entro tempi molto ristretti, a volte non compatibili con le procedure amministrative che determinano la definitiva acquisizione al bilancio dello Stato.

Tra le attività dell'Autorità rientranti negli obiettivi fissati dal documento programmatico accluso al bilancio di previsione, inoltre, una particolare attenzione e un impegno significativo è stato dedicato alle funzioni di documentazione, informazione e comunicazione, anche al fine di promuovere tra il pubblico i princìpi ispiratori della disciplina in materia di riservatezza dei dati personali.

In tale ottica, l'Autorità ha partecipato attivamente a eventi e manifestazioni, anche di rilievo internazionale, per divulgare la conoscenza e promuovere idonee campagne informative sui diritti dei cittadini.

L'Autorità ha svolto l'attività contrattuale applicando la normativa del nuovo codice dei contratti pubblici (d.lg. 12 aprile 2006, n. 163) e anche seguendo il regolamento del Garante n. 3/2000 concernente la gestione amministrativa e la contabilità.

In particolare, si è proceduto nel corso dell'anno, con la collaborazione del *broker* prescelto, a svolgere la gara europea per i servizi assicurativi in attuazione dell'art. 27, comma 4 del regolamento del Garante n. 2/2000, che prevede la possibilità di stipulare polizze per la *"copertura dei rischi di premorienza e per i danni causati a terzi dal personale in servizio nell'esercizio delle proprie funzioni, salvo che il fatto derivi da comportamento doloso"*.

La gara europea è stata ripartita in cinque lotti (incendio, *all risks* elettronica, responsabilità civile verso terzi, responsabilità civile patrimoniale, assicurazione vita e invalidità permanente) ed è stata vinta da quattro primarie società di assicurazione.

È stata inoltre rinnovata la convenzione della C.a.s.p.i.e. per un quadriennio.

Il lavoro ordinario di rinnovo dei contratti in scadenza è stato tuttavia prevalente: per il dipartimento risorse tecnologiche sono stati rinnovati oltre venticinque con-

tratti e si è proceduto a piccole gare per l'acquisizione di strumenti informatici necessari per l'attività degli uffici; per il servizio relazione con i mezzi d'informazione si è rinnovato il contratto con la società Telpress per il ricevimento *on-line* dei notiziari delle cinque agenzie giornalistiche "storiche" (Ansa, Adn Kronos, Radiocor, Asca, Agi) i cui contratti sono stati rinnovati, alle quali si sono aggiunte, per il solo 2007, le utenze per le agenzie Tm News e Dire.

Inoltre, ha iniziato a operare il servizio di rassegna della stampa quotidiana a seguito di contratto con la società Selpress, con il conseguente risparmio sull'acquisto materiale di giornali e riviste per la stesura quotidiana della rassegna stampa.

Si è inoltre proceduto alla gara per il nuovo *stand* del Garante per la partecipazione alle manifestazioni nazionali del *Forum Pa* e del *Com-Pa* 2007; per queste due manifestazioni si sono anche stipulati i contratti per i rispettivi allestimenti. Per lo stesso servizio altri contratti sono stati stipulati per lo sviluppo e la fornitura di *Dvd* e per la progettazione e realizzazione dei *Cd-rom* istituzionali, per la fornitura di ristampe dei volumi "Massimario", "Privacy e giornalismo", "Codice" e fornitura del notiziario bimestrale "GarantePrivacy.it", così come per la ristampa e l'ideazione di nuovi *dépliant.*

Nel 2007 con la firma digitale si sono completati parecchi acquisti tramite il *market place*, soprattutto per materiale di cancelleria e di materiale di consumo informatico. Il dipartimento contratti e risorse finanziarie ha anche curato la gara *on-line*, tramite Consip, per la scelta della ditta che si è aggiudicata il servizio di pulizia dei locali della sede e, a trattativa privata, quella per i servizi di portineria e *reception.*

22.2. *Le novità legislative e regolamentari e l'organizzazione dell'Ufficio*

Nel 2007 sono state adottate alcune importanti decisioni di carattere organizzativo per colmare la sproporzione, ripetutamente segnalata dal Garante, tra le risorse umane a disposizione e i nuovi e assai più articolati compiti assegnati all'Autorità dal Codice in materia di protezione dei dati personali e dalla normativa statale e comunitaria.

Come già segnalato nella *Relazione* 2006, il Garante si è avvalso della disposizione della legge finanziaria 2007 (l. 27 dicembre 2006, n. 296) che lo autorizzava ad incrementare la propria dotazione organica in misura non superiore al 25 per cento della consistenza massima già prevista (*cfr.* d.lg. 26 febbraio 1999, n. 51).

In attuazione di tale disposizione, nel luglio del 2007 è stata approvata la nuova pianta organica [doc. *web* n. 1429691] che prevede un incremento di venticinque unità, suddivise tra le diverse aree professionali di cui consta l'organico dell'Autorità.

Il predetto incremento è volto a perseguire il migliore espletamento, in particolare, dei compiti di controllo e vigilanza sul rispetto della normativa (art. 154, comma 1, lett. *a*), del Codice), con ulteriore impulso al programma diretto a incrementare il livello di sicurezza di dati e reti di comunicazione elettronica, nonché l'integrità di alcune grandi banche dati, di particolare rilevanza anche in ambito pubblico.

In coerenza con questi obiettivi, l'Autorità ha anche deciso di incrementare le professionalità disponibili nei settori informatico, della sicurezza informatica e della comunicazione elettronica, individuando le aree professionali e i profili tecnico-professionali utili e necessari per il raggiungimento di tali obiettivi.

Per la copertura del predetto incremento di organico, nel dicembre del 2007, come si dirà in seguito, sono stati banditi nuovi concorsi e procedure selettive per diverse qualifiche e tipologie contrattuali.

Nel quadro delle iniziative di consolidamento dell'organico, nel periodo di riferimento è stato portato a termine il concorso a tre posti di impiegato operativo, bandito nel 2006, ed è stato attuato uno scorrimento della graduatoria di merito, in corso di validità, del concorso per la qualifica di funzionario (anch'esso bandito nel 2006) per ulteriori quattro posti. Complessivamente, nel 2007 sono state immesse in servizio sette unità, che si aggiungono alle sette già assunte nell'anno precedente.

Nel periodo considerato, è stato inoltre introdotto e attuato un articolato sistema di valutazione del personale sia dirigenziale, sia appartenente alle aree direttiva e operativa, il quale prevede, in conformità alle pertinenti disposizioni regolamentari vigenti presso l'Autorità, la redazione di un rapporto valutativo annuale.

22.3. *Il personale e i collaboratori esterni*

Nel 2007 sono stati banditi nuovi concorsi e procedure selettive per reclutare personale appartenente alle aree, rispettivamente, dirigenziale nella misura di una unità, direttiva –nella misura di cinque unità per l'area giuridico-amministrativa e due unità per l'area informatica– e operativa nella misura di otto unità.

In tale contesto, sono state previste alcune riserve di posti (nella misura di due dei cinque posti di funzionario giuridico-amministrativo, di uno dei due posti di funzionario informatico, di tre degli otto posti di impiegato operativo) per il personale in servizio presso l'Ufficio in posizione di comando o di fuori ruolo o con contratto a tempo determinato nella qualifica per la quale si concorre ovvero con rapporto di collaborazione continuativa e coordinata o professionale che abbia maturato un'esperienza, anche non continuativa, non inferiore a un anno, purché in possesso di uno dei titoli di studio previsti dal relativo bando di concorso.

Sono state indette, inoltre, due selezioni per il reclutamento, con contratto a tempo determinato, di due funzionari informatici e di due funzionari per l'area comunicazione e sono stati riaperti i termini della procedura per reclutare (sino) a tre giovani laureati con contratto di specializzazione a tempo determinato della durata di un anno.

I relativi bandi sono stati pubblicati nella *Gazzetta Ufficiale* –quarta serie speciale– 8 gennaio 2008, n. 2.

Agli inizi di gennaio 2008 è stata pubblicata sul sito dell'Autorità una specifica manifestazione di interesse rivolta a dipendenti pubblici, eventualmente da collocare in fuori ruolo presso l'Ufficio, che abbiamo maturato un'esperienza professionale e lavorativa ed adeguati titoli culturali in diversi ambiti, in particolare in quello dell'analisi economica, dell'attività internazionale, della progettazione e analisi normativa e dell'attività di vigilanza e controllo. Con questa innovativa iniziativa, l'Autorità si è proposta di individuare, con specifica procedura, particolari risorse professionali.

Nel periodo considerato si sono svolti alcuni *stage* in collaborazione con diverse università.

Al 31 dicembre 2007 l'Ufficio può contare su un organico, a diverso titolo, di novanta unità, di cui ottantasette in servizio. L'Autorità si avvale, inoltre, di un contingente di personale a contratto di sole tredici unità, alcune delle quali peraltro assunte per brevi periodi.

Nel periodo considerato si è reso necessario ricorrere ad alcuni incarichi di collaborazione occasionali, in particolare per acquisire competenze qualificate in tema di telefonia fissa e mobile e di servizi telematici, finalizzate all'individuazione di misure e accorgimenti tecnici per il trattamento di dati di traffico telefonico e tele-

matico e per la successiva attività di controllo e verifica della congruità delle prescrizioni impartite dal Garante sul trattamento dei dati personali, nonché per attività di supporto ai componenti del Garante.

Avvalendosi delle convenzioni Consip, sono state conferite in *outsourcing* alcune attività di natura esecutiva che non richiedono un apporto lavorativo di elevato contenuto professionale (ad esempio, per l'attività di portineria e per compiti ausiliari).

22.4. *Il settore informatico e tecnologico*

Nel corso del 2007 il Dipartimento risorse tecnologiche ha visto accentuarsi il ruolo di unità di consulenza interna, a supporto dell'Ufficio e dell'Autorità nel suo complesso, nell'elaborazione di provvedimenti o per la trattazione di affari e procedimenti in cui sia stato rilevante il contenuto tecnologico.

Sono state completate, insieme ai dipartimenti giuridici interessati e al dipartimento ispettivo le attività ispettive iniziate nel 2006, che hanno visto l'impegno di personale del Dipartimento per la realizzazione di accessi a banche dati, per l'analisi e lo studio del materiale acquisito e per la stesura di rapporti.

Sviluppo dei sistemi informativi

È proseguito lo sviluppo del sistema informatico per la gestione dell'attività ispettiva e sanzionatoria, progettato con risorse interne dell'Ufficio grazie alla stretta collaborazione con il dipartimento ispettivo, interamente basato su strumenti *open source*. Il sistema permette un'efficiente gestione delle attività e dei flussi di lavoro, consentendo l'interazione con i soggetti esterni che alla stessa attività collaborano o svolgono su delega dell'Autorità (personale della Guardia di finanza operante nell'ambito della convenzione).

È proseguita l'attività di reportistica in funzione del controllo di gestione dell'Ufficio, con la predisposizione di automatismi e *procedure batch* che consegnano periodicamente le informazioni necessarie agli utenti interni, attingendo ai sistemi informativi e alle basi di dati.

È stata continuamente svolta attività di *help-desk* interno, di assistenza tecnica per l'intero sistema tecnologico e di supporto per le esigenze informatiche dell'Ufficio, nelle more della disponibilità dei servizi di assistenza tecnica da affidare in appalto.

Impegno per la sicurezza dell'Ufficio

Anche nel corso del 2007 nessun incidente informatico di rilievo è occorso nel dominio dell'Ufficio, e in particolare nessun evento relativo alla sicurezza ha mai prodotto danni o disservizi. Nessun *virus* informatico è penetrato sulla rete interna.

È stata portata a compimento un'azione formativa sul tema della sicurezza che ha riguardato il personale del Dipartimento risorse tecnologiche (due funzionari hanno conseguito la qualifica di *Certified Information Systems Auditor* Cisa Isaca) ma è stata anche estesa a personale di altre unità, con lo svolgimento preso la sede dell'ufficio di due corsi di formazione sul tema degli *standard* di sicurezza Bs 7779 e Iso 27001.

Attività di consulenza e cooperazione interna

È notevolmente cresciuto il coinvolgimento del Dipartimento nell'attività amministrativa propria dell'Autorità e nell'attività ispettiva. Il Dipartimento ha fornito continuo supporto per l'analisi tecnica richiesta nell'ambito di procedimenti curati dai dipartimenti giuridici; ha svolto consulenza interna *extra*-procedimentale e ha curato, con relazioni e note informative, l'approfondimento di argomenti a contenuto informatico-tecnologico, anche in relazione a esigenze dell'Autorità.

Tra le attività più significative si citano quelle connesse al provvedimento generale in tema di trattamento dei dati di traffico telefonico e telematico; ai provvedimenti di divieto di trattamento con cui il Garante ha impedito le attività di raccolta di dati di traffico effettuate da taluni fornitori di accesso alla rete Internet; ai ricorsi relativi a trattamenti di dati personali tramite la rete Internet o alle tecnologie informatiche nel-

l'ambito lavorativo; ai pareri su atti normativi in materia di immigrazione, visti, permessi di soggiorno, passaporti, diritto d'autore, sicurezza, reti di comunicazione elettronica, innovazione tecnologica della pubblica amministrazione.

Si è sviluppata in modo proficuo la collaborazione con le altre unità e, in particolare, con il Dipartimento comunicazioni e reti telematiche e il Dipartimento attività ispettive e sanzioni.

Contributo all'attività ispettiva

Il Dipartimento ha anche contribuito significativamente allo svolgimento di ispezioni e accertamenti svolti sia nell'ambito della programmazione stabilita dall'Autorità, in collaborazione con il Dipartimento attività ispettive e sanzioni, che nell'esercizio dei compiti di vigilanza su banche dati di sicurezza attribuiti dal Codice al Garante.

In particolare, ha partecipato alla campagna di accertamenti ispettivi sui trattamenti di dati di traffico telefonico e telematico conclusa nel marzo 2007. Successivamente, ha partecipato all'attività ispettiva relativa all'anagrafe tributaria, nell'ambito delle procedure di accertamento e acquisizione di informazioni che si estenderanno a parte del 2008.

Attività internazionale

Il Dipartimento ha inoltre contribuito all'attività internazionale nell'ambito del Gruppo art. 29, dell'*Oecd Working Party on Information Security and Privacy*, del Consiglio d'Europa, con studio di documenti e produzione di rapporti; ha partecipato ai lavori della *Internet Task Force* nel Gruppo art. 29.

22.5. *Il monitoraggio dell'efficacia e dell'efficienza e il supporto al controllo interno*

Nel corso del 2007 sono continuate, a cura della "Unità raccolta dati, flussi informativi e supporto al controllo interno", le rilevazioni dei carichi di lavoro delle unità organizzative dell'area giuridica dell'Ufficio.

Sono stati prodotti con cadenza mensile *report* analitici sulle lavorazioni assegnate, sull'andamento dell'attività e sulla concreta disponibilità di risorse umane, misurate in termini di ore/persona avute effettivamente a disposizione per essere utilizzate nei diversi processi di lavoro. Si tratta di rilevazioni impostate nella logica della "gestione per obiettivi" che consentono di conoscere i carichi di lavoro assegnati alle articolazioni monitorate e di orientare convenientemente l'azione di programmazione dei dirigenti apprezzando anche, in tempo utile e a ogni livello di responsabilità dell'Ufficio, il verificarsi di "picchi" di domanda.

L'Autorità si avvale, altresì, di un organo di controllo interno presieduto da un dirigente della Ragioneria generale dello Stato e composto da un magistrato della Corte dei conti e da un dirigente generale in quiescenza della medesima Ragioneria generale.

In sintonia con le indicazioni fornite dal Servizio di controllo interno ed in considerazione della pubblicazione dei regolamenti sui procedimenti amministrativi del Garante, è prevista per il 2008 l'ulteriore rilevazione dei prodotti e dei processi di lavoro –distinti per tipologie di procedimenti– delle unità organizzative dell'Ufficio, comprese quelle destinate alle attività strumentali e di supporto.

23 Dati statistici (*)

23.1. *Tabelle e grafici*

1. Principali attività dell'Autorità

Sintesi delle principali attività dell'Autorità	
Numero complessivo dei provvedimenti collegiali [1]	479
Ricorsi	316
Pareri a Presidenza del Consiglio dei ministri e ministeri (art. 154 del Codice)	16
Altri provvedimenti collegiali sul trattamento dei dati personali	147
Notificazioni pervenute nel 2007	978
Notificazioni complessivamente pervenute al 31 dicembre 2007	15.266
Violazioni amministrative contestate	228
Sanzioni applicate con ordinanza di ingiunzione	45
Violazioni penali segnalate all'autorità giudiziaria	15
Riscontri a segnalazioni e reclami	3.078
Risposte a quesiti	485
Accertamenti e controlli effettuati direttamente presso i titolari del trattamento	452
Altre richieste ai sensi dell'art. 157 del Codice	461
Prescrizioni sulle misure minime di sicurezza (a fini di estinzione del reato)	15
Verifiche preliminari per trattamenti che presentano rischi specifici	4
Comunicazioni al Garante su flussi di dati tra p.a. o in tema di ricerca (art. 39 del Codice)	21
Pareri a soggetti pubblici sul trattamento dei dati sensibili e giudiziari	28
Risposte a quesiti pervenuti da soggetti pubblici sul trattamento di dati sensibili e giudiziari	135
Risposte ad atti di sindacato ispettivo e controllo	2

2. Altre attività

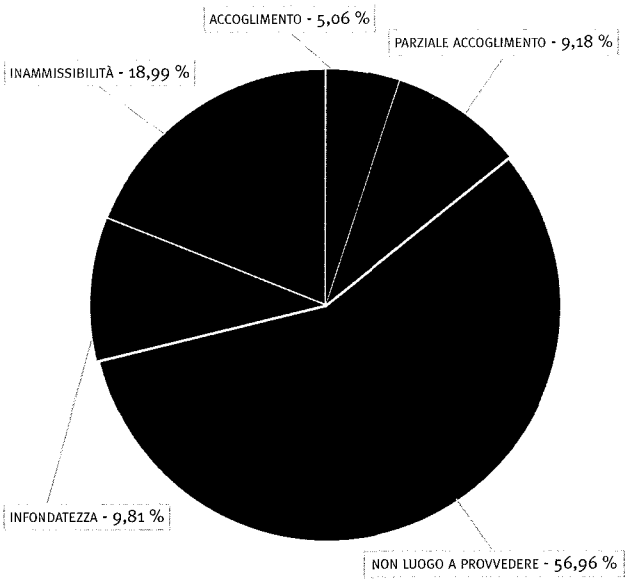
Altre attività dell'Autorità	
Comunicati stampa	47
Newsletter	14
Cd-rom (edizioni pubblicate)	1
Volumi pubblicati	1
Notiziario bimestrale	6
Depliant	1
Presenze internazionali e comunitarie in comitati e gruppi di lavoro	56
Conferenze internazionali	5

(*) Tutti i dati statistici riportati nella presente sezione sono riferiti all'anno solare 2007. Singole note indicano altri periodi o situazioni e casi specifici. I dati di cui alle tabelle 8, 9 e 10 si riferiscono ai fascicoli istituiti presso l'Ufficio

(1) Escluse deliberazioni di rilievo interno sull'attività dell'Autorità e sull'organizzazione e il funzionamento dell'Ufficio

3. Tipologia delle decisioni su ricorsi (tabella e grafico)

Decisioni su ricorsi	
tipi di decisione [1]	**numero ricorsi**
Accoglimento	16
Parziale accoglimento	29
Non luogo a provvedere [2]	180
Infondatezza	31
Inammissibilità	60
Totale	316

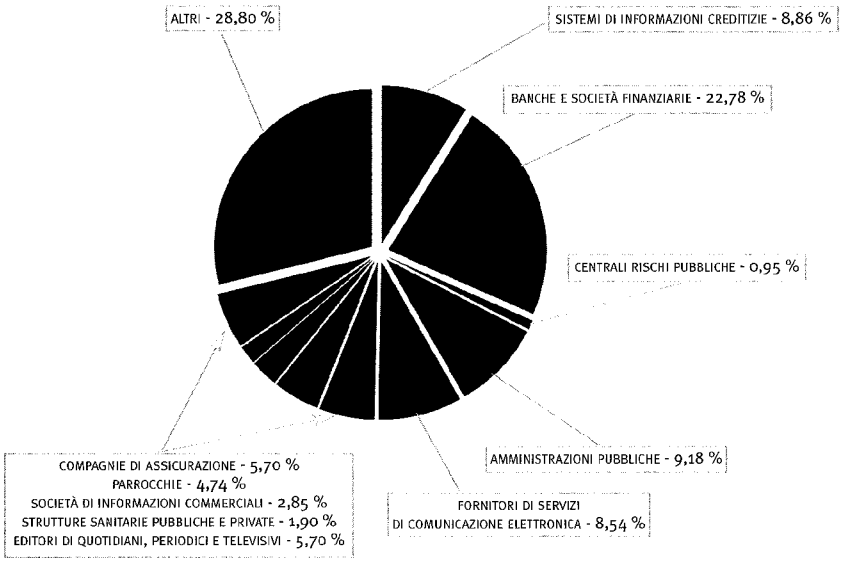


(1) Le decisioni sui ricorsi possono contenere più situazioni in base alle diverse richieste presentate: la statistica prende in esame, in tali casi, la statuizione più "favorevole" per il ricorrente

(2) Casi nei quali le richieste del ricorrente sono state soddisfatte nel corso del procedimento

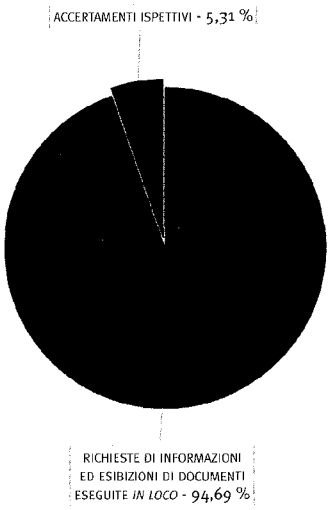
4. Suddivisione dei ricorsi in relazione alla categorie di titolari del trattamento (tabella e grafico)

Categorie di titolari	Numero ricorsi
Sistemi di informazioni creditizie	28
Banche e società finanziarie	72
Centrali rischi pubbliche	3
Amministrazioni pubbliche	29
Fornitori di servizi di comunicazione elettronica	27
Compagnie di assicurazione	18
Parrocchie	15
Società di informazioni commerciali	9
Strutture sanitarie pubbliche e private	6
Editori di quotidiani, periodici e televisivi	18
Altri	91
Totale	**316**



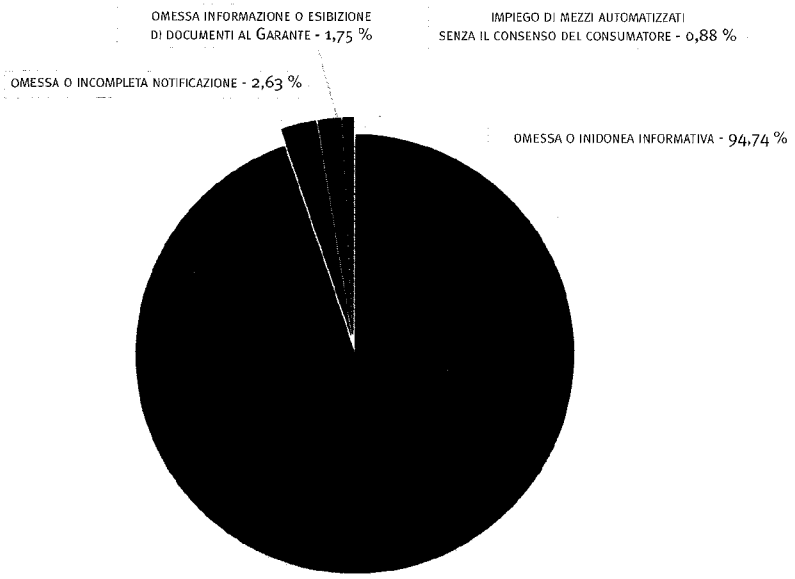
5. Accertamenti e controlli eseguiti (tabella e grafico)

Accertamenti e controlli eseguiti direttamente presso titolari del trattamento		
Richieste di informazioni ed esibizioni di documenti, eseguite *in loco* (art. 157 del Codice)		428
Accertamenti ispettivi (art. 158 del Codice)		24
	Totale	**452**



6. Violazioni amministrative contestate (tabella e grafico)

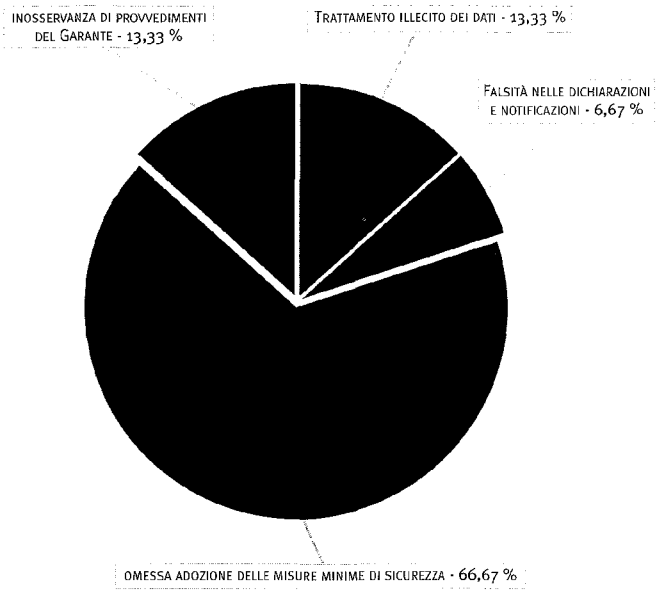
Violazioni amministrative contestate		
Omessa o inidonea informativa (art. 161 del Codice)		216
Omessa o incompleta notificazione (art. 163 del Codice)		6
Omessa informazione o esibizione di documenti al Garante (art. 164 del Codice)		4
Impiego di mezzi automatizzati senza il consenso del consumatore (art. 62 del Codice del consumo)		2
	Totale	**228**
Proventi riscossi a titolo di pagamento in misura ridotta (in euro)		**814.625**



7. Violazioni penali segnalate all'autorità giudiziaria (tabella e grafico)

Violazioni penali segnalate all'autorità giudiziaria

		segnalazioni	persone segnalate
Trattamento illecito dei dati (art. 167 del Codice)		2	2
Falsità nelle dichiarazioni e notificazioni (art. 168 del Codice)		1	1
Omessa adozione delle misure di sicurezza (art. 169 del Codice)		10	15
Inosservanza di provvedimento del Garante (art. 170 del Codice)		2	2
	Totale	**15**	**20**
Ammontare complessivo in euro delle somme riscosse in sede di "ravvedimento operoso" (art. 169 del Codice)			**185.329**



8. Pareri

Pareri (art. 154, comma 4, del Codice)

temi	riscontri resi nell'anno[1]
Giustizia	2
Informatizzazione e banche dati della p.a.	8
Informazione	1
Minori	2
Pubblica amministrazione	1
Sanità	1
Università	1
Totale	**16**

9. Quesiti

Quesiti

temi	pervenuti nell'anno	riscontri resi nell'anno [1]
Albi ed elenchi pubblici	11	4
Anagrafe e stato civile	15	11
Carte identificative, codice fiscale e numeri di identificazione personale	6	5
Dati (e fascicoli) personali di dipendenti	43	33
Giornalismo (cronache giudiziarie)	2	2
Giornalismo (minori)	1	2
Giornalismo (pubblicazioni occasionali)	4	3
Giornalismo (trasmissioni radiofoniche e televisive)	2	1
Giornalismo (altre questioni)	2	3
Giustizia (accertamenti di polizia)	1	---
Giustizia (casellario giudiziario e carichi pendenti)	1	1
Giustizia (modalità per notifiche e comunicazioni)	1	3
Giustizia (prove nel processo)	---	2
Giustizia (pubblicità dei provvedimenti)	1	1
Giustizia (raccolta di dati per finalità di difesa)	7	7
Giustizia (altre questioni)	8	3
Indicatori di condizioni economiche	1	1
Informatizzazione della p.a.	1	---
Internet (foto in Internet)	1	2
Internet (altre questioni)	13	18
Internet (*newsgroup*)	---	1
Internet (*spamming*)	---	1
Lavoro (controlli difensivi del datore di lavoro)	1	---
Lavoro (controlli sul lavoro)	3	4
Liste elettorali	8	16
Notificazioni in busta aperta	---	4
Polizia municipale	4	4
Pubblicità esiti scolastici	2	2

(segue)

(1) Inerenti anche ad affari pervenuti anteriormente al 2007

(segue)

Raccolte dati in ambito assicurativo e banca dati Isvap	---	1
Registro dei protesti	3	---
Ricerca genetica e genealogica	1	1
Rilevazioni biometriche	14	11
Riservatezza della corrispondenza	---	1
Sanità (cartelle cliniche)	2	2
Sanità (certificazioni di invalidità)	11	7
Sanità (certificazioni mediche)	3	1
Sanità (*Hiv*)	3	3
Sanità (monitoraggi sanitari)	3	4
Sanità (altre questioni)	21	10
Servizi di assistenza sociale	3	---
Sistemi informativi creditizi	18	16
Telefonia (chiamate di disturbo)	3	2
Telefonia (elenchi telefonici)	3	4
Telefonia (fatturazione dettagliata)	1	1
Telefonia (localizzazione)	3	---
Telefonia (*Sms* istituzionali)	---	1
Telefonia (altre questioni)	8	5
Test di maternità e paternità	1	1
Trasparenza (attività organi collegiali)	21	12
Trasparenza (legge n. 241/1990)	4	7
Trasparenza (altre questioni)	28	24
Trasporti pubblici	1	---
Tributi banche dati fiscali	1	2
Tributi (canone Rai)	1	3
Tributi (contenuto dichiarazione dei redditi)	4	1
Tributi (altre questioni)	2	---
Uffici tributi locali	1	---
Videosorveglianza (finalità di monitoraggio e controllo del traffico)	2	2
Videosorveglianza (finalità di prevenzione e repressione illeciti)	12	7
Videosorveglianza (finalità di rispetto disposizioni smaltimento rifiuti)	1	1
Videosorveglianza (finalità di sicurezza pubblica)	7	10
Videosorveglianza (da parte di privati)	20	11
Zone a traffico limitato e parcheggi riservati	1	2
Altro	121	198
Totale	**467**	**485**

10. Segnalazioni/Reclami

Segnalazioni e Reclami

temi	pervenuti nell'anno	riscontri resi nell'anno [1]
Albi ed elenchi pubblici	5	9
Anagrafe e stato civile	4	2
Carte identificative, codice fiscale e numeri di identificazione personale	17	10
Dati (e fascicoli) personali di dipendenti	142	72
Gas	1	1
Giornalismo (cronache giudiziarie)	3	5
Giornalismo (dati contenuti in sentenze)	4	2
Giornalismo (foto segnaletiche e di persone arrestate)	1	---

(1) Inerenti anche ad affari pervenuti anteriormente al 2007

(segue)

(segue)

Giornalismo(minori)	17	11
Giornalismo (pubblicazioni occasionali)	4	5
Giornalismo (trasmissioni radiofoniche e televisive)	38	28
Giornalismo (vittime di reato)	1	2
Giornalismo (altre questioni)	71	57
Giustizia (accertamenti di polizia)	5	4
Giustizia (archivi di polizia)	2	2
Giustizia (indagini del pubblico ministero)	4	3
Giustizia (modalità per notifiche e comunicazioni)	12	10
Giustizia (prove nel processo)	1	1
Giustizia (pubblicità dei provvedimenti)	7	2
Giustizia (raccolta dei dati per finalità di difesa)	2	9
Giustizia (altre questioni)	49	41
Indicatori di condizioni economiche	1	3
Internet (*Enum*)	---	1
Internet (foto in Internet)	6	8
Internet (*newsgroup*)	1	3
Internet (*software* spia, *cookies*)	---	2
Internet (*spamming*)	26	36
Internet (altre questioni)	97	112
Lavoro (controlli difensivi del datore di lavoro)	---	1
Lavoro (controlli sul lavoro)	17	17
Liste elettorali	1	3
Licenze e autorizzazioni	---	1
Mense e trasporti	1	1
Notificazione in busta aperta	1	4
Polizia municipale	21	6
Pubblicità esiti scolastici	3	3
Recapito pubblicità non gradita	75	62
Registro dei protesti	6	11
Rilevazioni biometriche	10	7
Riservatezza della corrispondenza	29	20
Sanità (cartelle cliniche)	12	17
Sanità (certificazioni di invalidità)	14	3
Sanità (certificazioni mediche)	9	9
Sanità (Hiv)	1	---
Sanità (monitoraggi sanitari)	---	1
Sanità (servizi di assistenza sociale)	12	3
Sanità (altre questioni)	53	22
Sistemi informazioni creditizie	458	377
Smaltimento rifiuti	6	3
Telefonia (chiamate di disturbo)	111	70
Telefonia (collegamenti a numerazioni con prefisso 709)	7	6
Telefonia (elenchi telefonici)	52	51
Telefonia (errata ricarica schede telefoniche)	1	2

(segue)

(segue)

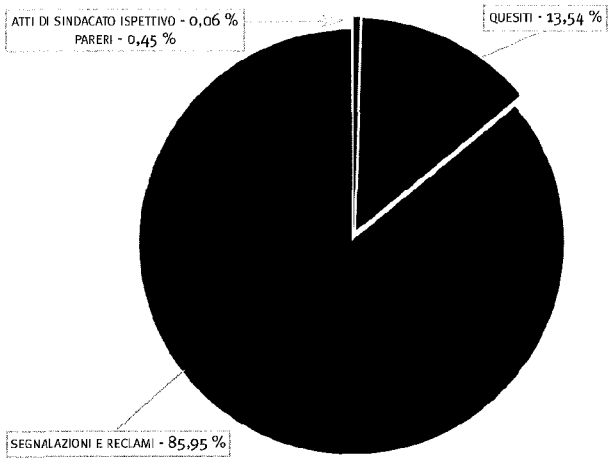
Telefonia (fatturazione dettagliata)	12	40
Telefonia (*fax* indesiderati)	37	15
Telefonia (localizzazione geografica)	---	1
Telefonia (numeri riservati)	3	29
Telefonia (servizi non richiesti)	179	192
Telefonia (*Sms* anonimi)	3	1
Telefonia (*Sms* istituzionali)	---	1
Telefonia (*Sms* pubblicitari)	26	21
Telefonia (altre questioni)	456	393
Test di maternità e paternità	2	1
Trasparenza (attività organi collegiali)	2	---
Trasparenza (legge n. 241/1990)	5	3
Trasparenza (altre questioni)	18	8
Trasporti pubblici	1	1
Tributi banche dati fiscali	1	---
Tributi (canone Rai)	30	246
Tributi (contenuti delle dichiarazioni dei redditi)	6	---
Tributi (altre questioni)	16	7
Uffici (tributi locali)	10	6
Videosorveglianza (finalità di monitoraggio e controllo del traffico)	3	---
Videosorveglianza (finalità di prevenzione e repressione illeciti)	20	6
Videosorveglianza (finalità di sicurezza pubblica)	6	1
Videosorveglianza (da parte di privati)	68	30
Videosorveglianza (altre questioni)	---	2
Altro	759	933
Totale	**3.084**	**3.078**

11. Atti di sindacato ispettivo e controllo

Atti di sindacato ispettivo e controllo

temi	pervenuti nell'anno	riscontri resi nell'anno
Internet (*spamming*)	1	1
Diritto d'autore	1	1
Totale	**2**	**2**

12. Tipologie dei riscontri resi a interessati e richiedenti

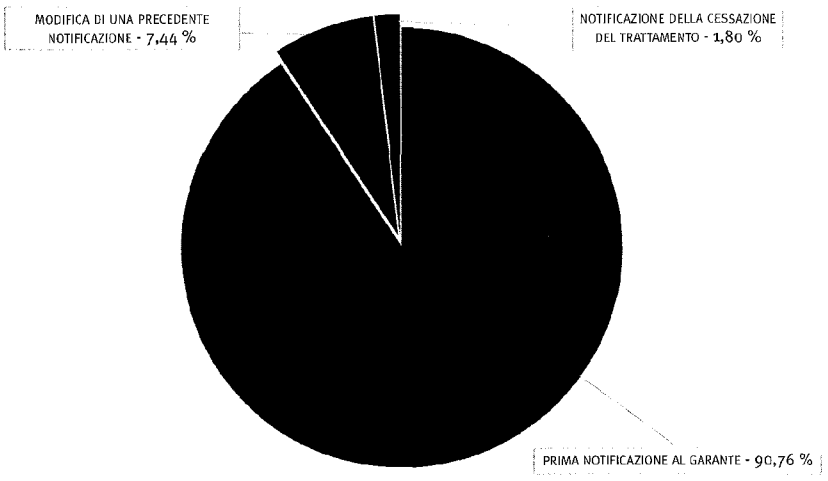


tipologia	da soggetti pubblici	da soggetti privati	totale pervenute [1]
Prima notificazione al Garante	32	566	598
Modifica di una precedente notificazione	13	292	305
Notificazione della cessazione del trattamento	6	69	75
Totale notificazioni[1]	**51**	**927**	**978**

13. Tipologie di notificazioni pervenute nel 2007

tipologia	da soggetti pubblici	da soggetti privati	totale pervenute [1]
Prima notificazione al Garante	977	12.878	13.855
Modifica di una precedente notificazione	43	1.093	1.136
Notificazione della cessazione del trattamento	26	249	275
Totale notificazioni [1]	**1.046**	**14.220**	**15.266**

14. Tipologie di notificazioni pervenute 2004-2007 (tabella e grafico)

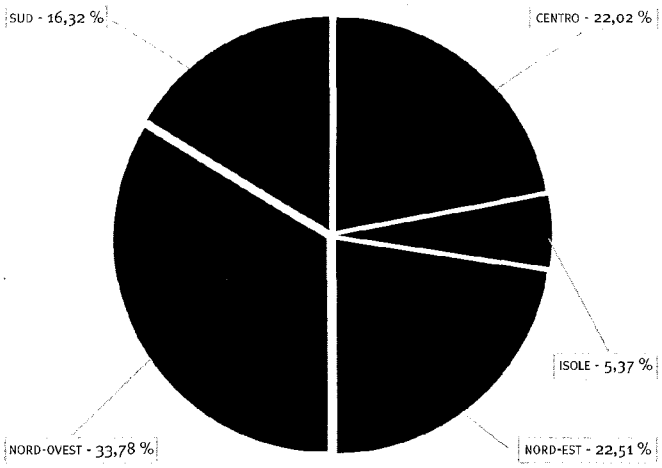


(1) Situazione alla data del 31 dicembre 2007

15. Provenienza geografica delle notificazioni 2004-2007 (tabella e grafico)

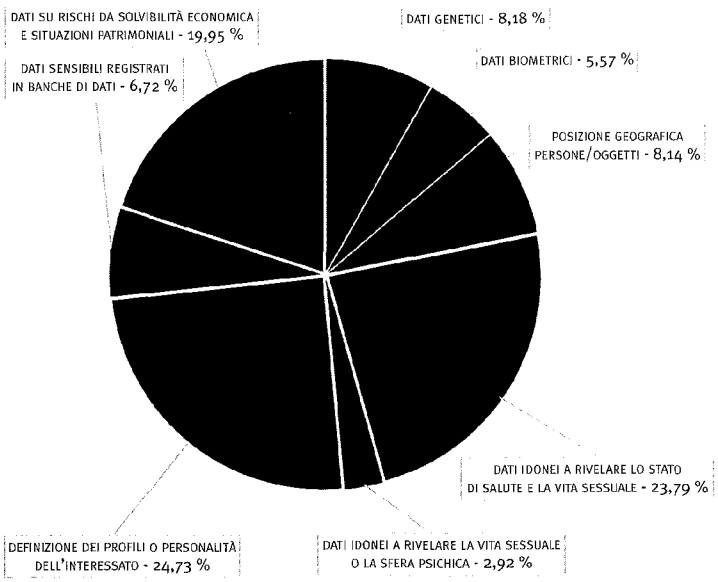
Italia

zone geografiche		pervenute
Centro		3.351
Isole		818
Nord-Est		3.426
Nord-Ovest		5.142
Sud		2.484
	Totale	**15.221**
Da altri Paesi		45



16. Suddivisione delle notificazioni per tipologia di trattamento svolto 2004-2007 (tabella e grafico)

Tabelle di notificazione compilate [1]	
Tabella 1 - Trattamento di dati genetici	1.842
Tabella 2 - Trattamento di dati biometrici	1.254
Tabella 3 - Trattamento di dati che indicano la posizione geografica di persone od oggetti mediante una rete di comunicazione elettronica	1.833
Tabella 4 - Trattamento di dati idonei a rivelare lo stato di salute e la vita sessuale, trattati a fini di procreazione assistita, prestazione di servizi sanitari per via telematica relativi a banche di dati o alla fornitura di beni, indagini epidemiologiche, rilevazione di malattie mentali, infettive e diffusive, sieropositività, trapianto di organi e tessuti e monitoraggio della spesa sanitaria	5.358
Tabella 5 - Trattamento di 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	658
Tabella 6 - Trattamento effettuato 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 l'esclusione dei trattamenti tecnicamente indispensabili per fornire i servizi medesimi	5.569
Tabella 7 - Trattamento di 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	1.514
Tabella 8 - Trattamento di 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	4.494
Totale	**22.522**



(1) Situazione alla data del 31 dicembre 2007

17. Modalità di inoltro delle notificazioni 2004-2007

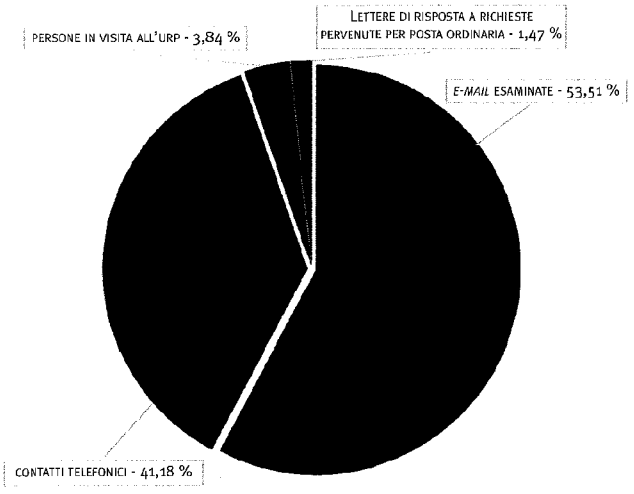
Modalità di inoltro delle notificazioni	Numero
Attraverso intermediari	8.278
Direttamente a cura dei titolari	6.988
Totale	**15.266**

18. Modalità di versamento utilizzate nel 2007

Modalità di versamento utilizzate		
tipo movimento	numero	totale euro
Versamento mediante bollettino postale	366	54.900
Versamento mediante bonifico bancario	325	48.750
Versamento mediante carta di credito	287	43.050
Totale	**978**	**146.700**

19. Prospetto delle attività dell'Ufficio relazioni con il pubblico 2006-2007 (tabella e grafico)

Ufficio relazioni con il pubblico	2006	2007	Totale
E-mail esaminate	19.500	24.419	**43.919**
Contatti telefonici	18.200	15.600	**33.800**
Persone in visita all'Urp	1.600	1.550	**3.150**
Lettere di risposta a richieste pervenute per posta ordinaria	520	689	**1.209**
Totale	**39.820**	**42.258**	**82.078**



20. Organico del Garante

Posti previsti in organico	
area	unità di personale
Segretario generale	1
Dirigenti	28
Funzionari	65
Operativi	30
Esecutivi	1
Totale	**125**
Personale a contratto	20

21. Personale in servizio presso il Garante

Personale in servizio[1]				
area	in ruolo (a)	collocato fuori ruolo (b)	comandato presso altre amministrazioni o in aspettativa (c)	impiegato dall'Ufficio (a+b-c)
Segretario generale		1		1
Dirigenti	16	3	2	17
Funzionari	47		1	46
Operativi	22	1		23
Esecutivi				0
Totali	**85**	**5**	**3**	**87**
A contratto				13

22. Risorse finanziarie

anno	trasferimenti da parte dello Stato		somme riscosse compreso il contributo dello Stato		somme pagate	
	lire	euro	lire	euro	lire	euro
1997	8.029.000.000	4.146.632,44	8.029.000.000	4.146.632,44	1.372.350.430	708.759,85
1998	12.045.000.000	6.220.723,35	12.045.000.000	6.220.723,35	5.491.467.960	2.836.106,51
1999	22.045.000.000	11.385.292,34	27.045.000.000	13.967.576,84	8.725.548.850	4.506.369,90
2000	22.045.000.000	11.385.292,34	22.293.735.850	11.513.753,69	14.235.888.830	7.352.223,00
2001	22.000.000.000	11.362.051,78	24.285.004.432	12.542.158,08	20.019.011.761	10.338.956,74
2002		10.849.996,00		12.186.883,99		11.510.285,48
2003		10.252.000,00		11.244.455,31		13.102.960,92
2004		9.618.000,00		12.694.621,09		12.618.901,26
2005		9.540.653,00		11.011.616,26		15.603.768,31
2006		19.600.000,00		20.992.331,75		16.609.468,51
2007		18.777.293,72		20.755.332,73		16.709.733,45

(1) Situazione alla data del 31 dicembre 2007

Documentazione

Provvedimenti del Garante

Regolamenti e provvedimenti generali

24 Regolamento concernente le procedure interne all'Autorità aventi rilevanza esterna, finalizzate allo svolgimento dei compiti demandati al Garante per la protezione dei dati personali (*) *(reg. n. 1/2007 del 14 dicembre 2007)*

Registro delle deliberazioni
n. 65 del 14 dicembre 2007

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Nella riunione odierna, in presenza del prof. Francesco Pizzetti, presidente, del dott. Giuseppe Chiaravalloti, vice presidente, del dott. Mauro Paissan e del dott. Giuseppe Fortunato, componenti e del dott. Giovanni Buttarelli, segretario generale;

Visto l'articolo 156, comma 3, lett. *a)* del Codice in materia di protezione dei dati personali (d.lg. 30 giugno 2003, n. 196), ai sensi del quale il Garante, con propri regolamenti pubblicati nella Gazzetta Ufficiale della Repubblica italiana, definisce l'organizzazione e il funzionamento dell'Ufficio, anche ai fini dello svolgimento dei compiti assegnati al Garante dall'articolo 154 del medesimo Codice;

Considerato che fra tali compiti figurano, tra l'altro, quelli di controllare se i trattamenti di dati personali sono effettuati nel rispetto della disciplina applicabile, di esaminare i reclami e le segnalazioni e di provvedere sui ricorsi presentati dagli interessati, di prescrivere anche d'ufficio ai titolari del trattamento le misure necessarie o opportune al fine di rendere il trattamento conforme alle disposizioni vigenti, di vietare anche d'ufficio, in tutto o in parte, il trattamento illecito o non corretto dei dati o di disporne il blocco, nonché di adottare gli altri provvedimenti previsti dalla disciplina applicabile al trattamento dei dati personali (art. 154 del Codice);

Rilevato che il Codice disciplina diversi aspetti relativi alla tutela degli interessati dinanzi al Garante, in particolare per quanto riguarda la presentazione di ricorsi, reclami e segnalazioni, di cui sono regolati vari profili concernenti il procedimento e le istruttorie preliminari (artt. 141-151); rilevato che ulteriori disposizioni di legge regolano altri profili relativi ai procedimenti dinanzi al Garante, anche per quanto riguarda gli accertamenti inerenti ai trattamenti da parte di forze di polizia o in ambito giudiziario o di difesa e sicurezza dello Stato (artt. da 46 a 58, 160, 173 e 175 del Codice), la disciplina generale del procedimento

(*) *G.U.* 9 gennaio 2008, n. 7
[doc. *web* n. 1477480]

amministrativo (l. 7 agosto 1990, n. 241 e successive modificazioni) e l'applicazione di sanzioni amministrative (l. 24 novembre 1981, n. 689 e successive modificazioni);

Visto il regolamento del Garante n. 1/2000 sull'organizzazione e il funzionamento dell'Ufficio del Garante (deliberazione 28 giugno 2000, n. 15, in *G.U.* 13 luglio 2000, n. 162) e, in particolare, il Capo III, relativo ai princìpi di trasparenza, partecipazione e contraddittorio cui si ispira l'attività dell'ufficio del Garante, all'assegnazione degli affari ai relativi dipartimenti e servizi, all'individuazione del responsabile del procedimento e alle funzioni del relatore quando si provvede con deliberazione del Garante;

Rilevata la necessità, dopo l'entrata in vigore del Codice e sulla base dell'esperienza acquisita, di consolidare l'attuazione delle disposizioni di legge sullo svolgimento dei compiti demandati all'Autorità e sull'organizzazione e il funzionamento dell'ufficio, con un atto regolamentare del Garante da adottare in base al predetto articolo 156, comma 3, lett. *a*); rilevata l'esigenza, in tale contesto, di specificare e rendere note le procedure interne all'Autorità aventi rilevanza esterna, in particolare per quanto riguarda quelle funzionali alla tutela degli interessati, avviate d'ufficio o su loro istanza, nonché l'esame di comunicazioni, richieste e notificazioni inoltrate all'Autorità dai titolari del trattamento; rilevata, altresì, l'esigenza di verificare la perdurante attualità e la persistenza dei presupposti per adottare provvedimenti in ordine a fatti oggetto di segnalazioni e reclami pervenuti all'Autorità in epoca antecedente all'insediamento dell'attuale collegio;

Visti gli atti d'ufficio;

Viste le proposte e le osservazioni dell'Ufficio formulate dal segretario generale ai sensi dell'art. 15, comma 1 del predetto regolamento n. 1/2000;

Relatore il prof. Francesco Pizzetti;

DELIBERA

è adottato il regolamento n. 1/2007 concernente le procedure interne all'Autorità aventi rilevanza esterna, finalizzate allo svolgimento dei compiti demandati al Garante per la protezione dei dati personali. Il regolamento è riportato in allegato alla presente deliberazione, di cui costituisce parte integrante, e ne è disposta la pubblicazione nella *Gazzetta Ufficiale* della Repubblica italiana, ai sensi dell'articolo 156, comma 3, lett. *a*), del Codice in materia di protezione dei dati personali.

Roma, 14 dicembre 2007

IL PRESIDENTE
Pizzetti

IL RELATORE
Pizzetti

IL SEGRETARIO GENERALE
Buttarelli

ALLEGATO

Regolamento concernente le procedure interne all'Autorità aventi rilevanza esterna, finalizzate allo svolgimento dei compiti demandati al Garante per la protezione dei dati personali. (artt. 154 e 156 d.lg. 30 giugno 2003, n. 196)

CAPO I - DISPOSIZIONI GENERALI

Art. 1 - Definizioni

1. Ai fini del presente regolamento si applicano le definizioni contenute nell'art. 4 del Codice in materia di protezione dei dati personali, approvato con d.lg. 30 giugno 2003, n. 196, di seguito denominato "Codice".

Art. 2 - Oggetto del regolamento

1. Il presente regolamento disciplina le procedure interne all'Autorità aventi rilevanza esterna, avviate su istanza di parte o d'ufficio e finalizzate allo svolgimento dei compiti demandati al Garante.

Art. 3 - Princìpi generali

1. Nell'esercizio dei compiti demandati al Garante dalla normativa vigente e dalla disciplina comunque rilevante in materia di trattamento dei dati personali, in particolare per quanto riguarda il controllo sulla liceità e correttezza dei trattamenti, l'Autorità ispira la propria azione a princìpi di trasparenza, ragionevolezza, proporzionalità e non discriminazione, realizzando l'interesse pubblico connesso a ciascuna attività secondo criteri di buona amministrazione, economicità e adeguatezza e valorizzando l'utilizzo di tecniche informatiche e della telematica. A tal fine, si tiene conto anche della natura e della gravità degli illeciti da accertare in rapporto ai relativi effetti e all'entità del pregiudizio che essi possono comportare per uno o più interessati, della probabilità di comprovarne la sussistenza, nonché dell'impiego di risorse al tal fine necessario in rapporto anche alle entrate disponibili in base al bilancio di previsione.

Art. 4 - Programmazione

1. Il Garante, in applicazione dei princìpi e criteri di cui all'articolo 3, e ai sensi dell'articolo 2, comma 1, lett. *a*) e *c*), del proprio regolamento n. 1/2000, determina e aggiorna periodicamente con cadenza almeno semestrale:

a) la programmazione dei lavori del collegio;

b) le linee di priorità nell'esame di reclami e segnalazioni da parte dell'ufficio;

c) la programmazione delle attività ispettive.

Art. 5 - Qualificazione e trattazione degli affari

1. Nell'assegnare gli affari al dipartimento, servizio o altra unità organizzativa competente ai sensi dell'articolo 14 del regolamento del Garante n. 1/2000, il segretario generale ne qualifica allo stato degli atti la natura, individuando in particolare se si tratta di ricorsi, reclami, segnalazioni, richieste di parere o quesiti.

2. Il dirigente del dipartimento, servizio o altra unità organizzativa di primo livello cui è assegnato l'affare può qualificarlo diversamente a seguito della sua trattazione dandone comunicazione al segretario generale; può anche segnalare a quest'ultimo, anche per l'esigenza di una diversa qualificazione dell'affare, l'opportunità di una sua riassegnazione ad un diverso dipartimento, servizio o altra unità organizzativa.

3. Le assegnazioni e la qualificazione data agli affari sono annotate e aggiornate costantemente nel sistema informativo dell'Autorità.

4. Il dipartimento, servizio o altra unità organizzativa tratta l'affare assegnato rispettando quanto previsto dalla normativa vigente, dal presente regolamento e da altri regolamenti approvati dal Garante. Il relativo dirigente dà tempestiva notizia dell'eventuale mancato rispetto dei termini previsti, in particolare, per l'istruttoria preliminare o per il procedimento amministrativo al segretario generale, il quale impartisce disposizioni e può sostituirsi nella trattazione ai sensi dell'art. 7 del regolamento n. 1/2000. Il segretario generale è informato altresì riguardo alle segnalazioni per le quali è disposta la messa agli atti ai sensi dell'art. 13, comma 4, o non è avviata l'istruttoria preliminare in conformità all'art. 14, comma 1, anche ai fini della menzione di tali casi nelle informative al collegio di cui all'art. 19.

Art. 6 - Eventuale avvio di un procedimento amministrativo e relativo responsabile

1. Il dirigente, anche su proposta del funzionario cui assegna l'affare, avvia un procedimento amministrativo nei casi in cui d'ufficio o sulla base di un'istanza, e in conformità al presente regolamento, ciò è necessario ai sensi della normativa vigente, e cura che si proceda agli atti, alle comunicazioni e agli adempimenti previsti nel medesimo procedimento.

2. Il responsabile del procedimento amministrativo avviato ai sensi del comma 1 è il dirigente o funzionario preposto all'unità organizzativa cui è assegnato l'affare, oppure il funzionario da essi incaricato di trattarlo, il quale cura gli atti, le comunicazioni e gli adempimenti di cui al comma 1 anche ai sensi dell'art. 14, comma 3, del regolamento n. 1/2000.

CAPO II - PROCEDURE CONCERNENTI LA TUTELA DINANZI AL GARANTE

SEZIONE I - RICORSI

Art. 7 - Procedimento

1. Il responsabile del procedimento amministrativo relativo a un ricorso che non deve essere regolarizzato procede nei modi di cui agli articoli 148, 149 e 150 del Codice e, quando il ricorso non è dichiarato inammissibile o manifestamente infondato, cura l'inoltro al titolare del trattamento dell'invito di cui al medesimo articolo 149, comma 1, con il quale si comunica anche l'avvio del procedimento.

2. Concluso il procedimento, dopo aver inoltrato alle parti il provvedimento del collegio di cui all'articolo 150, comma 2, del Codice, il responsabile del procedimento verifica preliminarmente se l'eventuale adempimento che deriva a carico del titolare del trattamento dal medesimo provvedimento risulta effettuato correttamente, promuovendo ove necessario le verifiche a tal fine opportune; cura, su richiesta, l'apposizione su una copia del provvedimento della formula esecutiva relativa alle spese e ai diritti del procedimento, nonché la riassegnazione dell'affare al dipartimento, servizio o altra unità organizzativa quando al provvedimento del collegio può conseguire l'avvio di un'autonoma istruttoria preliminare o di un autonomo procedimento amministrativo.

3. Nei casi di cui all'articolo 150, comma 5, del Codice, quando le difficoltà o le contestazioni sorte riguardo all'esecuzione del provvedimento non sono risolvibili agevolmente, il responsabile del procedimento predispone lo schema dell'ulteriore provvedimento del collegio.

SEZIONE II - RECLAMI

Art. 8 - Reclami

1. Sono qualificabili come reclami gli atti che indicano specificamente, anche sulla base del modello appositamente predisposto dall'Autorità, gli elementi previsti dall'articolo 142, commi 1 e 2, del Codice.

2. Il Garante determina, in via generale, con propria deliberazione, i casi in cui è possibile la regolarizzazione del reclamo.

3. Il reclamo che non contiene gli elementi di cui al comma 1, o che non è regolarizzato, può essere esaminato a titolo di segnalazione.

Art. 9 - Trattazione del reclamo

1. L'esame del reclamo, nel corso dell'istruttoria preliminare e del successivo procedimento amministrativo eventualmente avviato ai sensi dell'art. 2 della l. 7 agosto 1990, n. 241, e successive modificazioni, nonché dell'art. 6, comma 1, è orientato a criteri di semplicità delle forme osservate, speditezza ed economicità, anche in riferimento al contraddittorio.

Art. 10 - Istruttoria preliminare

1. Il reclamo regolarmente presentato è esaminato dall'Autorità, ma non comporta la necessaria adozione di un provvedimento del collegio ai sensi dell'art. 143, comma 1, del Codice.

2. Il dipartimento, servizio o altra unità organizzativa cui il reclamo è assegnato avvia un'istruttoria preliminare entro tre mesi dalla data del suo ricevimento da parte della competente unità organizzativa, fermo restando quanto previsto dall'articolo 8.

3. Il dipartimento, servizio o altra unità organizzativa verifica, con un esame sommario, se sussistono idonei elementi in ordine alle presunte violazioni e alle misure richieste dall'interessato. A tal fine, il dipartimento, servizio o altra unità organizzativa esamina la docu-

mentazione pervenuta e può curare l'acquisizione di precisazioni e informazioni in ordine ai fatti e alle circostanze cui si riferisce il reclamo, di regola mediante richiesta di elementi sottoscritta dal dirigente competente ovvero, nei casi in cui risulta necessario, mediante richiesta di informazioni o di esibizione di documenti ai sensi dell'articolo 157 del Codice sottoscritta dal segretario generale.

4. Al fine di promuovere l'esame organico di questioni che possono rendere opportuna anche l'adozione di un eventuale provvedimento di carattere generale, l'istruttoria preliminare può essere svolta contestualmente in relazione a più reclami aventi il medesimo oggetto o che riguardano il medesimo titolare o responsabile del trattamento, oppure trattamenti di dati tra loro correlati.

Art. 11 - Chiusura dell'istruttoria preliminare

1. Al termine dell'istruttoria preliminare, che deve essere completata entro sei mesi dalla presentazione o avvenuta regolarizzazione del reclamo, ovvero entro nove mesi nei casi complessi che richiedono approfondimenti per motivate esigenze, il dipartimento, servizio o altra unità organizzativa conclude l'esame del reclamo senza promuovere l'adozione di un provvedimento del collegio ai sensi dell'art. 143, comma 1, del Codice, quando:

a) la questione prospettata con il reclamo non è riconducibile alla protezione dei dati personali o ai compiti demandati all'Autorità;

b) non sono ravvisati, allo stato degli atti, gli estremi di una violazione della disciplina rilevante in materia di protezione dei dati personali o, comunque, per promuovere l'adozione del predetto provvedimento del collegio;

c) la questione prospettata con il reclamo è stata già esaminata dall'Autorità in particolare con un provvedimento collegiale di carattere generale, o può essere esaminata richiamando provvedimenti o questioni già affrontate dal Garante, oppure esprimendo un prudente avviso su questioni che non presentano particolare rilevanza sul piano generale;

d) pur essendo riscontrata una condotta non conforme alla disciplina applicabile, non sono ravvisati i presupposti per adottare, allo stato degli atti, un provvedimento prescrittivo o inibitorio del collegio, in particolare quando la condotta è particolarmente risalente nel tempo o ha esaurito i suoi effetti, oppure quando tali effetti sono stati rimossi o sono state fornite idonee assicurazioni da parte del titolare del trattamento.

2. Nei casi di cui al comma 1 al proponente è fornito comunque un riscontro indicando succintamente le ragioni per le quali, ai sensi del medesimo comma, non è promossa l'adozione di un provvedimento del collegio.

3. Quando l'esame del reclamo non si conclude ai sensi del comma 1, il dipartimento, servizio o altra unità organizzativa, al termine dell'istruttoria preliminare, avvia il procedimento amministrativo funzionale all'adozione di un provvedimento collegiale, comunicandone alle parti l'avvio in conformità alla legge e ai regolamenti.

4. Delle determinazioni di cui ai commi 1 e 2 è informato il collegio nei modi di cui all'art. 19.

Art. 12 - Procedimento amministrativo conseguente al reclamo

1. Il responsabile del procedimento amministrativo cura gli accertamenti necessari per la decisione sul reclamo e garantisce la partecipazione delle parti al procedimento, se del caso sentendo personalmente o a mezzo di procuratore speciale l'interessato, il titolare o il responsabile del trattamento i quali possono comunque presentare memorie e documenti; può curare, altresì, l'invio di un invito ad eseguire spontaneamente le misure richieste con il reclamo, procedendo secondo le forme di cui al comma 1 dell'articolo 149 del Codice.

2. Il responsabile del procedimento procede, in riferimento alle formalità da osservare, nel rispetto delle disposizioni della l. 7 agosto 1990, n. 241, e successive modificazioni, con particolare riguardo agli avvisi alle parti, a comunicazioni interlocutorie previste e al diritto di visione degli atti.

3. Il termine previsto per concludere il procedimento amministrativo può essere sospeso per un periodo non superiore a centoventi giorni nei casi particolarmente complessi, o in relazione a eventuali accertamenti ispettivi, oppure in caso di riunione di procedimenti ai sensi del comma 5.

4. Al termine del procedimento amministrativo, il responsabile cura che l'esame del reclamo sia concluso nei modi di cui all'articolo 11, comma 1, quando nuovi elementi

sopravvenuti nel corso del medesimo procedimento evidenziano, parimenti, la manifesta infondatezza del reclamo o la certa insussistenza dei presupposti per adottare un provvedimento del collegio.

5. L'eventuale riunione o separazione di procedimenti è disposta dal dirigente del dipartimento, servizio o unità organizzativa, anche su proposta del responsabile del procedimento, in relazione a reclami aventi o meno il medesimo oggetto o che riguardano o meno il medesimo titolare o responsabile del trattamento, oppure trattamenti di dati tra loro direttamente correlati. Per i procedimenti di pertinenza di più unità organizzative, la riunione o separazione è disposta dal segretario generale. La riunione o separazione è comunicata al relatore se già designato.

6. Fuori dei casi di cui al comma 4, il responsabile del procedimento cura la predisposizione del provvedimento del collegio, di cui risulta redattore, e il dirigente dell'unità organizzativa procede poi nei modi di cui all'articolo 15 del regolamento del Garante n. 1/2000. Il collegio provvede con propria deliberazione nel rispetto di quanto previsto dagli articoli 143 e 154 del Codice, anche quando rileva l'inammissibilità o l'infondatezza del reclamo.

SEZIONE III - SEGNALAZIONI

Art. 13 - Esame delle segnalazioni

1. Sono qualificabili come segnalazioni gli atti che ai sensi dell'articolo 141, comma 1, lett. *b*), del Codice, e in quanto diversi dalle richieste di parere e dai quesiti, non presentano le caratteristiche di cui all'articolo 8, comma 1, e sono volti a sollecitare un controllo da parte del Garante sulla disciplina rilevante in materia di trattamento dei dati personali.

2. La segnalazione è presentata da un interessato identificato. L'Autorità può utilizzare le notizie indicate in eventuali segnalazioni che non provengono da un interessato identificato, qualora ritenga di dover avviare controlli su casi nei quali ravvisa il rischio di seri pregiudizi o di ritorsioni ai danni dell'interessato, oppure ricorre comunque un caso di particolare gravità.

3. La segnalazione è esaminata dall'Autorità, ma non comporta la necessaria adozione di un provvedimento del collegio.

4. Il dipartimento, servizio o altra unità organizzativa può, anche tenuto conto di quanto previsto dall'art. 3, concludere l'esame della segnalazione disponendone la messa agli atti, nonché l'eventuale inoltro ad altro soggetto pubblico competente, quando ricorre manifestamente uno dei presupposti di cui all'articolo 11, comma 1, oppure in caso di segnalazioni del tutto generiche. Si considerano tali le segnalazioni che si limitano a imputare a un soggetto fatti del tutto privi di elementi circostanziati o che non contengono elementi tali da consentire un'agevole individuazione del titolare del trattamento.

5. La trattazione delle segnalazioni non richiede il versamento di diritti di segreteria.

6. Delle determinazioni di cui ai commi 2 e 4 è informato il collegio nei modi di cui all'art. 19.

Art. 14 - Istruttoria preliminare ed eventuale procedimento amministrativo

1. Fermi restando i casi in cui la segnalazione è messa agli atti ai sensi dell'articolo 13, comma 4, il dipartimento, servizio o altra unità organizzativa può avviare un'istruttoria preliminare entro il termine di tre mesi dalla data del suo ricevimento da parte della competente unità organizzativa.

2. Se è avviata un'istruttoria preliminare e nel corso dell'eventuale procedimento amministrativo si osservano le disposizioni per i reclami di cui agli articoli da 9 a 12, anche per quanto riguarda l'informativa al collegio ai sensi dell'art. 19, e al segnalante può essere fornito un riscontro. L'eventuale procedimento è orientato in ogni caso al principio della massima semplificazione anche per ciò che riguarda i rapporti con le parti.

CAPO III - ATTIVITÀ DI CONTROLLO E SANZIONATORIA

Art. 15 - Controlli e provvedimenti adottati senza istanza di parte

1. Nell'esercizio dei compiti di controllo o comunque esercitabili dal Garante anche per legge, l'Autorità, valutati gli elementi in suo possesso e anche in assenza di ricorso, reclamo o segnalazione, può avviare d'ufficio un'istruttoria preliminare per verificare la sussistenza di idonei elementi in ordine a possibili violazioni della disciplina rilevante in materia di protezione dei dati personali.

2. Per l'istruttoria preliminare e nel corso dell'eventuale procedimento amministrativo si osservano le disposizioni di cui agli articoli da 9 a 12 anche per quanto riguarda l'informativa al collegio ai sensi dell'art. 19. L'apertura del procedimento amministrativo è comunicata al collegio preventivamente.

Art. 16 - Attività ispettive e applicazione di sanzioni

1. Il dipartimento attività ispettive e sanzioni cura l'istruttoria preliminare relativa ai controlli *in loco* effettuati d'ufficio ai sensi degli articoli 157 e 158 del Codice nel rispetto della programmazione dell'attività ispettiva disposta dal collegio ai sensi dell'art. 4, comma 1, lett. *c*). Effettuati gli accertamenti relativi agli elementi idonei in ordine alle presunte violazioni, il dipartimento inoltra gli atti al segretario generale per l'assegnazione alla competente unità organizzativa ai sensi dell'art. 14 del regolamento del Garante n. 1/2000, per il seguito di trattazione che concerne profili diversi dall'applicazione di sanzioni per i quali, invece, procede direttamente.

2. Il dipartimento attività ispettive e sanzioni cura, altresì, i controlli ai sensi degli articoli 157 e 158 del Codice nell'ambito delle istruttorie preliminari e dei procedimenti amministrativi comunque avviati presso altre unità organizzative, cui è restituito l'esito per la successiva trattazione.

3. Il dipartimento attività ispettive e sanzioni, quando non cura l'archiviazione degli atti relativi alla presunta violazione amministrativa, predispone la contestazione delle violazioni amministrative di competenza del Garante, in conformità alla legge 24 novembre 1981, n. 689 e successive modificazioni e al relativo termine prescritto.

4. Fuori dei casi in cui sono effettuate dal personale operante in sede di controllo, le violazioni amministrative sono contestate con atto sottoscritto dal dirigente del dipartimento attività ispettive e sanzioni o, nei casi di maggiore gravità o che rendono facoltativo applicare una sanzione accessoria ai sensi dell'articolo 165 del Codice, dal segretario generale.

5. Quando non è effettuato il pagamento in misura ridotta, il dirigente del dipartimento attività ispettive e sanzioni e, rispettivamente, il segretario generale nei casi previsti dal comma 4 dispongono in conformità alla legge l'eventuale archiviazione degli atti a seguito di idonee deduzioni difensive.

6. L'ordinanza-ingiunzione è adottata dal collegio nei casi in cui la contestazione è stata effettuata dal segretario generale e da quest'ultimo nei casi residui.

7. Delle attività svolte ai sensi del presente articolo è informato il collegio anche nei modi di cui all'art. 19.

CAPO IV - ALTRE ATTIVITÀ DELL'AUTORITÀ

Art. 17 - Altri procedimenti

1. Nei casi di cui al comma 2, il responsabile del procedimento valuta la completezza degli elementi istruttori, verifica l'esistenza dei presupposti per le decisioni da parte dell'Autorità e cura la predisposizione del provvedimento del collegio, di cui risulta redattore, in tempo utile per la sua adozione nel termine previsto. Il dirigente dell'unità organizzativa competente procede poi nei modi di cui all'articolo 15 del regolamento del Garante n. 1/2000.

2. Si procede nei modi di cui al comma 1 nei casi in cui il collegio deve provvedere con propria deliberazione, anche d'ufficio, riguardo a:

a) casi di informativa semplificata all'interessato previsti dalla disciplina in materia di protezione dei dati personali;
b) casi di informativa all'interessato che comporterebbe un impiego di mezzi che il Garante dichiari manifestamente sproporzionati o che si riveli impossibile;
c) verifiche preliminari per i trattamenti che presentano rischi specifici;
d) trattamenti consentiti per perseguire un legittimo interesse del titolare o di un terzo;
e) autorizzazioni al trattamento di dati sensibili o giudiziari;
f) altre autorizzazioni, anche relative al trasferimento di dati personali all'estero;
g) trattamenti oggetto di notificazione al Garante;
h) obblighi di comunicazione al Garante da parte di soggetti pubblici;
i) pareri previsti dalla legge;
j) ogni altro caso in cui, fuori dalle ipotesi di cui al Capo II del presente regolamento, è prevista l'adozione di un provvedimento del collegio.

Art. 18 - Quesiti e richieste di parere

1. Con riferimento al compito di curare la conoscenza tra il pubblico della disciplina rilevante in materia di trattamento di dati personali e delle relative finalità, e subordinatamente alle linee di priorità di cui all'articolo 4, comma 1, lett. *b*), il dipartimento, servizio o altra unità organizzativa competente può, anche tenuto conto di quanto previsto dall'art. 3, fornire riscontro a quesiti, oppure a richieste di parere diverse da quelle per le quali provvede il collegio anche ai sensi dell'articolo 154, comma 4, del Codice, quando riguardano questioni di specifico interesse per la protezione dei dati personali o sono posti da interessati che versano in situazioni particolari meritevoli di adeguata considerazione.

2. L'ufficio relazioni con il pubblico, cui sono assegnati gli altri quesiti o richieste di parere cui in base a quanto previsto nel comma 1 non può essere fornita una risposta analitica, informa per quanto possibile i soggetti richiedenti di tale circostanza, o fornisce loro eventuali brevi informazioni anche su iniziative e provvedimenti già assunti dall'Autorità.

Art. 19 - Rapporto informativo sullo stato della trattazione degli affari

1. Il segretario generale cura per il collegio, con cadenza almeno bimestrale e avvalendosi del sistema informativo dell'Autorità, la predisposizione di un rapporto informativo sullo stato degli affari di cui ai capi II, III e IV trattati dalle unità organizzative, indicando le tipologie di determinazioni da esse adottate o in via di adozione nei casi individuati, nonché il relativo oggetto, anche avvalendosi di codici numerici.

CAPO V - DISPOSIZIONI TRANSITORIE E FINALI

Art. 20 - Applicazione del regolamento a trattazioni in corso

1. Le disposizioni di cui alle sezioni II e III del capo II si applicano anche alle segnalazioni e reclami in fase di esame, fuori dei casi di cui all'articolo 21, commi 1 e 4. A tal fine, l'eventuale regolarizzazione di un reclamo ai sensi dell'art. 8, comma 2, può essere effettuata ai sensi della medesima disposizione entro trenta giorni dalla data di pubblicazione del provvedimento di cui al medesimo art. 8, comma 2.

Art. 21 - Trattazione di affari pregressi

1. Entro il termine di sessanta giorni dalla data di entrata in vigore del presente regolamento, i soggetti che dimostrano il loro attuale interesse possono presentare all'Autorità motivata richiesta di trattazione dei reclami e segnalazioni pervenuti entro il 30 aprile 2005.

2. La richiesta di cui al comma 1 non riguarda i reclami e le segnalazioni di cui si è già esaurito l'esame, o di cui l'Autorità ha già esaminato nel corso del 2006 un motivato sollecito o una richiesta di trattazione, o per i quali l'Autorità è a conoscenza, anche a seguito di sua denuncia, che sui fatti oggetto di reclamo o segnalazione è in corso un procedimento penale.

3. Entro quindici giorni dalla data di entrata in vigore del presente regolamento l'Autorità provvede a dare notizia di quanto previsto dai commi 1 e 2 mediante avviso pubblicato nel proprio sito Internet e trasmesso, altresì, all'Ufficio pubblicazioni leggi e decreti del Ministero della giustizia per la sua pubblicazione nella *Gazzetta Ufficiale* della Repubblica italiana.

4. In caso di mancata presentazione di un'idonea richiesta di trattazione ai sensi del comma 1, e salvo quanto previsto dal comma 2, il reclamo o segnalazione è improcedibile.

Art. 22 - Modifica del regolamento n. 1/2000

1. Nell'articolo 14, comma 3, del regolamento del Garante n. 1/2000 approvato con deliberazione 28 giugno 2000, n. 15, sono soppresse le parole: "preliminare e".

Art. 23 - Entrata in vigore

1. Il presente regolamento entra in vigore il quindicesimo giorno successivo a quello della sua pubblicazione nella *Gazzetta Ufficiale* della Repubblica italiana.

25 Regolamento concernente l'individuazione dei termini e delle unità organizzative responsabili dei procedimenti amministrativi presso il Garante per la protezione dei dati personali (*) *(reg. n. 2/2007 del 14 dicembre 2007)*

Registro delle deliberazioni
n. 66 del 14 dicembre 2007

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Nella riunione odierna, in presenza del prof. Francesco Pizzetti, presidente, del dott. Giuseppe Chiaravalloti, vice presidente, del dott. Mauro Paissan e del dott. Giuseppe Fortunato, componenti e del dott. Giovanni Buttarelli, segretario generale;

Visto l'articolo 2, comma 2, della legge 7 agosto 1990, n. 241, e successive modificazioni apportate da ultimo con legge 11 febbraio 2005, n. 15, ai sensi del quale le pubbliche amministrazioni determinano per ciascun tipo di procedimento, in quanto non sia già direttamente disposto per legge o per regolamento, il termine entro cui il procedimento deve concludersi;

Visto l'articolo 4 della medesima legge 7 agosto 1990, n. 241 ai sensi del quale le pubbliche amministrazioni, se non è già stabilito direttamente per legge o per regolamento, determinano per ciascun tipo di procedimento relativo ad atti di loro competenza l'unità organizzativa responsabile del procedimento;

Rilevato che diversi termini di procedimenti amministrativi sono specificamente determinati da norme di legge o di regolamento, anche in materia di contratti pubblici;

Visto l'articolo 156, comma 3, lett. *a*) del Codice in materia di protezione dei dati personali (d.lg. 30 giugno 2003, n. 196), ai sensi del quale il Garante, con propri regolamenti pubblicati nella *Gazzetta Ufficiale* della Repubblica italiana, definisce l'organizzazione e il funzionamento dell'Ufficio anche ai fini dello svolgimento dei compiti previsti dall'articolo 154 del medesimo Codice;

Visto il regolamento del Garante n. 1/2000 sull'organizzazione e il funzionamento dell'Ufficio del Garante (deliberazione 28 giugno 2000, n. 15, in *G.U.* 13 luglio 2000, n. 162) e, in particolare, l'art. 13, comma 2, che prevede l'adozione di disposizioni sulla durata dei procedimenti amministrativi di competenza dell'Autorità;

Vista la ricognizione dei procedimenti di competenza dell'Autorità, delle unità organizzative in cui è articolato l'ufficio del Garante e delle relative competenze;

VISTI gli atti d'ufficio;

Viste le proposte e le osservazioni dell'Ufficio formulate dal segretario generale ai sensi dell'art. 15, comma 1 del predetto regolamento n. 1/2000;

Relatore il prof. Francesco Pizzetti;

(*) *G.U.* 9 gennaio 2008, n. 7
[doc. *web* n. 1477624]

DELIBERA

è adottato il regolamento n. 2/2007, concernente l'individuazione dei termini e delle unità organizzative responsabili dei procedimenti amministrativi presso il Garante per la protezione dei dati personali, riportato in allegato alla presente deliberazione di cui costituisce parte integrante e di cui è disposta la pubblicazione nella *Gazzetta Ufficiale* della Repubblica italiana, ai sensi dell'articolo 156, comma 3, lett. *a*), del Codice in materia di protezione dei dati personali.

Roma, 14 dicembre 2007

IL PRESIDENTE
Pizzetti

IL RELATORE
Pizzetti

IL SEGRETARIO GENERALE
Buttarelli

ALLEGATO

Regolamento concernente l'individuazione dei termini e delle unità organizzative responsabili dei procedimenti amministrativi presso il Garante per la protezione dei dati personali (artt. 2, comma 2, e 4 l. 7 agosto 1990, n. 241; art. 156 d.lg. 30 giugno 2003, n. 196)

Art. 1 - Definizioni

1. Ai fini del presente regolamento si applicano le definizioni elencate nell'art. 4 del Codice in materia di protezione dei dati personali, approvato con d.lg. 30 giugno 2003, n. 196, di seguito denominato "Codice".

Art. 2 - Oggetto del regolamento

1. Il presente regolamento disciplina la durata dei procedimenti amministrativi presso il Garante e individua le unità organizzative responsabili di tali procedimenti.

Art. 3 - Ambito di applicazione

1. Il presente regolamento si applica ai procedimenti di competenza del Garante, conseguenti a una iniziativa di parte o avviati d'ufficio, e alle fasi procedimentali svolte presso il Garante in procedimenti di competenza di altri soggetti pubblici, indicati nelle allegate tabelle A e B che costituiscono parte integrante del presente regolamento.

2. Nella tabella A è riportato il termine entro il quale ciascun procedimento o fase procedimentale deve essere concluso per legge, nonché l'unità organizzativa competente e la fonte normativa di riferimento; nella tabella B è individuato il termine entro il quale ciascun procedimento deve essere comunque concluso, nonché l'unità organizzativa competente e la fonte normativa di riferimento.

3. Per i procedimenti volti all'emanazione di regolamenti il termine e l'unità organizzativa competente sono individuati nei singoli casi.

4. Se non è altrove diversamente previsto, per i procedimenti di modifica di provvedimenti già adottati si applica lo stesso termine previsto per il procedimento principale.

5. Eventuali altri procedimenti amministrativi avviati e non indicati nella tabella B si concludono nel termine stabilito da altra fonte normativa o, in mancanza, in quello di novanta giorni ai sensi dell'articolo 2, comma 3, della legge 7 agosto 1990, n. 241 e successive modificazioni.

Art. 4 - Decorrenza del termine per i procedimenti di competenza del Garante

1. Per i procedimenti amministrativi avviati d'ufficio e per i procedimenti amministrativi relativi alle segnalazioni e ai reclami di cui all'articolo 141, comma 1, lett. *a*) e *b*), del Codice, il termine decorre dalla data in cui il procedimento è avviato in conformità al regolamento del Garante n. 1/2007.

2. Salvo diversa indicazione contenuta nelle tabelle allegate, per ogni altro procedimento amministrativo di competenza del Garante il termine decorre dalla data di ricevimento della domanda, richiesta, comunicazione o del diverso atto di iniziativa, comunque denominato, da parte del dipartimento o altra unità organizzativa competente.

Art. 5 - Decorrenza del termine per le fasi procedimentali

1. Per le fasi procedimentali relative a procedimenti di competenza di altri soggetti pubblici il termine decorre dal ricevimento dell'atto di impulso proveniente dal soggetto pubblico che procede.

Art. 6 - Sospensione del decorso dei termini

1. Il decorso dei termini è sospeso dal 1° agosto al 15 settembre di ciascun anno e riprende a decorrere dalla fine del periodo di sospensione, salvo i casi in cui sussiste per taluno un pregiudizio imminente e irreparabile. Se il decorso ha inizio durante tale periodo, l'inizio stesso è differito alla fine del periodo medesimo.

2. Oltre che nelle ipotesi previste dall'art. 12, comma 3, del regolamento n. 1/2007 per i casi complessi, o di accertamenti ispettivi o di riunione di procedimenti, il decorso dei termini è sospeso, altresì, in ogni caso in cui una fonte normativa prevede la sospensione del procedimento amministrativo o del termine per una decisione da parte dell'Autorità. La sospensione opera per il periodo di tempo espressamente previsto e il termine riprende a decorrere dalla fine del periodo di sospensione.

3. Il decorso dei termini è, inoltre, sospeso per il tempo in cui documenti necessari per la trattazione del procedimento sono indisponibili per effetto di provvedimenti dell'autorità giudiziaria.

4. Il responsabile del procedimento amministrativo informa le parti interessate della data di inizio o di cessazione della sospensione.

Art. 7 - Attività istruttoria

1. Salvo quanto previsto da specifiche norme di legge o di regolamento, se il richiedente è invitato dall'Autorità a fornire notizie, integrazioni o precisazioni o a esibire documenti necessari, i termini previsti nelle tabelle A e B per provvedere sulla richiesta, istanza o diverso atto di iniziativa comunque denominato sono sospesi e decorrono nuovamente dalla data di scadenza del termine fissato per l'adempimento richiesto.

Art. 8 - Pareri obbligatori

1. Ove debba essere sentito obbligatoriamente un organo in funzione consultiva e il parere non intervenga entro il termine stabilito dalla legge o da regolamento o, se mancante, dall'articolo 16, commi 1 e 4, della legge 7 agosto 1990, n. 241, il responsabile del procedimento amministrativo può procedere indipendentemente dall'espressione del parere. Qualora ritenga di non avvalersi di tale facoltà, il responsabile del procedimento amministrativo cura la comunicazione alle parti interessate della determinazione di attendere il parere per un ulteriore periodo di tempo definito, che non è computato ai fini del termine finale del procedimento e che non può essere superiore a quarantacinque giorni. Decorso inutilmente tale ulteriore periodo, l'Autorità procede indipendentemente dall'acquisizione del parere.

2. Nell'ipotesi di cui all'articolo 16, comma 3, della legge 7 agosto 1990, n. 241 l'Autorità, decorso inutilmente l'ulteriore periodo di cui al comma 1 del presente articolo, comunica all'organo interpellato per il parere l'impossibilità di proseguire i propri lavori, informandone le parti interessate.

3. Quando, per legge o regolamento, l'adozione di un provvedimento deve essere preceduta dall'acquisizione di valutazioni tecniche di organi o enti appositi e questi non provvedono e non rappresentano esigenze istruttorie ai sensi e nei termini di cui all'articolo 17 della legge 7 agosto 1990, n. 241, il responsabile del procedimento amministrativo cura la richiesta delle suddette valutazioni tecniche agli altri organismi di cui al comma 1 del medesimo articolo 17 e partecipa alle parti interessate l'intervenuta richiesta. In tali casi, il tempo occorrente per l'acquisizione delle valutazioni tecniche non è computato ai fini del termine finale del procedimento.

4. Nell'ipotesi di cui al comma 2 dell'articolo 17 della legge 7 agosto 1990, n. 241 si applica la disposizione di cui al comma 2 del presente articolo.

Art. 9 - Pareri facoltativi

1. Quando, in conformità alla legge, risulta opportuno acquisire un parere non obbligatorio da parte del Consiglio di Stato o dell'Avvocatura dello Stato, il responsabile del procedimento ne dà notizia alle parti interessate, riassumendone le ragioni. In tal caso, il periodo di tempo occorrente per l'acquisizione del parere, a decorrere dalla richiesta sino alla sua ricezione, non è computato nel termine finale del procedimento, se il parere medesimo è reso nel termine di cui all'articolo 16 della legge 7 agosto 1990, n. 241. L'Autorità procede prescindendo dal parere, se questo non è reso nei termini suddetti.

2. L'acquisizione in via facoltativa di pareri e di valutazioni tecniche di organi, amministrazioni o enti, fuori del caso di cui al comma 1, ha luogo rispettando il termine finale del procedimento.

Art. 10 - Fasi procedimentali presso altre autorità o amministrazioni

1. Fuori dei casi di cui agli articoli 8 e 9, se nel corso del procedimento amministrativo talune fasi sono di competenza di altri soggetti pubblici, il termine finale del procedimento deve intendersi non comprensivo dei periodi di tempo necessari per espletare le fasi stesse.

Art. 11 - Conclusione dei procedimenti

1. Nei casi di cui alla tabella A, i termini per la conclusione dei procedimenti amministrativi o delle fasi procedimentali si riferiscono alla data di adozione del provvedimento del collegio.

2. Nei casi di cui alla tabella B, i termini per la conclusione dei procedimenti si riferiscono alla data in cui l'unità organizzativa competente conclude l'esame dell'affare. Quando il procedimento è definito con provvedimento del collegio, il termine per l'adozione del medesimo provvedimento è non superiore a sessanta giorni dalla data di ricezione degli atti in conformità all'articolo 15 del regolamento del Garante n. 1/2000.

Art. 12 - Entrata in vigore

1. Il presente regolamento entra in vigore il quindicesimo giorno successivo a quello della sua pubblicazione nella *Gazzetta Ufficiale* della Repubblica italiana.

2. I termini indicati nella tabella B si osservano a decorrere dal 1° giugno 2008.

TABELLA A

RICOGNIZIONE DEI TERMINI PER I PROCEDIMENTI DIRETTAMENTE PREVISTI PER LEGGE

1) TERMINI PREVISTI NEL CODICE IN MATERIA DI PROTEZIONE DEI DATI PERSONALI (d.lg. 30 giugno 2003, n. 196)

PROCEDIMENTO E NORMATIVA	TERMINE	UNITÀ ORGANIZZATIVA COMPETENTE
Autorizzazione al trattamento di dati sensibili o genetici artt. 26, comma 2, 41 (76, 90, 107 e 110, comma 1)	45 gg. dal ricevimento della richiesta ovvero, se il richiedente è invitato a fornire informazioni o ad esibire documenti, dalla data di scadenza del termine fissato per l'adempimento richiesto	Dipartimento realtà economiche e produttive Dipartimento libertà pubbliche e sanità Dipartimento comunicazioni e reti telematiche Unità attività forense ordini professionali e pubblici servizi
Autorizzazione al trattamento di dati giudiziari artt. 21, comma 1, 27 e 41	45 gg. dal ricevimento della richiesta ovvero, se il richiedente è invitato a fornire informazioni o ad esibire documenti, dalla data di scadenza del termine fissato per l'adempimento richiesto	Dipartimento realtà economiche e produttive Dipartimento libertà pubbliche e sanità Dipartimento comunicazioni e reti telematiche Unità attività forense ordini professionali e pubblici servizi
Esame di comunicazioni al Garante da parte di soggetti pubblici art. 39 (19, comma 2, 55, 110, comma 1 e 175, comma 1)	45 gg. dal ricevimento della comunicazione salvo diversa determinazione del Garante	Dipartimento libertà pubbliche e sanità
Ricorso artt. 145, 146, 147, 148, 149, 150 e 151	60 gg. dalla data di presentazione del ricorso. Eventuale proroga per un periodo non superiore a ulteriori 40 gg. se gli accertamenti risultano particolarmente complessi o vi è l'assenso delle parti	Unità ricorsi
Parere al Presidente del *Consiglio dei ministri* e ai ministri art. 154, commi 4 e 5	45 gg. dal ricevimento della richiesta, *salvi i termini* più brevi previsti per legge. Ulteriori 20 gg. dal ricevimento degli elementi istruttori in caso di interruzione del termine di 45 gg. per esigenze istruttorie	Servizio relazioni istituzionali
Parere negli altri casi previsti dall'ordinamento art. 154, comma 1, lett. *g*) e comma 5	Si applica il termine espressamente individuato dalla norma che prevede l'acquisizione del parere dell'Autorità. In mancanza di tale espressa previsione, 45 gg. dal ricevimento della richiesta e ulteriori 20 gg. dal ricevimento degli elementi istruttori in caso di interruzione del termine di 45 gg. per esigenze istruttorie	Servizio relazioni istituzionali

2) TERMINI PREVISTI IN ALTRE DISPOSIZIONI NORMATIVE

PROCEDIMENTO E NORMATIVA	TERMINE	UNITÀ ORGANIZZATIVA COMPETENTE
Contestazione non immediata della violazione amministrativa art. 14, comma 2, l. 24 novembre 1981, n. 689	90 gg. dall'accertamento della violazione per la notificazione della stessa ai residenti nel territorio della Repubblica o 360 gg. per la notificazione ai residenti all'estero	Dipartimento attività ispettive e sanzioni
Ordinanza-ingiunzione in materia di sanzioni amministrative art. 166; art. 28, comma 1, l. 24 novembre 1981, n. 689	5 anni dal giorno in cui è stata commessa la violazione	Dipartimento attività ispettive e sanzioni
Parere alla Commissione per l'accesso ai documenti amministrativi art. 25, comma 4, l. 7 agosto 1990, n. 241, e successive modificazioni	10 gg. dalla richiesta	Servizio relazioni istituzionali

TABELLA B

TERMINI NON DIRETTAMENTE PREVISTI PER LEGGE

1) TERMINI RELATIVI A PROCEDIMENTI INDIVIDUATI NEL CODICE IN MATERIA DI PROTEZIONE DEI DATI PERSONALI

PROCEDIMENTO E NORMATIVA	TERMINE	*UNITÀ ORGANIZZATIVA* COMPETENTE
Modalità semplificate per l'informativa agli interessati art. 13, comma 3	90 gg.	Dipartimento realtà economiche e produttive Dipartimento libertà pubbliche e sanità Dipartimento comunicazioni e reti telematiche Unità attività forense ordini professionali e pubblici servizi
Informativa agli interessati che comporterebbe un impiego di mezzi sproporzionati o che si riveli impossibile art. 13, comma 5, lett. *c*)	90 gg.	Dipartimento realtà economiche e produttive Dipartimento libertà pubbliche e sanità Dipartimento comunicazioni e reti telematiche Unità attività forense ordini professionali e pubblici servizi
Verifiche preliminari per i trattamenti che presentano rischi specifici art. 17 (14, 55 e 91)	180 gg.	Dipartimento realtà economiche e produttive Dipartimento libertà pubbliche e sanità Dipartimento comunicazioni e reti telematiche Unità attività forense ordini professionali e pubblici servizi
Individuazione delle attività che perseguono finalità di rilevante interesse pubblico in relazione al trattamento di dati sensibili art. 20, comma 3	90 gg.	Dipartimento libertà pubbliche e sanità
Individuazione dei trattamenti consentiti per perseguire un legittimo interesse del titolare o di un terzo art. 24, comma 1, lett. *g*)	180 gg.	Dipartimento comunicazioni e reti telematiche Dipartimento realtà economiche e produttive

Individuazione dei trattamenti oggetto di notificazione al Garante art. 37, comma 2	120 gg.	Dipartimento realtà economiche e produttive Dipartimento libertà pubbliche e sanità Dipartimento comunicazioni e reti telematiche Dipartimento registro dei trattamenti Unità attività forense ordini professionali e pubblici servizi
Determinazione delle modalità di consultazione gratuita del registro dei trattamenti anche mediante convenzioni con soggetti pubblici art. 37, comma 4	90 gg.	Dipartimento registro dei trattamenti
Autorizzazioni generali art. 40 (76, 90, 107 e 110)	180 gg.	Dipartimento realtà economiche e produttive Dipartimento libertà pubbliche e sanità Dipartimento comunicazioni e reti telematiche Unità attività forense ordini professionali e pubblici servizi

Autorizzazione al trasferimento di dati personali all'estero art. 44	45 gg. dal ricevimento della richiesta ovvero, se il richiedente è invitato a fornire informazioni o ad esibire documenti, dalla data di scadenza del termine fissato per l'adempimento richiesto	Dipartimento realtà economiche e produttive Dipartimento libertà pubbliche e sanità Dipartimento comunicazioni e reti telematiche Unità attività forense ordini professionali e pubblici servizi
Adozione del divieto di trasferimento di dati personali verso un Paese non appartenente all'Unione europea art. 45	120 gg.	Dipartimento realtà economiche e produttive Dipartimento libertà pubbliche e sanità Dipartimento comunicazioni e reti telematiche Unità attività forense ordini professionali e pubblici servizi
Autorizzazione ad indicare nella fatturazione numeri completi delle comunicazioni elettroniche art. 124, comma 5	180 gg.	Dipartimento comunicazioni e reti telematiche
Provvedimento in tema di elenchi di abbonati art. 129, comma 1	180 gg.	Dipartimento comunicazioni e reti telematiche

Provvedimento in materia di procedure di filtraggio o analoghe art. 130, comma 6; art. 143, comma 1, lett. *b*)	180 gg.	Dipartimento comunicazioni e reti telematiche
Reclamo art. 143	180 gg. dalla chiusura dell'istruttoria preliminare. L'istruttoria preliminare è completata entro sei mesi (o, "nei casi complessi che richiedono approfondimenti per motivate esigenze", nove mesi) dalla presentazione o dall'avvenuta regolarizzazione del reclamo (art. 11 comma 1, reg. 1/2007) [1]	Dipartimento realtà economiche e produttive Dipartimento libertà pubbliche e sanità Dipartimento comunicazioni e reti telematiche Unità attività forense ordini professionali e pubblici servizi Affari legali e di giustizia
Segnalazione art. 144	180 gg. dalla chiusura dell'istruttoria preliminare. L'istruttoria preliminare è completata entro sei mesi (o, "nei casi complessi che richiedono approfondimenti per motivate esigenze", nove mesi) dalla presentazione della segnalazione (art. 14, comma 2, reg. n. 1/2007) [1]	Dipartimento realtà economiche e produttive Dipartimento libertà pubbliche e sanità Dipartimento comunicazioni e reti telematiche Unità attività forense ordini professionali e pubblici servizi Affari legali e di giustizia
Controllo avviato d'ufficio sulla liceità e correttezza dei trattamenti art. 154, comma 1, lett. *a*), *c*) e *d*); art. 143, comma 1	180 gg.	Dipartimento realtà economiche e produttive Dipartimento libertà pubbliche e sanità Dipartimento comunicazioni e reti telematiche Unità attività forense ordini professionali e pubblici servizi Affari legali e di giustizia
Accertamenti sui trattamenti di dati personali in ambito giudiziario e da parte di forze di polizia, disciplinati nei titoli I e II della parte seconda del Codice [2] art. 160	180 gg. ovvero 120 gg. in caso di segnalazione dell'interessato [2]	Componente del collegio, designato ai sensi dell'art. 160, comma 1, del Codice
Accertamenti sui trattamenti di dati personali per la difesa e la sicurezza dello Stato, disciplinati nel titolo III della parte seconda del Codice [3] art. 160	180 gg. ovvero 120 gg. in caso di segnalazione dell'interessato	Componente del collegio, designato ai sensi dell'art. 160, comma 1, del Codice

(1) Comunicato di rettifica in *G.U.* 7 giugno 2008, n. 132
(2) Gli accertamenti possono essere avviati anche sulla base di prime informazioni e notizie, acquisite nel termine previsto per le istruttorie preliminari (art. 14, comma 2, reg. del Garante n. 1/2007)
(3) Nei casi in esame, il procedimento s'intende avviato con la designazione del componente del collegio

2) TERMINI RELATIVI A PROCEDIMENTI PREVISTI NEL REGOLAMENTO DEL GARANTE N. 2/2000 CONCERNENTE IL TRATTAMENTO GIURIDICO ED ECONOMICO DEL PERSONALE

PROCEDIMENTO E NORMATIVA	TERMINE	UNITÀ ORGANIZZATIVA COMPETENTE
Dimissioni volontarie art. 60	30 gg. ulteriore periodo non superiore a 30 gg. qualora ricorrano gravi motivi di servizio	Dipartimento risorse umane
Cessazione a domanda per inabilità art. 61	30 gg.	Dipartimento risorse umane
Aspettativa per motivi personali, di famiglia, ovvero per incarichi istituzionali o presso privati art. 17; art. 23 *bis* d.lg. 30 marzo 2001, n. 165; eventuali altre disposizioni speciali di legge anche regionale	60 gg.	Dipartimento risorse umane
Permessi o aspettativa per motivi di studio e dottorato art. 18	30 gg.	Dipartimento risorse umane
Sospensione cautelare della retribuzione del dipendente art. 10, comma 2	30 gg.	Dipartimento risorse umane
Determinazione del limite annuale di ore di lavoro straordinario art. 14, comma 6	90 gg.	Dipartimento risorse umane

Procedimenti disciplinari - termine per riassumere il procedimento disciplinare sospeso in caso di procedimento penale - termine per la sospensione cautelare dal servizio artt. 24 e 26	-180 gg. dal termine del giudizio di primo grado -120 gg. dalla data in cui si è avuta conoscenza della richiesta di rinvio a giudizio	Dipartimento risorse umane
Assunzione del personale a tempo indeterminato o a contratto artt. 7 e 52	60 gg. dalla data di approvazione della graduatoria del concorso o della selezione	Dipartimento risorse umane
Cessazione del rapporto di impiego (liquidazione delle competenze e del Tfr / comunicazione dei dati contributivi per il trattamento di pensione) artt. 56, 58, 59	90 gg.	Dipartimento amministrazione e contabilità
Dispensa dal servizio art. 62	30 gg.	Dipartimento risorse umane
Licenziamento art. 63	60 gg.	Dipartimento risorse umane
Procedure selettive interne art. 5	180 gg.	Dipartimento risorse umane
Determinazione del trattamento economico del personale fondamentale e accessorio art. 27	60 gg.	Dipartimento risorse umane
Inquadramenti o ricostruzioni di posizioni economiche in attuazione di accordi negoziali o di disposizioni regolamentari e corresponsione di eventuali conguagli e arretrati artt. 7 e 27	120 gg.	Dipartimento risorse umane
Permanenza in servizio oltre il limite di età art. 59	90 gg. dalla ricezione dell'istanza	Dipartimento risorse umane
Comandi art. 23	60 gg.	Dipartimento risorse umane

26 Segnalazione al Parlamento e al Governo su dati genetici per fini di giustizia (*) *19 settembre 2007*

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

SEGNALAZIONE AL PARLAMENTO E AL GOVERNO
SULLA DISCIPLINA DELLE BANCHE DATI DEL DNA A FINI DI GIUSTIZIA
(Art. 154, comma 1, lett. *f*), d.lg. 30 giugno 2003, n. 196)

Il presente documento individua gli aspetti per i quali il Garante ritiene opportuno un intervento normativo sull'utilizzazione dei dati relativi al Dna per finalità di accertamento e repressione di reati.

Il Garante ravvisa l'urgenza di disciplinare organicamente questa tematica particolarmente delicata la cui regolamentazione è oggi carente, anche sul piano processuale, dei necessari punti di riferimento che vanno individuati dal legislatore.

Se da un lato è sentita l'esigenza di potenziare le tecniche di indagine a fini di giustizia e di cooperazione sul piano internazionale, vi sono rilevanti effetti sui diritti e le libertà fondamentali delle persone interessate i quali dovrebbero essere tutelati con pari attenzione ed efficacia.

Le scelte che il Parlamento è chiamato ad effettuare dovrebbero quindi tenere auspicabilmente conto di alcune problematiche complesse che si sono già poste sia a livello nazionale, sia all'estero. Possono fornire in tal senso un valido contributo taluni pronunciamenti di questa e di altre autorità di protezione dei dati in ambito europeo, come pure alcuni rilevanti atti a livello internazionale e comunitario provenienti anche dal Consiglio d'Europa.

Il Garante ha svolto in proposito un ampio esame anche sulla base dell'esperienza maturata nell'autorizzare il trattamento dei dati genetici in ambito sanitario e forense e nel definire alcuni casi di contenzioso riguardanti l'impiego del Dna in sede penale.

L'Autorità ne ha tratto la convinzione che il legislatore debba indicare precise linee direttrici nel caso in cui disponga l'istituzione di una banca dati del Dna a livello nazionale, prevista anche dal Trattato di Prüm e dalla correlata proposta di decisione del Consiglio dell'Unione europea sulla cooperazione transfrontaliera.

Sono auspicabili scelte normative chiare e tali da assicurare che le maggiori opportunità che verranno offerte per l'identificazione di persone nelle indagini penali siano accompagnate da garanzie concrete, effettive e inequivoche per le persone interessate.

Con questo spirito di sentita collaborazione istituzionale, il Garante ritiene di dover segnalare alcune principali problematiche per le quali avverte l'esigenza di pervenire ad un quadro organico di competenze, procedure e modalità di tutela degli interessati. Ciò, nei termini che il legislatore riterrà più appropriati, ma tenendo auspicabilmente conto sia della rapida evoluzione tecnologica del settore, sia delle attuali competenze istituzionali dell'Autorità che comprendono il compito di impartire misure e accorgimenti per i trattamenti di dati genetici e biometrici per finalità di giustizia e sicurezza (art. 55 del Codice).

Su queste basi, una normativa adeguata dovrebbe prendere in esame quantomeno i profili di seguito indicati:

1) finalità da perseguire e competenze istituzionali;
2) presupposti per registrare informazioni sul Dna in una banca dati;
3) effettivo rispetto della dignità degli interessati;

(*) [doc. *web* n. 1456163]

4) modalità e tempi di conservazione di profili e di campioni biologici;
5) tutela di particolari dati sulla salute;
6) accessi degli operatori alla banca dati e misure di sicurezza;
7) esercizio dei diritti degli interessati e loro altre prerogative;
8) garanzie in caso di prelievi del Dna comunque obbligatori per legge;
9) il controllo del Garante;
10) l'eventuale attività di monitoraggio del Parlamento.

In questo quadro, la nuova legge dovrebbe anzitutto evidenziare puntualmente che alla base dell'ipotizzata banca dati a livello nazionale dovrebbero esservi solo finalità specifiche di identificazione di persone. Ciò, in armonia con quanto previsto dal menzionato Trattato di Prüm e dalle decisioni in fase di maturazione a livello europeo.

L'individuazione dell'organismo presso il quale istituire la banca dati e che dovrà gestirla, nonché i compiti di eventuali altre entità interessate dovrebbero essere ovviamente previsti in armonia con tali finalità e con le rispettive competenze istituzionali.

Si rende anche auspicabile un'attenta valutazione dell'esperienza maturata in altri Paesi europei riguardo all'"architettura" della banca dati, essendosi già sperimentati modelli –diversi– di banche centralizzate gestite da un unico soggetto presso cui le forze di polizia e la magistratura fanno confluire dati, come pure banche dati locali efficacemente "federate" fra loro sul piano informatico.

La particolare delicatezza della materia induce a ritenere che debba essere la legge a contenere le scelte di fondo sui presupposti e sulle condizioni in presenza delle quali le informazioni riconducibili al Dna e raccolte in sede investigativa (in relazione a reperti rinvenuti sul luogo del delitto, a corpi del reato, a persone sottopostesi volontariamente a prelievo, ecc.) potranno essere conservate in modo organizzato in una banca dati a livello nazionale.

Ciò, non esclude peraltro che, anche in relazione alla rapida evoluzione tecnologica, un eventuale regolamento di attuazione possa contenere norme tecniche e regolare alcuni profili secondari.

Occorrono poi chiare indicazioni affinché i profili del Dna non siano duplicati in altre banche dati di singole forze di polizia, fatta salva la documentazione negli atti dei singoli procedimenti penali. Sono auspicabili quindi anche chiare indicazione sulla sorte di archivi di polizia oggi già esistenti.

Rispetto alle modalità di raccolta e di gestione dei dati, l'attività di indagine presenta peraltro alcune sue specificità rispetto ad altre attività che fanno uso di dati genetici. Andrebbe fatta in tal senso specifica applicazione dei noti principi di necessità e di proporzionalità, già sviluppati dal Garante in riferimento alla diversa area applicativa dell'autorizzazione generale in materia di dati genetici del 22 febbraio 2007, con particolare riferimento al prelievo.

Il prelievo dei campioni biologici e il trattamento dei dati dovrebbero essere altresì orientati a modalità concretamente rispettose della dignità delle persone.

Appare inoltre essenziale che nella banca dati a livello nazionale figurino solo profili del Dna di cui è necessaria la tenuta, registrati con modalità non direttamente connesse all'identità delle persone interessate. Il menzionato Trattato di Prüm e la correlata proposta di Decisione del Consiglio dell'Unione europea si riferiscono appunto ai soli profili.

Nella banca dati non dovrebbero quindi figurare campioni biologici, dei quali –nei casi in cui dovessero essere indispensabilmente preservati per il periodo strettamente necessario– dovrebbe essere comunque evitata, per quanto possibile, una gestione dei campioni biologici ovunque collocati che assuma la forma di banca dati. Peraltro, andrebbe colta l'occasione per verificare l'idoneità delle previsioni che regolano attualmente, anche sul piano processuale, le modalità di conservazione e di distruzione dei campioni biologici in sede locale. Ciò, tenendo anche conto di quanto previsto dal d.d.l. governativo A.C. n. 1967, già in discussione alla Camera dei deputati.

Il Garante segnala anche l'esigenza di regolare tempi e modalità di registrazione e di aggiornamento dei dati, anche in rapporto ai diversi sviluppi processuali eventualmente favorevoli agli interessati.

I periodi di conservazione dei predetti dati andrebbero individuati tenendo conto di quanto previsto dal Consiglio d'Europa il quale richiede (Raccomandazione n. R(92)1) che i risultati di analisi e le informazioni derivate –fatta salva la documentazione nel processo penale in cui sono stati raccolti- possano essere conservati se la persona interessata è stata condannata per gravi reati contro la vita, l'incolumità fisica e la sicurezza delle persone.

Andrebbero applicati sistemi di analisi che non consentano, anche nel procedimento penale, di individuare patologie di cui sia eventualmente affetto l'interessato se non quando sia indispensabile in relazione allo specifico reato da accertare.

Gli operatori aventi accesso alla banca dati dovrebbero essere individuati con modalità puntuali e selettive, in relazione a personale specificamente incaricato e solo in rapporto ad attività investigative previste e disposte sulla base della legge.

Occorrerebbe stabilire specifiche previsioni per assicurare un elevato livello di sicurezza e di qualità di dati, campioni e sistemi, adeguate alla particolare delicatezza dei dati conservati e che consentano di tracciare ogni accesso, nonché di svolgere periodicamente qualificate procedure di *audit*.

Si ravvisa peraltro l'esigenza anche di alcune specifiche indicazioni normative riguardo alle concrete modalità di esercizio dei diritti che il Codice in materia di protezione dei dati personali attribuisce già all'interessato riguardo all'accesso ai dati che lo riguardano, al loro aggiornamento e all'eventuale rettifica o cancellazione.

Inoltre, opportune disposizioni dovrebbero raccordare la nuova disciplina con i compiti istituzionali che il Codice in materia di protezione dei dati personali ha affidato al Garante per ciò che riguarda: a) le misure e gli accorgimenti a garanzia degli interessati che le forze di polizia devono osservare, riguardo all'utilizzazione di banche di dati genetici o biometrici (artt. 17 e 55 del Codice); b) al controllo sull'osservanza della disciplina del trattamento di dati personali (artt. 154 e 160 del Codice).

Infine, il Garante intende osservare che una banca dati a livello nazionale può essere già utilmente composta dai dati raccolti per esigenze investigative nell'ambito di procedimenti penali, che sono già assai numerosi.

In altre parole, l'istituzione della predetta banca dati non impone, di per sé, l'introduzione complementare di un prelievo del Dna comunque obbligatorio nei confronti di intere categorie di soggetti che a vario titolo, siano stati comunque interessati da una vicenda giudiziaria, anche quando non sussista alcuna esigenza investigativa o, in ipotesi, quando vi sia stato già, per esigenze investigative, un prelievo nel procedimento.

Si tratta di un aspetto che, ad avviso dell'Autorità, merita la massima attenzione, anche in relazione alle scelte che verranno comunque effettuate in rapporto alle finalità della banca dati.

Nel caso in cui il Parlamento ritenesse di prevedere che, in aggiunta ad una banca dati alimentata da informazioni raccolte per esigenze investigative nel corso dei procedimenti penali, alcune categorie di soggetti (quali fermati, arrestati, indagati, imputati o condannati per determinati reati) debbano essere sottoposti in ogni caso ad un prelievo obbligatorio di cui va chiarita la specifica finalità, occorrerebbe comunque individuare in maniera selettiva e proporzionata i soggetti interessati e i relativi reati che non potrebbero che essere definiti sulla base della loro particolare gravità. Ciò, tenendo conto del criterio di "appropriatezza" della menzionata Raccomandazione del Consiglio d'Europa e approfondendo anche in questo caso, ovviamente, il profilo della conservazione nella banca dati di informazioni relative a persone rivelatesi non responsabili di illeciti.

Da ultimo, il Garante rappresenta l'utilità di specifiche previsioni che confermino i compiti di controllo dell'Autorità, anche con riferimento ad un eventuale rapporto periodico al Parlamento sul funzionamento e la gestione della banca dati e dei connessi trattamenti, ovviamente con l'assegnazione all'Autorità delle risorse e delle competenze necessarie.

Roma, 19 settembre 2007

27 Autorizzazione al trattamento dei dati genetici *22 febbraio 2007* (*)

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

In data odierna, con la partecipazione del prof. Francesco Pizzetti, presidente, del dott. Giuseppe Chiaravalloti, vice presidente, del dott. Mauro Paissan e del dott. Giuseppe Fortunato, componenti, e del dott. Giovanni Buttarelli, segretario generale;

Visto il decreto legislativo 30 giugno 2003 n. 196, recante il Codice in materia di protezione dei dati personali nel seguito denominato "Codice";

Visto, in particolare, l'art. 90, comma 1, del citato Codice, secondo cui il trattamento dei dati genetici da chiunque effettuato è consentito nei soli casi previsti da apposita autorizzazione rilasciata dal Garante sentito il Ministro della salute che acquisisce, a tal fine, il parere del Consiglio superiore di sanità;

Visto, altresì, l'art. 90, comma 2, del Codice, in base al quale l'autorizzazione individua anche gli ulteriori elementi da includere nell'informativa ai sensi dell'art. 13, con particolare riguardo alla specificazione delle finalità perseguite e dei risultati conseguibili anche in relazione alle notizie inattese che possono essere conosciute per effetto del trattamento dei dati e al diritto di opporsi al medesimo trattamento per motivi legittimi;

Vista l'autorizzazione generale del Garante n. 2/2005 che richiama espressamente (punto 1.4) l'autorizzazione n. 2/2002 (punto 2, lett. *b*)), relativa al trattamento dei dati idonei a rivelare lo stato di salute e la vita sessuale, secondo la quale i dati genetici trattati per fini di prevenzione, di diagnosi o di terapia nei confronti dell'interessato, ovvero per finalità di ricerca scientifica, *"possono essere utilizzati unicamente per tali finalità o per consentire all'interessato di prendere una decisione libera e informata, ovvero per finalità probatorie in sede civile o penale, in conformità alla legge"*;

Considerata la necessità di assicurare, nella disciplina del trattamento dei dati personali, un elevato livello di tutela per i diritti e le libertà fondamentali, nonché per la dignità delle persone e, in particolare, per il diritto alla protezione dei dati personali sancito all'art. 1 del Codice; ciò, anche riducendo al minimo i rischi di danno o di pericolo valutati sulla base delle raccomandazioni adottate in materia di dati sanitari dal Consiglio d'Europa e, in particolare, dalla Raccomandazione n. R(97) 5; rilevato che in base a quest'ultima sono considerati dati genetici tutti i dati, di qualunque tipo, che riguardano i caratteri ereditari di un individuo o che sono in rapporto con i caratteri che formano il patrimonio di un gruppo di individui affini (*par.* 1), dati che, nel quadro della più ampia categoria dei "dati sanitari", possano essere trattati solo a determinate condizioni (*par.* 1);

Rilevato che la Raccomandazione del Consiglio d'Europa n. R(92) 3 sui *test* e gli *screening* genetici a fini di cura afferma (principio n. 8) che la raccolta e la conservazione di sostanze e di campioni biologici, così come il trattamento dei dati che ne derivano, devono essere effettuati in conformità ai principi fondamentali di protezione e di sicurezza dei dati stabiliti dalla Convenzione per la protezione degli individui con riguardo al trattamento automatizzato dei dati personali n. 108 del 28 gennaio 1981, nonché dalle pertinenti raccomandazioni del Comitato dei ministri in materia;

Rilevato che, riguardo al trattamento dei dati genetici, sono desumibili altri importanti princìpi da alcune fonti internazionali e comunitarie tra le quali figurano:

a) la Convenzione sui diritti dell'uomo e sulla biomedicina, fatta a Oviedo il 4 aprile 1997, che vieta qualsiasi forma di discriminazione nei confronti di una persona

(*) *G.U.* 19 marzo 2007, n. 65
[doc. *web* n. 1389918]

in ragione del suo patrimonio genetico (art. 11) e limita l'espletamento di *test* genetici predittivi ai soli fini medici o di ricerca medica e sulla base di una consulenza genetica appropriata (art. 12);

b) la Dichiarazione universale sul genoma umano e i diritti umani dell'Unesco dell'11 novembre 1997, che sancisce il diritto della persona al rispetto della dignità e dei propri diritti indipendentemente dalle sue caratteristiche genetiche (art. 2) e vieta ogni discriminazione basata sulle caratteristiche genetiche che abbia per fine o sortisca l'effetto di violare i diritti umani, le libertà fondamentali e la dignità umana (art. 6);

c) la Carta dei diritti fondamentali dell'Unione europea, proclamata a Nizza il 7 dicembre 2000, che vieta qualsiasi forma di discriminazione fondata, in particolare, sulle caratteristiche genetiche (art. 21);

d) la direttiva 2004/23/Ce del Parlamento europeo e del Consiglio del 31 marzo 2004, che prescrive l'adozione di misure necessarie di protezione dei dati, compresi quelli genetici, e di altre misure di salvaguardia relativamente ad informazioni raccolte nell'ambito di attività di donazione, approvvigionamento, controllo, lavorazione, conservazione, stoccaggio e distribuzione di tessuti e cellule umani destinati ad applicazioni sull'uomo, nonché di prodotti fabbricati derivati da tessuti e cellule umani destinati ad applicazioni sull'uomo (art. 14);

e) la Convenzione sui diritti dell'uomo e sulla biomedicina (art. 10), la Dichiarazione universale sul genoma umano e i diritti dell'uomo (art. 5, lett. *c*)) e la Dichiarazione internazionale sui dati genetici umani dell'Unesco (art. 10), le quali riconoscono, con diverso ambito, il diritto di ogni individuo di essere o non essere informato dei risultati degli esami genetici e delle loro conseguenze (ovvero dei risultati della ricerca medica e scientifica laddove i dati genetici, i dati proteomici dell'individuo o i campioni biologici siano utilizzati per tali scopi);

f) il Codice di condotta dell'Organizzazione internazionale del lavoro sulla protezione dei dati personali dei lavoratori (novembre 1996), in base al quale lo svolgimento di *screening* genetici sui lavoratori dovrebbe essere vietato o limitato a casi specifici autorizzati espressamente dalla legge (art. 6.12);

g) la Dichiarazione di Helsinki dell'Associazione medica mondiale (giugno 1964 e successive modificazioni), in base alla quale occorre acquisire l'assenso della persona legalmente incapace, in aggiunta a quello del legale rappresentante, laddove la stessa sia in grado di esprimere il proprio assenso a partecipare ad una ricerca (*par.* 25);

h) il documento di lavoro sui dati genetici adottato il 17 marzo 2004 (Wp 91) dal Gruppo per la tutela delle persone con riguardo al trattamento dei dati personali, istituito dall'art. 29 direttiva n. 95/46/Ce che, nell'individuare le necessarie garanzie in materia di dati genetici, afferma la necessità di prendere in considerazione e di disciplinare anche lo statuto giuridico dei campioni biologici, suscettibili anch'essi di costituire una fonte di dati personali;

Vista la legge 19 febbraio 2004, n. 40, recante "Norme in materia di procreazione medicalmente assistita";

Visto, altresì, l'Accordo del 15 luglio 2004 tra il Ministro della salute, le regioni e le province autonome di Trento e Bolzano sul documento recante le "Linee-guida per le attività di genetica medica" (in *G.U.* 23 settembre 2004, n. 224);

Visto il d.lg. 19 agosto 2005, n. 191, di attuazione della direttiva n. 2002/98/Ce, che stabilisce norme di qualità e di sicurezza per la raccolta, il controllo, la lavorazione, la conservazione e la distribuzione del sangue umano e dei suoi componenti;

Vista la legge 21 ottobre 2005, n. 219, che disciplina le attività trasfusionali e la produzione nazionale degli emoderivati, nonché, l'ordinanza del Ministro della salute del 13 aprile 2006 recante "Misure urgenti in materia di cellule staminali da cordone ombelicale" (in *G.U.* 9 maggio 2005, n. 106);

Considerato che, ai sensi degli artt. 76 e 81 del Codice, gli esercenti le professioni sanitarie e gli organismi sanitari pubblici possono trattare i dati personali idonei a rivelare lo stato di salute per finalità di tutela della salute o dell'incolumità fisica dell'interessato solo con il consenso di quest'ultimo, oppure (quando occorre tutelare la salute o l'incolumità fisica di un terzo o della collettività) anche senza il consenso dell'interessato, ma previa autorizzazione del Garante;

Considerato che gli artt. 77, 78 e 79 del Codice prevedono modalità semplificate per l'informativa di cui all'art. 13 del medesimo Codice da parte degli esercenti la professione sanitaria e degli organismi sanitari pubblici;

Visto il provvedimento del Garante del 19 luglio 2006 (in *www.garanteprivacy.it*, doc. *web* n. 1318699), con il quale, ai sensi degli artt. 78, comma 3, e 13, comma 3, del Codice, sono stati indicati gli elementi essenziali che il medico di medicina generale e il pediatra di libera scelta devono includere nell'informativa da fornire all'interessato relativamente al trattamento dei dati personali;

Considerato che, ai sensi degli artt. 23 e 26 del Codice, i privati e gli enti pubblici economici possono trattare i dati sensibili solo previa autorizzazione del Garante e, ove richiesto, con il consenso scritto dell'interessato;

Considerato che un elevato numero di trattamenti di dati genetici è effettuato per finalità di prevenzione, di diagnosi o di terapia nei confronti dell'interessato e per finalità di ricerca scientifica;

Considerato che l'art. 40 del Codice prevede il rilascio di autorizzazioni di carattere generale relative a determinate categorie di titolari o di trattamenti e che tali autorizzazioni sinora rilasciate sono risultate un idoneo strumento per prescrivere misure uniformi a garanzia degli interessati;

Ritenuto opportuno rilasciare la specifica autorizzazione prevista dall'art. 90 del Codice, in sostituzione delle prescrizioni già impartite in materia di dati genetici con l'autorizzazione generale del Garante n. 2/2002 richiamata dall'autorizzazione n. 2/2005;

Ritenuto opportuno prendere in considerazione con separato provvedimento il trattamento dei dati genetici effettuato da parte delle categorie di soggetti pubblici ricompresi nei titoli I, II, e III della parte II del Codice.

Considerato che, fuori dei casi appena indicati, ulteriori trattamenti di dati genetici non ricompresi nella presente autorizzazione non risultano allo stato leciti, anche in riferimento all'attività dei datori di lavoro volta a determinare l'attitudine professionale di lavoratori o di candidati all'instaurazione di un rapporto di lavoro, anche se basata sul consenso dell'interessato, nonché all'attività delle imprese di assicurazione;

Visti gli artt. 41 e 167 del Codice;

Ritenuto opportuno che anche la presente autorizzazione sia a tempo determinato e riservata ogni determinazione in ordine alla sua integrazione o modifica anche in relazione al rapido sviluppo della ricerca e delle tecnologie applicate alla genetica e all'evolversi delle conoscenze nel settore;

Visto, altresì, l'art. 11, comma 2, del Codice, il quale stabilisce che i dati trattati in violazione della disciplina rilevante in materia di trattamento di dati personali non possono essere utilizzati;

Visti gli articoli 31 e seguenti del Codice e il disciplinare tecnico di cui all'Allegato B al medesimo Codice, recanti disposizioni e regole sulle misure di sicurezza;

Sentito il Ministro della salute, che ha acquisito il parere del Consiglio superiore di sanità, ai sensi dell'art. 90 del Codice;

Esaminate le osservazioni formulate, su richiesta del Garante, da parte di qualificati esperti della materia;

Visti gli altri atti d'ufficio;

Viste le osservazioni dell'Ufficio formulate dal segretario generale ai sensi dell'art. 15 del regolamento del Garante n. 1/2000;

Relatore il prof. Francesco Pizzetti;

autorizza

ai sensi degli articoli 26, 40, 41 e 90 del Codice il trattamento dei dati genetici da parte dei soggetti sottoindividuati, secondo le prescrizioni di seguito indicate.

Prima di iniziare o proseguire il trattamento 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, in conformità all'art. 3 del Codice.

1) Definizioni

Ai fini della presente autorizzazione si intende per:

a) "dato genetico", il dato che, indipendentemente dalla tipologia, riguarda la costituzione genotipica di un individuo, ovvero i caratteri genetici trasmissibili nell'ambito di un gruppo di individui legati da vincoli di parentela;

b) "campione biologico", ogni campione di materiale biologico che contiene le informazioni genotipiche caratteristiche di un individuo;

c) "*test* genetico", l'analisi a scopo clinico di uno specifico gene o del suo prodotto o funzione o di altre parti del Dna o di un cromosoma, volta a effettuare una diagnosi o a confermare un sospetto clinico in un individuo già affetto (*test* diagnostico), oppure a individuare o escludere la presenza di una mutazione associata ad una malattia genetica che possa svilupparsi in un individuo sano (*test* presintomatico) o, ancora, a valutare la maggiore o minore suscettibilità di un individuo a sviluppare patologie comuni (*test* predittivo);

d) "*test* farmacogenetico", l'analisi finalizzata all'identificazione di sequenza nel Dna in grado di predire la risposta "individuale" a farmaci in termini di efficacia e di rischio relativo di eventi avversi;

e) "*test* sulla variabilità individuale", l'esame genetico volto a definire un rapporto di consanguineità o ad attribuire tracce biologiche a determinati individui;

f) "*screening* genetico", il *test* genetico effettuato su popolazioni o su gruppi definiti al fine di delinearne le caratteristiche genetiche comuni o di identificare precocemente soggetti affetti o portatori di patologie genetiche o di altre caratteristiche ereditarie;

g) "consulenza genetica", il processo di comunicazione consistente nell'aiutare l'individuo o la famiglia colpita da patologia genetica a comprendere le informazioni mediche che includono la diagnosi e il probabile decorso della malattia, le forme di assistenza disponibili, il contributo dell'ereditarietà al verificarsi della malattia e il rischio di ricorrenza esistente per sé e per altri familiari, nonché tutte le opzioni esistenti nell'affrontare il rischio di malattia e l'impatto che tale rischio può avere su scelte procreative; a tale processo partecipano, oltre al medico e/o al biologo specialisti in genetica medica, altre figure professionali competenti nella gestione delle problematiche psicologiche e sociali connesse alla genetica;

h) "informazione genetica", il processo informativo riguardante le specifiche caratteristiche degli *screening* genetici.

2) Ambito di applicazione

La presente autorizzazione è rilasciata:

a) agli esercenti le professioni sanitarie, in particolare ai genetisti medici, limitatamente ai dati e alle operazioni indispensabili per esclusive finalità di tutela della salute dell'interessato o di un terzo appartenente alla stessa linea genetica dell'interessato;

b) agli organismi sanitari pubblici e privati, in particolare alle strutture cliniche di genetica medica, limitatamente ai dati e alle operazioni indispensabili per esclusive finalità di tutela della salute dell'interessato o di un terzo appartenente alla stessa linea genetica dell'interessato;

c) a laboratori di genetica medica, limitatamente alle operazioni indispensabili rispetto a dati, parimenti indispensabili, destinati ad essere trattati per esclusive finalità di prevenzione e di diagnosi genetica nei confronti dell'interessato, o destinati ad essere utilizzati ad esclusivi fini di svolgimento delle indagini difensive o per far valere o difendere un diritto anche da parte di un terzo in sede giudiziaria o, ad esclusivi fini di ricongiungimento familiare, per l'accertamento della sussistenza di vincoli di consanguineità di cittadini di Stati non appartenenti all'Unione europea, apolidi e rifugiati;

d) alle persone fisiche o giuridiche, agli enti o agli istituti di ricerca, alle associazioni e agli altri organismi pubblici e privati aventi finalità di ricerca, limitatamente ai dati e alle operazioni indispensabili per esclusivi scopi di ricerca scientifica, anche statistica, finalizzata alla tutela della salute dell'interessato, di terzi o della collettività in campo medico, biomedico ed epidemiologico e antropologico, nell'ambito delle attività di pertinenza della genetica medica;

e) agli psicologi, ai consulenti tecnici e ai loro assistenti, nell'ambito di interventi pluridisciplinari di consulenza genetica, limitatamente ai dati e alle operazioni indispensabili per esclusive finalità di consulenza nei confronti dell'interessato o dei suoi familiari;

f) ai farmacisti, limitatamente ai dati e alle operazioni indispensabili per esclusive finalità di adempimento agli obblighi derivanti da un rapporto di fornitura di farmaci all'interessato;

g) ai difensori, anche a mezzo di sostituti, consulenti tecnici e investigatori privati autorizzati, limitatamente alle operazioni e ai dati indispensabili per esclusive finalità di svolgimento di investigazioni difensive di cui alla legge 7 dicembre 2000 n. 397; è altresì rilasciata per far valere o difendere un diritto –anche da parte di un terzo– in sede giudiziaria, sempre che il diritto sia di rango almeno pari a quello dell'interessato e i dati siano trattati esclusivamente per tali finalità e per il periodo strettamente necessario al loro perseguimento;

h) agli organismi internazionali ritenuti idonei dal Ministero degli affari esteri e alle rappresentanze diplomatiche o consolari per il rilascio delle certificazioni (allo stato disciplinate dall'art. 49 d.P.R. 5 gennaio 1967, n. 200) ad esclusivi fini di ricongiungimento familiare e limitatamente ai casi in cui l'interessato non possa fornire documenti ufficiali che provino i suoi vincoli di consanguineità, in ragione del suo status, ovvero della mancanza di un'autorità riconosciuta o della presunta inaffidabilità dei documenti rilasciati dall'autorità locale.

3) Finalità del trattamento

Possono essere trattati i dati genetici inerenti alle seguenti finalità che non possano essere adempiute, caso per caso, mediante il trattamento di dati anonimi o di dati personali di natura diversa:

a) tutela della salute, con particolare riferimento alle patologie di natura genetica e alla tutela dell'identità genetica dell'interessato, con il suo consenso, salvo quanto previsto dagli artt. 26 e 82 del Codice in riferimento al caso in cui l'interessato non possa prestare il proprio consenso per incapacità d'agire, impossibilità fisica o incapacità di intendere o di volere;

b) tutela della salute, con particolare riferimento alle patologie di natura genetica e tutela dell'identità genetica di un terzo appartenente alla stessa linea genetica dell'interessato, nel caso in cui il consenso non sia prestato o non possa essere prestato per impossibilità fisica, per incapacità di agire o per incapacità d'intendere

o di volere; ciò, limitatamente ai dati genetici già raccolti e qualora il trattamento sia indispensabile per consentire al terzo di compiere una scelta riproduttiva consapevole o sia giustificato dalla disponibilità, per il terzo, di interventi di natura preventiva o terapeutica;

c) ricerca scientifica e statistica, finalizzata alla tutela della salute della collettività in campo medico, biomedico ed epidemiologico (sempre che la disponibilità di dati solo anonimi su campioni della popolazione non permetta alla ricerca di raggiungere i suoi scopi), da svolgersi con il consenso dell'interessato salvo che nei casi di indagini statistiche o di ricerca scientifica previste dalla legge.

Nell'ambito delle finalità di cui alle precedenti lettere *a)* e *b)* del presente punto, l'autorizzazione è rilasciata anche all'esclusivo fine di consentire ai destinatari di adempiere o di esigere l'adempimento di specifici obblighi o di eseguire specifici compiti previsti dalla normativa comunitaria, da leggi o da regolamenti, in particolare in materia di igiene e di sanità pubblica, di prevenzione delle malattie professionali, di diagnosi e cura, anche per i trapianti di organi e tessuti, di riabilitazione degli stati di invalidità e di inabilità fisica e psichica, di tutela della salute mentale, di assistenza farmaceutica, in conformità alla legge. Il trattamento può riguardare anche la compilazione di cartelle cliniche, di certificati e di altri documenti di tipo sanitario.

La presente autorizzazione è rilasciata, altresì, quando il trattamento dei dati genetici sia indispensabile:

a) per lo svolgimento da parte del difensore delle investigazioni difensive di cui alla legge 7 dicembre 2000, n. 397, anche a mezzo di sostituti, di consulenti tecnici e investigatori privati autorizzati, o, comunque, per far valere o difendere un diritto anche da parte di un terzo in sede giudiziaria, anche senza il consenso dell'interessato eccetto il caso in cui il trattamento presupponga lo svolgimento di *test* genetici. Ciò, sempre che il diritto da far valere o difendere sia di rango pari a quello dell'interessato, ovvero consistente in un diritto della personalità o in un altro diritto o libertà fondamentale e inviolabile e i dati siano trattati esclusivamente per tali finalità e per il periodo strettamente necessario al loro perseguimento. Il trattamento deve essere comunque effettuato nel rispetto delle autorizzazioni generali del Garante al trattamento dei dati sensibili da parte dei liberi professionisti e da parte degli investigatori privati (allo stato, autorizzazioni nn. 4 e 6/2005). Il trattamento può comprendere anche le informazioni relative a stati di salute pregressi o relative ai familiari dell'interessato;

b) per adempiere o per esigere l'adempimento di specifici obblighi o per eseguire specifici compiti previsti espressamente dalla normativa comunitaria, da leggi o da regolamenti in materia di previdenza e assistenza o in materia di igiene e sicurezza del lavoro o della popolazione, anche senza il consenso dell'interessato, nei limiti previsti dall'autorizzazione generale del Garante al trattamento dei dati sensibili nei rapporti di lavoro (allo stato, l'autorizzazione n. 1/2005) e ferme restando le disposizioni del codice di deontologia e di buona condotta di cui all'articolo 111 del Codice. Il trattamento può comprendere anche le informazioni relative a stati di salute pregressi o relative ai familiari dell'interessato;

c) per l'accertamento dei vincoli di consanguineità per il ricongiungimento familiare di cittadini di Stati non appartenenti all'Unione europea, apolidi e rifugiati (attualmente disciplinato dal d.lg. 25 luglio 1998, n. 286). Non si considerano, in particolare, indispensabili i trattamenti di dati genetici effettuati nonostante la disponibilità di procedure alternative che non comportano il trattamenti dei dati medesimi.

4) Modalità di trattamento

I destinatari della presente autorizzazione conformano il prelievo e l'utilizzo dei campioni biologici e il trattamento dei dati genetici secondo modalità volte a prevenire la violazione dei diritti, delle libertà fondamentali e della dignità degli interessati. Tali attività sono effettuate, comunque, in modo lecito e secondo correttezza, nonché per scopi deter-

minati in conformità alla presente autorizzazione e resi noti all'interessato nei modi indicati al successivo punto 5.

Sono predisposte specifiche misure per accertare univocamente l'identità del soggetto al quale viene prelevato il materiale biologico per l'esecuzione dell'analisi (art. 11, comma 1, lett. *c*), del Codice).

Il trattamento dei dati genetici è effettuato unicamente con operazioni, nonché con logiche e mediante forme di organizzazione dei dati strettamente indispensabili in rapporto ai sopra indicati obblighi, compiti o finalità.

Restano fermi gli obblighi deontologici relativi alle singole figure professionali oggetto della presente autorizzazione.

4.1) *Raccolta e conservazione*

Quando le finalità del trattamento di dati genetici non possono essere realizzate senza l'identificazione anche temporanea degli interessati, il titolare adotta specifiche misure per mantenere separati i dati identificativi già al momento della raccolta, salvo che ciò risulti impossibile in ragione delle particolari caratteristiche del trattamento o richieda un impiego di mezzi manifestamente sproporzionato.

La raccolta di dati genetici effettuata per l'esecuzione di *test* e di *screening* genetici è limitata alle sole informazioni personali e familiari strettamente indispensabili all'esecuzione dell'analisi (art. 11, comma 1, lett. *d*), del Codice).

In particolare, nei trattamenti effettuati mediante *test* sulla variabilità individuale non sono raccolti dati sullo stato di salute o su altre caratteristiche degli interessati, ad eccezione del sesso. Il campione è prelevato da un incaricato del laboratorio di genetica medica o da un medico da esso designato ovvero, in caso di ricongiungimento familiare, da esercenti le professioni sanitarie appositamente incaricati dalle rappresentanze diplomatiche o consolari o da organismi internazionali ritenuti idonei dal Ministero degli affari esteri.

4.2) *Ricerca scientifica e statistica*

La ricerca scientifica e statistica, per il cui svolgimento è consentito il trattamento dei dati genetici e l'utilizzo dei campioni biologici, è effettuata, altresì, sulla base di un progetto redatto conformemente agli *standard* del pertinente settore disciplinare, anche al fine di documentare che il trattamento dei dati e l'utilizzo dei campioni biologici sia effettuato per idonei ed effettivi scopi scientifici. Possono essere utilizzati a tal fine i dati e i campioni biologici strettamente pertinenti agli scopi perseguiti, avuto riguardo ai dati disponibili e ai trattamenti già effettuati dallo stesso titolare, nonché all'esistenza di altre modalità che permettano di raggiungere gli scopi della ricerca mediante dati personali diversi da quelli identificativi o genetici, ovvero che non comportino il prelievo di campioni biologici.

Il progetto specifica le misure da adottare nel trattamento dei dati personali per garantire il rispetto della presente autorizzazione, nonché della normativa sulla protezione dei dati personali, anche per i profili riguardanti la custodia e la sicurezza dei dati e dei campioni biologici, e individua gli eventuali responsabili del trattamento (artt. 29, 31, 33, 34 e 35 del Codice e Allegato B al medesimo Codice). In particolare, laddove la ricerca preveda il prelievo e/o l'utilizzo di campioni biologici, il progetto indica l'origine, la natura e le modalità di prelievo e di conservazione dei campioni, nonché le misure adottate per garantire la volontarietà del conferimento del materiale biologico da parte dell'interessato.

Il progetto è conservato a cura del titolare in forma riservata almeno per un anno dopo la conclusione della ricerca. Il titolare fornisce le informazioni contenute nel progetto agli interessati che ne facciano richiesta.

4.3) *Misure di sicurezza*

Per la custodia e la sicurezza dei dati genetici e dei campioni biologici sono adottate, in ogni caso, le seguenti cautele.

L'accesso ai locali è controllato mediante incaricati della vigilanza o strumenti elettronici che prevedano specifiche procedure di identificazione anche mediante dispositivi biometrici. Le persone ammesse, a qualunque titolo, dopo l'orario di chiusura, sono identificate e registrate.

La conservazione, l'utilizzo e il trasporto dei campioni biologici sono posti in essere con modalità volte anche a garantirne la qualità, l'integrità, la disponibilità e la tracciabilità.

Il trasferimento dei dati genetici in formato elettronico è effettuato con posta elettronica certificata previa cifratura delle informazioni trasmesse da realizzarsi con firma digitale. É ammesso il ricorso a canali di comunicazione di tipo *"web application"* che prevedano protocolli di comunicazione sicuri e garantiscano, previa verifica, l'identità digitale del *server* che eroga il servizio e della postazione *client* da cui si effettua l'accesso ai dati, ricorrendo a certificati digitali emessi in conformità alla legge da un'autorità di certificazione.

La consultazione dei dati genetici trattati con strumenti elettronici è consentita previa adozione di sistemi di autenticazione basati sull'uso combinato di informazioni note agli incaricati e di dispositivi, anche biometrici, in loro possesso.

I dati genetici e i campioni biologici contenuti in elenchi, registri o banche di dati, sono trattati con tecniche di cifratura o mediante l'utilizzazione di codici identificativi o di altre soluzioni che li rendano temporaneamente inintelligibili anche a chi è autorizzato ad accedervi e permettano di identificare gli interessati solo in caso di necessità, in modo da ridurre al minimo i rischi di conoscenza accidentale e di accesso abusivo o non autorizzato. Laddove gli elenchi, i registri o le banche di dati contengano anche dati riguardanti la genealogia o lo stato di salute degli interessati, le predette tecniche devono consentire, altresì, il trattamento disgiunto dei dati genetici e sanitari dagli altri dati personali che permettono di identificare direttamente le persone interessate.

Restano comunque fermi gli altri obblighi previsti dagli articoli 11, 14, 22 e 31 e seguenti del Codice e le modalità tecniche in materia di misure minime di sicurezza indicate nel disciplinare tecnico allegato al medesimo Codice, anche per ciò che attiene alla conservazione e al trasporto dei dati all'esterno dei locali protetti e all'accesso controllato a tali locali. Tali obblighi vanno osservati anche in riferimento ai campioni biologici.

5) Informativa

Salvo che per i trattamenti non sistematici di dati genetici effettuati dal medico di medicina generale e dal pediatra di libera scelta nell'ambito degli ordinari rapporti con l'interessato per la tutela della salute e dell'incolumità fisica di quest'ultimo, l'informativa evidenzia, oltre agli elementi previsti in base agli artt. 13, 77 e 78 del Codice:

a) l'esplicitazione analitica di tutte le specifiche finalità perseguite;
b) i risultati conseguibili anche in relazione alle notizie inattese che possono essere conosciute per effetto del trattamento dei dati genetici;
c) il diritto dell'interessato di opporsi al trattamento dei dati genetici per motivi legittimi;
d) la facoltà o meno, per l'interessato, di limitare l'ambito di comunicazione dei dati genetici e il trasferimento dei campioni biologici, nonché l'eventuale l'utilizzo di questi per ulteriori scopi;
e) il periodo di conservazione dei dati genetici e dei campioni biologici.

Dopo il raggiungimento della maggiore età l'informativa è fornita all'interessato anche ai fini dell'acquisizione di una nuova manifestazione del consenso quando questo è necessario (art. 82, comma 4, del Codice).

Per i trattamenti effettuati per scopi di ricerca scientifica e statistica l'informativa evidenzia, altresì:

a) che il consenso è manifestato liberamente ed è revocabile in ogni momento senza che ciò comporti alcuno svantaggio o pregiudizio per l'interessato, salvo che i dati e i campioni biologici, in origine o a seguito di trattamento, non consentano più di identificare il medesimo interessato;

b) gli accorgimenti adottati per consentire l'identificabilità degli interessati soltanto per il tempo necessario agli scopi della raccolta o del successivo trattamento (art. 11, comma 1, lett. *e*), del Codice);
c) l'eventualità che i dati e/o i campioni biologici siano conservati e utilizzati per altri scopi di ricerca scientifica e statistica, per quanto noto, adeguatamente specificati anche con riguardo alle categorie di soggetti ai quali possono essere eventualmente comunicati i dati oppure trasferiti i campioni;
d) le modalità con cui gli interessati che ne facciano richiesta possono accedere alle informazioni contenute nel progetto di ricerca.

Per i trattamenti effettuati mediante *test* e *screening* genetici per finalità di tutela della salute, di ricerca o di ricongiungimento familiare, l'informativa è resa all'interessato prima del prelievo, ovvero dell'utilizzo del suo campione biologico qualora lo stesso sia stato già prelevato, anche in forma scritta, in modo specifico e comprensibile, anche quando il trattamento è effettuato da esercenti la professione sanitaria o da organismi sanitari pubblici e privati che abbiano informato in precedenza il medesimo interessato utilizzando le modalità semplificate previste dagli artt. 77, 78 e 79 del Codice.

I trattamenti per lo svolgimento delle investigazioni difensive o per l'esercizio di un diritto in sede giudiziaria possono essere effettuati mediante l'esecuzione di test genetici soltanto previa informativa all'interessato da rendersi con le modalità sopra indicate.

5.1) *Consulenza genetica e attività di informazione*
Per i trattamenti effettuati mediante *test* genetici per finalità di tutela della salute o di ricongiungimento familiare è fornita all'interessato una consulenza genetica prima e dopo lo svolgimento dell'analisi, nel corso della quale l'interessato riceve informazioni complete e accurate su tutte le possibili implicazioni dei risultati. Prima dell'introduzione di *screening* genetici finalizzati alla tutela della salute sono adottate idonee misure per garantire un'attività di informazione al pubblico in merito alla disponibilità dei *test* effettuati, alla loro natura, alle loro specifiche finalità e conseguenze, anche nell'ambito di pubblicazioni istituzionali e mediante reti di comunicazione elettronica.

Il consulente genetista aiuta i soggetti interessati a prendere in piena autonomia le decisioni ritenute più adeguate, tenuto conto del rischio genetico, delle aspirazioni familiari e dei loro principi etico-religiosi, aiutandoli ad agire coerentemente con le scelte compiute, nonché a realizzare il miglior adattamento possibile alla malattia e/o al rischio di ricorrenza della malattia stessa.

Nei casi in cui il *test* sulla variabilità individuale è volto ad accertare la paternità o la maternità gli interessati sono, altresì, informati circa la normativa in materia di filiazione, ponendo in evidenza le eventuali conseguenze psicologiche e sociali dell'esame.

L'attuazione di ricerche scientifiche su isolati di popolazione è preceduta da un'attività di informazione presso le comunità interessate, anche mediante mezzi di comunicazione di massa su base locale e presentazioni pubbliche, volta ad illustrare la natura della ricerca, le finalità perseguite, le modalità di attuazione, le fonti di finanziamento e i rischi o benefici attesi per le popolazioni coinvolte. L'attività di informazione evidenzia anche gli eventuali rischi di discriminazione o stigmatizzazione delle comunità interessate, nonché quelli inerenti alla conoscibilità di inattesi rapporti di consanguineità e le azioni intraprese per ridurre al minimo tali rischi.

6) Consenso
In conformità a quanto previsto dagli artt. 23 e 26 del Codice, i dati genetici possono essere trattati e i campioni biologici utilizzati soltanto per gli scopi indicati nella presente autorizzazione e rispetto ai quali la persona abbia manifestato previamente e per iscritto il proprio consenso informato.

In conformità all'art. 23 del Codice, il consenso resta valido solo se l'interessato è libero da ogni condizionamento o coercizione e resta revocabile liberamente in ogni momento.

Nel caso in cui l'interessato revochi il consenso al trattamento dei dati per scopi di ricerca, è distrutto anche il campione biologico sempre che sia stato prelevato per tali scopi, salvo che, in origine o a seguito di trattamento, il campione non possa più essere riferito ad una persona identificata o identificabile.

Per i trattamenti effettuati mediante *test* genetici, compreso lo *screening*, anche a fini di ricerca o di ricongiungimento familiare, deve essere acquisito il consenso informato dei soggetti cui viene prelevato il materiale biologico necessario all'esecuzione dell'analisi. In questi casi, all'interessato è richiesto di dichiarare se vuole conoscere o meno i risultati dell'esame o della ricerca, comprese eventuali notizie inattese che lo riguardano, qualora queste ultime rappresentino per l'interessato un beneficio concreto e diretto in termini di terapia o di prevenzione o di consapevolezza delle scelte riproduttive.

Per le informazioni relative ai nascituri il consenso è validamente prestato dalla gestante. Nel caso in cui il trattamento effettuato mediante *test* prenatale possa rivelare anche dati genetici relativi alla futura insorgenza di una patologia del padre, è previamente acquisito anche il consenso di quest'ultimo.

Quando il trattamento è necessario per la salvaguardia della vita e dell'incolumità fisica dell'interessato, e quest'ultimo non può prestare il proprio consenso per impossibilità fisica, incapacità d'agire o 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 applicano le disposizioni di cui all'art. 82 del Codice.

L'opinione del minore, nella misura in cui lo consente la sua età e il suo grado di maturità, è presa in considerazione. Negli altri casi di incapacità d'agire, impossibilità fisica o di incapacità di intendere o di volere, il trattamento è consentito se le finalità perseguite comportano un beneficio diretto per l'interessato e la sua opinione è, nei limiti del possibile, presa in considerazione.

I trattamenti di dati connessi all'esecuzione di *test* genetici presintomatici possono essere effettuati sui minori non affetti, ma a rischio per patologie genetiche solo nel caso in cui esistano concrete possibilità di terapie o di trattamenti preventivi prima del raggiungimento della maggiore età. I *test* sulla variabilità individuale non possono essere condotti su minori senza che venga acquisito il consenso di ambedue i genitori, ove esercitano entrambi la potestà sul minore.

I trattamenti di dati connessi all'esecuzione di *test* genetici per lo svolgimento delle investigazioni difensive o per l'esercizio di un diritto in sede giudiziaria possono essere effettuati soltanto con il consenso informato della persona cui appartiene il materiale biologico necessario all'indagine, salvo che un'espressa disposizione di legge disponga altrimenti.

7) Trattamenti in settori particolari

I dati genetici trattati e i campioni biologici prelevati per l'esecuzione di test sulla variabilità individuale ai fini dello svolgimento delle investigazioni difensive o per l'esercizio di un diritto in un procedimento penale non possono essere utilizzati per altri fini. I dati trattati e i campioni biologici prelevati per l'esecuzione di *test* genetici a fini di prevenzione, di diagnosi o di terapia nei confronti dell'interessato o per finalità di ricerca scientifica e statistica possono essere utilizzati per lo svolgimento delle investigazioni difensive o per l'esercizio di un diritto in un procedimento penale, nel rispetto delle pertinenti disposizioni di legge.

8) Conservazione dei dati e dei campioni

Con riferimento all'obbligo previsto dall'art. 11, comma 1, lett. *e*), del Codice, i campioni biologici e i dati genetici possono essere conservati per il periodo di tempo non superiore a quello strettamente necessario per adempiere agli obblighi o ai compiti indicati al punto 3 della presente autorizzazione o per perseguire le finalità ivi menzionate per le quali sono stati raccolti o successivamente utilizzati.

I campioni biologici prelevati e i dati genetici trattati per l'esecuzione di *test* e di *screening* genetici sono conservati per un periodo di tempo non superiore a quello necessario allo svolgimento dell'analisi o al perseguimento degli scopi per i quali sono stati raccolti o successivamente utilizzati.

I dati genetici trattati a fini di ricongiungimento familiare sono conservati per un periodo di tempo non superiore a quello necessario all'esame dell'istanza di ricongiungimento, salvo che per l'eventuale conservazione, a norma di legge, dell'atto o del documento che li contiene. A seguito del rigetto o dell'accoglimento dell'istanza, i campioni prelevati per l'accertamento dei vincoli di consanguineità devono essere distrutti (art. 11, comma 1, lett. *e*), del Codice).

Ai sensi dell'art. 11, comma 1, lett. *c*), *d*) ed *e*), del Codice, i soggetti autorizzati verificano periodicamente l'esattezza e l'aggiornamento dei dati, nonché la loro pertinenza, completezza, non eccedenza e indispensabilità rispetto alle finalità perseguite nei singoli casi, anche con riferimento ai dati che l'interessato fornisce di propria iniziativa. I dati che, anche a seguito delle verifiche, risultano eccedenti o non pertinenti o non indispensabili non possono essere utilizzati.

I campioni biologici prelevati e i dati genetici raccolti per scopi di tutela della salute possono essere conservati ed utilizzati per finalità di ricerca scientifica o statistica, ferma restando la necessità di acquisire il consenso informato delle persone interessate, eccetto che nei casi di indagini statistiche o ricerche scientifiche previste dalla legge. La conservazione e l'ulteriore utilizzo di campioni biologici e di dati genetici raccolti per la realizzazione di progetti di ricerca e indagini statistiche, diversi da quelli per i quali è stato originariamente acquisito il consenso informato degli interessati, sono consentiti limitatamente al perseguimento di scopi scientifici e statistici direttamente collegati con quelli originari. Ciò, a meno che venga nuovamente acquisito il consenso degli interessati, ovvero i campioni biologici e i dati genetici, in origine o a seguito di trattamento, non consentano più di identificare i medesimi interessati, oppure a causa di particolari ragioni non sia possibile informarli malgrado sia stato compiuto ogni ragionevole sforzo per raggiungerli e il programma di ricerca, oggetto di motivato parere favorevole del competente comitato etico a livello territoriale, sia autorizzato appositamente dal Garante ai sensi dell'art. 90 del Codice.

9) Comunicazione e diffusione dei dati

I dati genetici non possono essere comunicati e i campioni biologici non possono essere messi a disposizione di terzi salvo che sia indispensabile per il perseguimento delle finalità indicate dalla presente autorizzazione.

I dati genetici e i campioni biologici raccolti per scopi di ricerca scientifica e statistica possono essere comunicati o trasferiti a enti e istituti di ricerca, alle associazioni e agli altri organismi pubblici e privati aventi finalità di ricerca, esclusivamente nell'ambito di progetti congiunti.

I dati genetici e i campioni biologici raccolti per scopi di ricerca scientifica e statistica possono essere comunicati o trasferiti ai soggetti sopra indicati, non partecipanti a progetti congiunti, limitatamente alle informazioni prive di dati identificativi, per scopi scientifici direttamente collegati a quelli per i quali sono stati originariamente raccolti e chiaramente determinati per iscritto nella richiesta dei dati e/o dei campioni. In tal caso, il soggetto richiedente si impegna a non trattare i dati e/o utilizzare i campioni per fini diversi da quelli indicati nella richiesta e a non comunicarli o trasferirli ulteriormente a terzi.

I dati genetici raccolti a fini di ricongiungimento familiare possono essere comunicati unicamente alle rappresentanze diplomatiche o consolari competenti all'esame della documentazione prodotta dall'interessato o all'organismo internazionale ritenuto idoneo dal Ministero degli affari esteri cui questi si sia rivolto. I campioni biologici prelevati ai medesimi fini possono essere trasferiti unicamente al laboratorio designato per l'effettuazione del test sulla variabilità individuale o all'organismo internazionale ritenuto idoneo dal Ministero degli affari esteri.

Fermo restando quanto previsto dall'art. 84 del Codice, i dati genetici devono essere resi noti di regola direttamente all'interessato o a persone diverse dal diretto interessato sulla base di una delega scritta di quest'ultimo, adottando ogni mezzo idoneo a prevenire la conoscenza non autorizzata da parte di soggetti anche compresenti. La comunicazione nelle mani di un delegato dell'interessato è eseguita in plico chiuso.

Gli esiti di *test* e di *screening* genetici, nonché i risultati delle ricerche qualora comportino per l'interessato un beneficio concreto e diretto in termini di terapia, prevenzione o di consapevolezza delle scelte riproduttive, devono essere comunicati al medesimo interessato anche nel rispetto della sua dichiarazione di volontà di conoscere o meno tali eventi e, ove necessario, con un'appropriata consulenza genetica.

I risultati delle ricerche, qualora comportino un beneficio concreto e diretto in termini di terapia, prevenzione o di consapevolezza delle scelte riproduttive, anche per gli appartenenti alla stessa linea genetica dell'interessato, possono essere comunicati a questi ultimi, qualora ne facciano richiesta e l'interessato vi abbia espressamente acconsentito, o sia deceduto e, in vita, non abbia espressamente fornito indicazioni contrarie.

In caso di ricerche condotte su popolazioni isolate, devono essere resi noti alle comunità interessate e alle autorità locali gli eventuali risultati della ricerca che rivestono un'importanza terapeutica o preventiva per la tutela della salute delle persone appartenenti a tali comunità.

I dati genetici non possono essere diffusi. I risultati delle ricerche non possono essere diffusi se non in forma aggregata, ovvero secondo modalità che non rendano identificabili gli interessati neppure tramite dati identificativi indiretti, anche nell'ambito di pubblicazioni.

10) Richieste di autorizzazione

I titolari dei trattamenti che rientrano nell'ambito di applicazione della presente autorizzazione non sono tenuti a presentare una richiesta di autorizzazione a questa Autorità, qualora il trattamento che si intende effettuare sia conforme alle prescrizioni suddette.

Le richieste di autorizzazione pervenute o che perverranno anche successivamente alla data di adozione del presente provvedimento, devono intendersi accolte nei termini di cui al provvedimento medesimo.

Il Garante non prenderà in considerazione richieste di autorizzazione per trattamenti da effettuarsi in difformità alle prescrizioni del presente provvedimento, salvo che il loro accoglimento sia giustificato da circostanze del tutto particolari o da situazioni eccezionali non considerate nella presente autorizzazione, relative, ad esempio, al caso in cui la raccolta del consenso comporti un impiego di mezzi manifestamente sproporzionato in ragione, in particolare, del numero di persone interessate.

11) Norme finali

Restano fermi gli obblighi previsti da norme di legge o di regolamento, ovvero dalla normativa comunitaria, che stabiliscono divieti o limiti in materia di trattamento di dati genetici.

Resta fermo per il titolare del trattamento di dati genetici l'obbligo di effettuare, nei casi previsti, la notificazione al Garante prima dell'inizio del trattamento medesimo (artt. 37 e 163 del Codice).

12) Efficacia temporale e disciplina transitoria

La presente autorizzazione ha efficacia dal 1° aprile 2007 al 31 dicembre 2008.

Qualora alla data di pubblicazione della presente autorizzazione il trattamento non sia già

conforme alle sue prescrizioni, il titolare deve adeguarsi ad esse entro il 1° settembre 2007.

La presente autorizzazione sarà pubblicata nella *Gazzetta Ufficiale* della Repubblica italiana.

Roma, 22 febbraio 2007

IL PRESIDENTE
Pizzetti

IL RELATORE
Pizzetti

IL SEGRETARIO GENERALE
Buttarelli

28 Autorizzazione n. 1/2007 al trattamento dei dati sensibili nei rapporti di lavoro (*) *28 giugno 2007*

Registro delle deliberazioni
n. 24 del 28 giugno 2007

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

In data odierna, con la partecipazione del prof. Francesco Pizzetti, presidente, del dott. Giuseppe Chiaravalloti, vice presidente, del dott. Mauro Paissan e del dott. Giuseppe Fortunato, componenti, e del dott. Giovanni Buttarelli, segretario generale;

Visto il decreto legislativo 30 giugno 2003, n. 196, recante il Codice in materia di protezione dei dati personali;

Visto, in particolare, l'art. 4, comma 1, lett. *d*), del citato Codice, il quale individua i dati sensibili;

Considerato che, ai sensi dell'art. 26, comma 1, del Codice, i soggetti privati e gli enti pubblici economici possono trattare i dati sensibili solo previa autorizzazione di questa Autorità e, ove necessario, con il consenso scritto degli interessati, nell'osservanza dei presupposti e dei limiti stabiliti dal Codice, nonché dalla legge e dai regolamenti;

Visto il comma 4, lett. *d*), del medesimo art. 26, il quale stabilisce che i dati sensibili possono essere oggetto di trattamento anche senza consenso, previa autorizzazione del Garante, quando il trattamento medesimo è necessario per adempiere a specifici obblighi o compiti previsti dalla legge, da un regolamento o dalla normativa comunitaria per la gestione del rapporto di lavoro, anche in materia di igiene e sicurezza del lavoro e della popolazione e di previdenza e assistenza, nei limiti previsti dall'autorizzazione e ferme restando le disposizioni del codice di deontologia e di buona condotta di cui all'art. 111 del Codice;

Considerato che il trattamento dei dati in questione può essere autorizzato dal Garante anche d'ufficio con provvedimenti di carattere generale, relativi a determinate categorie di titolari o di trattamenti (art. 40 del Codice);

Considerato che le autorizzazioni di carattere generale sinora rilasciate sono risultate uno strumento idoneo per prescrivere misure uniformi a garanzia degli interessati, rendendo altresì superflua la richiesta di singoli provvedimenti di autorizzazione da parte di numerosi titolari del trattamento;

Ritenuto opportuno rilasciare nuove autorizzazioni in sostituzione di quelle in scadenza il 30 giugno 2007, armonizzando le prescrizioni già impartite alla luce dell'esperienza maturata;

Ritenuto opportuno che anche tali nuove autorizzazioni siano provvisorie e a tempo determinato, ai sensi dell'art. 41, comma 5, del Codice e, in particolare, efficaci per il periodo di dodici mesi;

Considerata la necessità di garantire il rispetto di alcuni principi volti a ridurre al minimo i rischi di danno o di pericolo che i trattamenti potrebbero comportare per i diritti e le libertà fondamentali, nonché per la dignità delle persone, e, in particolare, per il diritto alla protezione dei dati personali sancito dall'art. 1 del Codice;

(*) ***G.U.*** **24 agosto 2007, n. 196**
[doc. *web* n. 1429762]

Considerato che un elevato numero di trattamenti di dati sensibili è effettuato nell'ambito dei rapporti di lavoro;

Visto l'art. 167 del Codice;

Visto l'art. 11, comma 2, del Codice, il quale stabilisce che i dati trattati in violazione della disciplina rilevante in materia di trattamento di dati personali non possono essere utilizzati;

Visti gli articoli 31 e seguenti del Codice e il disciplinare tecnico di cui all'Allegato B) al medesimo Codice recanti norme e regole sulle misure di sicurezza;

Visto l'art. 41 del Codice;

Visti gli atti d'ufficio;

Viste le osservazioni dell'Ufficio formulate dal segretario generale ai sensi dell'art. 15 del regolamento del Garante n. 1/2000;

Relatore il prof. Francesco Pizzetti;

Autorizza

il trattamento dei dati sensibili di cui all'art. 4, comma 1, lett. *d*), del Codice, finalizzato alla gestione dei rapporti di lavoro, secondo le prescrizioni di seguito indicate.

Prima di iniziare o proseguire il trattamento 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, in conformità all'art. 3 del Codice.

1) Ambito di applicazione

La presente autorizzazione è rilasciata:

a) alle persone fisiche e giuridiche, alle imprese, anche sociali, agli enti, alle associazioni e agli organismi che sono parte di un rapporto di lavoro o che utilizzano prestazioni lavorative anche atipiche, parziali o temporanee, o che comunque conferiscono un incarico professionale alle figure indicate al successivo punto 2, lettere b) e c);

b) ad organismi paritetici o che gestiscono osservatori in materia di lavoro, previsti dalla normativa comunitaria, dalle leggi, dai regolamenti o dai contratti collettivi anche aziendali;

l'autorizzazione riguarda anche l'attività svolta:

c) dal medico competente in materia di igiene e di sicurezza del lavoro, in qualità di libero professionista o di dipendente dei soggetti di cui alla lettera a) o di strutture convenzionate;

d) da associazioni, organizzazioni, federazioni o confederazioni rappresentative di categorie di datori di lavoro, al solo fine di perseguire le finalità di cui al punto 3), lettera *h*).

2) Interessati ai quali i dati si riferiscono

Il trattamento può riguardare i dati sensibili attinenti:

a) a lavoratori subordinati, anche se parti di un contratto di apprendistato, o di formazione e lavoro, o di inserimento, o di lavoro ripartito, o di lavoro intermittente o a chiamata, ovvero prestatori di lavoro nell'ambito di un contratto di somministrazione, o in rapporto di tirocinio, ovvero ad associati anche in compartecipazione e, se necessario in base ai punti 3) e 4), ai relativi familiari e conviventi;

b) a consulenti e a liberi professionisti, ad agenti, rappresentanti e mandatari;

c) a soggetti che effettuano prestazioni coordinate e continuative, anche nella modalità di lavoro a progetto, o ad altri lavoratori autonomi in rapporto di collaborazione, anche sotto forma di prestazioni di lavoro accessorio, con i soggetti di cui al punto 1);
d) a candidati all'instaurazione dei rapporti di lavoro di cui alle lettere precedenti;
e) a persone fisiche che ricoprono cariche sociali o altri incarichi nelle persone giuridiche, negli enti, nelle associazioni e negli organismi di cui al punto 1);
f) a terzi danneggiati nell'esercizio dell'attività lavorativa o professionale dai soggetti di cui alle precedenti lettere.

3) Finalità del trattamento

Il trattamento dei dati sensibili deve essere indispensabile:

a) per adempiere o per esigere l'adempimento di specifici obblighi o per eseguire specifici compiti previsti dalla normativa comunitaria, da leggi, da regolamenti o da contratti collettivi anche aziendali, in particolare ai fini dell'instaurazione, gestione ed estinzione del rapporto di lavoro, nonché dell'applicazione della normativa in materia di previdenza ed assistenza anche integrativa, o in materia di igiene e sicurezza del lavoro o della popolazione, nonché in materia fiscale, sindacale, di tutela della salute, dell'ordine e della sicurezza pubblica;
b) anche fuori dei casi di cui alla lettera a), in conformità alla legge e per scopi determinati e legittimi, ai fini della tenuta della contabilità o della corresponsione di stipendi, assegni, premi, altri emolumenti, liberalità o benefici accessori;
c) per perseguire finalità di salvaguardia della vita o dell'incolumità fisica dell'interessato o di un terzo;
d) per far valere o difendere un diritto anche da parte di un terzo in sede giudiziaria, nonché in sede amministrativa o nelle procedure di arbitrato e di conciliazione nei casi previsti dalle leggi, dalla normativa comunitaria, dai regolamenti o dai contratti collettivi, sempre che i dati siano trattati esclusivamente per tali finalità e per il periodo strettamente necessario al loro perseguimento. Qualora i dati siano idonei a rivelare lo stato di salute e la vita sessuale, il diritto da far valere o difendere deve essere di rango pari a quello dell'interessato, ovvero consistente in un diritto della personalità o in un altro diritto o libertà fondamentale e inviolabile;
e) per esercitare il diritto di accesso ai documenti amministrativi, nel rispetto di quanto stabilito dalle leggi e dai regolamenti in materia;
f) per adempiere ad obblighi derivanti da contratti di assicurazione finalizzati alla copertura dei rischi connessi alla responsabilità del datore di lavoro in materia di igiene e di sicurezza del lavoro e di malattie professionali o per i danni cagionati a terzi nell'esercizio dell'attività lavorativa o professionale;
g) per garantire le pari opportunità;
h) per perseguire scopi determinati e legittimi individuati dagli statuti di associazioni, organizzazioni, federazioni o confederazioni rappresentative di categorie di datori di lavoro o dai contratti collettivi, in materia di assistenza sindacale ai datori di lavoro.

4) Categorie di dati

Il trattamento può avere per oggetto i dati strettamente pertinenti ai sopra indicati obblighi, compiti o finalità che non possano essere adempiuti o realizzati, caso per caso, mediante il trattamento di dati anonimi o di dati personali di natura diversa, e in particolare:

a) nell'ambito dei dati idonei a rivelare le convinzioni religiose, filosofiche o di altro genere, ovvero l'adesione ad associazioni od organizzazioni a carattere religioso o filosofico, i dati concernenti la fruizione di permessi e festività religiose o di servizi di mensa, nonché la manifestazione, nei casi previsti dalla legge, dell'obiezione di coscienza;
b) nell'ambito dei dati idonei a rivelare le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere politico o sindacale, i dati concernenti l'esercizio di funzioni pubbliche e di incarichi politici, di attività o di incarichi sindacali (sempre che il trattamento sia effettuato ai fini della fruizione di permessi o di periodi di aspettativa riconosciuti dalla legge o, eventualmente, dai contratti collettivi anche aziendali), ovvero l'organizzazione di pubbliche iniziative, nonché i dati inerenti alle trattenute per il versamento delle quote di ser-

vizio sindacale o delle quote di iscrizione ad associazioni od organizzazioni politiche o sindacali;

c) nell'ambito dei dati idonei a rivelare lo stato di salute, i dati raccolti e ulteriormente trattati in riferimento a invalidità, infermità, gravidanza, puerperio o allattamento, ad infortuni, ad esposizioni a fattori di rischio, all'idoneità psicofisica a svolgere determinate mansioni, all'appartenenza a determinate categorie protette, nonché i dati contenuti nella certificazione sanitaria attestante lo stato di malattia, anche professionale dell'interessato, o comunque relativi anche all'indicazione della malattia come specifica causa di assenza del lavoratore.

5) Modalità di trattamento

Fermi restando gli obblighi previsti dagli articoli 11 e 14 del Codice, nonché dagli articoli 31 e seguenti del Codice e dall'Allegato B) al medesimo Codice, il trattamento dei dati sensibili deve essere effettuato unicamente con operazioni, nonché con logiche e mediante forme di organizzazione dei dati strettamente indispensabili in rapporto ai sopra indicati obblighi, compiti o finalità.

I dati sono raccolti, di regola, presso l'interessato.

La comunicazione di dati all'interessato deve avvenire di regola direttamente a quest'ultimo o a un suo delegato (fermo restando quanto previsto dall'art. 84, comma 1, del Codice), in plico chiuso o con altro mezzo idoneo a prevenire la conoscenza da parte di soggetti non autorizzati, anche attraverso la previsione di distanze di cortesia.

Restano inoltre fermi gli obblighi di informare l'interessato e, ove necessario, di acquisirne il consenso scritto, in conformità a quanto previsto dagli articoli 13, 23 e 26 del Codice.

6) Conservazione dei dati

Nel quadro del rispetto dell'obbligo previsto dall'art. 11, comma 1, lettera *e*), del Codice, i dati sensibili possono essere conservati per un periodo non superiore a quello necessario per adempiere agli obblighi o ai compiti di cui al punto 3), ovvero per perseguire le finalità ivi menzionate. A tal fine, anche mediante controlli periodici, deve essere verificata costantemente la stretta pertinenza, non eccedenza e indispensabilità dei dati rispetto al rapporto, alla prestazione o all'incarico in corso, da instaurare o cessati, anche con riferimento ai dati che l'interessato fornisce di propria iniziativa. I dati che, anche a seguito delle verifiche, risultano eccedenti o non pertinenti o non indispensabili non possono essere utilizzati, salvo che per l'eventuale conservazione, a norma di legge, dell'atto o del documento che li contiene. Specifica attenzione è prestata per l'indispensabilità dei dati riferiti a soggetti diversi da quelli cui si riferiscono direttamente le prestazioni e gli adempimenti.

7) Comunicazione e diffusione dei dati

I dati sensibili possono essere comunicati e, ove necessario, diffusi nei limiti strettamente pertinenti agli obblighi, ai compiti o alle finalità di cui al punto 3), a soggetti pubblici o privati, ivi compresi organismi sanitari, casse e fondi di previdenza ed assistenza sanitaria integrativa anche aziendale, istituti di patronato e di assistenza sociale, centri di assistenza fiscale, agenzie per il lavoro, associazioni ed organizzazioni sindacali di datori di lavoro e di prestatori di lavoro, liberi professionisti, società esterne titolari di un autonomo trattamento di dati e familiari dell'interessato.

Ai sensi dell'art. 26, comma 5, del Codice, i dati idonei a rivelare lo stato di salute non possono essere diffusi.

8) Richieste di autorizzazione

I titolari dei trattamenti che rientrano nell'ambito di applicazione della presente autorizzazione non sono tenuti a presentare una richiesta di autorizzazione a questa Autorità, qualora il trattamento che si intende effettuare sia conforme alle prescrizioni suddette.

Le richieste di autorizzazione pervenute o che perverranno anche successivamente alla data di adozione del presente provvedimento, devono intendersi accolte nei termini di cui al provvedimento medesimo.

Il Garante non prenderà in considerazione richieste di autorizzazione per trattamenti da effettuarsi in difformità dalle prescrizioni del presente provvedimento, salvo che, ai sensi dell'art. 41 del Codice, il loro accoglimento sia giustificato da circostanze del tutto particolari o da situazioni eccezionali non considerate nella presente autorizzazione.

9) Norme finali

Restano fermi gli obblighi previsti da norme di legge o di regolamento, ovvero dalla normativa comunitaria, che stabiliscono divieti o limiti in materia di trattamento di dati personali e, in particolare, dalle disposizioni contenute:

a) nell'art. 8 della legge 20 maggio 1970, n. 300, che vieta al datore di lavoro ai fini dell'assunzione e nello svolgimento del rapporto di lavoro, di effettuare indagini, anche a mezzo di terzi, sulle opinioni politiche, religiose o sindacali del lavoratore, nonché su fatti non rilevanti ai fini della valutazione dell'attitudine professionale del lavoratore;

b) nell'art. 6 della legge 5 giugno 1990, n. 135, che vieta ai datori di lavoro lo svolgimento di indagini volte ad accertare, nei dipendenti o in persone prese in considerazione per l'instaurazione di un rapporto di lavoro, l'esistenza di uno stato di sieropositività;

c) nelle norme in materia di pari opportunità o volte a prevenire discriminazioni;

d) fermo restando quanto disposto dall'art. 8 della legge 20 maggio 1970, n. 300, nell'art. 10 del decreto legislativo 10 settembre 2003, n. 276, che vieta alle agenzie per il lavoro e agli altri soggetti privati autorizzati o accreditati di effettuare qualsivoglia indagine o comunque trattamento di dati ovvero di preselezione di lavoratori, anche con il loro consenso, in base alle convinzioni personali, alla affiliazione sindacale o politica, al credo religioso, al sesso, all'orientamento sessuale, allo stato matrimoniale o di famiglia o di gravidanza, alla età, all'*handicap*, alla razza, all'origine etnica, al colore, alla ascendenza, all'origine nazionale, al gruppo linguistico, allo stato di salute e ad eventuali controversie con i precedenti datori di lavoro, nonché di trattare dati personali dei lavoratori che non siano strettamente attinenti alle loro attitudini professionali e al loro inserimento lavorativo.

10) Efficacia temporale e disciplina transitoria

La presente autorizzazione ha efficacia a decorrere dal 1° luglio 2007 fino al 30 giugno 2008, salve eventuali modifiche che il Garante ritenga di dover apportare in conseguenza di eventuali novità normative rilevanti in materia.

La presente autorizzazione sarà pubblicata nella *Gazzetta Ufficiale* della Repubblica italiana.

Roma, 28 giugno 2007

IL PRESIDENTE
Pizzetti

IL RELATORE
Pizzetti

IL SEGRETARIO GENERALE
Buttarelli

29 Autorizzazione n. 2/2007 al trattamento dei dati idonei a rivelare lo stato di salute e la vita sessuale (*) *28 giugno 2007*

Registro delle deliberazioni
n. 25 del 28 giugno 2007

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

In data odierna, con la partecipazione del prof. Francesco Pizzetti, presidente, del dott. Giuseppe Chiaravalloti, vicepresidente, del dott. Mauro Paissan e del dott. Giuseppe Fortunato, componenti, e del dott. Giovanni Buttarelli, segretario generale;

Visto il decreto legislativo 30 giugno 2003, n. 196, recante il Codice in materia di protezione dei dati personali;

Visto, in particolare, l'art. 4, comma 1, lett. *d*), del citato Codice, il quale individua i dati sensibili;

Considerato che, ai sensi dell'art. 26, comma 1, del Codice, i soggetti privati e gli enti pubblici economici possono trattare i dati sensibili solo previa autorizzazione di questa Autorità e, ove necessario, con il consenso scritto degli interessati, nell'osservanza dei presupposti e dei limiti stabiliti dal Codice, nonché dalla legge e dai regolamenti;

Visto l'art. 76 del Codice, secondo cui gli esercenti le professioni sanitarie e gli organismi sanitari pubblici, anche nell'ambito di un'attività di rilevante interesse pubblico ai sensi dell'articolo 85 del medesimo Codice, possono trattare i dati personali idonei a rivelare lo stato di salute anche senza il consenso dell'interessato, previa autorizzazione del Garante, se il trattamento riguarda dati e operazioni indispensabili per perseguire una finalità di tutela della salute o dell'incolumità fisica di un terzo o della collettività;

Considerato che il trattamento dei dati in questione può essere autorizzato dal Garante anche d'ufficio con provvedimenti di carattere generale, relativi a determinate categorie di titolari o di trattamenti (art. 40 del Codice);

Considerato che le autorizzazioni di carattere generale sin ora rilasciate sono risultate uno strumento idoneo per prescrivere misure uniformi a garanzia degli interessati, rendendo altresì superflua la richiesta di singoli provvedimenti di autorizzazione da parte di numerosi titolari del trattamento;

Ritenuto opportuno rilasciare nuove autorizzazioni in sostituzione di quelle in scadenza il 30 giugno 2007, armonizzando le prescrizioni già impartite alla luce dell'esperienza maturata;

Ritenuto opportuno che anche tali nuove autorizzazioni siano provvisorie e a tempo determinato, ai sensi dell'art. 41, comma 5, del Codice e, in particolare, efficaci per il periodo di dodici mesi;

Considerata la necessità di garantire il rispetto di alcuni principi volti a ridurre al minimo i rischi di danno o di pericolo che i trattamenti potrebbero comportare per i diritti e le libertà fondamentali, nonché per la dignità delle persone, e, in particolare, per il diritto alla protezione dei dati personali sancito dall'art. 1 del Codice, principi valutati anche sulla base delle raccomandazioni adottate in materia di dati sanitari dal Consiglio d'Europa ed in particolare dalla Raccomandazione N. R (97) 5, in base alla quale i dati sanitari devono

(*) *G.U.* 24 agosto 2007, n. 196
[doc. *web* n. 1429775]

essere trattati, di regola, solo nell'ambito dell'assistenza sanitaria o sulla base di regole di segretezza e di efficacia pari a quelle previste in tale ambito;

Considerato che un elevato numero di trattamenti idonei a rivelare lo stato di salute e la vita sessuale è effettuato per finalità di prevenzione o di cura, per la gestione di servizi socio-sanitari, per ricerche scientifiche o per la fornitura all'interessato di prestazioni, beni o servizi;

Visto l'art. 167 del Codice;

Visto l'art. 11, comma 2, del Codice, il quale stabilisce che i dati trattati in violazione della disciplina rilevante in materia di trattamento di dati personali non possono essere utilizzati;

Visti gli articoli 31 e seguenti del Codice e il disciplinare tecnico di cui all'Allegato B) al Codice in materia di protezione dei dati personali recanti norme e regole sulle misure di sicurezza;

Visto l'art. 41 del Codice;

Visti gli atti d'ufficio;

Viste le osservazioni dell'Ufficio formulate dal segretario generale ai sensi dell'art. 15 del regolamento del Garante n. 1/2000;

Relatore il prof. Francesco Pizzetti;

Autorizza

a) gli esercenti le professioni sanitarie a trattare i dati idonei a rivelare lo stato di salute, qualora i dati e le operazioni siano indispensabili per tutelare l'incolumità fisica o la salute di un terzo o della collettività, e il consenso non sia prestato o non possa essere prestato per effettiva irreperibilità;
b) gli organismi e le case di cura private, nonché ogni altro soggetto privato, a trattare con il consenso i dati idonei a rivelare lo stato di salute e la vita sessuale;
c) gli organismi sanitari pubblici, istituiti anche presso università, ivi compresi i soggetti pubblici allorché agiscano nella qualità di autorità sanitarie, a trattare i dati idonei a rivelare lo stato di salute, qualora ricorrano contemporaneamente le seguenti condizioni:
   1) il trattamento sia finalizzato alla tutela dell'incolumità fisica e della salute di un terzo o della collettività;
   2) manchi il consenso (articolo 76, comma 1, lett. *b*), del Codice), in quanto non sia prestato o non possa essere prestato per effettiva irreperibilità;
   3) non si tratti di attività amministrative correlate a quelle di prevenzione, diagnosi, cura e riabilitazione ai sensi dell'art. 85, commi 1 e 2, del Codice;
d) anche soggetti diversi da quelli di cui alle lettere a), b) e c) a trattare i dati idonei a rivelare lo stato di salute e la vita sessuale, qualora il trattamento sia necessario per la salvaguardia della vita o dell'incolumità fisica di un terzo. Se la medesima finalità riguarda l'interessato e quest'ultimo non può prestare il proprio consenso per impossibilità fisica, per incapacità di agire o per incapacità d'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.

Per l'informativa e, ove previsto, il consenso si osservano anche le disposizioni di cui agli articoli 13, 23, 26 e da 75 a 82 del Codice.

1) Ambito di applicazione e finalità del trattamento

1.1. L'autorizzazione è rilasciata:
a) ai medici-chirurghi, ai farmacisti, agli odontoiatri, agli psicologi e agli altri esercenti le professioni sanitarie iscritti in albi o in elenchi;

b) al personale sanitario infermieristico, tecnico e della riabilitazione che esercita l'attività in regime di libera professione;
c) alle istituzioni e agli organismi sanitari privati, anche quando non operino in rapporto con il servizio sanitario nazionale.

In tali casi, l'autorizzazione è rilasciata anche per consentire ai destinatari di adempiere o di esigere l'adempimento di specifici obblighi o di eseguire specifici compiti previsti da leggi, dalla normativa comunitaria o da regolamenti, in particolare in materia di igiene e di sanità pubblica, di prevenzione delle malattie professionali e degli infortuni, di diagnosi e cura, ivi compresi i trapianti di organi e tessuti, di riabilitazione degli stati di invalidità e di inabilità fisica e psichica, di profilassi delle malattie infettive e diffusive, di tutela della salute mentale, di assistenza farmaceutica, di medicina scolastica e di assistenza sanitaria alle attività sportive o di accertamento, in conformità alla legge, degli illeciti previsti dall'ordinamento sportivo. Il trattamento può riguardare anche la compilazione di cartelle cliniche, di certificati e di altri documenti di tipo sanitario, ovvero di altri documenti relativi alla gestione amministrativa la cui utilizzazione sia necessaria per i fini appena indicati.

Qualora il perseguimento di tali fini richieda l'espletamento di compiti di organizzazione o di gestione amministrativa, i destinatari della presente autorizzazione devono esigere che i responsabili e gli incaricati del trattamento preposti a tali compiti osservino le stesse regole di segretezza alle quali sono sottoposti i medesimi destinatari della presente autorizzazione, nel rispetto di quanto previsto anche dall'art. 83, comma 1, del Codice.

1.2. L'autorizzazione è rilasciata, altresì, ai seguenti soggetti:
a) alle persone fisiche o giuridiche, agli enti, alle associazioni e agli altri organismi privati, per scopi di ricerca scientifica, anche statistica, finalizzata alla tutela della salute dell'interessato, di terzi o della collettività in campo medico, biomedico o epidemiologico, allorché si debba intraprendere uno studio delle relazioni tra i fattori di rischio e la salute umana, o indagini su interventi sanitari di tipo diagnostico, terapeutico o preventivo, ovvero sull'utilizzazione di strutture socio-sanitarie, e la disponibilità di dati solo anonimi su campioni della popolazione non permetta alla ricerca di raggiungere i suoi scopi. In tali casi occorre acquisire il consenso (in conformità a quanto previsto dagli articoli 106, 107 e 110 del Codice), e il trattamento successivo alla raccolta non deve permettere di identificare gli interessati anche indirettamente, salvo che l'abbinamento al materiale di ricerca dei dati identificativi dell'interessato sia temporaneo ed essenziale per il risultato della ricerca, e sia motivato, altresì, per iscritto. I risultati della ricerca non possono essere diffusi se non in forma anonima. Resta fermo quanto previsto dall'art. 98 del Codice;
b) alle organizzazioni di volontariato o assistenziali, limitatamente ai dati e alle operazioni indispensabili per perseguire scopi determinati e legittimi previsti, in particolare, nelle rispettive norme statutarie;
c) alle comunità di recupero e di accoglienza, alle case di cura e di riposo, limitatamente ai dati e alle operazioni indispensabili per perseguire scopi determinati e legittimi previsti, in particolare, nelle rispettive norme statutarie;
d) agli enti, alle associazioni e alle organizzazioni religiose riconosciute, relativamente ai dati e alle operazioni indispensabili per perseguire scopi determinati e legittimi nei limiti di quanto stabilito dall'art. 26, comma 4, lettera *a)*, del Codice, fermo restando quanto previsto per le confessioni religiose dagli articoli 26, comma 3, lettera *a)*, e 181, comma 6, del Codice e dell'autorizzazione n. 3/2007;
e) alle persone fisiche e giuridiche, alle imprese, anche sociali, agli enti, alle associazioni e ad altri organismi, limitatamente ai dati, ove necessario attinenti anche alla vita sessuale, e alle operazioni indispensabili per adempiere agli obblighi, anche precontrattuali, derivanti da un rapporto di fornitura all'interessato di beni, di prestazioni o di servizi.
Se il rapporto intercorre con istituti di credito, imprese assicurative o riguarda valori mobiliari, devono considerarsi indispensabili i soli dati ed operazioni necessari per fornire specifici prodotti o servizi richiesti dall'interessato. Il rapporto può riguardare anche la fornitura di strumenti di ausilio per la vista, per l'udito o per la deambulazione;

f) alle persone fisiche e giuridiche, agli enti, alle associazioni e agli altri organismi che gestiscono impianti o strutture sportive, limitatamente ai dati e alle operazioni indispensabili per accertare l'idoneità fisica alla partecipazione ad attività sportive o agonistiche;
g) alle persone fisiche e giuridiche e ad altri organismi, limitatamente ai dati dei beneficiari e dei donatori e alle operazioni indispensabili per effettuare trapianti di organi e tessuti, nonché donazioni di sangue.

1.3. La presente autorizzazione è rilasciata, altresì, quando il trattamento dei dati idonei a rivelare lo stato di salute e la vita sessuale sia necessario per:
a) lo svolgimento delle investigazioni difensive di cui alla legge 7 dicembre 2000, n. 397, o comunque per far valere o difendere un diritto anche da parte di un terzo in sede giudiziaria, nonché in sede amministrativa o nelle procedure di arbitrato e di conciliazione nei casi previsti dalle leggi, dalla normativa comunitaria, dai regolamenti o dai contratti collettivi, sempre che il diritto sia di rango pari a quello dell'interessato, ovvero consistente in un diritto della personalità o in altro diritto o libertà fondamentale e inviolabile, e i dati siano trattati esclusivamente per tali finalità e per il periodo strettamente necessario per il loro perseguimento;
b) adempiere o esigere l'adempimento di specifici obblighi o per eseguire specifici compiti previsti dalla normativa comunitaria, da leggi, da regolamenti o da contratti collettivi per la gestione del rapporto di lavoro, nonché della normativa in materia di previdenza e assistenza o in materia di igiene e sicurezza del lavoro o della popolazione, nei limiti previsti dalla autorizzazione generale del Garante n. 1/2007 e ferme restando le disposizioni del codice di deontologia e di buona condotta di cui all'articolo 111 del Codice.

1.4. Il trattamento di dati genetici resta autorizzato nei limiti e alle condizioni individuati nell'autorizzazione del 22 febbraio 2007, pubblicata nella *Gazzetta Ufficiale* n. 65 del 19 marzo 2007.

2) Categorie di dati oggetto di trattamento

Prima di iniziare o proseguire il trattamento 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, in conformità all'art. 3 del Codice.

Il trattamento può avere per oggetto i dati strettamente pertinenti ai sopra indicati obblighi, compiti o finalità che non possano essere adempiuti o realizzati, caso per caso, mediante il trattamento di dati anonimi o di dati personali di natura diversa, e può comprendere le informazioni relative a stati di salute pregressi.

Devono essere considerate sottoposte all'ambito di applicazione della presente autorizzazione anche le informazioni relative ai nascituri, che devono essere trattate alla stregua dei dati personali in conformità a quanto previsto dalla citata Raccomandazione N. R (97) 5 del Consiglio d'Europa.

3) Modalità di trattamento

Fermi restando gli obblighi previsti dagli articoli 11 e 14 del Codice, nonché dagli articoli 31 e seguenti del Codice e dall'Allegato B) al medesimo Codice, il trattamento dei dati sensibili deve essere effettuato unicamente con operazioni, nonché con logiche e mediante forme di organizzazione dei dati strettamente indispensabili in rapporto ai sopra indicati obblighi, compiti o finalità.

I dati sono raccolti, di regola, presso l'interessato.

La comunicazione di dati all'interessato deve avvenire di regola direttamente a quest'ultimo o a un suo delegato (fermo restando quanto previsto dall'art. 84, comma 1, del Codice), in plico chiuso o con altro mezzo idoneo a prevenire la conoscenza da parte di soggetti non autorizzati, anche attraverso la previsione di distanze di cortesia.

Per le informazioni relative ai nascituri, il consenso è prestato dalla gestante. Dopo il raggiungimento della maggiore età l'informativa è fornita all'interessato anche ai fini della acquisizione di una nuova manifestazione del consenso quando questo è necessario (art. 82, comma 4, del Codice).

4) Conservazione dei dati

Nel quadro del rispetto dell'obbligo previsto dall'art. 11, comma 1, lett. *e)* del Codice, i dati possono essere conservati per un periodo non superiore a quello necessario per adempiere agli obblighi o ai compiti sopra indicati, ovvero per perseguire le finalità ivi menzionate. A tal fine, anche mediante controlli periodici, deve essere verificata costantemente la stretta pertinenza, non eccedenza e indispensabilità dei dati rispetto al rapporto, alla prestazione o all'incarico in corso, da instaurare o cessati, anche con riferimento ai dati che l'interessato fornisce di propria iniziativa. I dati che, anche a seguito delle verifiche, risultano eccedenti o non pertinenti o non indispensabili non possono essere utilizzati, salvo che per l'eventuale conservazione, a norma di legge, dell'atto o del documento che li contiene. Specifica attenzione è prestata per l'indispensabilità dei dati riferiti a soggetti diversi da quelli cui si riferiscono direttamente le prestazioni e gli adempimenti.

5) Comunicazione e diffusione dei dati

Salvo quanto previsto per i dati genetici al punto 9 della citata autorizzazione del 22 febbraio 2007, i dati idonei a rivelare lo stato di salute possono essere comunicati, nei limiti strettamente pertinenti agli obblighi, ai compiti e alle finalità di cui al punto 1), a soggetti pubblici e privati, ivi compresi i fondi e le casse di assistenza sanitaria integrativa, le aziende che svolgono attività strettamente correlate all'esercizio di professioni sanitarie o alla fornitura all'interessato di beni, di prestazioni o di servizi, gli istituti di credito e le imprese assicurative, le associazioni od organizzazioni di volontariato e i familiari dell'interessato.

Ai sensi degli artt. 22, comma 8, e 26, comma 5, del Codice, i dati idonei a rivelare lo stato di salute non possono essere diffusi.

I dati idonei a rivelare la vita sessuale non possono essere diffusi, salvo il caso in cui la diffusione riguardi dati resi manifestamente pubblici dall'interessato e per i quali l'interessato stesso non abbia manifestato successivamente la sua opposizione per motivi legittimi.

6) Richieste di autorizzazione

I titolari dei trattamenti che rientrano nell'ambito di applicazione della presente autorizzazione non sono tenuti a presentare una richiesta di autorizzazione a questa Autorità, qualora il trattamento che si intende effettuare sia conforme alle prescrizioni suddette.

Le richieste di autorizzazione pervenute o che perverranno anche successivamente alla data di adozione del presente provvedimento, devono intendersi accolte nei termini di cui al provvedimento medesimo.

Il Garante non prenderà in considerazione richieste di autorizzazione per trattamenti da effettuarsi in difformità alle prescrizioni del presente provvedimento, salvo che, ai sensi dell'art. 41 del Codice, il loro accoglimento sia giustificato da circostanze del tutto particolari o da situazioni eccezionali non considerate nella presente autorizzazione, relative, ad esempio, al caso in cui la raccolta del consenso comporti un impiego di mezzi manifestamente sproporzionato in ragione, in particolare, del numero di persone interessate.

7) Norme finali

Restano fermi gli obblighi previsti da norme di legge o di regolamento o dalla normativa comunitaria che stabiliscono divieti o limiti più restrittivi in materia di trattamento di dati personali e, in particolare:

a) dall'art. 5, comma 2, della legge 5 giugno 1990, n. 135, come modificato dall'art. 178 del Codice, secondo cui la rilevazione statistica della infezione da Hiv deve essere effettuata con modalità che non consentano l'identificazione della persona;

b) dall'art. 11 della legge 22 maggio 1978, n. 194, il quale dispone che l'ente ospedaliero, la casa di cura o il poliambulatorio nei quali è effettuato un intervento di interruzione di gravidanza devono inviare al medico provinciale competente per territorio una dichiarazione che non faccia menzione dell'identità della donna;

c) dall'art. 734-*bis* del codice penale, il quale vieta la divulgazione non consensuale delle generalità o dell'immagine della persona offesa da atti di violenza sessuale.

Restano altresì fermi gli obblighi di legge che vietano la rivelazione senza giusta causa e l'impiego a proprio o altrui profitto delle notizie coperte dal segreto professionale, nonché gli obblighi deontologici previsti, in particolare, dal codice di deontologia medica adottato dalla Federazione nazionale degli ordini dei medici chirurghi e degli odontoiatri.

Resta ferma, infine, la possibilità di diffondere dati anonimi anche aggregati e di includerli, in particolare, nelle pubblicazioni a contenuto scientifico o finalizzate all'educazione, alla prevenzione o all'informazione di carattere sanitario.

8) Efficacia temporale e disciplina transitoria

La presente autorizzazione ha efficacia a decorrere dal 1° luglio 2007 fino al 30 giugno 2008, salve eventuali modifiche che il Garante ritenga di dover apportare in conseguenza di eventuali novità normative rilevanti in materia.

La presente autorizzazione sarà pubblicata nella *Gazzetta Ufficiale* della Repubblica italiana.

Roma, 28 giugno 2007

IL PRESIDENTE
Pizzetti

IL RELATORE
Pizzetti

IL SEGRETARIO GENERALE
Buttarelli

30 Autorizzazione n. 3/2007 al trattamento dei dati sensibili da parte degli organismi di tipo associativo e delle fondazioni (*) *28 giugno 2007*

Registro delle deliberazioni
n. 26 del 28 giugno 2007

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

In data odierna, con la partecipazione del prof. Francesco Pizzetti, presidente, del dott. Giuseppe Chiaravalloti, vice presidente, del dott. Mauro Paissan e del dott. Giuseppe Fortunato, componenti, e del dott. Giovanni Buttarelli, segretario generale;

Visto il decreto legislativo 30 giugno 2003, n. 196, recante il Codice in materia di protezione dei dati personali;

Visto, in particolare, l'art. 4, comma 1, lett. *d*), del citato Codice, il quale individua i dati sensibili;

Considerato che, ai sensi dell'art. 26, comma 1, del Codice, i soggetti privati e gli enti pubblici economici possono trattare i dati sensibili solo previa autorizzazione di questa Autorità e, ove necessario, con il consenso scritto degli interessati, nell'osservanza dei presupposti e dei limiti stabiliti dal Codice, nonché dalla legge e dai regolamenti;

Visto altresì il comma 4, lett. *a*), del citato art. 26, il quale stabilisce che i dati sensibili possono essere oggetto di trattamento anche senza consenso, previa autorizzazione del Garante, *"quando il trattamento è effettuato da associazioni, enti ed organismi senza scopo di lucro, anche non riconosciuti, a carattere politico, filosofico, religioso o sindacale, ivi compresi partiti e movimenti politici, per il perseguimento di scopi determinati e legittimi individuati dall'atto costitutivo, dallo statuto o dal contratto collettivo, relativamente ai dati personali degli aderenti o dei soggetti che in relazione a tali finalità hanno contatti regolari con l'associazione, ente od organismo, sempre che i dati non siano comunicati all'esterno o diffusi e l'ente, associazione od organismo determini idonee garanzie relativamente ai trattamenti effettuati, prevedendo espressamente le modalità di utilizzo dei dati con determinazione resa nota agli interessati all'atto dell'informativa ai sensi dell'articolo 13"*;

Visto il comma 3, lettere *a*) e *b*), del predetto art. 26, il quale stabilisce che la disciplina di cui al relativo comma 1 non si applica al trattamento: 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; 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;

Rilevato che le confessioni di cui alla lettera *a*) devono determinare, ai sensi del medesimo art. 26, comma 3, lett. *a*), idonee garanzie relativamente ai trattamenti effettuati, nel rispetto dei principi indicati al riguardo con autorizzazione del Garante;

Visto l'art. 181, comma 6, del Codice secondo cui le confessioni religiose che, prima dell'adozione del medesimo Codice, abbiano determinato e adottato nell'ambito del rispettivo ordinamento le garanzie di cui al predetto art. 26, comma 3, lett. *a*), possono proseguire l'attività di trattamento nel rispetto delle medesime;

(*) *G.U.* 24 agosto 2007, n. 196
[doc. *web* n. 1429795]

Considerato che il trattamento dei dati in questione può essere autorizzato dal Garante anche d'ufficio con provvedimenti di carattere generale, relativi a determinate categorie di titolari o di trattamenti (art. 40 del Codice);

Considerato che le autorizzazioni di carattere generale sinora rilasciate sono risultate uno strumento idoneo per prescrivere misure uniformi a garanzia degli interessati, rendendo altresì superflua la richiesta di singoli provvedimenti di autorizzazione da parte di numerosi titolari del trattamento;

Ritenuto opportuno rilasciare nuove autorizzazioni in sostituzione di quelle in scadenza il 30 giugno 2007, armonizzando le prescrizioni già impartite alla luce dell'esperienza maturata;

Ritenuto opportuno che anche tali nuove autorizzazioni siano provvisorie e a tempo determinato, ai sensi dell'art. 41, comma 5, del Codice e, in particolare, efficaci per il periodo di dodici mesi;

Considerata la necessità di garantire il rispetto di alcuni principi volti a ridurre al minimo i rischi di danno o di pericolo che i trattamenti potrebbero comportare per i diritti e le libertà fondamentali, nonché per la dignità delle persone, e in particolare, per il diritto alla protezione dei dati personali sancito dall'art. 1 del Codice;

Considerato che un elevato numero di trattamenti di dati sensibili è effettuato da enti ed organizzazioni di tipo associativo e da fondazioni, per la realizzazione di scopi determinati e legittimi individuati dall'atto costitutivo, dallo statuto o da un contratto collettivo;

Visto l'art. 167 del Codice;

Visto l'art. 11, comma 2, del Codice, il quale stabilisce che i dati trattati in violazione della disciplina rilevante in materia di trattamento di dati personali non possono essere utilizzati;

Visti gli articoli 31 e seguenti del Codice e il disciplinare tecnico di cui all'Allegato B) al medesimo Codice, recanti norme e regole sulle misure di sicurezza;

Visto l'art. 41 del Codice;

Visti gli atti d'ufficio;

Viste le osservazioni dell'Ufficio formulate dal segretario generale ai sensi dell'art. 15 del regolamento del Garante n. 1/2000;

Relatore il dott. Mauro Paissan;

Autorizza

il trattamento dei dati sensibili di cui art. 4, comma 1, lett. *d*), del Codice da parte di associazioni, fondazioni, comitati ed altri organismi di tipo associativo, secondo le prescrizioni di seguito indicate.

Prima di iniziare o proseguire il trattamento 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, in conformità all'art. 3 del Codice.

1) Ambito di applicazione

La presente autorizzazione è rilasciata:

a) alle associazioni anche non riconosciute, ai partiti e ai movimenti politici, alle associazioni e alle organizzazioni sindacali, ai patronati e alle associazioni di categoria,

alle casse di previdenza, alle organizzazioni assistenziali o di volontariato, nonché alle federazioni e confederazioni nelle quali tali soggetti sono riuniti in conformità, ove esistenti, allo statuto, all'atto costitutivo o ad un contratto collettivo;

b) alle fondazioni, ai comitati e ad ogni altro ente, consorzio od organismo senza scopo di lucro, dotati o meno di personalità giuridica, ivi comprese le organizzazioni non lucrative di utilità sociale (Onlus);

c) alle cooperative sociali e alle società di mutuo soccorso di cui, rispettivamente, alle leggi 8 novembre 1991, n. 381 e 15 aprile 1886, n. 3818.

L'autorizzazione è rilasciata altresì agli istituti scolastici anche di tipo non associativo, limitatamente al trattamento dei dati idonei a rivelare le convinzioni religiose e per le operazioni strettamente necessarie per l'applicazione dell'articolo 310 del decreto legislativo 16 aprile 1994, n. 297 e degli artt. 3 e 10 del decreto legislativo 19 febbraio 2004, n. 59.

Resta fermo l'obbligo per le confessioni religiose di determinare, ai sensi dell'art. 26, comma 3, lett. *a)* del Codice, idonee garanzie relativamente ai trattamenti effettuati nel rispetto dei principi indicati con la presente autorizzazione.

Ai sensi dell'art. 181, comma 6, del Codice, le confessioni religiose che, prima dell'adozione del medesimo Codice, abbiano determinato e adottato nell'ambito del rispettivo ordinamento le garanzie di cui all'art. 26, comma 3, lett. *a)*, del Codice possono proseguire l'attività di trattamento effettuato dai relativi organi, ovvero da enti civilmente riconosciuti, nel rispetto delle medesime.

2) Finalità del trattamento

L'autorizzazione è rilasciata per il perseguimento di scopi determinati e legittimi individuati dall'atto costitutivo, dallo statuto o dal contratto collettivo, ove esistenti, e in particolare per il perseguimento di finalità culturali, religiose, politiche, sindacali, sportive o agonistiche di tipo non professionistico, di istruzione anche con riguardo alla libertà di scelta dell'insegnamento religioso, di formazione, di ricerca scientifica, di patrocinio, di tutela dell'ambiente e delle cose d'interesse artistico e storico, di salvaguardia dei diritti civili, nonché di beneficenza, assistenza sociale o socio-sanitaria.

La presente autorizzazione è rilasciata, altresì, per far valere o difendere un diritto anche da parte di un terzo in sede giudiziaria, nonché in sede amministrativa o nelle procedure di arbitrato e di conciliazione nei casi previsti dalla normativa comunitaria, dalle leggi, dai regolamenti o dai contratti collettivi.

La presente autorizzazione è rilasciata per l'esercizio del diritto di accesso ai documenti amministrativi, nei limiti di quanto stabilito dalle leggi e dai regolamenti in materia.

Per i fini predetti, il trattamento dei dati sensibili può riguardare anche la tenuta di registri e scritture contabili, di elenchi, di indirizzari e di altri documenti necessari per la gestione amministrativa dell'associazione, della fondazione, del comitato o del diverso organismo, o per l'adempimento di obblighi fiscali, ovvero per la diffusione di riviste, bollettini e simili.

Qualora i soggetti di cui alle lettere a), b) e c) si avvalgano di persone giuridiche o di altri organismi con scopo di lucro o di liberi professionisti per perseguire le predette finalità, ovvero richiedano ad essi la fornitura di beni, prestazioni o servizi, la presente autorizzazione è rilasciata anche ai medesimi organismi, persone giuridiche o liberi professionisti.

I soggetti di cui alle lettere a), b) e c) possono comunicare alle persone giuridiche e agli organismi con scopo di lucro titolari di un autonomo trattamento, i soli dati sensibili strettamente indispensabili per le attività di effettivo ausilio alle predette finalità, con particolare riferimento alle generalità degli interessati e ad indirizzari, sulla base di un atto scritto che individui con precisione le informazioni comunicate, le modalità del successivo utilizzo, le particolari misure di sicurezza, nonché, ove previsto, le idonee garanzie determinate. La dichiarazione scritta di consenso degli interessati deve porre tale circostanza in particolare evidenza e deve recare la precisa menzione dei titolari del trattamento e delle finalità da essi

perseguite. Le persone giuridiche e gli organismi con scopo di lucro, oltre a quanto previsto nei punti 4) e 6) in tema di pertinenza, non eccedenza e indispensabilità dei dati, possono trattare i dati così acquisiti solo per scopi di ausilio alle finalità predette, ovvero per scopi amministrativi e contabili.

3) Interessati ai quali i dati si riferiscono

Il trattamento può riguardare i dati sensibili attinenti:

a) agli associati, ai soci e, se strettamente indispensabile per il perseguimento delle finalità di cui al punto 1), ai relativi familiari e conviventi;

b) agli aderenti, ai sostenitori o sottoscrittori, nonché ai soggetti che presentano richiesta di ammissione o di adesione o che hanno contatti regolari con l'associazione, la fondazione o il diverso organismo;

c) ai soggetti che ricoprono cariche sociali o onorifiche;

d) ai beneficiari, agli assistiti e ai fruitori delle attività o dei servizi prestati dall'associazione o dal diverso organismo, limitatamente ai soggetti individuabili in base allo statuto o all'atto costitutivo, ove esistenti, o comunque a coloro nell'interesse dei quali i soggetti menzionati al punto 1) possono operare in base ad una previsione normativa;

e) agli studenti iscritti o che hanno presentato domanda di iscrizione agli istituti di cui al punto 1) e, qualora si tratti di minori, ai loro genitori o a chi ne esercita la potestà;

f) ai lavoratori dipendenti degli associati e dei soci, limitatamente ai dati idonei a rivelare l'adesione a sindacati, associazioni od organizzazioni a carattere sindacale e alle operazioni necessarie per adempiere a specifici obblighi derivanti da contratti collettivi anche aziendali.

4) Categorie di dati oggetto di trattamento

L'autorizzazione non riguarda i dati idonei a rivelare lo stato di salute e la vita sessuale, ai quali si riferisce l'autorizzazione generale n. 2/2007.

Il trattamento può avere per oggetto gli altri dati sensibili di cui all'articolo 4, comma 1, lett. *d*) del Codice, 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.

Il trattamento può riguardare i dati e le operazioni indispensabili per perseguire le finalità di cui al punto 1) o, comunque, per adempiere ad obblighi derivanti dalla legge, dalla normativa comunitaria, dai regolamenti o dai contratti collettivi, che non possano essere perseguiti o adempiuti, caso per caso, mediante il trattamento di dati anonimi o di dati personali di natura diversa.

A tal fine, anche mediante controlli periodici, deve essere verificata costantemente la stretta pertinenza, non eccedenza e indispensabilità dei dati rispetto ai predetti obblighi e finalità, in particolare per quanto riguarda i dati che rivelano le opinioni e le intime convinzioni, anche con riferimento ai dati che l'interessato fornisce di propria iniziativa. I dati che, anche a seguito delle verifiche, risultano eccedenti o non pertinenti o non indispensabili non possono essere utilizzati, salvo per l'eventuale conservazione, a norma di legge, dell'atto o del documento che li contiene.

5) Modalità di trattamento

Fermi restando gli obblighi previsti dagli articoli 11 e 14 del Codice, e dagli articoli 31 e seguenti del Codice e dall'Allegato B) al medesimo Codice, il trattamento dei dati sensibili deve essere effettuato unicamente con operazioni, nonché con logiche e mediante forme di organizzazione dei dati strettamente indispensabili in rapporto alle finalità, agli scopi e agli obblighi di cui al punto 2).

I dati sono raccolti, di regola, presso l'interessato.

Fermo restando quanto previsto ai punti 2) e 7) della presente autorizzazione, se è indispensabile, in conformità al medesimo punto 7), comunicare o diffondere dati all'esterno dell'associazione, della fondazione, del comitato o del diverso organismo, il consenso scritto è acquisito previa idonea informativa resa agli interessati ai sensi dell'art. 13 del Codice, la quale deve precisare le specifiche modalità di utilizzo dei dati tenuto conto delle idonee garanzie adottate relativamente ai trattamenti effettuati.

6) Conservazione dei dati

Nel quadro del rispetto dell'obbligo previsto dall'art. 11, comma 1, lett. *e*) del Codice, i dati sensibili possono essere conservati per un periodo non superiore a quello necessario per perseguire le finalità e gli scopi di cui al punto 2), ovvero per adempiere agli obblighi ivi menzionati.

Le verifiche di cui al punto 4) devono riguardare anche la pertinenza, non eccedenza e indispensabilità dei dati rispetto all'attività svolta dall'interessato o al rapporto che intercorre tra l'interessato e i soggetti di cui al punto 1), tenendo presente il genere di prestazione, di beneficio o di servizio offerto all'interessato e la posizione di quest'ultimo rispetto ai soggetti stessi.

7) Comunicazione e diffusione dei dati

I dati sensibili possono essere comunicati a soggetti pubblici o privati, e ove necessario diffusi, solo se strettamente pertinenti alle finalità, agli scopi e agli obblighi di cui al punto 2) e tenendo presenti le altre prescrizioni sopraindicate.

I dati sensibili possono essere comunicati alle autorità competenti se necessario per finalità di prevenzione, accertamento o repressione dei reati, con l'osservanza delle norme che regolano la materia.

I dati relativi allo stato di salute e alla vita sessuale non possono essere diffusi.

8) Richieste di autorizzazione

I titolari dei trattamenti che rientrano nell'ambito di applicazione della presente autorizzazione non sono tenuti a presentare una richiesta di autorizzazione a questa Autorità, qualora il trattamento che si intende effettuare sia conforme alle prescrizioni suddette.

Le richieste di autorizzazione pervenute o che perverranno anche successivamente alla data di adozione del presente provvedimento, devono intendersi accolte nei termini di cui al provvedimento medesimo.

Il Garante non prenderà in considerazione richieste di autorizzazione per trattamenti da effettuarsi in difformità alle prescrizioni del presente provvedimento, salvo che, ai sensi dell'art. 41 del Codice, il loro accoglimento sia giustificato da circostanze del tutto particolari o da situazioni eccezionali non considerate nella presente autorizzazione.

9) Norme finali

Restano fermi gli obblighi previsti dalla normativa comunitaria, da norme di legge o di regolamento che stabiliscono divieti o limiti in materia di trattamento di dati personali.

Restano inoltre ferme le norme volte a prevenire discriminazioni, e in particolare le disposizioni contenute nel decreto-legge 26 aprile 1993, n. 122, convertito, con modificazioni, dalla legge 25 giugno 1993, n. 205, in materia di discriminazione per motivi razziali, etnici, nazionali o religiosi e di delitti di genocidio, nel decreto legislativo 9 luglio 2003, n. 215 di attuazione della direttiva 2000/43/Ce per la parità di trattamento tra le persone indipendentemente dalla razza e dall'origine etnica e nel decreto legislativo 9 luglio 2003, n. 216, di attuazione della direttiva 2000/78/Ce per la parità di trattamento in materia di occupazione e di condizioni di lavoro.

10) Efficacia temporale e disciplina transitoria

La presente autorizzazione ha efficacia a decorrere dal 1° luglio 2007 fino al 30 giugno 2008, salve eventuali modifiche che il Garante ritenga di dover apportare in conseguenza di eventuali novità normative rilevanti in materia.

La presente autorizzazione sarà pubblicata nella *Gazzetta Ufficiale* della Repubblica italiana.

Roma, 28 giugno 2007

IL PRESIDENTE
Pizzetti

IL RELATORE
Paissan

IL SEGRETARIO GENERALE
Buttarelli

31 Autorizzazione n. 4/2007 al trattamento dei dati sensibili da parte dei liberi professionisti (*) *28 giugno 2007*

Registro delle deliberazioni
n. 27 del 28 giugno 2007

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

In data odierna, con la partecipazione del prof. Francesco Pizzetti, presidente, del dott. Giuseppe Chiaravalloti, vice presidente, del dott. Mauro Paissan e del dott. Giuseppe Fortunato, componenti, e del dott. Giovanni Buttarelli, segretario generale;

Visto il decreto legislativo 30 giugno 2003, n. 196, recante il Codice in materia di protezione dei dati personali;

Visto, in particolare, l'art. 4, comma 1, lett. *d*), del citato Codice, il quale individua i dati sensibili;

Considerato che, ai sensi dell'art. 26, comma 1, del Codice, i soggetti privati e gli enti pubblici economici possono trattare i dati sensibili solo previa autorizzazione di questa Autorità e, ove necessario, con il consenso scritto degli interessati, nell'osservanza dei presupposti e dei limiti stabiliti dal Codice, nonché dalla legge e dai regolamenti;

Visto il comma 4, lett. *c*), del medesimo art. 26, il quale stabilisce che i dati sensibili possono essere oggetto di trattamento anche senza consenso, previa autorizzazione del Garante, quando il trattamento medesimo è necessario ai fini dello svolgimento delle investigazioni difensive ai sensi della legge 7 dicembre 2000, n. 397 o, comunque per far valere o difendere in sede giudiziaria un diritto, sempre che i dati siano trattati esclusivamente per tali finalità e per il periodo strettamente necessario al loro perseguimento, e che, quando i dati siano idonei a rivelare lo stato di salute e la vita sessuale il diritto sia di rango pari a quello dell'interessato, ovvero consista in un diritto della personalità o in un altro diritto o libertà fondamentale inviolabile;

Considerato che il trattamento dei dati in questione può essere autorizzato dal Garante anche d'ufficio con provvedimenti di carattere generale, relativi a determinate categorie di titolari o di trattamenti (art. 40 del Codice);

Considerato che le autorizzazioni di carattere generale sinora rilasciate sono risultate uno strumento idoneo per prescrivere misure uniformi a garanzia degli interessati, rendendo altresì superflua la richiesta di singoli provvedimenti di autorizzazione da parte di numerosi titolari del trattamento;

Ritenuto opportuno rilasciare nuove autorizzazioni in sostituzione di quelle in scadenza il 30 giugno 2007, armonizzando le prescrizioni già impartite alla luce dell'esperienza maturata;

Ritenuto opportuno che anche tali nuove autorizzazioni siano provvisorie e a tempo determinato, ai sensi dell'art. 41, comma 5, del Codice e, in particolare, efficaci per il periodo di dodici mesi;

Considerata la necessità di garantire il rispetto di alcuni principi volti a ridurre al minimo i rischi di danno o di pericolo che i trattamenti potrebbero comportare per i diritti e le libertà fondamentali, nonché per la dignità delle persone, e, in particolare, per il diritto alla protezione dei dati personali sancito dall'art. 1 del Codice;

(*) ***G.U.*** **24 agosto 2007, n. 196**
[doc. *web* n. 1429823]

Considerato che un elevato numero di trattamenti di dati sensibili è effettuato da liberi professionisti iscritti in albi o elenchi professionali per l'espletamento delle rispettive attività professionali;

Visto l'art. 167 del Codice;

Visto l'art. 11, comma 2, del Codice, il quale stabilisce che i dati trattati in violazione della disciplina rilevante in materia di trattamento di dati personali non possono essere utilizzati;

Visti gli articoli 31 e seguenti del Codice e il disciplinare tecnico di cui all'Allegato B) al medesimo Codice recanti norme e regole sulle misure di sicurezza;

Visto l'art. 41 del Codice;

Visti gli atti d'ufficio;

Viste le osservazioni dell'Ufficio formulate dal segretario generale ai sensi dell'art. 15 del regolamento del Garante n. 1/2000;

Relatore il dott. Giuseppe Chiaravalloti;

Autorizza

i liberi professionisti iscritti in albi o elenchi professionali a trattare i dati sensibili di cui all'art. 4, comma 1, lett. *d*), del Codice, secondo le prescrizioni di seguito indicate.

Prima di iniziare o proseguire il trattamento 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, in conformità all'art. 3 del Codice.

1) Ambito di applicazione

L'autorizzazione è rilasciata, anche senza richiesta, ai liberi professionisti tenuti ad iscriversi in albi o elenchi per l'esercizio di un'attività professionale in forma individuale o associata, anche in conformità al decreto legislativo 2 febbraio 2001, n. 96, o alle norme di attuazione dell'art. 24, comma 2, della legge 7 agosto 1997, n. 266, in tema di attività di assistenza e consulenza.

Sono equiparati ai liberi professionisti i soggetti iscritti nei corrispondenti albi o elenchi speciali istituiti anche ai sensi dell'art. 34 del regio decreto-legge 27 novembre 1933, n. 1578 e successive modificazioni e integrazioni, recante l'ordinamento della professione di avvocato.

L'autorizzazione è rilasciata anche ai sostituti e agli ausiliari che collaborano con il libero professionista ai sensi dell'art. 2232 del Codice civile, ai praticanti e ai tirocinanti presso il libero professionista, qualora tali soggetti siano titolari di un autonomo trattamento o siano contitolari del trattamento effettuato dal libero professionista.

Il presente provvedimento non si applica al trattamento dei dati sensibili effettuato:

a) dagli esercenti la professione sanitaria e dagli psicologi, dal personale sanitario infermieristico, tecnico e della riabilitazione, ai quali si riferisce l'autorizzazione generale n. 2/2007;
b) per la gestione delle prestazioni di lavoro o di collaborazione di cui si avvale il libero professionista o taluno dei soggetti sopra indicati, alla quale si riferisce l'autorizzazione generale n. 1/2007;
c) da soggetti privati che svolgono attività investigative, dai giornalisti, dai pubblicisti e dai praticanti giornalisti di cui agli articoli 26 e 33 della legge 3 febbraio 1963, n. 69.

2) Interessati ai quali i dati si riferiscono e categorie di dati
Il trattamento può riguardare i dati sensibili relativi ai clienti.

I dati sensibili relativi ai terzi possono essere trattati ove ciò sia strettamente indispensabile per l'esecuzione di specifiche prestazioni professionali richieste dai clienti per scopi determinati e legittimi.

In ogni caso, i dati devono essere strettamente pertinenti e non eccedenti rispetto ad incarichi conferiti che non possano essere svolti mediante il trattamento di dati anonimi o di dati personali di natura diversa.

Il trattamento dei dati idonei a rivelare lo stato di salute e la vita sessuale deve essere effettuato anche nel rispetto della citata autorizzazione generale n. 2/2007.

3) Finalità del trattamento
Il trattamento dei dati sensibili può essere effettuato ai soli fini dell'espletamento di un incarico che rientri tra quelli che il libero professionista può eseguire in base al proprio ordinamento professionale, e in particolare:

a) per curare gli adempimenti in materia di lavoro, di previdenza ed assistenza sociale e fiscale nell'interesse di altri soggetti che sono parte di un rapporto di lavoro dipendente o autonomo, ai sensi della legge 11 gennaio 1979, n. 12, che disciplina la professione di consulente del lavoro;
b) ai fini dello svolgimento da parte del difensore delle investigazioni difensive di cui alla legge 7 dicembre 2000, n. 397, anche a mezzo di sostituti e di consulenti tecnici, o, comunque, per far valere o difendere un diritto anche da parte di un terzo in sede giudiziaria, nonché in sede amministrativa o nelle procedure di arbitrato e di conciliazione nei casi previsti dalla normativa comunitaria, dalle leggi, dai regolamenti o dai contratti collettivi. Qualora i dati siano idonei a rivelare lo stato di salute e la vita sessuale, il diritto da far valere o difendere deve essere di rango pari a quello dell'interessato, ovvero consistente in un diritto della personalità o in un altro diritto o libertà fondamentale e inviolabile;
c) per l'esercizio del diritto di accesso ai documenti amministrativi, nei limiti di quanto stabilito dalle leggi e dai regolamenti in materia, salvo quanto previsto dall'art. 60 del Codice in relazione ai dati sullo stato di salute e sulla vita sessuale.

4) Modalità di trattamento
Il trattamento dei dati sensibili deve essere effettuato unicamente con logiche e mediante forme di organizzazione dei dati strettamente indispensabili in rapporto all'incarico conferito dal cliente.

Restano fermi gli obblighi previsti dagli articoli 11 e 14 del Codice, nonché dagli articoli 31 e seguenti del Codice e dall'Allegato B) al medesimo Codice.

Restano inoltre fermi gli obblighi di informare l'interessato ai sensi dell'art. 13, commi 1, 4 e 5, del Codice, anche quando i dati sono raccolti presso terzi, e di acquisire, ove necessario, il consenso scritto.

Se i dati sono raccolti per l'esercizio di un diritto in sede giudiziaria o per le indagini difensive (punto 3), lettera b), l'informativa relativa ai dati raccolti presso terzi, e il consenso scritto, sono necessari solo se i dati sono trattati per un periodo superiore a quello strettamente necessario al perseguimento di tali finalità, oppure per altre finalità con esse non incompatibili.

Le informative devono permettere all'interessato di comprendere agevolmente se il titolare del trattamento è un singolo professionista o un'associazione di professionisti, ovvero se ricorre un'ipotesi di contitolarità tra più liberi professionisti o di esercizio della professione in forma societaria ai sensi del decreto legislativo 2 febbraio 2001, n. 96.

Resta ferma la facoltà del libero professionista di designare quali responsabili o incaricati del trattamento i sostituti, gli ausiliari, i tirocinanti e i praticanti presso il libero professionista, i quali, in tal caso, possono avere accesso ai soli dati strettamente pertinenti alla collaborazione ad essi richiesta.

Analoga cautela deve essere adottata in riferimento agli incaricati del trattamento preposti all'espletamento di compiti amministrativi.

5) Conservazione dei dati

Nel quadro del rispetto dell'obbligo previsto dall'art. 11, comma 1, lett. e), del Codice, i dati sensibili possono essere conservati, per il periodo di tempo previsto dalla normativa comunitaria, da leggi, o da regolamenti e, comunque, per un periodo non superiore a quello strettamente necessario per adempiere agli incarichi conferiti.

A tal fine, anche mediante controlli periodici, deve essere verificata la stretta pertinenza, non eccedenza e indispensabilità dei dati rispetto agli incarichi in corso, da instaurare o cessati, anche con riferimento ai dati che l'interessato fornisce di propria iniziativa. I dati che, anche a seguito delle verifiche, risultano eccedenti o non pertinenti o non indispensabili non possono essere utilizzati, salvo che per l'eventuale conservazione, a norma di legge, dell'atto o del documento che li contiene. Specifica attenzione è prestata per l'indispensabilità dei dati riferiti a soggetti diversi da quelli cui si riferiscono direttamente le prestazioni e gli adempimenti.

I dati acquisiti in occasione di precedenti incarichi possono essere mantenuti se pertinenti, non eccedenti e indispensabili rispetto a successivi incarichi.

6) Comunicazione e diffusione dei dati

I dati sensibili possono essere comunicati e ove necessario diffusi, a soggetti pubblici o privati, nei limiti strettamente pertinenti all'espletamento dell'incarico conferito e nel rispetto, in ogni caso, del segreto professionale.

I dati idonei a rivelare lo stato di salute possono essere comunicati solo se necessario per finalità di prevenzione, accertamento o repressione dei reati, con l'osservanza delle norme che regolano la materia.

I dati relativi allo stato di salute e alla vita sessuale non possono essere diffusi.

7) Richieste di autorizzazione

I titolari dei trattamenti che rientrano nell'ambito di applicazione della presente autorizzazione non sono tenuti a presentare una richiesta di autorizzazione a questa Autorità, qualora il trattamento che si intende effettuare sia conforme alle prescrizioni suddette.

Le richieste di autorizzazione pervenute o che perverranno anche successivamente alla data di adozione del presente provvedimento, devono intendersi accolte nei termini di cui al provvedimento medesimo.

Il Garante non prenderà in considerazione richieste di autorizzazione per trattamenti da effettuarsi in difformità alle prescrizioni del presente provvedimento, salvo che, ai sensi dell'art. 41 del Codice, il loro accoglimento sia giustificato da circostanze del tutto particolari o da situazioni eccezionali non considerate nella presente autorizzazione.

8) Norme finali

Restano fermi gli obblighi previsti da norme di legge o di regolamento o dalla normativa comunitaria che stabiliscono divieti o limiti più restrittivi in materia di trattamento di dati personali e, in particolare, dalle leggi 20 maggio 1970, n. 300, e 5 giugno 1990, n. 135, come modificata dall'art. 178 del Codice, nonché dalle norme volte a prevenire discriminazioni.

Restano fermi, altresì, gli obblighi di legge che vietano la rivelazione senza giusta causa e l'impiego a proprio o altrui profitto delle notizie coperte dal segreto professionale, nonché gli obblighi deontologici o di buona condotta relativi alle singole figure professionali.

9) Efficacia temporale e disciplina transitoria

La presente autorizzazione ha efficacia a decorrere dal 1° luglio 2007 fino al 30 giugno 2008, salve eventuali modifiche che il Garante ritenga di dover apportare in conseguenza di eventuali novità normative rilevanti in materia.

La presente autorizzazione sarà pubblicata nella *Gazzetta Ufficiale* della Repubblica italiana.

Roma, 28 giugno 2007

IL PRESIDENTE
Pizzetti

IL RELATORE
Chiaravalloti

IL SEGRETARIO GENERALE
Buttarelli

32 Autorizzazione n. 5/2007 al trattamento dei dati sensibili da parte di diverse categorie di titolari (*)

28 giugno 2007

Registro delle deliberazioni
n. 28 del 28 giugno 2007

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

In data odierna, con la partecipazione del prof. Francesco Pizzetti, presidente, del dott. Giuseppe Chiaravalloti, vice presidente, del dott. Mauro Paissan e del dott. Giuseppe Fortunato, componenti, e del dott. Giovanni Buttarelli, segretario generale;

Visto il decreto legislativo 30 giugno 2003, n. 196, recante il Codice in materia di protezione dei dati personali;

Visto, in particolare, l'art. 4, comma 1, lett. *d*) del citato Codice, il quale individua i dati sensibili;

Considerato che, *ai sensi* dell'art. 26, comma 1, del Codice, i soggetti privati e gli enti pubblici economici possono trattare i dati sensibili solo previa autorizzazione di questa Autorità e, ove necessario, con il consenso scritto degli interessati, nell'osservanza dei presupposti e dei limiti stabiliti dal Codice, nonché dalla legge e dai regolamenti;

Considerato che il trattamento dei dati in questione può essere autorizzato dal Garante anche d'ufficio con provvedimenti di carattere generale, relativi a determinate categorie di titolari o di trattamenti (art. 40 del Codice);

Considerato che le autorizzazioni di carattere generale sinora rilasciate sono risultate uno strumento idoneo per prescrivere misure uniformi a garanzia degli interessati, rendendo altresì superflua la richiesta di singoli provvedimenti di autorizzazione da parte di numerosi titolari del trattamento;

Ritenuto opportuno rilasciare nuove autorizzazioni in sostituzione di quelle in scadenza il 30 giugno 2007, armonizzando le prescrizioni già impartite alla luce dell'esperienza maturata;

Ritenuto opportuno che anche tali nuove autorizzazioni siano provvisorie e a tempo determinato, ai sensi dell'art. 41, comma 5, del Codice, e, in particolare, efficaci per il periodo di dodici mesi;

Considerata la necessità di garantire il rispetto di alcuni principi volti a ridurre al minimo i rischi di danno o di pericolo che i trattamenti potrebbero comportare per i diritti e le libertà fondamentali, nonché per la dignità delle persone, e in particolare, per il diritto alla protezione dei dati personali sancito dall'art. 1 del Codice;

Considerato che un elevato numero di trattamenti di dati sensibili è effettuato da parte di soggetti operanti in diversi settori di attività economiche di seguito individuate;

Visto l'art. 167 del Codice;

Visto l'art. 11, comma 2, del Codice, il quale stabilisce che i dati trattati in violazione della disciplina rilevante in materia di trattamento di dati personali non possono essere utilizzati;

(*) ***G.U.*** **24 agosto 2007, n. 196**
[doc. *web* n. 1429855]

Visti gli articoli 31 e seguenti del Codice e il disciplinare tecnico di cui all'Allegato B) al medesimo Codice, recanti norme e regole sulle misure di sicurezza;

Visto l'art. 41 del Codice;

Visti gli atti d'ufficio;

Viste le osservazioni dell'Ufficio formulate dal segretario generale ai sensi dell'art. 15 del regolamento del Garante n. 1/2000;

Relatore il dott. Giuseppe Fortunato;

Autorizza

il trattamento dei dati sensibili di cui all'art. 4, comma 1, lett. *d*), del Codice, fatta eccezione dei dati idonei a rivelare la vita sessuale, secondo le prescrizioni di seguito indicate.

Prima di iniziare o proseguire il trattamento 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, in conformità all'art. 3 del Codice.

CAPO I - ATTIVITÀ BANCARIE, CREDITIZIE, ASSICURATIVE, DI GESTIONE DI FONDI, DEL SETTORE TURISTICO, DEL TRASPORTO ED ALTRE ATTIVITÀ AUTORIZZATE

1) Soggetti ai quali è rilasciata l'autorizzazione:

a) imprese autorizzate all'esercizio dell'attività bancaria e creditizia o assicurativa ed organismi che le riuniscono, anche se in stato di liquidazione coatta amministrativa;
b) società ed altri organismi che gestiscono fondi-pensione o di assistenza, ovvero fondi o casse di previdenza;
c) società ed altri organismi di intermediazione finanziaria, in particolare per la gestione o l'intermediazione di fondi comuni di investimento o di valori mobiliari;
d) società ed altri organismi che emettono carte di credito o altri mezzi di pagamento, o che ne gestiscono le relative operazioni;
e) imprese che svolgono autonome attività strettamente connesse e strumentali a quelle indicate nelle precedenti lettere, e relative alla rilevazione dei rischi, al recupero dei crediti, a lavorazioni massive di documenti, alla trasmissione dati, all'imbustamento o allo smistamento della corrispondenza, nonché alla gestione di esattorie o tesorerie;
f) imprese che operano nel settore turistico o alberghiero o del trasporto, agenzie di viaggio e operatori turistici;
g) operatori economici autorizzati a svolgere la propria attività in base ad autorizzazione comunque resa ai sensi delle norme contenute nel regio decreto 18 giugno 1931, n. 773 (T.u.l.p.s.) o nel decreto legislativo 31 marzo 1998, n. 112.

2) Finalità del trattamento

La presente autorizzazione è rilasciata, anche senza richiesta, limitatamente ai dati e alle operazioni indispensabili per adempiere agli obblighi anche precontrattuali che i soggetti di cui al punto 1) assumono, nel proprio settore di attività, al fine di fornire specifici beni, prestazioni o servizi richiesti dall'interessato.

L'autorizzazione è rilasciata anche per adempiere o per esigere l'adempimento ad obblighi previsti, anche in materia fiscale e contabile, dalla normativa comunitaria, dalla legge, dai regolamenti, o dai contratti collettivi, o prescritti da autorità od organi di vigilanza o di controllo nei casi indicati dalla legge o dai regolamenti.

Il trattamento avente tali finalità può riguardare anche la tenuta di registri e scritture contabili, di elenchi, di indirizzari e di altri documenti necessari per espletare compiti di organizzazione o di gestione amministrativa di imprese, società, cooperative o consorzi.

3) Interessati ai quali i dati si riferiscono e categorie di dati trattati

Il trattamento può riguardare i dati sensibili attinenti ai soggetti ai quali sono forniti i beni, le prestazioni o i servizi, in misura strettamente pertinente a quanto specificamente richiesto dall'interessato che, ove necessario, abbia manifestato il proprio consenso scritto ed informato. Nei medesimi limiti, è possibile trattare dati relativi a terzi, allorché non sia altrimenti possibile procedere alla fornitura al beneficiario dei beni, delle prestazioni o dei servizi.

Qualora il consenso sia richiesto nei confronti di distinti titolari di trattamenti, la manifestazione di volontà deve riferirsi specificamente a ciascuno di essi.

4) Comunicazione e diffusione dei dati

I dati sensibili possono essere comunicati, nei limiti strettamente pertinenti al perseguimento delle finalità di cui al punto 2), a soggetti pubblici o privati, ivi compresi fondi e casse di previdenza ed assistenza o società controllate e collegate ai sensi dell'art. 2359 del codice civile, nonché, ove necessario, ai familiari dell'interessato.

I titolari del trattamento, anche ai fini dell'eventuale comunicazione ad altri titolari delle modifiche apportate ai dati in accoglimento di una richiesta dell'interessato (art. 7, comma 3, lettera *c*), del Codice), devono conservare un elenco dei destinatari delle comunicazioni effettuate, recante un'annotazione delle specifiche categorie di dati comunicati.

I dati sensibili non possono essere diffusi.

CAPO II - SONDAGGI E RICERCHE

1) Soggetti ai quali è rilasciata l'autorizzazione e finalità del trattamento

Imprese, società, istituti ed altri organismi o soggetti privati, ai soli fini del compimento di sondaggi di opinione, di ricerche di mercato o di altre ricerche campionarie.

Il sondaggio o la ricerca devono essere effettuati per scopi puntualmente determinati e legittimi, noti all'interessato.

2) Interessati ai quali i dati si riferiscono e categorie di dati trattati

Il trattamento può riguardare i dati attinenti ai soggetti che abbiano manifestato il proprio consenso informato e che abbiano risposto a questionari o ad interviste effettuate nell'ambito di sondaggi di opinione, di ricerche di mercato o di altre ricerche campionarie.

Il consenso deve essere manifestato in ogni caso per iscritto.

I dati personali di natura sensibile possono essere trattati solo se il trattamento di dati anonimi non permette al sondaggio o alla ricerca di raggiungere i suoi scopi.

3) Conservazione dei dati

Il trattamento successivo alla raccolta non deve permettere di identificare gli interessati, neanche indirettamente, mediante un riferimento ad una qualsiasi altra informazione.

I dati personali, individuali o aggregati, devono essere distrutti o resi anonimi subito dopo la raccolta, e comunque non oltre la fase contestuale alla registrazione dei campioni raccolti. La registrazione deve essere effettuata senza ritardo anche nel caso in cui i campioni siano stati raccolti in numero elevato.

Entro tale ambito temporale, resta ferma la possibilità per il titolare della raccolta, nonché per i suoi responsabili o incaricati, di utilizzare i dati personali al fine di verificare presso gli interessati la veridicità o l'esattezza dei campioni.

4) Comunicazione dei dati

I dati sensibili non possono essere né comunicati, né diffusi.

I campioni del sondaggio o della ricerca possono essere comunicati o diffusi in forma individuale o aggregata, sempre che non possano essere associati, anche a seguito di trattamento, ad interessati identificati o identificabili.

CAPO III - ATTIVITÀ DI ELABORAZIONE DI DATI

1) Soggetti ai quali è rilasciata l'autorizzazione

Imprese, società, istituti ed altri organismi o soggetti privati, titolari autonomi di un'attività svolta nell'interesse di altri soggetti, e che presuppone l'elaborazione di dati ed altre operazioni di trattamento eseguite in materia di lavoro, ovvero a fini contabili, retributivi, previdenziali, assistenziali e fiscali.

2) Prescrizioni applicabili

Il trattamento è regolato dalle autorizzazioni:

a) n. 1/2007, rilasciata il 28 giugno 2007, concernente il trattamento dei dati sensibili a cura, in particolare, delle parti di un rapporto di lavoro qualora le finalità perseguite siano quelle indicate al punto 3) di tale autorizzazione;

b) n. 4/2007, rilasciata il 28 giugno 2007, riguardante il trattamento dei dati sensibili ad opera dei liberi professionisti e di altri soggetti equiparati, qualora le finalità perseguite siano quelle indicate al punto 3) di tale autorizzazione.

Qualora il consenso sia richiesto nei confronti di distinti titolari di trattamenti, la manifestazione di volontà deve riferirsi specificamente a ciascuno di essi.

CAPO IV - ATTIVITÀ DI SELEZIONE DEL PERSONALE

1) Soggetti ai quali è rilasciata l'autorizzazione e finalità del trattamento

La presente autorizzazione è rilasciata, anche senza richiesta, alle agenzie per il lavoro e agli altri soggetti che, in conformità alla legge, svolgono, nell'interesse di terzi, attività di intermediazione, ricerca e selezione del personale o supporto alla ricollocazione professionale.

2) Interessati ai quali i dati si riferiscono e categorie di dati trattati

Il trattamento può riguardare i dati idonei a rivelare lo stato di salute e l'origine razziale ed etnica dei candidati all'instaurazione di un rapporto di lavoro o di collaborazione, solo se la loro raccolta è giustificata da scopi determinati e legittimi ed è strettamente indispensabile per instaurare tale rapporto.

Il trattamento dei dati idonei a rivelare lo stato di salute dei familiari o dei conviventi dei candidati è consentito con il consenso scritto degli interessati e qualora sia finalizzato al riconoscimento di uno specifico beneficio in favore dei candidati, in particolare ai fini di un'assunzione obbligatoria o del riconoscimento di un titolo derivante da invalidità o infermità, da eventi bellici o da ragioni di servizio.

Qualora il consenso sia richiesto nei confronti di distinti titolari di trattamenti, la manifestazione di volontà deve riferirsi specificamente a ciascuno di essi.

Il trattamento deve riguardare le sole informazioni strettamente pertinenti a tale finalità, sia in caso di risposta a questionari inviati anche per via telematica, sia nel caso in cui i can-

didati forniscano dati di propria iniziativa, in particolare attraverso l'invio di *curricula*. Non è consentito il trattamento dei dati:

a) idonei a rivelare le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni a carattere religioso, filosofico, politico o sindacale, l'origine razziale ed etnica, e la vita sessuale;
b) inerenti a fatti non rilevanti ai fini della valutazione dell'attitudine professionale del lavoratore;
c) in violazione delle norme in materia di pari opportunità o volte a prevenire discriminazioni.

3) Comunicazione e diffusione dei dati

I dati idonei a rivelare lo stato di salute e l'origine razziale ed etnica possono essere comunicati nei limiti strettamente pertinenti al perseguimento delle finalità di cui ai punti 1) e 2), a soggetti pubblici o privati che siano specificamente menzionati nella dichiarazione di consenso dell'interessato.

I dati sensibili non possono essere diffusi.

4) Norme finali

Restano fermi gli ulteriori obblighi previsti dalla legge e dai regolamenti.

CAPO V - MEDIAZIONE A FINI MATRIMONIALI

1) Soggetti ai quali è rilasciata l'autorizzazione

La presente autorizzazione è rilasciata alle imprese, alle società, agli istituti e agli altri organismi o soggetti privati che esercitano, anche attraverso agenzie autorizzate, un'attività di mediazione a fini matrimoniali o di instaurazione di un rapporto di convivenza.

2) Finalità del trattamento

L'autorizzazione è rilasciata ai soli fini dell'esecuzione dei singoli incarichi conferiti in conformità alle leggi e ai regolamenti.

3) Interessati ai quali i dati si riferiscono

Il trattamento può riguardare i soli dati sensibili attinenti alle persone direttamente interessate al matrimonio o alla convivenza.

Non è consentito il trattamento di dati relativo a persone minori di età in base all'ordinamento del Paese di appartenenza o, comunque, in base alla legge italiana.

4) Categorie di dati oggetto di trattamento

Il trattamento può riguardare i soli dati e le sole operazioni che risultino indispensabili in relazione allo specifico profilo o alla personalità descritto o richiesto dalle persone interessate al matrimonio o alla convivenza.

I dati devono essere forniti personalmente dai medesimi interessati.

L'informativa preliminare al consenso scritto deve porre in particolare evidenza le categorie di dati trattati e le modalità della loro comunicazione a terzi.

5) Comunicazione dei dati

I dati possono essere comunicati nei limiti strettamente pertinenti all'esecuzione degli specifici incarichi ricevuti.

I titolari del trattamento, anche ai fini dell'eventuale comunicazione ad altri titolari delle modifiche apportate ai dati in accoglimento di una richiesta dell'interessato (art. 7, comma 3, lettera *c*), del Codice), devono conservare un elenco dei destinatari delle comunicazioni effettuate, recante un'annotazione delle specifiche categorie di dati comunicati.

L'eventuale diffusione anche per via telematica di taluni dati sensibili deve essere oggetto di apposita autorizzazione di questa Autorità.

6) Norme finali

Restano fermi gli ulteriori obblighi previsti dalla legge e dai regolamenti, in particolare nell'ambito della legge penale e della disciplina di pubblica sicurezza, nonché in materia di tutela dei minori.

CAPO VI - PRESCRIZIONI COMUNI A TUTTI I TRATTAMENTI

Per quanto non previsto dai capi che precedono, ai trattamenti ivi indicati si applicano, altresì, le seguenti prescrizioni:

1) Dati idonei a rivelare lo stato di salute

Il trattamento dei dati idonei a rivelare lo stato di salute deve essere effettuato anche nel rispetto dell'autorizzazione n. 2/2007.

Il trattamento di dati genetici resta autorizzato nei limiti e alle condizioni individuati nell'autorizzazione del 22 febbraio 2007, pubblicata nella *Gazzetta Ufficiale* n. 65 del 19 marzo 2007.

2) Modalità di trattamento

Fermi restando gli obblighi previsti dagli articoli 11 e 14 del Codice, dagli articoli 31 e seguenti del Codice e dall'Allegato B) al Codice, il trattamento dei dati sensibili deve essere effettuato unicamente con operazioni, nonché con logiche e mediante forme di organizzazione dei dati strettamente indispensabili in rapporto alle finalità indicate nei capi che precedono. La comunicazione di dati all'interessato deve avvenire di regola direttamente a quest'ultimo o a un suo delegato (fermo restando quanto previsto dall'art. 84, comma 1, del Codice), in plico chiuso o con altro mezzo idoneo a prevenire la conoscenza da parte di soggetti non autorizzati, anche attraverso la previsione di distanze di cortesia.

Resta inoltre fermo l'obbligo di informare l'interessato, ai sensi dell'art. 13, commi 1, 4 e 5 del Codice, anche quando i dati sono raccolti presso terzi.

3) Conservazione dei dati

Nel quadro del rispetto dell'obbligo previsto dall'art. 11, comma 1, lett. *e*) del Codice, i dati sensibili possono essere conservati per un periodo non superiore a quello necessario per perseguire le finalità, ovvero per adempiere agli obblighi o agli incarichi menzionati nei precedenti capi. A tal fine, anche mediante controlli periodici, deve essere verificata costantemente la stretta pertinenza, non eccedenza e indispensabilità dei dati rispetto al rapporto, alla prestazione o all'incarico in corso, da instaurare o cessati, anche con riferimento ai dati che l'interessato fornisce di propria iniziativa. I dati che, anche a seguito delle verifiche, risultano eccedenti o non pertinenti o non indispensabili non possono essere utilizzati, salvo che per l'eventuale conservazione, a norma di legge, dell'atto o del documento che li contiene. Specifica attenzione è prestata per l'indispensabilità dei dati riferiti a soggetti diversi da quelli cui si riferiscono direttamente le prestazioni e gli adempimenti.

Restano fermi i diversi termini di conservazione previsti dalle leggi o dai regolamenti.

Resta altresì fermo quanto previsto nel capo II in materia di sondaggi e di ricerche.

4) Richieste di autorizzazione

I titolari dei trattamenti che rientrano nell'ambito di applicazione della presente autorizzazione non sono tenuti a presentare una richiesta di autorizzazione a questa Autorità, qualora il trattamento che si intende effettuare sia conforme alle prescrizioni suddette.

Le richieste di autorizzazione pervenute o che perverranno anche successivamente alla data di adozione del presente provvedimento, devono intendersi accolte nei termini di cui al provvedimento medesimo.

Il Garante non prenderà in considerazione richieste di autorizzazione per trattamenti da effettuarsi in difformità alle prescrizioni del presente provvedimento, salvo che, ai sensi dell'art. 41 del Codice, il loro accoglimento sia giustificato da circostanze del tutto particolari o da situazioni eccezionali non considerate nella presente autorizzazione.

5) Norme finali

Restano fermi gli obblighi previsti da norme di legge o di regolamento e dalla normativa comunitaria, che stabiliscono divieti o limiti più restrittivi in materia di trattamento di dati personali e, in particolare:

a) dalla legge 20 maggio 1970, n. 300;
b) dalla legge 5 giugno 1990, n. 135;
c) dal decreto legislativo 10 settembre 2003, n. 276.

Restano altresì fermi gli obblighi di legge che vietano la rivelazione senza giusta causa e l'impiego a proprio o altrui profitto delle notizie coperte dal segreto professionale, nonché gli obblighi deontologici, previsti anche dai codici deontologici e di buona condotta adottati in attuazione dell'art. 12 del Codice.

Resta ferma, infine, la possibilità di diffondere dati anonimi anche aggregati.

6) Efficacia temporale e disciplina transitoria

La presente autorizzazione ha efficacia a decorrere dal 1° luglio 2007 fino al 30 giugno 2008, salve eventuali modifiche che il Garante ritenga di dover apportare in conseguenza di eventuali novità normative rilevanti in materia.

La presente autorizzazione sarà pubblicata nella *Gazzetta Ufficiale* della Repubblica italiana.

Roma, 28 giugno 2007

IL PRESIDENTE
Pizzetti

IL RELATORE
Fortunato

IL SEGRETARIO GENERALE
Buttarelli

33 Autorizzazione n. 6/2007 al trattamento dei dati sensibili da parte degli investigatori privati (*) *28 giugno 2007*

Registro delle deliberazioni
n. 29 del 28 giugno 2007

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

In data odierna, con la partecipazione del prof. Francesco Pizzetti, presidente, del dott. Giuseppe Chiaravalloti, vice presidente, del dott. Mauro Paissan e del dott. Giuseppe Fortunato, componenti, e del dott. Giovanni Buttarelli, segretario generale;

Visto il decreto legislativo 30 giugno 2003, n. 196, recante il Codice in materia di protezione dei dati personali;

Visto, in particolare, l'art. 4, comma 1, lett. *d*), del citato Codice, il quale individua i dati sensibili;

Considerato che, ai sensi dell'art. 26, comma 1, del Codice, i soggetti privati e gli enti pubblici economici possono trattare i dati sensibili solo previa autorizzazione di questa Autorità e, ove necessario, con il consenso scritto degli interessati, nell'osservanza dei presupposti e dei limiti stabiliti dal Codice, nonché dalla legge e dai regolamenti;

Visto il comma 4, lett. *c*), del medesimo art. 26, il quale stabilisce che i dati sensibili possono essere oggetto di trattamento anche senza consenso, previa autorizzazione del Garante, quando il trattamento medesimo è necessario per svolgere una investigazione difensiva ai sensi della legge 7 dicembre 2000, n. 397 o, comunque, per far valere o difendere in sede giudiziaria un diritto, sempre che i dati siano trattati esclusivamente per tali finalità e per il periodo strettamente necessario al loro perseguimento, e che, quando i dati siano idonei a rivelare lo stato di salute e la vita sessuale dell'interessato il diritto sia di rango pari a quello dell'interessato, ovvero consista in un diritto della personalità o in un altro diritto o libertà fondamentale inviolabile;

Considerato che il trattamento dei dati in questione può essere autorizzato dal Garante anche d'ufficio con provvedimenti di carattere generale, relativi a determinate categorie di titolari o di trattamenti (art. 40 del Codice);

Considerato che le autorizzazioni di carattere generale sinora rilasciate sono risultate uno strumento idoneo per prescrivere misure uniformi a garanzia degli interessati, rendendo altresì superflua la richiesta di singoli provvedimenti di autorizzazione da parte di numerosi titolari del trattamento;

Ritenuto opportuno rilasciare nuove autorizzazioni in sostituzione di quelle in scadenza il 30 giugno 2007, armonizzando le prescrizioni già impartite alla luce dell'esperienza maturata;

Ritenuto opportuno che anche tali nuove autorizzazioni siano provvisorie e a tempo determinato, ai sensi dell'art. 41, comma 5, del Codice, e, in particolare, efficaci per il periodo di dodici mesi;

Considerata la necessità di garantire il rispetto di alcuni principi volti a ridurre al minimo i rischi di danno o di pericolo che i trattamenti potrebbero comportare per i diritti e le libertà fondamentali, nonché per la dignità delle persone, e, in particolare, per il diritto alla protezione dei dati personali sancito dall'art. 1 del Codice;

(*) *G.U.* 24 agosto 2007, n. 196
[doc. *web* n. 1429963]

Considerato che il Garante ha rilasciato un'autorizzazione di ordine generale relativa ai dati idonei a rivelare lo stato di salute e la vita sessuale (n. 2/2007, rilasciata il 28 giugno 2007), anche in riferimento alle predette finalità di ordine giudiziario;

Considerato che numerosi trattamenti aventi tali finalità sono effettuati con l'ausilio di investigatori privati, e che è pertanto opportuno integrare anche le prescrizioni dell'autorizzazione n. 2/2007 mediante un ulteriore provvedimento di ordine generale che tenga conto dello specifico contesto dell'investigazione privata, anche al fine di armonizzare le prescrizioni da impartire alla categoria;

Considerato che ulteriori misure ed accorgimenti saranno prescritti dal Garante all'atto della sottoscrizione del citato codice di deontologia e di buona condotta in via di emanazione (art. 12 del Codice);

Visto l'art. 167 del Codice;

Visto l'art. 11, comma 2, del Codice, il quale stabilisce che i dati trattati in violazione della disciplina rilevante in materia di trattamento di dati personali non possono essere utilizzati;

Visti gli articoli 31 e seguenti del Codice e il disciplinare tecnico di cui all'Allegato B) al medesimo Codice recanti norme e regole sulle misure di sicurezza;

Visti gli articoli 42 e seguenti del Codice in materia di trasferimento di dati personali all'estero;

Visto l'art. 41 del Codice;

Visti gli atti d'ufficio;

Viste le osservazioni dell'Ufficio formulate dal segretario generale ai sensi dell'art. 15 del regolamento del Garante n. 1/2000;

Relatore il dott. Giuseppe Fortunato;

Autorizza

gli investigatori privati a trattare i dati sensibili di cui all'art. 4, comma 1, lett. *d*), del Codice, secondo le prescrizioni di seguito indicate.

Prima di iniziare o proseguire il trattamento 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, in conformità all'art. 3 del Codice.

1) Ambito di applicazione

La presente autorizzazione è rilasciata, anche senza richiesta, alle persone fisiche e giuridiche, agli istituti, agli enti, alle associazioni e agli organismi che esercitano un'attività di investigazione privata autorizzata con licenza prefettizia (art. 134 del regio decreto 18 giugno 1931, n. 773, e successive modificazioni e integrazioni).

2) *Finalità* del trattamento

Il trattamento può essere effettuato unicamente per l'espletamento dell'incarico ricevuto dai soggetti di cui al punto 1) e in particolare:

a) per permettere a chi conferisce uno specifico incarico di far valere o difendere in sede giudiziaria un proprio diritto, che, quando i dati siano idonei a rivelare lo stato di salute e la vita sessuale dell'interessato, deve essere di rango pari a quello

del soggetto al quale si riferiscono i dati, ovvero consistente in un diritto della personalità o in un altro diritto o libertà fondamentale ed inviolabile;

b) su incarico di un difensore in riferimento ad un procedimento penale, per ricercare e individuare elementi a favore del relativo assistito da utilizzare ai soli fini dell'esercizio del diritto alla prova (art. 190 del codice di procedura penale e legge 7 dicembre 2000, n. 397).

Restano ferme le altre autorizzazioni generali rilasciate ai fini dello svolgimento delle investigazioni in relazione ad un procedimento penale o per l'esercizio di un diritto in sede giudiziaria, in particolare:

a) nell'ambito dei rapporti di lavoro (autorizzazione n. 1/2007, rilasciata il 28 giugno 2007);
b) relativamente ai dati idonei a rivelare lo stato di salute e la vita sessuale (autorizzazione n. 2/2007, rilasciata il 28 giugno 2007);
c) da parte degli organismi di tipo associativo e delle fondazioni (autorizzazione n. 3/2007, rilasciata il 28 giugno 2007);
d) da parte dei liberi professionisti iscritti in albi o elenchi professionali, ivi inclusi i difensori e i relativi sostituti ed ausiliari (autorizzazione n. 4/2007, rilasciata il 28 giugno 2007);
e) relativamente ai dati di carattere giudiziario (autorizzazione n. 7/2007, rilasciata il 28 giugno 2007).

3) Categorie di dati e interessati ai quali i dati si riferiscono

Il trattamento può riguardare i dati sensibili di cui all'art. 4, comma 1, lett. d) del Codice, qualora ciò sia strettamente indispensabile per eseguire specifici incarichi conferiti per scopi determinati e legittimi nell'ambito delle finalità di cui al punto 1), che non possano essere adempiute mediante il trattamento di dati anonimi o di dati personali di natura diversa.

I dati devono essere pertinenti e non eccedenti rispetto agli incarichi conferiti.

4) Modalità di trattamento

Gli investigatori privati non possono intraprendere di propria iniziativa investigazioni, ricerche o altre forme di raccolta di dati. Tali attività possono essere eseguite esclusivamente sulla base di un apposito incarico conferito per iscritto, anche da un difensore, per le esclusive finalità di cui al punto 2).

L'atto di incarico deve menzionare in maniera specifica il diritto che si intende esercitare in sede giudiziaria, ovvero il procedimento penale al quale l'investigazione è collegata, nonché i principali elementi di fatto che giustificano l'investigazione e il termine ragionevole entro cui questa deve essere conclusa.

Fermi restando gli obblighi previsti dagli articoli 11 e 14 del Codice, nonché dagli articoli 31 e seguenti del Codice e dall'Allegato B) al medesimo Codice, il trattamento dei dati sensibili deve essere effettuato unicamente con operazioni, nonché con logiche e mediante forme di organizzazione dei dati strettamente indispensabili in rapporto alle finalità di cui al punto 2).

L'interessato o la persona presso la quale sono raccolti i dati deve essere informata ai sensi dell'art. 13 del Codice, ponendo in particolare evidenza l'identità e la qualità professionale dell'investigatore, nonché la natura facoltativa del conferimento dei dati.

Nel caso in cui i dati sono raccolti presso terzi, è necessario informare l'interessato e acquisire il suo consenso scritto (art. 13, commi 1, 4 e 5 e art. 26, comma 4, del Codice), solo se i dati sono trattati per un periodo superiore a quello strettamente necessario per esercitare il diritto in sede giudiziaria o per svolgere le investigazioni difensive, oppure se i dati sono utilizzati per ulteriori finalità non incompatibili con quelle precedentemente perseguite.

Il difensore o il soggetto che ha conferito l'incarico devono essere informati periodicamente dell'andamento dell'investigazione, anche al fine di permettere loro una valutazione tempestiva circa le determinazioni da adottare riguardo all'esercizio del diritto in sede giudiziaria o al diritto alla prova.

L'investigatore privato deve eseguire personalmente l'incarico ricevuto e non può avvalersi di altri investigatori non indicati nominativamente all'atto del conferimento dell'incarico.

Nel caso in cui si avvalga di collaboratori interni designati quali responsabili o incaricati del trattamento in conformità a quanto previsto dagli articoli 29 e 30 del Codice, l'investigatore privato deve vigilare con cadenza almeno settimanale sulla puntuale osservanza delle norme di legge e delle istruzioni impartite. Tali soggetti possono avere accesso ai soli dati strettamente pertinenti alla collaborazione ad essi richiesta.

Per quanto non previsto nella presente autorizzazione, il trattamento dei dati idonei a rivelare lo stato di salute e la vita sessuale deve essere effettuato nel rispetto delle ulteriori prescrizioni contenute nell'autorizzazione generale n. 2/2007 e, per ciò che riguarda le informazioni relative ai dati genetici, nel rispetto dell'autorizzazione del 22 febbraio 2007, pubblicata nella *Gazzetta Ufficiale* n. 65 del 19 marzo 2007.

Il trattamento dei dati deve inoltre rispettare le prescrizioni del codice di deontologia e di buona condotta di cui all'articolo 135 del Codice in via di definizione.

5) Conservazione dei dati

Nel quadro del rispetto dell'obbligo previsto dall'art. 11, comma 1, lett. *e*), del Codice i dati sensibili possono essere conservati per un periodo non superiore a quello strettamente necessario per eseguire l'incarico ricevuto.

A tal fine deve essere verificata costantemente, anche mediante controlli periodici, la stretta pertinenza, non eccedenza e indispensabilità dei dati rispetto alle finalità perseguite e all'incarico conferito.

Una volta conclusa la specifica attività investigativa, il trattamento deve cessare in ogni sua forma, fatta eccezione per l'immediata comunicazione al difensore o al soggetto che ha conferito l'incarico.

La mera pendenza del procedimento al quale l'investigazione è collegata, ovvero il passaggio ad altre fasi di giudizio in attesa della formazione del giudicato, non costituiscono, di per se stessi, una giustificazione valida per la conservazione dei dati da parte dell'investigatore privato.

6) Comunicazione e diffusione dei dati

I dati possono essere comunicati unicamente al soggetto che ha conferito l'incarico.

I dati non possono essere comunicati ad un altro investigatore privato, salvo che questi sia stato indicato nominativamente nell'atto di incarico e la comunicazione sia necessaria per lo svolgimento dei compiti affidati.

I dati idonei a rivelare lo stato di salute possono essere comunicati alle autorità competenti solo se è necessario per finalità di prevenzione, accertamento o repressione dei reati, con l'osservanza delle norme che regolano la materia.

I dati relativi allo stato di salute e alla vita sessuale non possono essere diffusi.

7) Richieste di autorizzazione

I titolari dei trattamenti che rientrano nell'ambito di applicazione della presente autorizzazione non sono tenuti a presentare una richiesta di autorizzazione a questa Autorità, qua-

lora il trattamento che si intende effettuare sia conforme alle prescrizioni suddette.

Le richieste di autorizzazione pervenute o che perverranno anche successivamente alla data di adozione del presente provvedimento, devono intendersi accolte nei termini di cui al provvedimento medesimo.

Il Garante non prenderà in considerazione richieste di autorizzazione per trattamenti da effettuarsi in difformità alle prescrizioni del presente provvedimento, salvo che, ai sensi dell'art. 41 del Codice, il loro accoglimento sia giustificato da circostanze del tutto particolari o da situazioni eccezionali non considerate nella presente autorizzazione.

8) Norme finali

Restano fermi gli obblighi previsti dalla normativa comunitaria, ovvero da norme di legge o di regolamento, che stabiliscono divieti o limiti in materia di trattamento di dati personali e, in particolare:

a) dagli articoli 4 (impianti e apparecchiature per finalità di controllo a distanza dei lavoratori) e 8 (indagini sulle opinioni del lavoratore o su altri fatti non rilevanti ai fini della valutazione dell'attitudine professionale) della legge 20 maggio 1970, n. 300 e dall'art. 10 (indagini sulle opinioni del lavoratore e trattamenti discriminatori) del decreto legislativo 10 settembre 2003, n. 276;
b) dalla legge 5 giugno 1990, n. 135, in materia di sieropositività e di infezione da Hiv;
c) dalle norme volte a prevenire discriminazioni;
d) dall'art. 734-*bis* del codice penale, il quale vieta la divulgazione non consensuale delle generalità o dell'immagine della persona offesa da atti di violenza sessuale.

Restano fermi, in particolare, gli obblighi previsti in tema di liceità e di correttezza nell'uso di strumenti o apparecchiature che permettono la raccolta di informazioni anche sonore o visive, ovvero in tema di accesso a banche dati o di cognizione del contenuto della corrispondenza e di 8 comunicazioni o conversazioni telefoniche, telematiche o tra soggetti presenti.

Resta ferma la facoltà per le persone fisiche di trattare direttamente dati per l'esclusivo fine della tutela di un proprio diritto in sede giudiziaria, anche nell'ambito delle investigazioni relative ad un procedimento penale. In tali casi, il Codice non si applica anche se i dati sono comunicati occasionalmente ad una autorità giudiziaria o a terzi, sempre che i dati non siano destinati ad una comunicazione sistematica o alla diffusione (art. 5, comma 3, del Codice).

9) Efficacia temporale e disciplina transitoria

La presente autorizzazione ha efficacia a decorrere dal 1° luglio 2007 fino al 30 giugno 2008, salve eventuali modifiche che il Garante ritenga di dover apportare in conseguenza di eventuali novità normative rilevanti in materia.

La presente autorizzazione sarà pubblicata nella *Gazzetta Ufficiale* della Repubblica italiana.

Roma, 28 giugno 2007

IL PRESIDENTE
Pizzetti

IL RELATORE
Fortunato

IL SEGRETARIO GENERALE
Buttarelli

34 Autorizzazione n. 7/2007 al trattamento dei dati a carattere giudiziario da parte di privati, di enti pubblici economici e di soggetti pubblici (*)

28 giugno 2007

Registro delle deliberazioni
n. 29 del 28 giugno 2007

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

In data odierna, con la partecipazione del prof. Francesco Pizzetti, presidente, del dott. Giuseppe Chiaravalloti, vice presidente, del dott. Mauro Paissan e del dott. Giuseppe Fortunato, componenti, e del dott. Giovanni Buttarelli, segretario generale;

Visto il decreto legislativo 30 giugno 2003, n. 196, recante il Codice in materia di protezione dei dati personali;

Visto l'art. 4, comma 1, lett. *e*), del Codice, il quale individua i dati giudiziari;

Visti, in particolare, gli articoli 21, comma 1, e 27 del Codice, che consentono il trattamento di dati giudiziari, rispettivamente, da parte di soggetti pubblici e di privati o di enti pubblici economici, soltanto se autorizzato da espressa disposizione di legge o provvedimento del Garante che specifichino le finalità di rilevante interesse pubblico del trattamento, i tipi di dati trattati e le precise operazioni eseguibili;

Visti gli articoli 20, commi 2 e 4, e le disposizioni relative a specifici settori di cui alla Parte II, del Codice e, in particolare, i Capi III e IV del Titolo IV, nel quale sono indicate finalità di rilevante interesse pubblico che rendono ammissibile il trattamento di dati giudiziari da parte di soggetti pubblici;

Visto l'art. 22 del Codice, il quale prevede i principi applicabili al trattamento di dati sensibili e giudiziari da parte di soggetti pubblici;

Considerato che il trattamento dei dati in questione può essere autorizzato dal Garante anche d'ufficio con provvedimenti di carattere generale, relativi a determinate categorie di titolari o di trattamenti (art. 40 del Codice);

Considerato che le autorizzazioni di carattere generale sinora rilasciate sono risultate uno strumento idoneo per prescrivere misure uniformi a garanzia degli interessati, rendendo altresì superflua la richiesta di singoli provvedimenti di autorizzazione da parte di numerosi titolari del trattamento;

Ritenuto opportuno rilasciare nuove autorizzazioni in sostituzione di quelle in scadenza il 30 giugno 2007, armonizzando le prescrizioni già impartite alla luce dell'esperienza maturata;

Ritenuto opportuno che anche tali nuove autorizzazioni siano provvisorie e a tempo determinato, ai sensi dell'art. 41, comma 5, del Codice, e, in particolare, efficaci per il periodo di dodici mesi;

(*) ***G.U.*** **24 agosto 2007, n. 196**
[doc. *web* n. 1430147]

Visti gli articoli 51 e 52 del Codice in materia di informatica giuridica e ritenuta la necessità di favorire la prosecuzione dell'attività di documentazione, studio e ricerca in campo giuridico, in particolare per quanto riguarda la diffusione di dati relativi a precedenti giurisprudenziali, in ragione anche dell'affinità che tali attività presentano con quelle di manifestazione del pensiero già disciplinate dall'art. 137 del Codice;

Considerata la necessità di garantire il rispetto di alcuni principi volti a ridurre al minimo i rischi di danno o di pericolo che i trattamenti potrebbero comportare per i diritti e le libertà fondamentali, nonché per la dignità delle persone, e, in particolare, per il diritto alla protezione dei dati personali sancito dall'art. 1 del Codice;

Visto l'art. 167 del Codice;

Visto l'art. 11, comma 2, del Codice, il quale stabilisce che i dati trattati in violazione della disciplina rilevante in materia di trattamento di dati personali non possono essere utilizzati;

Visti gli articoli 31 e seguenti del Codice e il disciplinare tecnico di cui all'Allegato B) al medesimo Codice recanti norme e regole sulle misure di sicurezza;

Visto l'art. 41 del Codice;

Visti gli atti d'ufficio;

Viste le osservazioni dell'Ufficio formulate dal segretario generale ai sensi dell'art. 15 del regolamento del Garante n. 1/2000;

Relatore il dott. Giuseppe Chiaravalloti;

Autorizza

i trattamenti di dati giudiziari per le finalità di rilevante interesse pubblico di seguito specificate ai sensi degli articoli 21 e 27 del Codice, secondo le prescrizioni di seguito indicate.

Prima di iniziare o proseguire il trattamento 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, in conformità all'art. 3 del Codice.

CAPO I - RAPPORTI DI LAVORO

1) Ambito di applicazione e finalità del trattamento

L'autorizzazione è rilasciata, anche senza richiesta, a persone fisiche e giuridiche, enti, associazioni ed organismi che:

a) sono parte di un rapporto di lavoro;
b) utilizzano prestazioni lavorative anche atipiche, parziali o temporanee;
c) conferiscono un incarico professionale a consulenti, liberi professionisti, agenti, rappresentanti e mandatari.

Il trattamento deve essere indispensabile per adempiere o per esigere l'adempimento di specifici obblighi o per eseguire specifici compiti previsti da leggi, dalla normativa comunitaria, da regolamenti o da contratti collettivi, anche aziendali, e ai soli fini della gestione del rapporto di lavoro, anche autonomo o non retribuito od onorario.

L'autorizzazione è altresì rilasciata a soggetti che in relazione ad un'attività di composizione di controversie esercitata in conformità alla legge svolgono un trattamento indispensabile al medesimo fine.

2) Interessati ai quali i dati si riferiscono

Il trattamento può riguardare dati attinenti a soggetti che hanno assunto o intendono assumere la qualità di:

a) lavoratori subordinati, anche se parti di un contratto di apprendistato, o di formazione e lavoro, o di inserimento, o di lavoro ripartito, o di lavoro intermittente o a chiamata, ovvero prestatori di lavoro nell'ambito di un contratto di somministrazione, o in rapporto di tirocinio, ovvero di associati anche in compartecipazione o di titolari di borse di lavoro e di rapporti analoghi;
b) amministratori o membri di organi esecutivi o di controllo;
c) consulenti e liberi professionisti, agenti, rappresentanti e mandatari.

CAPO II - ORGANISMI DI TIPO ASSOCIATIVO E FONDAZIONI

1) Ambito di applicazione e finalità del trattamento

L'autorizzazione è rilasciata anche senza richiesta:

a) ad associazioni anche non riconosciute, ivi compresi partiti e movimenti politici, associazioni ed organizzazioni sindacali, patronati, associazioni a scopo assistenziale o di volontariato, a fondazioni, comitati e ad ogni altro ente, consorzio od organismo senza scopo di lucro, dotati o meno di personalità giuridica, nonché a cooperative sociali e società di mutuo soccorso di cui, rispettivamente, alle leggi 8 novembre 1991, n. 381 e 15 aprile 1886, n. 3818;
b) ad enti ed associazioni anche non riconosciute che curano il patrocinio, il recupero, l'istruzione, la formazione professionale, l'assistenza socio-sanitaria, la beneficenza e la tutela di diritti in favore dei soggetti cui si riferiscono i dati o dei relativi familiari e conviventi.

Il trattamento deve essere indispensabile per perseguire scopi determinati e legittimi individuati dall'atto costitutivo, dallo statuto o da un contratto collettivo.

2) Interessati ai quali i dati si riferiscono

Il trattamento può riguardare dati attinenti:

a) ad associati, soci e aderenti, nonché, nei casi in cui l'utilizzazione dei dati sia prevista dall'atto costitutivo o dallo statuto, a soggetti che presentano richiesta di ammissione o di adesione;
b) a beneficiari, assistiti e fruitori delle attività o dei servizi prestati dall'associazione, dall'ente o dal diverso organismo.

CAPO III - LIBERI PROFESSIONISTI

1) Ambito di applicazione e finalità del trattamento

L'autorizzazione è rilasciata anche senza richiesta ai:

a) liberi professionisti, anche associati, tenuti ad iscriversi in albi o elenchi per l'esercizio di un'attività professionale in forma individuale o associata, anche in conformità al decreto legislativo 2 febbraio 2001, n. 96 o alle norme di attuazione dell'art. 24, comma 2, della legge 7 agosto 1997, n. 266, in tema di attività di assistenza e consulenza;
b) soggetti iscritti nei corrispondenti albi o elenchi speciali, istituiti anche ai sensi dell'art. 34 del regio decreto-legge 27 novembre 1933, n. 1578 e successive modificazioni e integrazioni, recante l'ordinamento della professione di avvocato;
c) sostituti e ausiliari che collaborano con il libero professionista ai sensi dell'art. 2232 del codice civile, praticanti e tirocinanti, qualora tali soggetti siano titolari di un autonomo trattamento o siano contitolari del trattamento effettuato dal libero professionista.

2) Interessati ai quali i dati si riferiscono

Il trattamento può riguardare dati attinenti ai clienti.

I dati relativi ai terzi possono essere trattati solo ove ciò sia strettamente indispensabile per eseguire specifiche prestazioni professionali richieste dai clienti per scopi determinati e legittimi.

CAPO IV - IMPRESE BANCARIE ED ASSICURATIVE ED ALTRI TITOLARI DEI TRATTAMENTI

1) Ambito di applicazione e finalità del trattamento

L'autorizzazione è rilasciata, anche senza richiesta:

a) ad imprese autorizzate o che intendono essere autorizzate all'esercizio dell'attività bancaria e creditizia, assicurativa o dei fondi pensione, anche se in stato di liquidazione coatta amministrativa, ai fini:
   1) dell'accertamento, nei casi previsti dalle leggi e dai regolamenti, del requisito di onorabilità nei confronti di soci e titolari di cariche direttive o elettive;
   2) dell'accertamento, nei soli casi espressamente previsti dalla legge, di requisiti soggettivi e di presupposti interdittivi;
   3) dell'accertamento di responsabilità in relazione a sinistri o eventi attinenti alla vita umana;
   4) dell'accertamento di situazioni di concreto rischio per il corretto esercizio dell'attività assicurativa, in relazione ad illeciti direttamente connessi con la medesima attività. Per questi ultimi casi, limitatamente ai trattamenti di dati registrati in una specifica banca di dati ai sensi dell'art. 4, comma 1, lett. *p*), del Codice, il titolare deve inviare al Garante una dettagliata relazione sulle modalità del trattamento;

b) a soggetti titolari di un trattamento di dati svolto nell'ambito di un'attività di richiesta, acquisizione e consegna di atti e documenti presso i competenti uffici pubblici, effettuata su incarico degli interessati;

c) alle società di intermediazione mobiliare, alle società di investimento a capitale variabile, alle società di gestione del risparmio e dei fondi pensione e alle società di gestione dei mercati regolamentati o alle società di gestione accentrata di strumenti finanziari ai fini dell'accertamento dei requisiti di onorabilità in applicazione della normativa in materia di intermediazione finanziaria e di previdenza o di forme pensionistiche complementari, e di eventuali altre norme di legge o di regolamento.

2) Ulteriori trattamenti

L'autorizzazione è rilasciata altresì:

a) a chiunque, per far valere o difendere un diritto anche da parte di un terzo in sede giudiziaria, nonché in sede amministrativa o nelle procedure di arbitrato e di conciliazione nei casi previsti dalle leggi, dalla normativa comunitaria, dai regolamenti o dai contratti collettivi, sempre che il diritto da far valere o difendere sia di rango pari a quello dell'interessato e i dati siano trattati esclusivamente per tale finalità e per il periodo strettamente necessario per il suo perseguimento;

b) a chiunque, per l'esercizio del diritto di accesso ai documenti amministrativi, nei limiti di quanto previsto dalle leggi e dai regolamenti in materia;

c) a persone fisiche e giuridiche, istituti, enti ed organismi che esercitano un'attività di investigazione privata autorizzata con licenza prefettizia (art. 134 del regio decreto 18 giugno 1931, n. 773, e successive modificazioni e integrazioni).

Il trattamento deve essere necessario:

1. per permettere a chi conferisce uno specifico incarico di far valere o difendere in sede giudiziaria un proprio diritto di rango pari a quello del soggetto al quale si riferiscono i dati, ovvero di un diritto della personalità o di un altro diritto fondamentale ed inviolabile;
2. su incarico di un difensore in riferimento ad un procedimento penale, per ricercare e individuare elementi a favore del relativo assistito da utilizzare ai soli fini dell'esercizio del diritto alla prova (articolo 190 del codice di procedura penale e legge 7 dicembre 2000, n. 397);

d) a chiunque, per adempiere ad obblighi previsti da disposizioni di legge in materia di comunicazioni e certificazioni antimafia o in materia di prevenzione della

delinquenza di tipo mafioso e di altre gravi forme di manifestazione di pericolosità sociale, contenute anche nella legge 19 marzo 1990, n. 55, e successive modificazioni ed integrazioni, o per poter produrre la documentazione prescritta dalla legge per partecipare a gare d'appalto;

e) a chiunque, ai fini dell'accertamento del requisito di idoneità morale di coloro che intendono partecipare a gare d'appalto, in adempimento di quanto previsto dalla normativa in materia di appalti.

CAPO V - DOCUMENTAZIONE GIURIDICA

1) Ambito di applicazione e finalità del trattamento

L'autorizzazione è rilasciata per il trattamento, ivi compresa la diffusione, di dati per finalità di documentazione, di studio e di ricerca in campo giuridico, in particolare per quanto riguarda la raccolta e la diffusione di dati relativi a pronunce giurisprudenziali, nel rispetto di quanto previsto dagli articoli 51 e 52 del Codice.

CAPO VI - PRESCRIZIONI COMUNI A TUTTI I TRATTAMENTI

Per quanto non previsto dai capi che precedono, ai trattamenti ivi indicati si applicano, altresì, le seguenti prescrizioni:

1) Dati trattati

Possono essere trattati i soli dati essenziali per le finalità per le quali è ammesso il trattamento e che non possano essere adempiute, caso per caso, mediante il trattamento di dati anonimi o di dati personali di natura diversa.

2) Modalità di trattamento

Il trattamento dei dati deve essere effettuato unicamente con operazioni, nonché con logiche e mediante forme di organizzazione dei dati strettamente indispensabili in rapporto agli obblighi, ai compiti o alle finalità precedentemente indicati. Fuori dei casi previsti dai Capi IV, punto 2 e V, o nei quali la notizia è acquisita da fonti accessibili a chiunque, i dati devono essere forniti dagli interessati nel rispetto della disciplina prevista dal d.P.R.14 novembre 2002, n. 313 e successive variazioni.

3) Conservazione dei dati

Con riferimento all'obbligo previsto dall'art. 11, comma 1, lett. *e)* del Codice, i dati possono essere conservati per il periodo di tempo previsto da leggi o regolamenti e, comunque, per un periodo non superiore a quello strettamente necessario per le finalità perseguite.

Ai sensi dell'art. 11, comma 1, lett. *c*), *d*) ed *e*) del Codice, i soggetti autorizzati verificano periodicamente l'esattezza e l'aggiornamento dei dati, nonché la loro pertinenza, completezza, non eccedenza e necessità rispetto alle finalità perseguite nei singoli casi. Al fine di assicurare che i dati siano strettamente pertinenti, non eccedenti e indispensabili rispetto alle finalità medesime, i soggetti autorizzati valutano specificamente il rapporto tra i dati e i singoli obblighi, compiti e prestazioni. I dati che, anche a seguito delle verifiche, risultino eccedenti o non pertinenti o non indispensabili non possono essere utilizzati, salvo che per l'eventuale conservazione, a norma di legge, dell'atto o del documento che li contiene. Specifica attenzione è prestata per la verifica dell'essenzialità dei dati riferiti a soggetti diversi da quelli cui si riferiscono direttamente gli obblighi, i compiti e le prestazioni.

4) Comunicazione e diffusione

I dati possono essere comunicati e, ove previsto dalla legge, diffusi, a soggetti pubblici o privati nei limiti strettamente indispensabili per le finalità perseguite e nel rispetto, in ogni caso, del segreto professionale e delle altre prescrizioni sopraindicate.

5) Richieste di autorizzazione

I titolari dei trattamenti che rientrano nell'ambito di applicazione della presente autorizzazione non sono tenuti a presentare una richiesta di autorizzazione al Garante, qualora il trattamento che si intende effettuare sia conforme alle prescrizioni suddette.

Le richieste di autorizzazione pervenute o che perverranno anche successivamente alla data di adozione del presente provvedimento, devono intendersi accolte nei termini di cui al provvedimento medesimo.

Il Garante si riserva l'adozione di ogni altro provvedimento per i trattamenti non considerati nella presente autorizzazione.

Per quanto riguarda invece i trattamenti disciplinati nel presente provvedimento, il Garante non prenderà in considerazione richieste di autorizzazione per trattamenti da effettuarsi in difformità alle relative prescrizioni, salvo che, ai sensi dell'art. 41 del Codice, il loro accoglimento sia giustificato da circostanze del tutto particolari o da situazioni eccezionali non considerate nella presente autorizzazione.

Restano fermi gli obblighi previsti da norme di legge o di regolamento o dalla normativa comunitaria che stabiliscono divieti o limiti più restrittivi in materia di trattamento di dati personali e, in particolare, dalle disposizioni contenute nell'art. 8 della legge 20 maggio 1970, n. 300, fatto salvo dall'art. 113 del Codice, che vieta al datore di lavoro ai fini dell'assunzione e nello svolgimento del rapporto di lavoro, di effettuare indagini, anche a mezzo di terzi, sulle opinioni politiche, religiose o sindacali del lavoratore, nonché su fatti non rilevanti ai fini della valutazione dell'attitudine professionale del lavoratore e dall'art. 10 del d.lg. 10 settembre 2003, n. 276, che vieta alle agenzie per il lavoro e agli altri soggetti privati autorizzati o accreditati di effettuare determinate indagini o comunque trattamenti di dati ovvero di preselezione di lavoratori.

6) Efficacia temporale e disciplina transitoria

La presente autorizzazione ha efficacia a decorrere dal 1° luglio 2007 fino al 30 giugno 2008, salve eventuali modifiche che il Garante ritenga di dover apportare in conseguenza di eventuali novità normative rilevanti in materia.

La presente autorizzazione sarà pubblicata nella *Gazzetta Ufficiale* della Repubblica italiana.

Roma, 28 giugno 2007

IL PRESIDENTE
Pizzetti

IL RELATORE
Chiaravalloti

IL SEGRETARIO GENERALE
Buttarelli

35 Misure e accorgimenti a garanzia degli interessati in tema di conservazione di dati di traffico telefonico e telematico per finalità di accertamento e repressione dei reati (*)

19 settembre 2007

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Nella riunione odierna, in presenza del prof. Francesco Pizzetti, presidente, del dott. Giuseppe Chiaravalloti, vice presidente, del dott. Mauro Paissan e del dott. Giuseppe Fortunato, componenti, e del dott. Giovanni Buttarelli, segretario generale;

Visto il Codice in materia di protezione dei dati personali (d.lg. 30 giugno 2003, n. 196, di seguito, "Codice") e, in particolare, i relativi articoli 17 e 132, comma 5;

Considerato che l'Autorità ha concluso i primi approfondimenti inerenti alle misure e agli accorgimenti che il Garante deve prescrivere in base al Codice in riferimento ai dati del traffico telefonico e telematico che devono essere conservati, in base alla legge, dai fornitori di servizi di comunicazione elettronica, per esclusive finalità di accertamento e repressione di reati;

RILEVATA l'opportunità che la prescrizione di tali misure ed accorgimenti, che allo stato sono individuati dal Garante nell'unito documento, sia preceduta da una consultazione pubblica, in particolare dei predetti fornitori, di organismi rappresentativi di utenti e abbonati interessati, nonché del Ministero della giustizia, del Ministero dell'interno e del Consiglio superiore della magistratura, anche al fine di acquisire ulteriori riscontri sull'adeguatezza delle medesime prescrizioni, nonché sulle relative modalità attuative;

Viste le osservazioni formulate dal segretario generale ai sensi dell'art. 15 del regolamento del Garante n. 1/2000;

Relatore il prof. Francesco Pizzetti;

DELIBERA

a) di adottare l' unito documento che forma parte integrante della presente deliberazione ("Misure e accorgimenti a garanzia degli interessati in tema di conservazione di dati di traffico telefonico e telematico per finalità di accertamento e repressione dei reati");
b) di avviare una consultazione pubblica sul documento di cui alla lettera a).

L'obiettivo della consultazione è quello di acquisire osservazioni e commenti, in particolare da parte di fornitori di servizi di comunicazione elettronica, loro organismi rappresentativi e analoghi organismi relativi a utenti e abbonati interessati, nonché del Ministero della giustizia, del Ministero dell'interno e del Consiglio superiore della magistratura.

Osservazioni e commenti potranno pervenire entro il 31 ottobre 2007 all'indirizzo dell'Autorità di Piazza di Monte Citorio n. 121, 00186 Roma, ovvero all'indirizzo di posta elettronica *datiditraffico@garanteprivacy.it.*

(*) [doc. *web* n. 1442463]

La presente deliberazione verrà pubblicata sul sito *web* del Garante *www.garanteprivacy.it* e verrà inviato un avviso all'Ufficio pubblicazione leggi e decreti del Ministero della giustizia affinché sia riportato sulla *Gazzetta Ufficiale* della Repubblica italiana.

Roma, 19 settembre 2007

IL PRESIDENTE
Pizzetti

IL RELATORE
Pizzetti

IL SEGRETARIO GENERALE
Buttarelli

MISURE E ACCORGIMENTI A GARANZIA DEGLI INTERESSATI IN TEMA DI CONSERVAZIONE DI DATI DI TRAFFICO TELEFONICO E TELEMATICO PER FINALITÀ DI ACCERTAMENTO E REPRESSIONE DEI REATI (*)

1. Considerazioni preliminari

I dati relativi al traffico telefonico e telematico sono informazioni che dovrebbero riguardare solo alcune caratteristiche esteriori delle conversazioni, delle chiamate e delle comunicazioni, senza permettere di desumerne, almeno direttamente, i contenuti.

Tuttavia, tali caratteristiche permettono di individuare analiticamente quando, tra chi e come sono intercorsi contatti telefonici o per via telematica. Innumerevoli informazioni, quando divengono oggetto di una conservazione massiva e capillare sia pure solo per determinate finalità di giustizia, consentono di ricostruire anche a notevole distanza di tempo intere sfere di relazioni personali, professionali, commerciali e istituzionali e di formare anche delicati profili interpersonali: si tratta in altre parole di dati che possiedono un'"accentuata valenza divulgativa di notizie caratterizzanti la personalità dell'autore". (1)

Vi è, quindi, un'incidenza sulla libertà stessa di comunicazione. Inoltre, specifici segreti attinenti a determinate attività, relazioni e professioni possono essere esposti a un serio pregiudizio.

Quando tali dati devono essere conservati per un'eccezionale necessità prevista dalla legge, la loro custodia deve essere pertanto basata su elevate cautele, volte a prevenire rischi specifici per la dignità, i diritti e le libertà fondamentali degli interessati, nei cui confronti eventuali abusi possono comportare importanti ripercussioni. (2)

Per le comunicazioni attraverso reti telematiche si possono porre, poi, ulteriori aspetti critici rispetto alle tradizionali forme di conversazione telefonica. Non di rado, i dati esteriori a tali comunicazioni possono essere infatti anche indirettamente espressivi del contenuto di messaggi, consultazioni in rete di documenti e di dialoghi, sempre in rete, tra soggetti definiti. Taluni dati possono permettere anche di desumere particolari orientamenti, convincimenti e abitudini di ordine politico, sindacale o religioso o attinenti alla sfera della salute o della vita sessuale.

2. Quadro normativo di riferimento

2.1. *Normativa comunitaria*

La direttiva n. 2002/58/Ce, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche, impone agli Stati membri di proteggere la riservatezza delle comunicazioni elettroniche e vieta la conservazione dei dati relativi al traffico generati nel corso delle comunicazioni, ad eccezione della conservazione espressamente autorizzata per i fini indicati nella direttiva medesima. Questi fini comprendono la prevenzione, ricerca, accertamento e perseguimento dei reati.

(*) ***Le note sono in calce al testo***

Il legislatore comunitario definisce i dati relativi al traffico come quei dati sottoposti a trattamento *"ai fini della trasmissione di una comunicazione su una rete di comunicazione elettronica o della relativa fatturazione"* (*cfr.* art. 2 della predetta direttiva 2002/58/Ce, nonché il relativo considerando 15 [3]). Precisa, inoltre, quanto all'ambito applicativo, che la direttiva ha ad oggetto il trattamento dei dati personali connesso alla fornitura di servizi di comunicazione elettronica accessibili al pubblico su reti pubbliche di comunicazione (*cfr.* art. 3).

In tale prospettiva, la direttiva, nell'imporre agli Stati membri l'adozione di disposizioni di legge nazionali che assicurino la riservatezza delle comunicazioni effettuate tramite la rete pubblica di comunicazione e i servizi di comunicazione elettronica accessibili al pubblico, pone l'accento sui dati di traffico generati dai servizi medesimi (art. 5 [4]). Precisa, inoltre, che tali dati, trattati e memorizzati dal fornitore della rete pubblica o del servizio pubblico di comunicazione elettronica, devono essere cancellati o resi anonimi quando non sono più necessari ai fini della trasmissione della comunicazione, fatte salve alcune eccezioni, indicate ai paragrafi 2 [5], 3 [6] e 5 [7] dell'art. 6 [8] e all'articolo 15, paragrafo 1 della direttiva.

Quest'ultimo stabilisce, fra l'altro, che gli Stati membri possono adottare disposizioni legislative volte a limitare i diritti e gli obblighi di cui ai predetti articoli 5 e 6 qualora tale restrizione costituisca *"una misura necessaria, opportuna e proporzionata all'interno di una società democratica per la salvaguardia della sicurezza nazionale (cioè della sicurezza dello Stato), della difesa, della sicurezza pubblica; e la prevenzione, ricerca, accertamento e perseguimento dei reati, ovvero dell'uso non autorizzato del sistema di comunicazione elettronica"*.

Il medesimo art. 15 dispone che a tal fine gli Stati membri possano tra l'altro adottare misure legislative le quali prevedano che, per tali motivi, i dati siano conservati per un periodo di tempo limitato.

2.2. *Normativa nazionale*

Il legislatore italiano ha recepito la direttiva 2002/58/Ce, con il Titolo X del Codice, rubricato "Comunicazioni elettroniche".

Più precisamente, nel Capo I di tale Titolo, intitolato *"Servizi di comunicazione elettronica"*, sono contenute alcune disposizioni normative che rilevano ai fini della disciplina sulla conservazione dei dati di traffico.

Ci si riferisce, in particolare, all'art. 121 che, nell'individuare i *"Servizi interessati"*, chiarisce che le disposizioni del Titolo X *"si applicano al trattamento dei dati personali connesso alla fornitura di servizi di comunicazione elettronica accessibili al pubblico su reti pubbliche di comunicazioni"*.

Ci si riferisce, inoltre, agli articoli 123 e 132 del Codice, con i quali sono stati trasposti nell'ordinamento italiano gli articoli 5, 6 e 15 della direttiva 2002/58/Ce in materia di trattamento dei dati personali e di tutela della vita privata nel settore delle comunicazioni elettroniche.

Partendo dal principio secondo il quale i dati non devono essere formati se non sono necessari e proporzionati ai fini della funzionalità della rete o della prestazione del servizio (artt. 3 e 11 del Codice), il legislatore ha stabilito il divieto generale di conservazione dei dati relativi al traffico (art. 123, comma 1 *cit.*), con le seguenti eccezioni:

- è consentito il trattamento di dati strettamente necessario a fini di fatturazione per l'abbonato, ovvero di pagamenti in caso di interconnessione (nei limiti e con le modalità di cui all'art. 123, comma 2) o, previo consenso dell'utente, a fini di commercializzazione di servizi di comunicazione elettronica, per la durata a ciò necessaria (art. 123, comma 3);
- è prescritta la conservazione dei dati di traffico per esclusive finalità di accertamento e repressione dei reati (art. 132 del Codice).

Nell'ambito della normativa nazionale sulla conservazione dei dati di traffico, è intervenuto nel 2005 il decreto legge 27 luglio 2005, n. 144 (poi convertito, con modificazioni,

dalla legge 31 luglio 2005, n. 155), *cd.* "Pacchetto Pisanu", che, in estrema sintesi, ha introdotto:

1) con riguardo ai dati di traffico telefonico, l'obbligo di conservazione delle chiamate senza risposta;
2) l'obbligo di conservazione, per sei mesi più sei, dei dati di traffico telematico, escludendone i contenuti;
3) con riferimento ai primi ventiquattro mesi di conservazione, la previsione che la richiesta di accesso venga effettuata dal *"pubblico ministero anche su istanza"* del difensore dell'imputato, della persona sottoposta alle indagini, della persona offesa e delle altre parti private e non già dal *"giudice su istanza del pubblico ministero"*;
4) un regime transitorio in virtù del quale, fino al 31 dicembre 2007, è sospesa l'applicazione di qualunque disposizione che prescriva o consenta la cancellazione dei dati di traffico, anche se non soggetti a fatturazione;
5) per i titolari o i gestori di esercizi pubblici o di circoli privati di qualsiasi specie, che si limitino a porre a disposizione del pubblico, dei clienti o dei soci apparecchi terminali utilizzabili per le comunicazioni, anche telematiche, esclusi i telefoni pubblici a pagamento abilitati esclusivamente alla telefonia vocale, alcuni specifici obblighi di identificazione e monitoraggio delle operazioni compiute dai clienti (*cfr.* anche il decreto ministeriale attuativo di tale previsione: d.m. 16 agosto 2005, pubblicato in *G.U.* 17 agosto 2005, n. 190).

Pertanto, tale decreto ha, da un lato, parzialmente emendato l'art. 132 del Codice (punti 1, 2 e 3 sopra descritti), dall'altro, introdotto un regime transitorio per la conservazione dei dati, nonché una disciplina speciale per determinati soggetti (punti 4 e 5).

L'attuale normativa di riferimento prescrive, quindi, ai fornitori di servizi di comunicazione elettronica di conservare, per finalità di accertamento e repressione di reati, i dati relativi al traffico telefonico, inclusi quelli concernenti le chiamate senza risposta, e i dati relativi al traffico telematico, esclusi comunque i contenuti delle comunicazioni, rispettivamente per ventiquattro e sei mesi (art. 132, comma 1 del Codice).

Prescrive, inoltre, agli stessi fornitori di conservare tali dati per un periodo ulteriore, rispettivamente di ventiquattro e sei mesi, per l'accertamento e la repressione dei delitti tassativamente individuati dall'art. 407, comma 2, lett. a), c.p.p., nonché dei delitti in danno di sistemi informatici o telematici (art. 132, comma 2).

Infine, prevede che la conservazione dei predetti dati sia effettuata nel rispetto di specifiche misure ed accorgimenti a garanzia degli interessati. L'individuazione di tali cautele è stata demandata al Garante per la protezione dei dati personali (*cfr.* artt. 17 e 132, comma 5, del Codice).

2.3. *Direttiva 2006/24/Ce*

Al fine di armonizzare le disposizioni degli Stati membri sul tema della conservazione dei dati di traffico a fini di indagine, accertamento e perseguimento di reati, è intervenuta anche la direttiva n. 2006/24/Ce del Parlamento europeo e del Consiglio del 15 marzo 2006, al cui recepimento il legislatore italiano è tenuto a provvedere entro il 15 settembre 2007.

Tale direttiva, pur non essendo direttamente applicabile nello Stato, contiene chiare e precise indicazioni sul risultato atteso a livello comunitario in ordine, tra l'altro, alla corretta ed uniforme individuazione delle "categorie di dati da conservare", analiticamente individuate all'art. 5 della direttiva medesima, in relazione agli specifici servizi ivi enucleati, ossia telefonia di rete fissa e telefonia mobile, accesso Internet, posta elettronica su Internet e telefonia via Internet.

Per tali ragioni, si ritiene necessario tenere conto, in questa sede, di tali indicazioni. Ciò, anche in considerazione del fatto che l'attuale quadro normativo di riferimento, pur fornendo una definizione generale di "dati relativi al traffico" (art. 4, comma 2, lett. *h*) del Codice), non distingue i dati relativi al traffico "telefonico" da quelli relativi al traffico "telematico" né li enumera.

Tale distinzione risulta, invece, necessaria in considerazione del fatto che il legislatore italiano, diversamente da quello comunitario, ha individuato due diversi periodi di conservazione in relazione alla natura "telefonica" o "telematica" del dato da conservare.

Si procederà, pertanto, a chiarire l'ambito soggettivo di applicazione dell'obbligo di conservazione dei dati, che risulta funzionale anche alla corretta definizione dei dati da conservare.

3. Ambito soggettivo di applicazione

Il "fornitore" sul quale incombe l'obbligo di conservazione ai sensi dell'art. 132 del Codice è il soggetto che mette a disposizione del pubblico servizi di comunicazione elettronica su reti pubbliche di comunicazione, laddove per *"servizi di comunicazione elettronica"* debbono intendersi quelli consistenti esclusivamente o prevalentemente *"nella trasmissione di segnali su reti di comunicazione elettroniche"* (art. 4, comma 2, lett. *d*) e *e*), del Codice).

Ciò, deriva non solo dalla collocazione della citata norma all'interno del Titolo X, capo I, del Codice e, in particolare, da quanto espressamente disposto dal citato art. 121 del Codice. Ma anche da quanto stabilisce il *cd.* "Pacchetto Pisanu", laddove si riferisce, nell'imporre la conservazione dei dati per il predetto regime transitorio, ai *"fornitori di una rete pubblica di comunicazioni o di un servizio di comunicazione elettronica accessibile al pubblico"*.

Posto quanto sopra, si ritiene siano tenuti alla conservazione dei dati ai sensi dell'art. 132 *cit.*, i soggetti che realizzano esclusivamente o prevalentemente una trasmissione di segnali su reti di comunicazioni elettroniche, a prescindere dall'assetto proprietario della rete e che offrono servizi a utenti finali secondo il principio di non discriminazione (*cfr.* direttiva 2002/22/Ce del Parlamento europeo e del Consiglio relativa al servizio universale e ai diritti degli utenti in materia di reti e di servizi di comunicazione elettronica e d.lg. n. 259/2003, Codice delle comunicazioni elettroniche).

Al contrario, potrebbero non rientrare nell'ambito applicativo del provvedimento:

- i soggetti che offrono servizi di comunicazione elettronica a gruppi delimitati di persone (come, a titolo esemplificativo, i soggetti pubblici o privati che consentono soltanto a propri dipendenti e collaboratori di effettuare comunicazioni telefoniche o telematiche);
- i soggetti che, pur offrendo servizi di comunicazione elettronica accessibili al pubblico, non generano o trattano direttamente i relativi dati di traffico [9], ma che dovranno conservare direttamente un'idonea documentazione attestante che la conservazione effettuata per loro conto presso terzi sia svolta in conformità a quanto previsto nel provvedimento medesimo;
- i titolari e i gestori di esercizi pubblici o di circoli privati di qualsiasi specie, che si limitino a porre a disposizione del pubblico, dei clienti o dei soci apparecchi terminali utilizzabili per le comunicazioni, anche telematiche, ovvero punti di accesso ad Internet utilizzando tecnologia senza fili, esclusi i telefoni pubblici a pagamento abilitati esclusivamente alla telefonia vocale [10];
- i gestori dei siti Internet che diffondono contenuti sulla rete (*cd. "content provider"*); i dati relativi a tale traffico degli utenti che accedono a questi siti sono infatti qualificabili come "contenuti", esclusi espressamente dall'obbligo di conservazione dall'art. 132 del Codice [11];
- i gestori di motori di ricerca; i dati di traffico telematico che essi trattano, consentendo di effettuare agevolmente il tracciamento delle operazioni compiute dall'utente in rete, sono infatti parimenti qualificabili alla stregua di "contenuti".

4. Ambito oggettivo di applicazione

L'obbligo di conservazione riguarda i dati relativi al traffico telefonico, inclusi quelli concernenti le chiamate senza risposta, e i dati relativi al traffico telematico, esclusi comunque i contenuti delle comunicazioni (art. 132 del Codice). In particolare, oggetto di conservazione sono i dati che i fornitori sottopongono a trattamento per la trasmissione della comunicazione o per la relativa fatturazione (art. 4, comma 2, lett. *h*), del Codice).

Pertanto, i fornitori (così come individuati nel precedente paragrafo 3) devono conservare, per esclusive finalità di accertamento e repressione di reati, solo i dati di traffico che risultano nella loro disponibilità in quanto derivanti da attività tecniche strumentali alla resa di un servizio, nonché alla sua fatturazione.

In tal senso, si esprime anche il *cd.* Pacchetto Pisanu che, all'art. 6, riconduce l'obbligo di conservazione alle *"informazioni che consentono la tracciabilità degli accessi, nonché, qualora disponibili, dei servizi"*.

Ed ancora, la direttiva 2006/24/Ce ribadisce che tale obbligo sussiste soltanto se i dati sono stati *"generati o trattati nel processo di fornitura di un [...] servizio di comunicazione"* del fornitore [12].

L'art. 5 di tale direttiva contiene, poi, un'elencazione specifica delle informazioni da conservare e individua diverse categorie di dati di traffico, specificandone i contenuti a seconda che si tratti di traffico telefonico o telematico.

Nell'ambito dei servizi di comunicazione elettronica, occorre infatti distinguere i servizi *"telefonici"* da quelli *"telematici"*.

Nei primi possono essere ricompresi:
- le chiamate telefoniche, incluse le chiamate vocali, di messaggeria vocale, in conferenza e di trasmissione dati tramite *telefax*;
- i servizi supplementari, inclusi l'inoltro e il trasferimento di chiamata;
- la messaggeria e i servizi multimediali, inclusi i servizi di messaggeria breve-*sms.* [13]

Nei secondi possono essere ricompresi:
- l'accesso alla rete Internet;
- la posta elettronica;
- i *fax* e i messaggi *sms* e *mms* via Internet;
- la telefonia via Internet (*cd. Voice over Internet Protocol-VoIP*).

Nell'allegato 1 sono riportati i dati di traffico che, alla luce del quadro normativo sopra descritto, devono essere oggetto di conservazione ai sensi dell'art. 132 del Codice, in relazione allo specifico servizio di comunicazione elettronica offerto.

5. Le finalità

Il vincolo secondo cui i dati conservati obbligatoriamente per legge possono essere utilizzati solo per finalità di accertamento e repressione di reati (individuati peraltro specificamente per il predetto secondo periodo di conservazione) comporta una precisa limitazione per i fornitori nell'eventualità in cui ricevano richieste volte a perseguire ulteriori scopi.

Ad esempio:
a) i medesimi fornitori non possono corrispondere ad eventuali richieste riguardanti tali dati formulate nell'ambito di una controversia civile, amministrativa e contabile;
b) sono tenuti a rispettare il predetto vincolo di finalità anche l'interessato che acceda ai dati che lo riguardano esercitando il diritto di accesso di cui all'art. 7 del Codice (e che può utilizzare quindi i dati acquisiti solo in riferimento alle predette finalità penali), nonché, nel procedimento penale, il difensore dell'imputato, della persona sottoposta alle indagini, della persona offesa e delle altre parti private (art. 132, comma 3, del Codice).

6. Modalità di acquisizione dei dati

Il Codice individua altresì le modalità con le quali possono essere acquisiti i dati di traffico conservati dai fornitori, prescrivendo, con riferimento al primo periodo di conservazione (i primi ventiquattro mesi e sei mesi, rispettivamente per il traffico telefonico e telematico), che la richiesta sia formulata con *"decreto motivato del pubblico ministero anche su*

istanza del difensore dell'imputato, della persona sottoposta alle indagini, della persona offesa e delle altri parti private" (art. 132, comma 3, del Codice).

Al difensore dell'imputato o della persona sottoposta alle indagini è riconosciuta la possibilità di richiedere, direttamente, al fornitore i dati di traffico limitatamente ai dati che si riferiscano *"alle utenze intestate al proprio assistito"*. La richiesta deve essere effettuata *"con le modalità indicate dall'articolo 391-quater del codice di procedura penale, ferme restando le condizioni di cui all'articolo 8, comma 2, lettera f), per il traffico entrante"* (art. 132, comma 3, *cit.*). Tale ultimo riferimento ai presupposti previsti dal Codice per l'accesso alle chiamate in entrata comporta, anche, la necessaria valutazione preliminare, da parte dei fornitori, della circostanza che dalla mancata conoscenza dei dati richiesti possa derivare un pregiudizio effettivo e concreto per lo svolgimento delle investigazioni difensive di cui alla legge 7 dicembre 2000, n. 397. A tal riguardo, si richiama quanto rilevato nel provvedimento adottato dal Garante in materia il 3 novembre 2005, consultabile sul sito dell'Autorità [doc. *web* n. 1189488].

In relazione al secondo periodo di conservazione, il comma 4 dell'art. 132 prevede che i dati conservati possano essere acquisiti soltanto in presenza di un decreto motivato del giudice, che autorizzi l'acquisizione qualora ritenga sussistenti sufficienti indizi dei delitti previsti dall'art. 407, comma 2, lettera a), c.p.p., nonché di quelli in danno di sistemi informatici o telematici.

7. Misure e accorgimenti da prescrivere

A seguito degli approfondimenti anche tecnici svolti nell'ambito e dopo diversi accertamenti ispettivi effettuati presso primari fornitori di servizi di comunicazione elettronica, sono state individuate misure e accorgimenti da porre a garanzia degli interessati nell'ambito della conservazione dei dati di traffico per finalità di accertamento e repressione di reati.

Tali cautele si pongono, ovviamente, senza pregiudizio di ogni altra misura di sicurezza che ciascun fornitore deve adottare ai sensi degli artt. 31 e ss. del Codice, e saranno oggetto di periodico aggiornamento in relazione allo sviluppo tecnologico.

Le misure e gli accorgimenti allo stato individuati dal Garante sono riportati nell' allegato 2.

Il Garante si riserva di stabilire il termine entro il quale le prescrizioni che saranno impartite dall'Autorità dovranno essere attuate dai fornitori, termine che allo stato risulta comunque congruo prevedere in un quadrimestre (semestre). Il Garante si riserva altresì di individuare alcuni trattamenti da notificare all'Autorità ai sensi dell'art. 37, comma 2, del Codice.

ALLEGATO 1
Dati di traffico oggetto di conservazione alla luce della direttiva 2006/24/Ce

Dati generati o trattati nell'ambito dei servizi telefonici

Con riferimento ai servizi telefonici, i fornitori sono tenuti a conservare i dati di traffico, compresi quelli relativi alle chiamate senza risposta, necessari a individuare:

- l'**origine** della comunicazione (numero telefonico chiamante, nome e indirizzo dell'abbonato o utente registrato);
- la **destinazione** della comunicazione (il numero o i numeri telefonici chiamati e, nei casi di servizi supplementari come l'inoltro o il trasferimento di chiamata, il numero o i numeri cui la chiamata è trasmessa);
- i riferimenti temporali della comunicazione (**data** e **ora** di inizio e fine della comunicazione);
- il **tipo** di comunicazione effettuata (servizio telefonico utilizzato);
- le tipologie di **apparecchiature** per la comunicazione, anche presunte, impiegate dagli utenti nella telefonia mobile: *International Mobile Subscriber Identity* (Imsi) e International *Mobile Equipment Identity* (Imei) del chiamante e del chiamato;

nel caso di servizi prepagati anonimi, data e ora dell'attivazione iniziale della carta e etichetta di ubicazione (Cell ID) dalla quale è stata effettuata l'attivazione;
- l'ubicazione delle apparecchiature mobili impiegate per la comunicazione (etichette di ubicazione –Cell ID– all'inizio della comunicazione e dati per identificare l'ubicazione geografica delle cellule, facendo riferimento alle loro etichette di ubicazione nel periodo in cui vengono conservati i dati sulle comunicazioni).

Dati generati o trattati nell'ambito dei servizi telematici
Con riferimento ai servizi telematici, occorre distinguere:

Accesso alla rete Internet
I fornitori sono tenuti a conservare i dati necessari a individuare:
- l'**origine** della comunicazione, ovvero le informazioni identificative del punto di accesso: nome e indirizzo dell'abbonato o dell'utente registrato al quale, al momento della comunicazione, risultavano assegnati uno o più indirizzi di protocollo Ip, un identificativo di utente o un numero telefonico;
- la **data**, l'**ora** e la **durata** dell'accesso (data e ora del *log-in* e del *log-off* al servizio di accesso Internet) unitamente all'**indirizzo Ip** o agli indirizzi Ip, dinamici o statici, assegnati dal fornitore di accesso Internet e l'identificativo dell'abbonato o dell'utente registrato; nel caso di accessi permanenti (in assenza di informazioni su *log-in* e *log-off*), gli indirizzi Ip, dinamici o statici, assegnati dal fornitore di accesso Internet o comunque in uso nelle postazioni dell'abbonato o utente;
- le **attrezzature** di comunicazione, anche presunte, utilizzate dagli utenti: numero della linea telefonica per l'accesso commutato tramite rete telefonica (*dial-up access*); *digital subscriber line number* (Dsl) o altro identificatore di chi è all'origine della comunicazione, nel caso di collegamenti su reti di tipo xDsl.

Posta elettronica
Relativamente ai messaggi spediti da propri utenti o abbonati, i fornitori di servizi di posta elettronica accessibili al pubblico sono tenuti a conservare i dati necessari a individuare:
- l'**origine** della comunicazione (identificativo dell'utente o dell'abbonato al servizio, indirizzo Ip utilizzato dalla postazione mittente e indirizzo di posta elettronica del mittente);
- la **destinazione** della comunicazione (indirizzo di posta elettronica del destinatario del messaggio e indirizzo Ip e nome a dominio pienamente qualificato del *mail exchanger host* a cui è stato trasmesso il messaggio, nel caso della tecnologia *Smtp*);
- la **data** e l'**ora** della comunicazione.

Telefonia, invio di fax, sms *e* mms *via Internet*
I fornitori sono tenuti a conservare i dati necessari a individuare:
- la **fonte** della comunicazione: indirizzo Ip ed eventuale identificativo dell'utente registrato; eventuale numero telefonico e dati anagrafici dell'utente registrato;
- la **destinazione** della comunicazione: numero chiamato e, nei casi di servizi supplementari come l'inoltro o il trasferimento di chiamata, numero o numeri a cui la chiamata è trasmessa;
- la **data**, l'**ora** e la **durata** della comunicazione: data e ora di inizio e fine della comunicazione;
- il **tipo** di comunicazione effettuata: il servizio utilizzato.

ALLEGATO 2
Prescrizioni tecnico-organizzative

Sistemi di autenticazione
Il trattamento dei dati di traffico telefonico e telematico oggetto delle prescrizioni del Garante è consentito agli incaricati solo previo utilizzo di specifici sistemi di autenticazione

informatica basati su tecniche di *strong authentication*, consistenti nell'uso combinato di almeno due differenti tecnologie di autenticazione. Una di tali tecnologie deve essere inoltre basata sull'elaborazione di caratteristiche biometriche.

Si può eventualmente prescindere da tali sistemi solo per i trattamenti effettuati nello svolgimento di mansioni tecniche di gestione dei sistemi e delle apparecchiature informatiche, per i quali resta fermo l'obbligo di assicurare le misure in tema di credenziali di autenticazione previste dall'Allegato B) al Codice in materia di protezione dei dati personali.

Sistemi di autorizzazione

Relativamente ai sistemi di autorizzazione devono essere adottate specifiche procedure in grado di garantire la separazione rigida delle funzioni tecniche di assegnazione di credenziali di autenticazione e di individuazione dei profili di autorizzazione rispetto a quelle di gestione tecnica dei sistemi e delle basi di dati. Tali differenti funzioni non possono essere attribuite contestualmente a uno stesso soggetto o, comunque, nell'ambito della stessa unità organizzativa.

I profili di autorizzazione da definire e da attribuire agli incaricati devono differenziare le funzioni di trattamento dei dati per finalità di accertamento e repressione dei reati distinguendo, al loro interno, incaricati abilitati al trattamento dei dati di cui al primo periodo di conservazione obbligatoria (art. 132, comma 1, del Codice), dagli incaricati abilitati al trattamento dei dati di cui al secondo periodo di conservazione obbligatoria (art. 132, comma 2, del Codice) e, infine, dalle funzioni di trattamento dei dati in caso di esercizio dei diritti dell'interessato (art. 7 del Codice).

Conseguentemente, un incaricato cui è attribuito un profilo di autorizzazione abilitante ad esempio al trattamento dei dati di cui al primo periodo di conservazione obbligatoria (art. 132, comma 1, del Codice) non può accedere, per ciò stesso e direttamente, a dati il cui trattamento richieda il possesso del profilo di autorizzazione relativo al secondo periodo di conservazione obbligatoria (art. 132, comma 2, del Codice).

Conservazione separata

I dati di traffico conservati per finalità di accertamento e repressione di reati vanno gestiti tramite sistemi informatici distinti fisicamente da quelli utilizzati per gestire dati di traffico per altre finalità, sia nelle componenti di elaborazione, sia di immagazzinamento dei dati (*storage*).

Più specificamente, i dati di traffico, i sistemi informatici e gli apparati di rete utilizzati per i trattamenti devono essere separati da quelli utilizzati per le altre funzioni aziendali ed essere altresì protetti contro il rischio di intrusione mediante idonei strumenti di protezione perimetrale.

Le attrezzature informatiche utilizzate per le finalità di giustizia di cui sopra devono essere collocate all'interno di aree ad accesso selezionato e controllato. L'accesso a tali aree deve avvenire previa identificazione e registrazione delle persone ammesse, con indicazione dei motivi dell'accesso e dei relativi riferimenti temporali, anche mediante l'utilizzo di sistemi elettronici.

Nell'ambito dei trattamenti per scopi di accertamento e repressione di reati, una volta decorso il termine di cui al comma 1 dell'art. 132 del Codice, i dati di traffico devono essere trattati con modalità che consentano l'accesso differenziato su base temporale, provvedendo a forme di separazione dei dati che garantiscano il rispetto del principio di finalità dei trattamenti.

La differenziazione può essere ottenuta:

- mediante separazione fisica, predisponendo sistemi del tutto separati nelle componenti di elaborazione e di archiviazione, oppure:
- mediante misure e accorgimenti informatici, intervenendo sulla struttura delle basi di dati, sui sistemi di indicizzazione e sui metodi di accesso (separazione logica).

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

Incaricati del trattamento

Gli incaricati che accedono ai dati di traffico conservati per le finalità di cui all'art. 132 del Codice, anche per consentire l'esercizio dei diritti di cui all'art. 7 del Codice, devono essere designati specificamente.

Il processo di designazione deve prevedere la frequenza di una periodica attività formativa concernente l'illustrazione delle istruzioni, il rispetto delle misure di sicurezza e le relative responsabilità. La partecipazione al corso deve essere documentata.

Per quanto riguarda le richieste per l'esercizio dei diritti di cui all'art. 7 del Codice che comportano l'estrazione dei dati di traffico, nei limiti in cui ciò è consentito ai sensi dell'art. 8, comma 2, lettera *f*) del Codice, il titolare del trattamento deve conservare in forma specifica la documentazione comprovante l'idonea verifica dell'identità del richiedente ai sensi dell'art. 9 del Codice, e adottare opportune cautele per comunicare i dati al solo soggetto legittimato in base al medesimo articolo.

Cancellazione dei dati

Allo scadere dei termini previsti dalle disposizioni vigenti, i dati di traffico sono resi immediatamente non disponibili per le elaborazioni dei sistemi informativi; sono altresì cancellati o resi anonimi senza ritardo, in tempi tecnicamente compatibili con l'esercizio delle procedure per la realizzazione di copie di sicurezza (*backup* e *disaster recovery*) adottate dal titolare anche in applicazione di misure previste dalla normativa vigente e, al più tardi, entro trenta giorni successivi alla scadenza dei termini di cui all'art. 132 del Codice.

Altre misure

Audit log

Devono essere adottate soluzioni informatiche idonee ad assicurare il controllo delle attività svolte sui dati di traffico da ciascun incaricato del trattamento, quali che siano la sua qualifica, le sue competenze e gli ambiti di operatività. Il controllo deve essere efficace e dettagliato anche per i trattamenti condotti su singoli elementi di informazione presenti sui diversi database utilizzati.

Tali soluzioni comprendono la registrazione, in un apposito *audit log*, delle operazioni compiute, direttamente o indirettamente, sui dati di traffico e sugli altri dati personali a essi connessi, sia quando consistono o derivano dall'uso interattivo dei sistemi, sia quando sono svolte tramite l'azione automatica di programmi informatici.

I sistemi di *audit log* devono garantire la completezza, l'immodificabilità, l'autenticità delle registrazioni in essi contenute, con riferimento a tutte le operazioni di trattamento e a tutti gli eventi relativi alla sicurezza informatica sottoposti ad *auditing*. A tali scopi devono essere adottati, per la registrazione dei dati di *auditing*, anche in forma centralizzata per ogni impianto di elaborazione o per datacenter, sistemi di scrittura non alterabili su dispositivi di tipo *Worm* (*write once/read many*). Prima della scrittura, i dati o i raggruppamenti di dati devono essere sottoposti a procedure per attestare la loro integrità, basate sull'utilizzo di tecnologie crittografiche e di firma digitale.

Audit interno–Report periodici

La gestione dei dati di traffico per finalità di accertamento e repressione di reati deve essere oggetto, con cadenza almeno annuale, di un'attività di controllo interno da parte dei titolari del trattamento, in modo che sia verificata costantemente la rispondenza alle misure organizzative, tecniche e di sicurezza riguardanti i trattamenti dei dati di traffico previste dalle norme vigenti e dal provvedimento del Garante, anche per ciò che riguarda la verifica della particolare selettività degli incaricati legittimati.

L'attività di controllo deve essere demandata ad un'unità organizzativa diversa rispetto a quella cui è affidato il trattamento dei dati per la finalità di accertamento e repressione dei reati.

I controlli devono comprendere anche verifiche sulla legittimità e liceità degli accessi ai dati effettuati dagli incaricati del trattamento utilizzando, a tale scopo, strumenti di analisi dei *log* registrati, anche tramite l'introduzione di sistemi di segnalazione automatica di comportamenti "anomali" rispetto al normale profilo di utilizzo del sistema da parte degli operatori (*ad es.*: interrogazioni massive non giustificate, reiterate interrogazioni nei confronti di una medesima anagrafica in un limitato lasso di tempo, interrogazioni effettuate al di fuori del normale orario di servizio). Sono svolte, altresì, verifiche periodiche sull'effettiva cancellazione dei dati decorso i periodi di conservazione.

L'attività di controllo deve essere adeguatamente documentata in modo tale che sia sempre possibile risalire ai sistemi verificati, alle operazioni tecniche su di essi effettuate, alle risultanze delle analisi condotte sugli accessi e alle eventuali criticità riscontrate.

L'esito dell'attività di controllo deve essere:

- comunicato alle persone e agli organi legittimati ad adottare decisioni e ad esprimere, a vari livelli in base al proprio ordinamento interno, la volontà della società;
- richiamato nell'ambito del documento programmatico sulla sicurezza (quando deve essere redatto come misura minima di sicurezza) nel quale devono essere indicati gli interventi eventualmente necessari per adeguare le misure di sicurezza;
- messo, a richiesta, a disposizione del Garante o dell'autorità giudiziaria.

Documentazione dei sistemi informativi

I sistemi informativi utilizzati per il trattamento dei dati di traffico devono essere documentati in modo idoneo secondo i princìpi dell'ingegneria del *software*, evitando soluzioni documentali non corrispondenti a metodi descrittivi *standard* o di ampia accettazione.

La descrizione deve comprendere, per ciascun sistema applicativo, l'architettura logico-funzionale, l'architettura complessiva e la struttura dei sistemi utilizzati per il trattamento, i flussi di input/output dei dati di traffico da e verso altri sistemi, l'architettura della rete di comunicazione, l'elenco di tutti i soggetti aventi legittimo accesso al sistema.

La documentazione va corredata con diagrammi di dislocazione delle applicazioni e dei sistemi, da cui deve risultare anche l'esatta ubicazione dei sistemi nei quali vengono trattati i dati per le finalità di accertamento e repressione di reati.

La documentazione tecnica deve essere aggiornata costantemente e messa a disposizione dell'Autorità su sua eventuale richiesta.

Cifratura e protezione dei dati

I dati di traffico vanno protetti con strumenti di cifratura, in particolare contro rischi di acquisizione fortuita derivanti da operazioni di manutenzione sugli apparati informatici o da ordinarie operazioni di amministrazione di sistema. In particolare, devono essere adottate soluzioni basate su tecnologie crittografiche che rendano le informazioni residenti nelle basi di dati a servizio delle applicazioni informatiche utilizzate per i trattamenti, nella loro interezza o in forma parziale, non intelligibili a chi non disponga di diritti di accesso e profili di autorizzazione idonei.

Tale misura deve essere efficace per evitare che incaricati di mansioni tecniche accessorie ai trattamenti (amministratori di sistema, *database administrator* e manutentori *hardware* e *software*) possano accedere indebitamente alle informazioni registrate, anche fortuitamente, acquisendone conoscenza nel corso di operazioni di accesso ai sistemi o di manutenzione di altro genere.

I flussi di trasmissione dei dati di traffico tra sistemi informatici devono aver luogo tramite protocolli di comunicazione sicuri, basati su tecniche crittografiche.

(1) Corte cost. 26 febbraio-11 marzo 1993, n. 81.

(2) Ciò, a prescindere dalle garanzie previste dall'art. 15 della Costituzione che, secondo la menzionata giurisprudenza costituzionale, operano comunque, anche fuori dei casi di intercettazione legale.

(3) *Cfr.* Considerando 15 direttiva n. 2002/58/Ce: *"Una comunicazione può comprendere qualsiasi informazione relativa al nome, al numero e all'indirizzo fornita da chi emette la comunicazione o dall'utente di un collegamento al fine di effettuare la comunicazione. I dati relativi al traffico possono comprendere qualsiasi traslazione dell'informazione da parte della rete sulla quale la comunicazione è trasmessa allo scopo di effettuare la trasmissione. I dati relativi al traffico possono tra l'altro consistere in dati che si riferiscono all'instradamento, alla durata, al tempo o al volume di una comunicazione, al protocollo usato, all'ubicazione dell'apparecchio terminale di chi invia o riceve, alla rete sulla quale la comunicazione si origina o termina, all'inizio, alla fine o alla durata di un collegamento. Possono anche consistere nel formato in cui la comunicazione è trasmessa dalla rete".*

(4) *Cfr.* art. 5, paragrafo 1, direttiva n. 2002/58/Ce: "*Gli Stati membri assicurano, mediante disposizioni di legge nazionali, la riservatezza delle comunicazioni effettuate tramite la rete pubblica di comunicazione e i servizi di comunicazione elettronica accessibili al pubblico, nonché dei relativi dati sul traffico [...]".*

(5) Art. 6, paragrafo 2, direttiva n. 2002/58/Ce: *"I dati relativi al traffico che risultano necessari ai fini della fatturazione per l'abbonato e dei pagamenti di interconnessione possono essere sottoposti a trattamento. Tale trattamento è consentito solo sino alla fine del periodo durante il quale può essere legalmente contestata la fattura o preteso il pagamento".*

(6) Art. 6, paragrafo 3, direttiva n. 2002/58/Ce: *"Ai fini della commercializzazione dei servizi di comunicazione elettronica o per la fornitura di servizi a valore aggiunto, il fornitore di un servizio di comunicazione elettronica accessibile al pubblico ha facoltà di sottoporre a trattamento i dati di cui al paragrafo 1 nella misura e per la durata necessaria per siffatti servizi, o per la commercializzazione, sempre che l'abbonato o l'utente a cui i dati si riferiscono abbia dato il proprio consenso. Gli abbonati o utenti hanno la possibilità di ritirare il loro consenso al trattamento dei dati relativi al traffico in qualsiasi momento".*

(7) Art. 6, paragrafo 5, direttiva n. 2002/58/Ce: "*Il trattamento dei dati relativi al traffico ai sensi dei paragrafi da 1 a 4 deve essere limitato alle persone che agiscono sotto l'autorità dei fornitori della rete pubblica di comunicazione elettronica e dei servizi di comunicazione elettronica accessibili al pubblico che si occupano della fatturazione o della gestione del traffico, delle indagini per conto dei clienti, dell'accertamento delle frodi, della commercializzazione dei servizi di comunicazione elettronica o della prestazione di servizi a valore aggiunto. Il trattamento deve essere limitato a quanto è strettamente necessario per lo svolgimento di tali attività".*

(8) Tale articolo integra le previsioni dell'articolo 6 della direttiva 95/46/Ce, che stabilisce: *"Gli Stati membri dispongono che i dati personali devono essere: [...] e) conservati in modo da consentire l'identificazione delle persone interessate per un arco di tempo non superiore a quello necessario al conseguimento delle finalità per le quali sono rilevati o sono successivamente trattati. Gli Stati membri prevedono garanzie adeguate per i dati personali conservati oltre il suddetto arco di tempo per motivi storici, statistici o scientifici".*

(9) *Cfr.* il considerando 23 della direttiva 2006/24/Ce.

(10) Essi sono comunque tenuti al rispetto delle specifiche misure e degli accorgimenti prescritti dal d.l. n. 144/2005, nonché dal decreto ministeriale 16 agosto 2005, in *G.U.* 17 agosto 2005, n. 190. Ciò, con riferimento ai dati registrati per il monitoraggio delle operazioni degli utenti previsto dall'art. 2 del predetto decreto ministeriale.

(11) *Cfr.* anche il considerando 13 e art. 1, comma 2, direttiva 2006/24/Ce, a mente del quale tale direttiva *"non si applica al contenuto delle comunicazioni elettroniche, ivi incluse le informazioni consultate utilizzando una rete di comunicazione elettronica".*

(12) *Cfr.* il considerando n. 23, direttiva 2006/24/Ce, *cit.*

(13) *Cfr.* art. 2, comma 2, lett. c), direttiva 2006/24/Ce *cit.*

36 Sicurezza dei dati di traffico telefonico e telematico (*)
17 gennaio 2008

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Nella riunione odierna, in presenza del prof. Francesco Pizzetti, presidente, del dott. Giuseppe Chiaravalloti, vice presidente, del dott. Mauro Paissan e del dott. Giuseppe Fortunato, componenti, e del dott. Giovanni Buttarelli, segretario generale;

Visto il Codice in materia di protezione dei dati personali (d.lg. 30 giugno 2003, n. 196, di seguito, "Codice");

Visti in particolare gli artt. 17, 123 e 132, comma 5, del Codice;

Vista la deliberazione del 19 settembre 2007 con la quale l'Autorità ha avviato una procedura di consultazione pubblica su un documento, adottato in pari data, riguardante *"Misure e accorgimenti a garanzia degli interessati in tema di conservazione di dati di traffico telefonico e telematico per finalità di accertamento e repressione di reati"* e pubblicato, unitamente alla medesima deliberazione, sul sito *web* dell'Autorità;

Visti i commenti e le osservazioni pervenuti a questa Autorità a seguito della consultazione pubblica per la quale era stato fissato il termine del 31 ottobre 2007;

Considerate le risultanze dei diversi incontri, anche di carattere tecnico, intercorsi con alcune associazioni di categoria che lo avevano richiesto;

Vista la documentazione in atti;

Viste le osservazioni formulate dal segretario generale ai sensi dell'art. 15 del regolamento del Garante n. 1/2000;

Relatore il prof. Francesco Pizzetti;

PREMESSO

1. Considerazioni preliminari

Il trattamento dei dati di traffico telefonico e telematico presenta rischi specifici per i diritti e le libertà fondamentali, nonché per la dignità dell'interessato.

Tali informazioni hanno una natura particolarmente delicata e la loro impropria utilizzazione può avere importanti ripercussioni sulla sfera personale di più soggetti interessati; possono avere un'*"accentuata valenza divulgativa di notizie caratterizzanti la personalità dell'autore"* e la loro conoscibilità richiede adeguate garanzie (*cfr.*, fra l'altro, Corte cost. 11 marzo 1993, n. 81 e 14 novembre 2006 n. 372).

I dati relativi al traffico telefonico e telematico dovrebbero peraltro riguardare solo alcune caratteristiche esteriori di conversazioni, chiamate e comunicazioni, senza permettere di desumerne i contenuti.

Inoltre, le stesse caratteristiche esteriori permettono di individuare analiticamente quando, tra chi e come sono intercorsi contatti telefonici o per via telematica, o sono avvenute determinate attività di accesso all'informazione in rete e persino il luogo dove si trovano i detentori di determinati strumenti.

(*) *G.U.* 5 febbraio 2008, n. 30
[doc. *web* n. 1482111]

L'intensità dei flussi di comunicazione comporta la formazione e, a volte, la conservazione di innumerevoli informazioni che consentono di ricostruire nel tempo intere sfere di relazioni personali, professionali, commerciali e istituzionali, e di formare anche delicati profili interpersonali. Ciò, specie quando i dati sono conservati massivamente dai fornitori per un periodo più lungo di quello necessario per prestare servizi a utenti e abbonati, al fine di adempiere a un distinto obbligo di legge collegato a eccezionali necessità di giustizia.

Per le comunicazioni telematiche, poi, si pongono ulteriori e più specifiche criticità rispetto alle comunicazioni telefoniche tradizionalmente intese, in quanto il dato apparentemente "esterno" a una comunicazione (*ad es.*, una pagina *web* visitata o un indirizzo Ip di destinazione) spesso identifica o rivela nella sostanza anche il suo contenuto: può permettere, quindi, non solo di ricostruire relazioni personali e sociali, ma anche di desumere particolari orientamenti, convincimenti e abitudini degli interessati.

Eventuali abusi (quali quelli emersi nel recente passato, allorché sono stati constatati gravi e diffusi fatti di utilizzazione illecita di dati), possono comportare importanti ripercussioni sulla sfera privata degli individui o anche violare specifici segreti attinenti a determinate attività, relazioni e professioni.

Emerge quindi la necessità, in attuazione di quanto previsto per legge, di assicurare che la conservazione di tali dati da parte dei fornitori, laddove essa sia necessaria per prestare un servizio o in quanto imposta dalla legge, avvenga comunque in termini adeguati per garantire una tutela maggiormente efficace dei diritti e delle libertà delle persone.

Per tali motivi, a prescindere dalle garanzie previste in termini più generali nell'ordinamento anche sul piano costituzionale e processuale, il legislatore all'art. 132 del Codice ha demandato al Garante per la protezione dei dati personali l'individuazione delle misure e degli accorgimenti che i fornitori dei servizi di comunicazione elettronica devono adottare a fronte della conservazione dei dati di traffico telefonico e telematico, allo stato prescritta per finalità di accertamento e repressione dei reati.

Il presente provvedimento è rivolto appunto a individuare le elevate cautele che devono essere osservate dai fornitori nella formazione e nella custodia dei dati del traffico telefonico e telematico.

Prima di indicare quali cautele risultano necessarie a seguito del complesso procedimento di accertamento curato dal Garante, sono opportune alcune altre premesse sull'attuale quadro normativo, sui fornitori e sui dati personali coinvolti.

2. Quadro di riferimento

2.1. *Normativa comunitaria*

La direttiva europea n. 2002/58/Ce, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche, impone agli Stati membri di proteggere la riservatezza delle comunicazioni elettroniche e vieta la conservazione dei dati relativi al traffico generati nel corso delle comunicazioni, a eccezione della conservazione espressamente autorizzata per i fini indicati nella direttiva medesima.

La direttiva riguarda (art. 3) il trattamento dei dati personali connesso alla fornitura di servizi di comunicazione elettronica accessibili al pubblico su reti pubbliche di comunicazione. I dati relativi al traffico sono definiti, in questa sede, quali quelli sottoposti a trattamento "ai fini della trasmissione di una comunicazione su una rete di comunicazione elettronica o della relativa fatturazione" (*cfr.* art. 2 e considerando n. 15 della direttiva 2002/58/Ce).

La medesima direttiva, nell'imporre agli Stati membri l'adozione di disposizioni di legge nazionali che assicurino la riservatezza delle comunicazioni effettuate tramite la rete pubblica di comunicazione e i servizi di comunicazione elettronica accessibili al pubblico, pone l'accento sui dati di traffico generati dai servizi medesimi (art. 5); tali dati, trattati e memo-

rizzati dal fornitore della rete pubblica o del servizio pubblico di comunicazione elettronica, devono essere cancellati o resi anonimi quando non sono più necessari ai fini della trasmissione della comunicazione, fatte salve alcune tassative eccezioni (*cfr.* art. 6, *par.* 2 , 3 e 5 e art. 15, *par.* 1; *v.*, fra gli altri, il Parere n. 1/2003 sulla memorizzazione ai fini di fatturazione dei dati relativi al traffico, adottato il 29 gennaio 2003 dal Gruppo dei garanti europei per la tutela dei dati personali).

L'art. 15, *par.* 1, della direttiva consente che gli Stati membri possano adottare disposizioni legislative volte a limitare i diritti e gli obblighi di cui ai predetti articoli 5 e 6 solo quando tale restrizione costituisca *"una misura necessaria, opportuna e proporzionata all'interno di una società democratica per la salvaguardia della sicurezza nazionale (cioé della sicurezza dello Stato), della difesa, della sicurezza pubblica e la prevenzione, ricerca, accertamento e perseguimento dei reati, ovvero dell'uso non autorizzato del sistema di comunicazione elettronica"*. A tal fine, gli Stati membri possono, tra l'altro, adottare misure legislative le quali prevedano che, per tali motivi, i dati siano conservati per un periodo di tempo limitato.

2.2. *Normativa nazionale*

La direttiva 2002/58/Ce è stata recepita con il Codice in materia di protezione dei dati personali (Titolo X ("Comunicazioni elettroniche"); *cfr.* art. 184). Nel Capo I di tale Titolo, intitolato "Servizi di comunicazione elettronica", è stata introdotta una nuova disciplina sulla conservazione dei dati di traffico telefonico.

Da un lato, l'art. 123 del Codice ha ridotto a sei mesi il previgente limite temporale per la conservazione dei dati di traffico telefonico per finalità di fatturazione, pagamenti in caso di interconnessione e di commercializzazione di servizi, termine che era in precedenza individuabile nella misura massima di cinque anni in base a quanto previsto dal d.lg. n. 171/1998.

Dall'altro, l'art. 132 del medesimo Codice, modificato prima della sua entrata in vigore (d.l. 24 dicembre 2003, n. 354, convertito in legge, con modificazioni, dall'art. 1 legge 26 febbraio 2004, n. 45) ha introdotto un distinto obbligo per i fornitori di servizi di comunicazione elettronica di conservare per finalità di accertamento e repressione dei reati dati di traffico telefonico relativi ai servizi offerti.

Tutto ciò, sullo sfondo del principio cardine in materia secondo cui i dati non devono essere formati se non sono necessari e proporzionati ai fini della funzionalità della rete o della prestazione del servizio (artt. 3 e 11 del Codice).

Dal contesto sopra riassunto emerge che è stata nel complesso vietata una conservazione generalizzata dei dati relativi al traffico (art. 123, comma 1, *cit.*), con le seguenti eccezioni:

- è stato consentito il trattamento di dati strettamente necessario a fini di fatturazione per l'abbonato, ovvero di pagamenti in caso di interconnessione (nei limiti e con le modalità di cui all'art. 123, comma 2) o, previo consenso dell'abbonato o dell'utente, a fini di commercializzazione di servizi di comunicazione elettronica o per la fornitura di servizi a valore aggiunto (art. 123, comma 3);
- è stata però prescritta in termini distinti la conservazione temporanea dei dati di traffico telefonico per esclusive finalità di accertamento e repressione dei reati per due periodi di ventiquattro mesi ciascuno (art. 132 del Codice).

Un successivo provvedimento d'urgenza del 2005 (d.l. 27 luglio 2005, n. 144, convertito in l., con modificazioni, dall'art. 1 della l. 31 luglio 2005, n. 155) ha poi introdotto, tra l'altro:

a) l'obbligo di conservare i dati di traffico telematico, escludendone i contenuti, per due periodi di sei mesi ciascuno;
b) l'obbligo di conservare dati relativi alle chiamate telefoniche senza risposta;
c) con riferimento ai primi ventiquattro mesi di conservazione dei dati del traffico telefonico e ai primi sei mesi di conservazione dei dati del traffico telematico, la previsione che la richiesta giudiziaria volta ad acquisirli, rivolta al fornitore, venga effettuata dal "pubblico ministero anche su istanza del difensore dell'imputato, della persona sottoposta alle indagini, della persona offesa e delle altre parti private e non già dal giudice su istanza del pubblico ministero";

d) un regime transitorio in virtù del quale è stata sospesa temporaneamente l'applicazione di qualunque disposizione che prescriva o consenta la cancellazione dei dati di traffico, anche se non soggetti a fatturazione (termine originariamente stabilito al 31 dicembre 2007, ma successivamente prorogato al 31 dicembre 2008 con l'art. 34 del recente d.l. 31 dicembre 2007, n. 248, in fase di conversione in legge);
e) per i titolari e i gestori di esercizi pubblici o di circoli privati di qualsiasi specie, che si limitino a porre a disposizione del pubblico, dei clienti o dei soci apparecchi terminali utilizzabili per le comunicazioni, anche telematiche, esclusi i telefoni pubblici a pagamento abilitati esclusivamente alla telefonia vocale, alcuni specifici obblighi di identificazione e monitoraggio delle operazioni compiute dai clienti (*cfr.* anche il d.m. 16 agosto 2005, in *G.U.* 17 agosto 2005, n. 190, attuativo di tale previsione).

Il decreto legge del 2005 ha quindi, da un lato, emendato l'art. 132 del Codice (punti *a*), *b*) e *c*) sopra indicati) e, dall'altro, ha introdotto un regime transitorio per la conservazione dei dati, nonché la predetta disciplina speciale applicabile solo a determinati soggetti.

Fermo restando il predetto regime, che prevede temporaneamente la conservazione (lett. d) sopra citata), la vigente normativa di riferimento prescrive ai fornitori di servizi di comunicazione elettronica di conservare comunque, per finalità di accertamento e repressione di reati, i dati relativi al traffico telefonico (inclusi quelli concernenti le chiamate senza risposta) e quelli inerenti al traffico telematico (esclusi i contenuti delle comunicazioni), rispettivamente per ventiquattro e sei mesi (art. 132, comma 1, del Codice).

La stessa normativa prescrive inoltre, ai medesimi fornitori, di conservare tali dati per un periodo ulteriore, rispettivamente di ventiquattro e sei mesi, per l'accertamento e la repressione dei delitti tassativamente individuati dall'art. 407, comma 2, lett. a), c.p.p., nonché dei delitti in danno di sistemi informatici o telematici (art. 132, comma 2).

Infine, prevede che la conservazione dei predetti dati sia effettuata nel rispetto di specifici accorgimenti e misure a garanzia degli interessati. L'individuazione di tali cautele, oggetto del presente provvedimento, è stata appunto demandata al Garante per la protezione dei dati personali (*cfr.* artt. 17 e 132, comma 5, del Codice).

2.3. *Altra disciplina comunitaria: la direttiva 2006/24/Ce*

Al fine di armonizzare le disposizioni degli Stati membri sul tema della conservazione dei dati di traffico per finalità di accertamento e repressione di reati è poi intervenuta la direttiva n. 2006/24/Ce del Parlamento europeo e del Consiglio del 15 marzo 2006, che doveva essere recepita entro il 15 settembre 2007.

Tale direttiva contiene specifiche indicazioni sul risultato convenuto a livello comunitario con riferimento sia ai tempi di conservazione dei dati di traffico (minimo sei mesi e massimo due anni), sia alla corretta e uniforme individuazione delle *"categorie di dati da conservare"* (analiticamente elencate nell'art. 5 della direttiva medesima); ciò, in relazione agli specifici servizi ivi enucleati, ovvero di telefonia di rete fissa e di telefonia mobile, di accesso a Internet, di posta elettronica in Internet e di telefonia via Internet.

In questo quadro risulta necessario tenere conto di tali indicazioni anche nell'ambito del presente provvedimento. Ciò, anche in considerazione del fatto che nell'attuale quadro normativo interno, pur sussistendo una definizione generale di "dati relativi al traffico" (art. 4, comma 2, lett. *h*) del Codice), tali dati non vengono enumerati, né vengono distinti espressamente i dati relativi al traffico "telefonico" da quelli inerenti al traffico "telematico".

Tale distinzione risulta, invece, necessaria in considerazione del fatto che il legislatore italiano, diversamente da quello comunitario, ha individuato due diversi periodi di conservazione in relazione alla natura "telefonica" o "telematica" del dato da conservare.

Ciò comporta l'esigenza di specificare l'ambito soggettivo di applicazione del presente provvedimento rispetto all'obbligo di conservazione dei dati.

3. I fornitori tenuti a conservare i dati di traffico

Il "fornitore" sul quale incombe l'obbligo di conservare i dati di traffico ai sensi del citato art. 132 del Codice è quello che mette a disposizione del pubblico servizi di comunicazione elettronica su reti pubbliche di comunicazione; per *"servizi di comunicazione elettronica"* devono intendersi quelli consistenti, esclusivamente o prevalentemente, *"nella trasmissione di segnali su reti di comunicazioni elettroniche"* (art. 4, comma 2, lett. *d*) e *e*), del Codice).

Ciò, deriva:

a) dalla collocazione del menzionato art. 132 all'interno del titolo X, capo I, del Codice e da quanto disposto dall'art. 121 del medesimo Codice il quale, nell'individuare i *"Servizi interessati"*, chiarisce che le disposizioni del titolo X *"si applicano al trattamento dei dati personali connesso alla fornitura di servizi di comunicazione elettronica accessibili al pubblico su reti pubbliche di comunicazioni"*;

b) da quanto stabilisce il citato decreto legge 27 luglio 2005, n. 144 nella parte in cui, nell'imporre la conservazione dei dati per il predetto regime transitorio, si riferisce ai *"fornitori di una rete pubblica di comunicazioni o di un servizio di comunicazione elettronica accessibile al pubblico"*.

Devono ritenersi quindi tenuti alla conservazione dei dati ai sensi del medesimo art. 132 i soggetti che realizzano esclusivamente, o prevalentemente, una trasmissione di segnali su reti di comunicazioni elettroniche, a prescindere dall'assetto proprietario della rete, e che offrono servizi a utenti finali secondo il principio di non discriminazione (*cfr.* anche direttiva 2002/21/Ce del Parlamento europeo e del Consiglio, che istituisce un quadro normativo comune per le reti e i servizi di comunicazione elettronica (*cd.* direttiva quadro) e d.lg. n. 259/2003 recante il Codice delle comunicazioni elettroniche).

Al contrario non rientrano, ad esempio, nell'ambito applicativo del presente provvedimento:

- i soggetti che offrono direttamente servizi di comunicazione elettronica a gruppi delimitati di persone (come, a titolo esemplificativo, i soggetti pubblici o privati che consentono soltanto a propri dipendenti e collaboratori di effettuare comunicazioni telefoniche o telematiche). Tali servizi, pur rientrando nella definizione generale di *"servizi di comunicazione elettronica"*, non possono essere infatti considerati come *"accessibili al pubblico"*. Qualora la comunicazione sia instradata verso un utente che si trovi al di fuori della *cd. "rete privata"*, i dati di traffico generati da tale comunicazione sono invece oggetto di conservazione (*ad es.*, da parte del fornitore di cui si avvale il destinatario della comunicazione, qualora si tratti di un messaggio di posta elettronica; *cfr.* documento di lavoro *"Tutela della vita privata su Internet - Un approccio integrato dell'EU alla protezione dei dati online"*, adottato dal Gruppo di lavoro per la tutela dei dati personali il 21 novembre 2000);
- i soggetti che, pur offrendo servizi di comunicazione elettronica accessibili al pubblico, non generano o trattano direttamente i relativi dati di traffico;
- i titolari e i gestori di esercizi pubblici o di circoli privati di qualsiasi specie che si limitino a porre a disposizione del pubblico, di clienti o soci apparecchi terminali utilizzabili per le comunicazioni, anche telematiche, ovvero punti di accesso a Internet utilizzando tecnologia senza fili, esclusi i telefoni pubblici a pagamento abilitati esclusivamente alla telefonia vocale;
- i gestori dei siti Internet che diffondono contenuti sulla rete (*cd. "content provider"*). Essi non sono, infatti, fornitori di un *"servizio di comunicazione elettronica"* come definito dall'art. 4, comma 2, lett. e) del Codice. Tale norma, infatti, nel rinviare, per i casi di esclusione, all'art. 2, lett. c) della direttiva 2002/21/Ce *cit.*, esclude essa stessa i *"servizi che forniscono contenuti trasmessi utilizzando reti e servizi di comunicazione elettronica* [...] ". Deve rilevarsi, inoltre, che i dati di traffico relativi alla comunicazione (come, ad esempio, la *cd.* "navigazione *web*" e le pagine visitate di un sito Internet) spesso identificano o rivelano nella sostanza anche il suo contenuto e pertanto l'eventuale conservazione di tali dati si porrebbe, in violazione di quanto disposto dall'art. 132 del Codice (come modificato dal citato d.l. n. 144/2005), laddove esclude dalla conservazione per finalità di giustizia i "contenuti" della comunicazione (*cfr.*, in tal senso, anche

l'art. 1, comma 2, della direttiva 2006/24/Ce, nella parte in cui esclude dal proprio ambito di applicazione la conservazione del "contenuto delle comunicazioni elettroniche, ivi incluse le informazioni consultate utilizzando una rete di comunicazioni elettroniche");
- i gestori di motori di ricerca. I dati di traffico telematico che essi trattano, consentendo di tracciare agevolmente le operazioni compiute dall'utente in rete, sono, comunque, parimenti qualificabili alla stregua di "contenuti".

4. I dati di traffico che devono essere conservati

L'obbligo di conservazione riguarda i dati relativi al traffico telefonico, inclusi quelli concernenti le chiamate senza risposta, nonché i dati inerenti al traffico telematico, esclusi comunque i contenuti delle comunicazioni (art. 132 del Codice). In particolare, sono oggetto di conservazione i dati che i fornitori sottopongono a trattamento per la trasmissione della comunicazione o per la relativa fatturazione (art. 4, comma 2, lett. *h*), del Codice).

Pertanto, i fornitori (come individuati nel precedente paragrafo 3) devono conservare, per esclusive finalità di accertamento e repressione di reati, solo i dati di traffico che risultino nella loro disponibilità in quanto derivanti da attività tecniche strumentali alla resa dei servizi offerti dai medesimi, nonché alla loro fatturazione. Ciò, in ossequio anche ai princìpi di pertinenza e non eccedenza stabiliti dagli artt. 3 e 11 del Codice.

In tal senso, si esprime anche il citato decreto legge 27 luglio 2005, n. 144 che, all'art. 6, riconduce l'obbligo di conservazione alle "informazioni che consentono la tracciabilità degli accessi, nonché, qualora disponibili, dei servizi". La direttiva 2006/24/Ce ribadisce che tale obbligo sussiste soltanto se i dati sono stati "generati o trattati nel processo di fornitura dei [...] servizi di comunicazione" del fornitore (*cfr.* considerando 23 e art. 3, *par.* 1, della direttiva 2006/24/Ce *cit.*).

L'art. 5 di tale direttiva contiene, poi, un'elencazione specifica delle informazioni da conservare e individua diverse categorie di dati di traffico, specificandone i contenuti a seconda che si tratti di traffico telefonico o telematico.

Nell'ambito dei servizi di comunicazione elettronica, occorre infatti distinguere i servizi "telefonici" da quelli "telematici".

Nei primi sono ricompresi:
- le chiamate telefoniche, incluse le chiamate vocali, di messaggeria vocale, in conferenza e di trasmissione dati tramite *telefax*;
- i servizi supplementari, inclusi l'inoltro e il trasferimento di chiamata;
- la messaggeria e i servizi multimediali, inclusi i servizi di messaggeria breve-*sms*.

Nei secondi sono ricompresi:
- l'accesso alla rete Internet;
- la posta elettronica;
- i *fax* (nonché i messaggi *sms* e *mms*) via Internet;
- la telefonia via Internet (*cd. Voice over Internet protocol-VoIp*).

Per quanto concerne specificamente la conservazione dei dati di traffico telefonico relativo alle "chiamate senza risposta", fermo restando allo stato quanto indicato dalla direttiva 2006/24/Ce al considerando 12 (laddove esclude dal proprio ambito di applicazione i "tentativi di chiamata non riusciti"), il fornitore, in forza delle modifiche apportate dal d.l. n. 144/2005 all'art. 132 del Codice, deve conservare solo i dati generati da chiamate telefoniche che sono state collegate con successo, ma non hanno ottenuto risposta oppure in cui vi è stato un intervento del gestore della rete (*cfr.* art. 2, comma 2, lett. f), direttiva 2006/24/Ce).

5. Finalità perseguibili

Il vincolo secondo cui i dati conservati obbligatoriamente per legge possono essere utilizzati

solo per finalità di accertamento e repressione di reati (individuati specificamente per legge in riferimento al predetto, secondo periodo di conservazione) comporta una precisa limitazione per i fornitori nell'eventualità in cui essi ricevano richieste volte a perseguire scopi diversi.

Ad esempio:

a) i medesimi fornitori non possono corrispondere a eventuali richieste riguardanti tali dati formulate nell'ambito di una controversia civile, amministrativa e contabile;
b) sono tenuti a rispettare il menzionato vincolo di finalità anche l'interessato che acceda ai dati che lo riguardano esercitando il diritto di accesso di cui all'art. 7 del Codice (e che può utilizzare quindi i dati acquisiti solo in riferimento alle predette finalità penali), nonché, nel procedimento penale, il difensore dell'imputato, della persona sottoposta alle indagini, della persona offesa e delle altre parti private (art. 132, comma 3, del Codice).

6. Modalità di acquisizione dei dati

Il Codice individua le modalità con le quali possono essere acquisiti i dati di traffico conservati dai fornitori prescrivendo, con riferimento al primo periodo di conservazione (i primi ventiquattro mesi e sei mesi, rispettivamente per il traffico telefonico e telematico), che la richiesta sia formulata con "decreto motivato del pubblico ministero anche su istanza del difensore dell'imputato, della persona sottoposta alle indagini, della persona offesa e delle altri parti private" (art. 132, comma 3, del Codice).

Al difensore dell'imputato o della persona sottoposta alle indagini è riconosciuta la facoltà di richiedere, direttamente, al fornitore i dati di traffico limitatamente ai dati che si riferiscano "alle utenze intestate al proprio assistito". La richiesta deve essere effettuata "con le modalità indicate dall'articolo 391-quater del codice di procedura penale, ferme restando le condizioni di cui all'articolo 8, comma 2, lettera f), per il traffico entrante" (art. 132, comma 3, *cit.*). Tale ultimo riferimento ai presupposti previsti dal Codice per l'accesso alle chiamate in entrata comporta, anche per i fornitori, la necessaria valutazione preliminare della circostanza che dalla mancata conoscenza dei dati richiesti possa derivare un pregiudizio effettivo e concreto per lo svolgimento delle investigazioni difensive di cui alla legge 7 dicembre 2000, n. 397. A tale riguardo si richiama quanto rilevato nel provvedimento adottato dal Garante in materia il 3 novembre 2005, consultabile sul sito dell'Autorità [doc. *web* n. 1189488].

In relazione al secondo periodo di conservazione, l'art. 132, comma 4, prevede che i dati conservati possano essere acquisiti soltanto in presenza di un decreto motivato del giudice che autorizzi l'acquisizione qualora ritenga sussistenti sufficienti indizi di uno o più delitti previsti dall'art. 407, comma 2, lettera a), c.p.p. o in danno di sistemi informatici o telematici.

7. Misure e accorgimenti da prescrivere

Come premesso, il Garante è stato preposto per disposizione di legge a individuare accorgimenti e misure da porre a garanzia degli interessati nell'ambito della conservazione dei dati di traffico telefonico e telematico per finalità di accertamento e repressione di reati (art. 132, comma 5, del Codice).

A tal fine, il Garante ha curato preliminarmente diversi approfondimenti tecnici con esperti del settore, nonché numerosi accertamenti ispettivi presso primari fornitori di servizi di comunicazione elettronica; ha, infine, indetto una specifica consultazione pubblica su un articolato documento indicante le misure e gli accorgimenti ritenuti idonei per la conservazione dei dati di traffico per finalità di giustizia.

Le cautele ipotizzate in sede di consultazione pubblica hanno trovato conforto all'esito della stessa, non essendo pervenuti all'Autorità sostanziali rilievi critici da parte dei soggetti interessati.

Tutte le riflessioni e commenti pervenuti sono stati comunque oggetto di specifica analisi e considerazione nell'elaborazione del presente provvedimento.

Nell'individuare le seguenti cautele che il Garante prescrive ai fornitori interessati al presente provvedimento, l'Autorità ha tenuto conto dei parametri indicati negli artt. 17 e 132, comma 5, del Codice, nonché:

a) dell'esigenza normativa volta a prevedere specifiche cautele rapportate alla quantità e qualità dei dati da proteggere e ai rischi indicati nell'art. 31 del Codice, rischi che i fornitori devono già oggi prevenire rispettando i comuni obblighi di sicurezza collegati alle misure non solo minime previste dal Codice (artt. 31 e ss.; Allegato B);
b) dell'opportunità di individuare, allo stato, misure protettive per i trattamenti svolti da tutti i fornitori interessati che siano verificabili anche in sede ispettiva, ai fini di una più incisiva messa in sicurezza dei dati di traffico telefonico e telematico;
c) della necessità di tenere in considerazione i costi derivanti dall'adozione delle misure e degli accorgimenti prescritti con il presente provvedimento, anche in ragione della variegata capacità tecnica ed economica dei soggetti interessati;
d) del contesto europeo di riferimento, specie alla luce dei pareri resi dal Gruppo per la tutela dei dati personali (*cfr.* pareri nn. 4/2005 sulla proposta di direttiva del Parlamento europeo e del Consiglio riguardante la conservazione di dati trattati nell'ambito della fornitura di servizi pubblici di comunicazione elettronica e che modifica la direttiva 2002/58/Ce; 3/2006 sulla direttiva 2006/24/Ce del Parlamento europeo e del Consiglio riguardante la conservazione di dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione che modifica la direttiva 2002/58/Ce; 8/2006 sulla revisione del quadro normativo per le reti ed i servizi di comunicazione elettronica, con particolare attenzione alla direttiva relativa alla vita privata e alle comunicazioni elettroniche);
e) dello stato dell'evoluzione tecnologica, alla luce del quale le seguenti prescrizioni devono pertanto ritenersi soggette ad aggiornamento periodico.

Di seguito, sono indicati gli accorgimenti e le misure prescritti dal Garante.

Per effetto del presente provvedimento:

7.1. *Sistemi di autenticazione*

Il trattamento dei dati di traffico telefonico e telematico da parte dei fornitori deve essere consentito solo agli incaricati del trattamento e unicamente sulla base del preventivo utilizzo di specifici sistemi di autenticazione informatica basati su tecniche di *strong authentication*, consistenti nell'uso contestuale di almeno due differenti tecnologie di autenticazione, qualunque sia la modalità, locale o remota, con cui si realizzi l'accesso al sistema di elaborazione utilizzato per il trattamento, evitando che questo possa aver luogo senza che l'incaricato abbia comunque superato una fase di autenticazione informatica nei termini anzidetti.

Per i dati di traffico conservati per esclusive finalità di accertamento e repressione dei reati (cioè quelli generati da più di sei mesi, oppure la totalità dei dati trattati per queste finalità se conservati separatamente dai dati trattati per le altre finalità fin dalla loro generazione), una di tali tecnologie deve essere basata sull'elaborazione di caratteristiche biometriche dell'incaricato, in modo tale da assicurare la presenza fisica di quest'ultimo presso la postazione di lavoro utilizzata per il trattamento.

Tali modalità di autenticazione devono essere applicate anche a tutti gli addetti tecnici (amministratori di sistema, di rete, di *database*) che possano accedere ai dati di traffico custoditi nelle banche dati del fornitore.

Limitatamente a tali addetti tecnici, circostanze legate a indifferibili interventi per malfunzionamenti, guasti, installazioni *hardware* e *software*, aggiornamento e riconfigurazione dei sistemi, possono determinare la necessità di accesso informatico a sistemi di elaborazione che trattano dati di traffico in assenza di autenticazione biometrica o di *strong authentication* per operazioni che comportano la presenza fisica dell'addetto che procede all'intervento in prossimità del sistema di elaborazione (per esempio, per lo svolgimento

di operazioni di amministrazione da console locale che implichino la disabilitazione dei servizi di rete e l'impossibilità di gestire operazioni di *input/output* tramite dispositivi accessori come quelli utilizzabili per la *strong authentication*).

In caso di accesso da parte degli addetti tecnici nei termini anzidetti, fermo restando l'obbligo di assicurare le misure minime in tema di credenziali di autenticazione previste dall'Allegato B) al Codice e, per quanto concerne i trattamenti di dati di traffico telefonico per esclusive finalità di giustizia, quanto specificato al successivo paragrafo 7.3, dovrà essere tenuta preventivamente traccia in un apposito "registro degli accessi" dell'evento, nonché delle motivazioni che lo hanno determinato, con una successiva descrizione sintetica delle operazioni svolte, anche mediante l'utilizzo di sistemi elettronici. Tale registro deve essere custodito dal fornitore presso le sedi di elaborazione e messo a disposizione del Garante nel caso di ispezioni o controlli, unitamente a un elenco nominativo dei soggetti abilitati all'accesso ai diversi sistemi di elaborazione con funzioni di amministratore di sistema, che deve essere formato e aggiornato costantemente dal fornitore.

7.2. *Sistemi di autorizzazione*

Relativamente ai sistemi di autorizzazione devono essere adottate specifiche procedure in grado di garantire la separazione rigida delle funzioni tecniche di assegnazione di credenziali di autenticazione e di individuazione dei profili di autorizzazione rispetto a quelle di gestione tecnica dei sistemi e delle basi di dati. Tali differenti funzioni non possono essere attribuite contestualmente a uno stesso soggetto.

I profili di autorizzazione da definire e da attribuire agli incaricati devono differenziare le funzioni di trattamento dei dati di traffico per finalità di ordinaria gestione da quelle per finalità di accertamento e repressione dei reati distinguendo, tra queste ultime, gli incaricati abilitati al solo trattamento dei dati di cui al primo periodo di conservazione obbligatoria (art. 132, comma 1, del Codice), dagli incaricati abilitati anche al trattamento dei dati di cui al secondo periodo di conservazione obbligatoria (art. 132, comma 2, del Codice) e, infine, dalle funzioni di trattamento dei dati in caso di esercizio dei diritti dell'interessato (art. 7 del Codice).

Conseguentemente, un incaricato cui sia attribuito un profilo di autorizzazione abilitante ad esempio al trattamento dei dati di cui al primo periodo di conservazione obbligatoria (art. 132, comma 1, del Codice) non può accedere, per ciò stesso e direttamente, a dati il cui trattamento richieda il possesso del profilo di autorizzazione relativo all'intero periodo di conservazione obbligatoria (art. 132, comma 2, del Codice).

Questa suddivisione non implica la moltiplicazione degli addetti ai servizi per scopi di giustizia; i fornitori hanno infatti la facoltà di utilizzare, per i loro incaricati, il profilo di autorizzazione che abilita al trattamento dei dati relativi al primo periodo o quello che abilita al trattamento dei dati relativi all'intero periodo di conservazione per scopi di giustizia.

7.3. *Conservazione separata*

I dati di traffico conservati per esclusive finalità di accertamento e repressione di reati vanno trattati necessariamente tramite sistemi informatici distinti fisicamente da quelli utilizzati per gestire dati di traffico anche per altre finalità, sia nelle componenti di elaborazione, sia nell'immagazzinamento dei dati *(storage)*.

Più specificamente, i sistemi informatici utilizzati per i trattamenti di dati di traffico conservati per esclusiva finalità di giustizia devono essere differenti da quelli utilizzati anche per altre funzioni aziendali (come fatturazione, *marketing*, antifrode) ed essere, altresì, protetti contro il rischio di intrusione mediante idonei strumenti di protezione perimetrale a salvaguardia delle reti di comunicazione e delle risorse di memorizzazione impiegate nei trattamenti.

I dati di traffico conservati per un periodo non superiore a sei mesi dalla loro generazione possono, invece, essere trattati per le finalità di giustizia sia prevedendone il trattamento con i medesimi sistemi di elaborazione e di immagazzinamento utilizzati per la generalità dei trattamenti, sia provvedendo alla loro duplicazione, con conservazione separata

rispetto ai dati di traffico trattati per le ordinarie finalità, per l'elaborazione con sistemi dedicati a questo specifico trattamento.

Questa prescrizione lascia ai fornitori la facoltà di scegliere, sulla base di propri modelli organizzativi e della propria dotazione tecnologica, l'architettura informatica più idonea per la conservazione obbligatoria dei dati di traffico e per le ordinarie elaborazioni aziendali; permette infatti che i dati di traffico conservati sino a sei mesi dalla loro generazione possano essere trattati, per finalità di giustizia, con sistemi informatici non riservati esclusivamente a tali elaborazioni; oppure, che gli stessi dati vengano duplicati per effettuare un trattamento dedicato esclusivamente al perseguimento delle finalità di giustizia. In quest'ultimo caso le misure e gli accorgimenti prescritti per i dati conservati per esclusive finalità di giustizia si applicano sin dall'inizio del trattamento.

Le attrezzature informatiche utilizzate per i trattamenti di dati di traffico per le esclusive finalità di giustizia di cui sopra devono essere collocate all'interno di aree ad accesso selezionato (ovvero riservato ai soli soggetti legittimati ad accedervi per l'espletamento di specifiche mansioni) e munite di dispositivi elettronici di controllo o di procedure di vigilanza che comportino la registrazione dei dati identificativi delle persone ammesse, con indicazione dei relativi riferimenti temporali.

Nel caso di trattamenti di dati di traffico telefonico per esclusive finalità di giustizia, il controllo degli accessi deve comprendere una procedura di riconoscimento biometrico.

Nell'ambito dei trattamenti per finalità di accertamento e repressione di reati, una volta decorso il termine di cui al comma 1 dell'art. 132 del Codice, i dati di traffico devono essere trattati con modalità che consentano l'accesso differenziato su base temporale, provvedendo a forme di separazione dei dati che garantiscano il rispetto del principio di finalità dei trattamenti e l'efficacia dei profili di autorizzazione definiti.

La differenziazione può essere ottenuta:
- mediante separazione fisica, predisponendo sistemi del tutto separati nelle componenti di elaborazione e di archiviazione, oppure
- mediante separazione logica, ovvero intervenendo sulla struttura delle basi di dati e/o sui sistemi di indicizzazione e/o sui metodi di accesso e/o sui profili di autorizzazione.

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

7.4. *Incaricati del trattamento*

Gli incaricati che accedono ai dati di traffico conservati per le finalità di cui all'art. 132 del Codice, anche per consentire l'esercizio dei diritti di cui all'art. 7 del Codice medesimo, devono essere designati specificamente in rapporto ai dati medesimi.

Il processo di designazione deve prevedere la frequenza di una periodica attività formativa concernente l'illustrazione delle istruzioni, il rispetto delle misure di sicurezza e le relative responsabilità. L'effettiva partecipazione al corso deve essere documentata.

Per quanto riguarda le richieste per l'esercizio dei diritti di cui all'art. 7 del Codice che comportano l'estrazione dei dati di traffico (menzionate anche nell'art. 132, comma 5, lett. *c*)), nei limiti in cui ciò è consentito ai sensi dell'art. 8, comma 2, lettera *f*) del Codice, il titolare del trattamento deve conservare in forma specifica la documentazione comprovante l'idonea verifica dell'identità del richiedente ai sensi dell'art. 9 del Codice stesso, e adottare opportune cautele per comunicare i dati al solo soggetto legittimato in base al medesimo articolo.

7.5. *Cancellazione dei dati*

Allo scadere dei termini previsti dalle disposizioni vigenti, i dati di traffico sono resi non disponibili per le elaborazioni dei sistemi informativi e le relative consultazioni; sono altresì cancellati o resi anonimi senza alcun ritardo, in tempi tecnicamente compatibili con l'eser-

cizio delle relative procedure informatiche, nei *database* e nei sistemi di elaborazione utilizzati per i trattamenti, nonché nei sistemi e nei supporti per la realizzazione di copie di sicurezza *(backup e disaster recovery)* effettuate dal titolare anche in applicazione di misure previste dalla normativa vigente, documentando tali operazioni al più tardi entro trenta giorni successivi alla scadenza dei termini di cui all'art. 132 del Codice.

7.6. *Altre misure*
Audit log
Devono essere adottate soluzioni informatiche idonee ad assicurare il controllo delle attività svolte sui dati di traffico da ciascun incaricato del trattamento, quali che siano la sua qualifica, le sue competenze e gli ambiti di operatività e le finalità del trattamento. Il controllo deve essere efficace e dettagliato anche per i trattamenti condotti sui singoli elementi di informazione presenti sui diversi *database* utilizzati.

Tali soluzioni comprendono la registrazione, in un apposito *audit log*, delle operazioni compiute, direttamente o indirettamente, sui dati di traffico e sugli altri dati personali a essi connessi, sia quando consistono o derivano dall'uso interattivo dei sistemi, sia quando sono svolte tramite l'azione automatica di programmi informatici.

I sistemi di *audit log* devono garantire la completezza, l'immodificabilità e l'autenticità delle registrazioni in essi contenute, con riferimento a tutte le operazioni di trattamento e a tutti gli eventi relativi alla sicurezza informatica sottoposti ad *auditing*. A tali scopi devono essere adottati, per la registrazione dei dati di *auditing*, anche in forma centralizzata per ogni impianto di elaborazione o per *datacenter*, sistemi di memorizzazione su dispositivi non alterabili. Prima della scrittura, i dati o i raggruppamenti di dati devono essere sottoposti a procedure informatiche per attestare la loro integrità, basate sull'utilizzo di tecnologie crittografiche.

Le misure di cui al presente paragrafo sono adottate nel rispetto dei princìpi in materia di controllo dei lavoratori sull'uso di strumenti elettronici, con particolare riguardo all'informativa agli interessati (*cfr. Provv.* 1° marzo 2007 [doc. *web* n. 1387522]).

7.7. *Audit interno–Rapporti periodici*
La gestione dei dati di traffico per finalità di accertamento e repressione di reati deve essere oggetto, con cadenza almeno annuale, di un'attività di controllo interno da parte dei titolari del trattamento, in modo che sia verificata costantemente la rispondenza alle misure organizzative, tecniche e di sicurezza riguardanti i trattamenti dei dati di traffico previste dalle norme vigenti e dal provvedimento del Garante, anche per ciò che riguarda la verifica della particolare selettività degli incaricati legittimati.

L'attività di controllo deve essere demandata a un'unità organizzativa o, comunque, a personale diverso rispetto a quelli cui è affidato il trattamento dei dati per la finalità di accertamento e repressione dei reati.

I controlli devono comprendere anche verifiche a posteriori, a campione o su eventuale allarme derivante da sistemi di *Alerting* e di *Anomaly Detection*, sulla legittimità e liceità degli accessi ai dati effettuati dagli incaricati, sull'integrità dei dati e delle procedure informatiche adoperate per il loro trattamento. Sono svolte, altresì, verifiche periodiche sull'effettiva cancellazione dei dati decorsi i periodi di conservazione.

L'attività di controllo deve essere adeguatamente documentata in modo tale che sia sempre possibile risalire ai sistemi verificati, alle operazioni tecniche su di essi effettuate, alle risultanze delle analisi condotte sugli accessi e alle eventuali criticità riscontrate.

L'esito dell'attività di controllo deve essere:
- comunicato alle persone e agli organi legittimati ad adottare decisioni e a esprimere, a vari livelli in base al proprio ordinamento interno, la volontà della società;
- richiamato nell'ambito del documento programmatico sulla sicurezza nel quale devono essere indicati gli interventi eventualmente necessari per adeguare le misure di sicurezza;
- messo, a richiesta, a disposizione del Garante o dell'autorità giudiziaria.

7.8. *Documentazione dei sistemi informativi*

I sistemi informativi utilizzati per il trattamento dei dati di traffico devono essere documentati in modo idoneo secondo i princìpi dell'ingegneria del *software*, evitando soluzioni documentali non corrispondenti a metodi descrittivi standard o di ampia accettazione.

La descrizione deve comprendere, per ciascun sistema applicativo, l'architettura logico-funzionale, l'architettura complessiva e la struttura dei sistemi utilizzati per il trattamento, i flussi di *input/output* dei dati di traffico da e verso altri sistemi, l'architettura della rete di comunicazione, l'indicazione dei soggetti o classi di soggetti aventi legittimo accesso al sistema.

La documentazione va corredata con diagrammi di dislocazione delle applicazioni e dei sistemi, da cui deve risultare anche l'esatta ubicazione dei sistemi nei quali vengono trattati i dati per le finalità di accertamento e repressione di reati.

La documentazione tecnica deve essere aggiornata e messa a disposizione dell'Autorità su sua eventuale richiesta, unitamente a informazioni di dettaglio sui soggetti aventi legittimo accesso ai sistemi per il trattamento dei dati di traffico.

7.9. *Cifratura e protezione dei dati*

I dati di traffico trattati per esclusive finalità di giustizia vanno protetti con tecniche crittografiche, in particolare contro rischi di acquisizione fortuita o di alterazione accidentale derivanti da operazioni di manutenzione sugli apparati informatici o da ordinarie operazioni di amministrazione di sistema. In particolare, devono essere adottate soluzioni che rendano le informazioni, residenti nelle basi di dati a servizio delle applicazioni informatiche utilizzate per i trattamenti, non intelligibili a chi non disponga di diritti di accesso e profili di autorizzazione idonei, ricorrendo a forme di cifratura od offuscamento di porzioni dei database o degli indici o ad altri accorgimenti tecnici basati su tecnologie crittografiche.

Tale misura deve essere efficace per ridurre al minimo il rischio che incaricati di mansioni tecniche accessorie ai trattamenti (amministratori di sistema, *database administrator* e manutentori *hardware* e *software*) possano accedere indebitamente alle informazioni registrate, anche fortuitamente, acquisendone conoscenza nel corso di operazioni di accesso ai sistemi o di manutenzione di altro genere, oppure che possano intenzionalmente o fortuitamente alterare le informazioni registrate.

Eventuali flussi di trasmissione dei dati di traffico tra sistemi informatici del fornitore devono aver luogo tramite protocolli di comunicazione sicuri, basati su tecniche crittografiche, o comunque evitando il ricorso alla trasmissione in chiaro dei dati. Protocolli di comunicazione sicuri devono essere adottati anche per garantire, più in generale, la sicurezza dei sistemi, evitando di esporli a vulnerabilità e a rischio di intrusione (a titolo esemplificativo, l'accesso interattivo in modalità "emulazione di terminale", anche per scopi tecnici, non deve essere consentito su canali non sicuri, così come deve essere evitata l'attivazione di servizi di rete non necessari che si possono prestare alla realizzazione di forme di intrusione).

7.10. *Tempi di adozione delle misure e degli accorgimenti*

Valutato il complesso delle misure e degli accorgimenti, tenuto conto del quadro delle cautele che emergono dalle risultanze ispettive essere già in atto presso i fornitori, nonché dei tempi tecnici necessari per completarne l'attuazione, anche alla luce di quanto emerso dalla consultazione pubblica, risulta dagli atti congruo fissare un termine transitorio per i trattamenti di dati in essere, prevedendo che tutti gli adempimenti di cui al presente punto 7 siano completati al più presto ed entro, e non oltre, il termine che è parimenti congruo stabilire per tutti i fornitori al 31 ottobre 2008. Entro tale termine, i fornitori dovranno dare conferma al Garante attestando formalmente l'integrale adempimento al presente provvedimento.

8. Applicazione di alcune misure a dati trattati per altre finalità

Le considerazioni svolte sulla natura particolarmente delicata dei dati di traffico, sulla necessità di garantire una tutela maggiormente efficace dei diritti e delle libertà delle persone e di prescrivere una più incisiva messa in sicurezza di dati rilevano anche per ogni altro trattamento di dati di traffico telefonico e telematico effettuato dai fornitori di cui al paragrafo 3.

Ciò, comporta l'improrogabile esigenza di assicurare che almeno alcuni tra gli accorgimenti e le misure di cui al precedente punto 7, limitatamente a quelli adattabili al caso di specie, siano applicati comunque dai predetti fornitori nell'ambito di analoghi trattamenti di dati di traffico telefonico e telematico effettuati per finalità non di giustizia, ma di fatturazione, pagamento in caso di interconnessione e commercializzazione di servizi, nel più breve periodo temporale indicato nel menzionato art. 123.

Per tali ragioni il Garante, contestualmente e distintamente da quanto va disposto ai sensi dell'art. 132, comma 5, del Codice, prescrive ai fornitori di cui al paragrafo 3, ai sensi dell'art. 17 del medesimo Codice, di adottare nel termine e con la modalità di cui al paragrafo 7.10. le misure e gli accorgimenti indicati nella lettera c) del seguente dispositivo.

Copia del presente provvedimento verrà trasmessa al Ministero della giustizia, anche ai fini della sua pubblicazione sulla *Gazzetta Ufficiale* della Repubblica italiana a cura dell'Ufficio pubblicazione leggi e decreti, nonché, per opportuna conoscenza, all'Autorità per le garanzie nelle comunicazioni.

TUTTO CIÒ PREMESSO IL GARANTE

a) ai sensi degli artt. 17, 123 e 132, comma 5, del Codice, prescrive ai fornitori di servizi di comunicazione elettronica individuati nel paragrafo 3 di adottare nel trattamento dei dati di traffico telefonico e telematico di cui al paragrafo 4 le misure e gli accorgimenti a garanzia degli interessati individuate nel presente provvedimento, provvedendo a (*par.* 7):

1. adottare specifici sistemi di autenticazione informatica basati su tecniche di *strong authentication*, consistenti nell'uso contestuale di almeno due differenti tecnologie di autenticazione, che si applichino agli accessi ai sistemi di elaborazione da parte di tutti gli incaricati di trattamento, nonché di tutti gli addetti tecnici (amministratori di sistema, di rete, di *database*) che possano accedere ai dati di traffico custoditi nelle banche dati del fornitore, qualunque sia la modalità, locale o remota, con cui si realizzi l'accesso al sistema di elaborazione utilizzato per il trattamento, evitando che questo possa aver luogo senza che l'incaricato abbia comunque superato una fase di autenticazione informatica nei termini anzidetti. Per i dati di traffico trattati per esclusive finalità di accertamento e repressione dei reati, una di tali tecnologie deve essere basata sull'elaborazione di caratteristiche biometriche dell'incaricato, in modo tale da assicurare la presenza fisica di quest'ultimo presso la postazione di lavoro utilizzata per il trattamento. Tali modalità di autenticazione devono essere applicate anche a tutti gli addetti tecnici (amministratori di sistema, di rete, di *database*) che possano accedere ai dati di traffico custoditi nelle banche dati del fornitore. Relativamente ai soli addetti tecnici indicati al presente punto 1, qualora circostanze legate a indifferibili interventi per malfunzionamenti, guasti, installazioni *hardware* e *software*, aggiornamento e riconfigurazione dei sistemi, determinino la necessità di accesso informatico a sistemi di elaborazione che trattano dati di traffico in assenza di *strong authentication*, fermo restando l'obbligo di assicurare le misure minime in tema di credenziali di autenticazione previste dall'Allegato B) al Codice, deve essere tenuta traccia dell'evento in un apposito "registro degli accessi", nonché delle motivazioni che li hanno determinati, con una successiva descrizione sintetica delle operazioni svolte, anche mediante l'utilizzo di sistemi elettronici. Tale registro deve essere custodito dal fornitore presso le sedi di elaborazione e messo a disposizione del Garante nel caso di ispezioni o controlli, unitamente a un elenco nominativo dei soggetti abilitati all'accesso ai diversi sistemi di elaborazione con funzioni di amministratore di sistema, che deve essere formato e aggiornato costantemente dal fornitore.
2. adottare specifiche procedure in grado di garantire la separazione rigida delle funzioni tecniche di assegnazione di credenziali di autenticazione e di individuazione dei profili di autorizzazione rispetto a quelle di gestione tecnica

dei sistemi e delle basi di dati. Il fornitore deve definire e attribuire agli incaricati specifici profili di autorizzazione differenziando le funzioni di trattamento dei dati di traffico per finalità di ordinaria gestione da quelle per finalità di accertamento e repressione dei reati e distinguendo, tra queste ultime, gli incaricati abilitati al solo trattamento dei dati di cui al primo periodo di conservazione obbligatoria (art. 132, comma 1, del Codice) dagli incaricati abilitati anche al trattamento dei dati di cui al secondo periodo di conservazione obbligatoria (art. 132, comma 2, del Codice) e, infine, dalle funzioni di trattamento dei dati in caso di esercizio dei diritti dell'interessato (art. 7 del Codice);

3. adottare, per la conservazione dei dati di traffico per esclusive finalità di accertamento e repressione di reati, sistemi informatici distinti fisicamente da quelli utilizzati per gestire dati di traffico anche per altre finalità, sia nelle componenti di elaborazione, sia di immagazzinamento dei dati (*storage*). I dati di traffico conservati per un periodo non superiore ai sei mesi dalla loro generazione possono, invece, essere trattati per le finalità di giustizia sia prevedendone il trattamento con i medesimi sistemi di elaborazione e di immagazzinamento utilizzati per la generalità dei trattamenti, sia provvedendo alla loro duplicazione, con conservazione separata rispetto ai dati di traffico trattati per le ordinarie finalità. Le attrezzature informatiche utilizzate per i trattamenti di dati di traffico per le esclusive finalità di giustizia di cui sopra devono essere collocate all'interno di aree ad accesso selezionato (ovvero riservato ai soli soggetti legittimati ad accedervi per l'espletamento di specifiche mansioni) e munite di dispositivi elettronici di controllo o di procedure di vigilanza che comportino la registrazione dei dati identificativi delle persone ammesse, con indicazione dei relativi riferimenti temporali. Nel caso di trattamenti di dati di traffico telefonico per esclusive finalità di giustizia, il controllo degli accessi deve comprendere una procedura di riconoscimento biometrico. Inoltre, nell'ambito dei trattamenti per finalità di accertamento e repressione di reati, una volta decorso il termine di cui al comma 1 dell'art. 132 del Codice, il fornitore deve trattare tali dati con modalità che consentano l'accesso differenziato su base temporale, tramite forme di separazione dei dati che garantiscano il rispetto del principio di finalità dei trattamenti e l'efficacia dei profili di autorizzazione definiti. Tale differenziazione può essere ottenuta mediante separazione fisica, predisponendo sistemi del tutto separati nelle componenti di elaborazione e di archiviazione, oppure mediante separazione logica, ovvero intervenendo sulla struttura delle basi di dati e/o sui sistemi di indicizzazione e/o sui metodi di accesso e/o sui profili di autorizzazione. Infine, il fornitore deve adottare misure idonee a garantire il ripristino dell'accesso ai dati in caso di danneggiamento degli stessi o degli strumenti elettronici in tempi compatibili con i diritti degli interessati e comunque non superiori a sette giorni;
4. designare specificamente gli incaricati che possono accedere ai dati di traffico conservati per le finalità di cui all'art. 132 del Codice, anche per consentire l'esercizio dei diritti di cui all'art. 7 del Codice medesimo. Il processo di designazione deve prevedere la documentata frequenza di una periodica attività formativa concernente l'illustrazione delle istruzioni, il rispetto delle misure di sicurezza e le relative responsabilità. Per quanto riguarda le richieste per l'esercizio dei diritti di cui all'art. 7 del Codice che comportano l'estrazione dei dati di traffico, nei limiti in cui ciò è consentito ai sensi dell'art. 8, comma 2, lettera *f*) del Codice, il fornitore deve conservare in forma specifica la documentazione comprovante l'idonea verifica dell'identità del richiedente ai sensi dell'art. 9 del Codice stesso, e adottare opportune cautele per comunicare i dati al solo soggetto legittimato in base al medesimo articolo;
5. rendere i dati di traffico immediatamente non disponibili per le elaborazioni dei sistemi informativi allo scadere dei termini previsti dalle disposizioni vigenti. Il fornitore deve cancellare o rendere anonimi senza ritardo tali

dati, in tempi tecnicamente compatibili con l'esercizio delle relative procedure informatiche, nei *database* e nei sistemi di elaborazione utilizzati per i trattamenti nonché nei sistemi e nei supporti per la realizzazione di copie di sicurezza *(backup e disaster recovery)* effettuate dal titolare anche in applicazione di misure previste dalla normativa vigente e, al più tardi, documentando tale operazione entro i trenta giorni successivi alla scadenza dei termini di cui all'art. 132 del Codice;

6. adottare soluzioni informatiche idonee ad assicurare il controllo delle attività svolte sui dati di traffico da ciascun incaricato del trattamento, quali che siano la sua qualifica, le sue competenze e gli ambiti di operatività e le finalità del trattamento. Il controllo deve essere efficace e dettagliato anche per i trattamenti condotti sui singoli elementi di informazione presenti sui diversi *database* utilizzati. Tali soluzioni comprendono la registrazione, in un apposito *audit log*, delle operazioni compiute, direttamente o indirettamente, sui dati di traffico e sugli altri dati personali a essi connessi, sia quando consistono o derivano dall'uso interattivo dei sistemi, sia quando sono svolte tramite l'azione automatica di programmi informatici. I sistemi di *audit log* devono garantire la completezza, l'immodificabilità, l'autenticità delle registrazioni in essi contenute, con riferimento a tutte le operazioni di trattamento e a tutti gli eventi relativi alla sicurezza informatica sottoposti ad *auditing*. A tali scopi il fornitore deve adottare, per la registrazione dei dati di *auditing*, anche in forma centralizzata per ogni impianto di elaborazione o per *datacenter*, sistemi di memorizzazione su dispositivi non alterabili. Prima della scrittura, i dati o i raggruppamenti di dati devono essere sottoposti a procedure informatiche per attestare la loro integrità, basate sull'utilizzo di tecnologie crittografiche;
7. svolgere, con cadenza almeno annuale, un'attività di controllo interno per verificare costantemente la rispondenza alle misure organizzative, tecniche e di sicurezza riguardanti i trattamenti dei dati di traffico previste dalle norme vigenti e dal provvedimento del Garante, anche per ciò che riguarda la verifica della particolare selettività degli incaricati legittimati. Tale attività di controllo deve essere demandata a un'unità organizzativa o, comunque, a personale diverso rispetto a quelli cui è affidato il trattamento dei dati per la finalità di accertamento e repressione dei reati. I controlli devono comprendere anche verifiche a posteriori, a campione o su eventuale allarme derivante da sistemi di *Alerting* e di *Anomaly Detection*, sulla legittimità e liceità degli accessi ai dati effettuati dagli incaricati, sull'integrità dei dati e delle procedure informatiche adoperate per il loro trattamento. Sono svolte, altresì, verifiche periodiche sull'effettiva cancellazione dei dati decorsi i periodi di conservazione. L'attività di controllo deve essere adeguatamente documentata in modo tale che sia sempre possibile risalire ai sistemi verificati, alle operazioni tecniche su di essi effettuate, alle risultanze delle analisi condotte sugli accessi e alle eventuali criticità riscontrate. L'esito dell'attività di controllo deve essere: comunicato alle persone e agli organi legittimati ad adottare decisioni e ad esprimere, a vari livelli in base al proprio ordinamento interno, la volontà della società; richiamato nell'ambito del documento programmatico sulla sicurezza nel quale devono essere indicati gli interventi eventualmente necessari per adeguare le misure di sicurezza; messo, a richiesta, a disposizione del Garante o dell'autorità giudiziaria;
8. documentare i sistemi informativi utilizzati per il trattamento dei dati di traffico in modo idoneo secondo i princìpi dell'ingegneria del *software*, evitando soluzioni documentali non corrispondenti a metodi descrittivi *standard* o di ampia accettazione. La descrizione deve comprendere, per ciascun sistema applicativo, l'architettura logico-funzionale, l'architettura complessiva e la struttura dei sistemi utilizzati per il trattamento, i flussi di *input/output* dei dati di traffico da e verso altri sistemi, l'architettura della rete di comunicazione, l'indicazione dei soggetti o classi di soggetti aventi legittimo accesso al sistema. La documentazione va corre-

data con diagrammi di dislocazione delle applicazioni e dei sistemi, da cui deve risultare anche l'esatta ubicazione dei sistemi nei quali vengono trattati i dati per le finalità di accertamento e repressione di reati. La documentazione tecnica deve essere aggiornata e messa a disposizione dell'Autorità su sua eventuale richiesta, unitamente a informazioni di dettaglio sui soggetti aventi legittimo accesso ai sistemi per il trattamento dei dati di traffico;

9. proteggere i dati di traffico trattati per esclusive finalità di giustizia con tecniche crittografiche, in particolare contro rischi di acquisizione fortuita o di alterazione accidentale derivanti da operazioni di manutenzione sugli apparati informatici o da ordinarie operazioni di amministrazione di sistema. Il fornitore deve adottare soluzioni che rendano le informazioni residenti nelle basi di dati a servizio delle applicazioni informatiche utilizzate per i trattamenti, non intelligibili a chi non disponga di diritti di accesso e profili di autorizzazione idonei, ricorrendo a forme di cifratura od offuscamento di porzioni dei *database* o degli indici o ad altri accorgimenti tecnici basati su tecnologie crittografiche. Tale misura deve essere efficace per ridurre al minimo il rischio che incaricati di mansioni tecniche accessorie ai trattamenti (amministratori di sistema, *database administrator* e manutentori *hardware* e *software*) possano accedere indebitamente alle informazioni registrate, anche fortuitamente, acquisendone conoscenza nel corso di operazioni di accesso ai sistemi o di manutenzione di altro genere, oppure che possano intenzionalmente o fortuitamente alterare le informazioni registrate. Eventuali flussi di trasmissione dei dati di traffico tra sistemi informatici del fornitore devono aver luogo tramite protocolli di comunicazione sicuri, basati su tecniche crittografiche, o comunque evitando il ricorso alla trasmissione in chiaro dei dati. Protocolli di comunicazione sicuri devono essere adottati anche per garantire più in generale la sicurezza dei sistemi evitando di esporli a vulnerabilità e a rischio di intrusione;

b) ai sensi dei medesimi artt. 17, 123 e 132, comma 5 del Codice, nonché dell'art. 157 del Codice, prescrive ai predetti fornitori titolari del trattamento di effettuare tutti gli adempimenti di cui alla precedente lett. a) al più presto e, comunque, entro e non oltre il termine del 31 ottobre 2008, dandone conferma al Garante attestando entro lo stesso termine l'integrale adempimento;

c) ai sensi dell'art. 17 del Codice prescrive ai medesimi fornitori titolari del trattamento di adottare, rispetto ai dati di traffico trattati per le finalità di cui all'art. 123 del Codice, entro e non oltre il termine del 31 ottobre 2008, dandone ai sensi dell'art. 157 del Codice conferma al Garante e attestando entro lo stesso termine l'integrale adempimento, i seguenti accorgimenti e misure (*par.* 8):

1. adottare specifici sistemi di autenticazione informatica basati su tecniche di *strong authentication*, consistenti nell'uso contestuale di almeno due differenti tecnologie di autenticazione, che si applichino agli accessi ai sistemi di elaborazione da parte di tutti gli incaricati di trattamento nonché di tutti gli addetti tecnici (amministratori di sistema, di rete, di *database*) che abbiano la possibilità concreta di accedere ai dati di traffico custoditi nelle banche dati del fornitore, qualunque sia la modalità, locale o remota, con cui si realizzi l'accesso al sistema di elaborazione utilizzato per il trattamento, evitando che questo possa aver luogo senza che l'incaricato abbia comunque superato una fase di autenticazione informatica nei termini anzidetti. Qualora circostanze eccezionali, legate a indifferibili interventi per malfunzionamenti, guasti, installazione *hardware* e *software*, aggiornamento e riconfigurazione dei sistemi, determinino la necessità di accesso a sistemi di elaborazione che trattano dati di traffico da parte di addetti tecnici in assenza di *strong authentication*, fermo restando l'obbligo di assicurare le misure minime in tema di credenziali di autenticazione previste dall'Allegato B) al Codice in materia di protezione dei dati personali, deve essere tenuta traccia in un apposito "registro degli accessi" dell'eventuale accesso fisico ai locali in cui sono

installati i sistemi di elaborazione oggetto di intervento e dell'accesso logico ai sistemi, nonché delle motivazioni che li hanno determinati, con una descrizione sintetica delle operazioni svolte, anche mediante l'utilizzo di sistemi elettronici. Tale registro deve essere custodito dal fornitore presso le sedi di elaborazione e messo a disposizione del Garante nel caso di ispezioni o controlli, unitamente a un elenco nominativo dei soggetti abilitati all'accesso ai diversi sistemi di elaborazione con funzioni di amministratore di sistema, che deve essere formato e aggiornato costantemente dal fornitore;

2. adottare procedure in grado di garantire la separazione rigida delle funzioni tecniche di assegnazione di credenziali di autenticazione e di individuazione dei profili di autorizzazione rispetto a quelle di gestione tecnica dei sistemi e delle basi di dati;
3. rendere i dati di traffico immediatamente non disponibili per le elaborazioni dei sistemi informativi allo scadere dei termini previsti dalle disposizioni vigenti, provvedendo alla loro cancellazione o trasformazione in forma anonima, in tempi tecnicamente compatibili con l'esercizio delle relative procedure informatiche, nei *database* e nei sistemi di elaborazione utilizzati per i trattamenti nonché nei sistemi e nei supporti per la realizzazione di copie di sicurezza (*backup* e *disaster recovery*) effettuate dal titolare anche in applicazione di misure previste dalla normativa vigente e, al più tardi, documentando tale operazione entro i trenta giorni successivi alla scadenza dei termini di conservazione (art. 123 del Codice);
4. adottare soluzioni informatiche idonee ad assicurare il controllo delle attività svolte sui dati di traffico da ciascun incaricato del trattamento, quali che siano la sua qualifica, le sue competenze e gli ambiti di operatività e le finalità del trattamento. Il controllo deve essere efficace e dettagliato anche per i trattamenti condotti sui singoli elementi di informazione presenti sui diversi *database* utilizzati. Tali soluzioni comprendono la registrazione, in un apposito *audit log*, delle operazioni compiute, direttamente o indirettamente, sui dati di traffico e sugli altri dati personali a essi connessi, sia quando consistono o derivano dall'uso interattivo dei sistemi, sia quando sono svolte tramite l'azione automatica di programmi informatici. I sistemi di *audit log* devono garantire la completezza, l'immodificabilità, l'autenticità delle registrazioni in essi contenute, con riferimento a tutte le operazioni di trattamento e a tutti gli eventi relativi alla sicurezza informatica sottoposti ad *auditing*. A tali scopi il fornitore deve adottare, per la registrazione dei dati di *auditing*, anche in forma centralizzata per ogni impianto di elaborazione o per *datacenter*, sistemi di memorizzazione su dispositivi non alterabili. Prima della scrittura, i dati o i raggruppamenti di dati devono essere sottoposti a procedure informatiche per attestare la loro integrità, basate sull'utilizzo di tecnologie crittografiche;
5. documentare i sistemi informativi utilizzati per il trattamento dei dati di traffico in modo idoneo secondo i princìpi dell'ingegneria del *software*, evitando soluzioni documentali non corrispondenti a metodi descrittivi *standard* o di ampia accettazione. La descrizione deve comprendere, per ciascun sistema applicativo, l'architettura logico-funzionale, l'architettura complessiva e la struttura dei sistemi utilizzati per il trattamento, i flussi di *input/output* dei dati di traffico da e verso altri sistemi, l'architettura della rete di comunicazione, l'indicazione dei soggetti o classi di soggetti aventi legittimo accesso al sistema. La documentazione va corredata con diagrammi di dislocazione delle applicazioni e dei sistemi, da cui deve risultare anche l'esatta ubicazione dei sistemi nei quali vengono trattati i dati per le finalità di accertamento e repressione di reati. La documentazione tecnica deve essere aggiornata e messa a disposizione dell'Autorità su sua eventuale richiesta, unitamente a informazioni di dettaglio sui soggetti aventi legittimo accesso ai sistemi per il trattamento dei dati di traffico;

d) dispone che copia del presente provvedimento sia trasmessa al Ministero della giustizia anche ai fini della sua pubblicazione sulla *Gazzetta Ufficiale* della Repubblica italiana a cura dell'Ufficio pubblicazione leggi e decreti, nonché, per opportuna conoscenza, all'Autorità per le garanzie nelle comunicazioni.

Roma, 17 gennaio 2008

IL PRESIDENTE
Pizzetti

IL RELATORE
Pizzetti

IL SEGRETARIO GENERALE
Buttarelli

37 Adempimenti semplificati per il *customer care* (*) 15 novembre 2007

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Nella riunione odierna, in presenza del prof. Francesco Pizzetti, presidente, del dott. Giuseppe Chiaravalloti, vice presidente, del dott. Mauro Paissan e del dott. Giuseppe Fortunato, componenti, e del dott. Giovanni Buttarelli, segretario generale;

Visto il Codice in materia di protezione dei dati personali (d.lg. 30 giugno 2003, n. 196), con particolare riguardo agli artt. 2 e 13;

Viste le osservazioni formulate dal segretario generale ai sensi dell'art. 15 del regolamento del Garante n. 1/2000;

Relatore il prof. Francesco Pizzetti;

PREMESSO

1. Misure di semplificazione e trattamento di dati nell'ambito di servizi telefonici di assistenza e informazione al pubblico

1.1. La disciplina di protezione dei dati personali prevede che il trattamento dei dati deve assicurare un livello elevato di tutela dei diritti e delle libertà fondamentali *"nel rispetto dei princìpi di semplificazione, armonizzazione ed efficacia"* (art. 1, comma 2, del Codice).

Specifiche disposizioni attuano tali princìpi semplificando il contenuto e le modalità per informare gli interessati rispetto al trattamento, in particolare per quanto riguarda i servizi telefonici di assistenza e di informazione al pubblico (art. 13, commi 2 e 3, del Codice).

Il Garante intende sviluppare ulteriormente tali disposizioni attraverso il presente provvedimento che tiene conto del principio secondo cui l'informativa, quando i dati sono raccolti presso gli interessati, *"può non comprendere gli elementi già noti alla persona che fornisce i dati"* (art. 13, comma 2).

1.2. Numerosi soggetti pubblici e privati utilizzano in modo crescente servizi telefonici di assistenza e di informazione al pubblico nello svolgimento della propria attività istituzionale, professionale, commerciale o di natura personale.

Alcune scelte organizzative valorizzano il mezzo telefonico quale canale di contatto privilegiato con l'utenza, specie nell'ambito di società di grandi dimensioni e di enti pubblici, il che può accrescere l'economicità e l'efficienza nei servizi resi (*cfr.* in merito art. 3 dir. min. 21 dicembre 2001, Linee-guida in materia di digitalizzazione dell'amministrazione, in *G.U.* 5 febbraio 2002, n. 30; dir. min. 4 gennaio 2005, Linee-guida in materia di digitalizzazione dell'amministrazione, in *G.U.* 12 febbraio 2005, n. 35).

La gestione del flusso delle chiamate, attraverso appositi servizi di assistenza telefonica, può assumere in talune circostanze una particolare complessità, strutturandosi su un insieme integrato di sistemi informativi e di risorse umane.

A seconda delle caratteristiche dei servizi e dei relativi destinatari è possibile individuare una vasta gamma di funzioni. Tra le più ricorrenti, possono evidenziarsi quelle di informazione e/o di assistenza alla clientela (*cd. "customer care"*), con riferimento all'instaurazione e

(*) *G.U.* 7 dicembre 2007, n. 285
[doc. *web* n. 1462788]

all'esecuzione di rapporti contrattuali in vari contesti (prenotazione di servizi, *phone-banking*, ecc.), quelle svolte a vantaggio della collettività da parte di amministrazioni pubbliche (si pensi alle chiamate di pubblica utilità, incluse le chiamate ai numeri di emergenza) o soggetti privati anche per quanto riguarda servizi a sovrapprezzo di tipo sociale-informativo, di assistenza, di consulenza tecnico-professionale e di intrattenimento.

1.3. Il presente provvedimento riguarda solo le attività che comportano un trattamento di dati personali prestate in modalità *inbound*, ossia oggetto di una chiamata dell'interessato anche se effettuate senza la mediazione di un operatore (attraverso canali di comunicazione interamente automatizzati).

Non formano invece oggetto di esame i servizi *cd.* outbound, di solito ricorrenti nello svolgimento di attività di *tele-marketing*, nell'ambito delle quali vengono contattati destinatari di comunicazioni commerciali anche attraverso *call center*: al riguardo, vige infatti un apposito quadro normativo (*cfr.* art. 58 del Codice del consumo di cui al d.lg. 6 settembre 2005, n. 206; art. 130 del Codice in materia di protezione dei dati personali; in merito, *v.* pure i *Provv.* 30 maggio 2007 [doc. *web* n. 1412626, doc. *web* n. 1412610, doc. *web* n. 1412598, doc. *web* n. 1412557, doc. *web* n. 1412586].

1.4. Il Garante, tenendo anche conto delle indicazioni e delle richieste di chiarimento formulate (con specifico riguardo ai rapporti con i committenti) da un'associazione di categoria rappresentativa delle società di *call center* operanti in *outsourcing*, intende altresì precisare alcune modalità di comportamento da osservare nella gestione dei servizi telefonici di assistenza e informazione al pubblico (*v. infra* punti 2, 3, 4 e 5).

2. Tipologie di dati e modalità del loro trattamento

Nello svolgimento delle attività qui considerate possono essere utilizzate legittimamente solo le informazioni personali pertinenti e non eccedenti in relazione ai servizi richiesti, informazioni che sono di regola comunicate direttamente dall'interessato.

Le tipologie di informazioni trattate sono piuttosto varie comprendendo dati sia comuni (ad esempio, anagrafici o di natura economica), sia sensibili (si pensi, esemplificativamente, alle informazioni raccolte nell'ambito di servizi prestati da strutture sanitarie). Alcune informazioni personali sono trattate mediante sistemi automatizzati (ad esempio, con l'ausilio di risponditori vocali automatici o grazie a sistemi informatici integrati idonei a fornire informazioni sulla linea chiamante, attraverso il dispositivo di individuazione della medesima).

La raccolta anche automatizzata di tali informazioni da parte dell'operatore che gestisce il servizio di assistenza telefonica al pubblico può avvenire senza che gli interessati ne siano specificamente consapevoli, come ad esempio nel caso di registrazione automatica dei numeri chiamanti da terminali che lo consentono e che permettono, quindi, di risalire all'identità dei relativi utilizzatori.

In relazione a questo contesto il Garante, prima di provvedere in merito all'informativa agli interessati, intende richiamare l'attenzione degli operatori del settore su alcuni profili connessi a tale problematica, utili per assicurare una piena conformità del trattamento alle disposizioni vigenti in materia di protezione dei dati personali dei trattamenti effettuati nell'ambito dei servizi telefonici di assistenza e informazione al pubblico.

3. Titolare e responsabile del trattamento

3.1. Il soggetto pubblico e privato "titolare del trattamento" può svolgere le attività volte a fornire servizi di assistenza e di informazione al pubblico per via telefonica, tramite personale operante sotto la sua diretta autorità in qualità di "incaricato del trattamento" (art. 30 del Codice) o terzi cui è affidato il servizio all'esterno sulla base di contratti di collaborazione (*cd. outsourcing*) che disciplinano le modalità per prestare questa attività strumentale.

Questa seconda soluzione è volta ad assecondare legittime esigenze organizzative. Mentre in altre discipline settoriali possono essere previste specifiche cautele (si pensi, esemplificativamente, a quelle contenute nel Comunicato della Banca d'Italia, in *G.U.* 21 agosto 2002, n. 195, Esternalizzazione di attività di sportello e, sulla medesima materia, nella Comunicazione della Commissione nazionale per la società e la borsa n. Din/2073042 del 7 novembre 2002) la disciplina di protezione dei dati personali ammette e non ostacola tale esternalizzazione. L'outsourcer va però designato quale "responsabile del trattamento" preposto ad attuare in concreto le decisioni del "titolare del trattamento" sulle finalità e modalità del trattamento, sugli strumenti utilizzati e sulla sicurezza (artt. 4, 28 e 29 del Codice; *v.* pure *Provv.* 16 febbraio 2006, punto 6, [doc. *web* n. 1242592]).

3.2. Al fine di garantire una rigorosa osservanza dei princìpi di protezione dei dati personali (e apprestare una tutela più intensa a favore degli interessati), il Codice richiede che chi operi in tale veste debba essere particolarmente qualificato –dovendo essere *"individuato tra soggetti che per esperienza, capacità ed affidabilità forniscano idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza"* (art. 29, comma 2, del Codice)– e, nell'ambito dei compiti che gli sono assegnati, debba conformare il proprio operato alle istruzioni del *"titolare del trattamento"* (art. 29, commi 4 e 5, del Codice).

Il titolare del trattamento è chiamato a svolgere un'analisi anche preventiva al trattamento delle implicazioni che le modalità operative prescelte possono comportare in ordine ai diritti degli interessati, e a porre particolare cura nella valutazione delle capacità professionali, nonché dell'adeguatezza organizzativa del responsabile del trattamento, tenuto conto della natura dei dati trattati. Questa valutazione d'insieme deve riguardare anche l'adeguatezza delle soluzioni tecnico-organizzative e di quelle concernenti la sicurezza dei dati e dei sistemi.

In questo quadro assume una particolare criticità la situazione nella quale un medesimo outsourcer si trovi a gestire contemporaneamente, specie se in un contesto logistico di promiscuità, una pluralità di servizi di assistenza telefonica al pubblico per distinti committenti titolari del trattamento. Tale concorrenza di attività non deve tradursi, in concreto, in un abbassamento o in una banalizzazione dei livelli di sicurezza, né, tantomeno, in una sostanziale commistione tra i differenti insiemi di dati da utilizzare per prestare distinti servizi per più titolari.

Occorre poi assicurare le condizioni per uno svolgimento corretto e trasparente delle relazioni con l'utenza, la quale deve poter individuare in maniera univoca il titolare del trattamento con il quale viene in contatto tramite il servizio di assistenza telefonica al pubblico.

Acquista quindi rilievo l'opportunità di un'approfondita verifica che le parti e, in particolare, il "titolare del trattamento", dovrebbero effettuare in sede di stipula e di attuazione del contratto di fornitura del servizio.

Il titolare del trattamento deve esercitare in concreto reali funzioni di controllo della corretta attuazione delle decisioni che è chiamato ad assumere, anche per ciò che riguarda le modalità di consultazione ed eventuale riproduzione degli archivi del titolare posti a disposizione dell'*outsourcer* e in relazione alla cessazione del loro utilizzo all'atto dell'estinzione del rapporto contrattuale.

4. Finalità, necessità, pertinenza e non eccedenza dei dati trattati

4.1. Nel rendere il servizio di assistenza e di informazione al pubblico non devono essere utilizzati dati personali di abbonati e di utenti che non siano necessari per prestare il servizio, come può avvenire in caso di servizi di natura meramente informativa. Efficaci analisi e monitoraggi della funzionalità e dell'effettiva prestazione del servizio possono essere a volte compiuti a volte disponendo solo di dati statistici anonimi (art. 3 del Codice).

Il trattamento di dati personali che sia realmente necessario per il servizio (anche quando si tratta di dati non direttamente identificativi, ma agevolmente riconducibili a un soggetto identificabile come nel caso degli identificativi delle linee chiamanti) deve comunque avvenire nel rispetto dei princìpi di pertinenza e non eccedenza (artt. 3 e 11 del Codice).

4.2. Occorre assicurare un quadro di correttezza nei riguardi dell'utenza. In particolare, le informazioni raccolte devono essere utilizzate solo per scopi determinati, espliciti e legittimi. I soggetti privati devono di regola raccogliere il consenso informato qualora intendano utilizzare i dati per finalità diverse e compatibili, come nel caso del *marketing* o della creazione di profili relativi all'utenza (artt. 23 e 24 del Codice), mentre i soggetti pubblici devono operare pur sempre per dichiarate finalità istituzionali, nell'osservanza delle pertinenti disposizioni del Codice (*cfr.* artt. 18 ss. del Codice).

Eventuali registrazioni legittime del contenuto delle comunicazioni, effettuate con l'operatore o per il tramite di dispositivi automatici, possono essere conservate solo per un periodo di tempo necessario al corretto assolvimento delle operazioni richieste dagli utenti o alle eventuali esigenze di fatturazione, nei casi di servizi a pagamento, salva l'osservanza di specifici obblighi di legge che ne legittimino l'ulteriore conservazione.

5. Informativa agli interessati e modalità semplificate (art. 13, commi 2 e 3, del Codice)

5.1. I servizi di assistenza telefonica al pubblico sono prestati, non di rado, senza trattare specificamente dati di carattere personale.

In secondo luogo, nei casi in cui, sulla base del principio di necessità, occorre utilizzare alcune informazioni di carattere personale, è di regola possibile fornire alla clientela un'idonea informativa *una tantum* sulle finalità e sulle caratteristiche essenziali del trattamento, già in occasione dell'instaurazione del rapporto contrattuale che spesso precede i contatti telefonici con il servizio (si pensi, ad esempio, ai servizi di assistenza tecnica *post*-vendita).

In tutti questi casi, non è quindi necessario fornire un'informativa in occasione del contatto telefonico con il servizio.

5.2. Tuttavia, può verificarsi il caso in cui il servizio non è preceduto da un contratto o da contatti in occasione dei quali vi sia stata già la possibilità di informare adeguatamente l'interessato.

Anche per questi casi, non è però necessario informare l'interessato rispetto agli elementi che gli siano già noti in base alle circostanze del caso.

A questo riguardo, se si pone attenzione alle specifiche caratteristiche dei servizi di assistenza e di informazione al pubblico, si può infatti constatare agevolmente che diversi elementi che dovrebbero far parte dell'informativa (art. 13 del Codice) sono già chiaramente evidenti, in particolare per quanto riguarda:

a) gli estremi identificativi del titolare del trattamento (art. 13, comma 1, lett. *f*));
b) le varie circostanze che emergono comunque, sotto altro profilo, nel corso della conversazione telefonica (ad esempio, le conseguenze di un eventuale rifiuto di rispondere e la natura obbligatoria o facoltativa del conferimento: art. 13, comma 1, lett. *b*) e *c*));
c) la finalità del servizio e l'ambito di utilizzazione dei dati (art. 13, comma 1, lett. *a*) e *d*)), in particolare quando non si perseguono altri scopi quali quelli di *marketing* o di profilazione per i quali dovrebbe essere peraltro acquisito il consenso.

5.3. Per ogni altro caso in cui risulti comunque opportuno o necessario indicare alcuni elementi dell'informativa in occasione di un contatto telefonico, deve tenersi conto della peculiarità di questo mezzo di comunicazione e della natura dei servizi resi i quali devono poter essere svolti con celerità e senza costi aggiuntivi.

Il principio di semplificazione richiamato nell'art. 2 del Codice esige che ogni eventuale altro elemento da indicare all'interessato e che non gli sia stato eventualmente già spiegato gli venga comunque rappresentato con formule sintetiche, chiare e di immediata comprensione, anche mediante brevi messaggi preregistrati nel corso di eventuali tempi di attesa del servizio.

Come premesso, il Garante intende sviluppare ulteriormente tali modalità semplificate autorizzando coloro che prestano i servizi in esame a indicare la modalità attraverso la quale l'interessato potrà consultare o ascoltare a richiesta un'informativa più specifica, ad esempio mediante un sito *web* o tramite operatore o messaggio registrato ascoltabile digitando una cifra sulla tastiera del telefono (art. 13, comma 3, del Codice).

I fornitori del servizio titolari del trattamento sono già autorizzati ad avvalersi di tutte le predette opportunità senza rivolgere al Garante alcuna richiesta, da formulare eventualmente solo per specifiche situazioni ritenute meritevoli di apposito esame.

5.4. Va infine disposto che i servizi abilitati in base alla legge a ricevere chiamate d'emergenza (d.m. Min. comunicazioni 27 aprile 2006 sul servizio "112" quale numero unico europeo d'emergenza; *v.* anche *Parere* del Garante 6 aprile 2006, [doc. *web* n. 1269346]), attesa la loro peculiare natura, possano rendere l'informativa agli interessati (se dovuta in base al Codice: *cfr.* art. 53) inserendola nei siti *web* di riferimento.

TUTTO CIÒ PREMESSO IL GARANTE

1. individua le seguenti linee-guida per i titolari del trattamento che prestano servizi di assistenza e di informazione al pubblico, in particolare ove si avvalgano di soggetti esterni designati "responsabili del trattamento" (punti 2, 3, 4 e 5):

   a. la raccolta delle informazioni personali deve limitarsi a quelle pertinenti e non eccedenti in relazione ai servizi richiesti;
   b. deve essere effettuata una previa analisi delle implicazioni che il trattamento di dati personali mediante servizi di assistenza telefonica al pubblico potranno comportare, anche tenuto conto della natura dei dati trattati;
   c. il contratto di fornitura del servizio di assistenza telefonica al pubblico deve contenere concrete modalità operative idonee ad assicurare condizioni di trasparente e corretto svolgimento delle relazioni con l'utenza, indicando altresì le misure di sicurezza idonee che dovranno essere adottate, anche al fine di prevenire commistioni tra distinti archivi gestiti dal medesimo responsabile del trattamento;
   d. deve essere posta particolare cura, ai sensi dell'art. 29 del Codice, nella valutazione delle capacità professionali e dell'adeguatezza organizzativa della struttura deputata a svolgere la funzione di servizi di assistenza telefonica al pubblico;
   e. le informazioni raccolte devono essere utilizzate solo per scopi determinati, espliciti e legittimi;
   f. eventuali registrazioni legittime del contenuto delle comunicazioni possono essere conservate solo per un periodo di tempo necessario al corretto assolvimento delle operazioni richieste dagli utenti o alle eventuali esigenze di fatturazione;
   g. non è necessario fornire l'informativa quando non sono trattati dati personali o in relazione ai diversi elementi già noti all'interessato; nei soli casi in cui è invece necessario rappresentare alcuni elementi, vanno comunque utilizzate formule sintetiche, chiare e di immediata comprensione;

2. autorizza i titolari del trattamento che prestano servizi di assistenza e di informazione al pubblico anche con la collaborazione di terzi designati responsabili del trattamento, ai sensi dell'art. 13, comma 3, del Codice, a rappresentare in modo semplificato ad abbonati e utenti interessati gli eventuali elementi dell'informativa che risulti necessario fornire, indicando la modalità attraverso la quale l'interessato potrà consultare o ascoltare a richiesta un'informativa più specifica, ad esempio mediante un sito *web* o tramite operatore o messaggio ascoltabile digitando una cifra sulla tastiera del telefono (punto 5.3.);

3. autorizza i servizi abilitati in base alla legge a ricevere chiamate d'emergenza, ai sensi dell'art. 13, comma 3, del Codice, a rendere l'informativa semplificata inserendola in un sito Internet (punto 5.4.);

4. dispone che copia del presente provvedimento sia trasmessa al Ministero della giustizia-Ufficio pubblicazione leggi e decreti, per la sua pubblicazione sulla *Gazzetta Ufficiale* della Repubblica italiana ai sensi dell'art. 143, comma 2, del Codice.

Roma, 15 novembre 2007

IL PRESIDENTE
Pizzetti

IL RELATORE
Pizzetti

IL SEGRETARIO GENERALE
Buttarelli

38 Bollette telefoniche: indicazione delle ultime tre cifre (*)

13 marzo 2008

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Nella riunione odierna, in presenza del prof. Francesco Pizzetti, presidente, del dott. Giuseppe Chiaravalloti, vice presidente, del dott. Mauro Paissan e del dott. Giuseppe Fortunato, componenti, e del dott. Giovanni Buttarelli, segretario generale;

Visto il Codice in materia di protezione dei dati personali (d.lg. 30 giugno 2003, n. 196, di seguito "Codice");

Visto il provvedimento adottato dal Garante il 5 ottobre 1998 (in *www.garanteprivacy.it* doc. *web* n. 40751) sulla non menzione, nella fatturazione dettagliata, da parte dei fornitori di servizi di comunicazione elettronica accessibili al pubblico, delle ultime tre cifre dei numeri telefonici chiamati; visto altresì il parere reso in materia da questa Autorità al Ministero delle comunicazioni il 5 ottobre 1999 (in *www.garanteprivacy.it* doc. *web* n. 39881);

Visto l'art. 124, comma 4, del Codice il quale stabilisce che nella fatturazione all'abbonato non sono evidenziate le ultime tre cifre dei numeri chiamati;

Visto l'art. 124, comma 2, del Codice che prevede l'obbligo per il fornitore del servizio di comunicazione elettronica accessibile al pubblico di abilitare l'utente a effettuare comunicazioni e a richiedere servizi da qualsiasi terminale, gratuitamente e in modo agevole, avvalendosi per il pagamento di modalità alternative alla fatturazione, anche impersonali, quali carte di credito o di debito o carte prepagate;

Rilevato che l'art. 124, comma 5, del Codice prevede che il Garante, accertata l'effettiva disponibilità delle predette modalità alternative alla fatturazione indicate al comma 2 del medesimo articolo, può autorizzare il fornitore a indicare nella fatturazione dettagliata richiesta dagli abbonati i numeri completi delle comunicazioni;

Vista l'istruttoria preliminare avviata dall'Autorità nel corso dell'anno 2007 volta a verificare il rispetto della disciplina in materia di protezione dei dati personali, relativamente all'effettiva e diffusa disponibilità per abbonati e utenti di modalità di pagamento alternative alla fatturazione, anche impersonali, ai sensi dell'art. 124, comma 2, del Codice;

VISTI gli elementi acquisiti, nei quali i principali fornitori di servizi di comunicazione elettronica accessibili al pubblico hanno attestato, sotto la propria responsabilità, di aver abilitato i propri utenti a effettuare comunicazioni e a richiedere servizi mediante l'utilizzo di modalità alternative alla fatturazione;

Rilevato che la maggior parte dei predetti fornitori ha altresì attestato, sotto la propria responsabilità, di aver attualmente reso reperibili sul territorio nazionale proprie modalità alternative alla fatturazione, anche di tipo impersonale, quali carte a codice e carte prepagate, oppure di aver abilitato i propri utenti all'uso di carte di debito o di credito;

Tenuto conto che i fornitori hanno altresì attestato che tali carte sono fruibili e distribuite sul territorio, essendo acquistabili presso tabaccherie, edicole, siti *web*, circuiti bancari Atm e ricevitorie della rete Sisal o Lottomatica, nonché presso negozi dove sono disponibili prodotti dei fornitori;

Considerato che, nell'ambito dell'istruttoria preliminare compiuta è emerso che, oltre a

(*) *G.U.* 3 aprile 2008, n. 79
[doc. *web* n. 1501106]

modalità alternative alla fatturazione messe a disposizione direttamente da fornitori, ve ne sono altre che risultano distribuite da parte di soggetti diversi dai fornitori di servizi di comunicazione elettronica (*ad es.*, Poste italiane S.p.A.);

Tenuto conto che dagli elementi acquisiti nell'ambito dell'istruttoria preliminare emerge anche che, rispetto al periodo in cui è stato disciplinato il mascheramento delle ultime tre cifre, si è registrato un enorme incremento dell'utilizzo della telefonia mobile con particolare riferimento a quella *cd.* prepagata, che costituisce di per sé una sostanziale modalità alternativa di pagamento (allo stato, le linee attive risultano superare gli 80 milioni e, di queste, l'89% risulta appartenere alla categoria delle prepagate);

Viste le osservazioni del 6 febbraio 2008 formulate da parte dell'associazione di categoria rappresentativa dei maggiori fornitori di servizi di telecomunicazioni, (Assotelecomunicazioni-Asstel);

Considerato che sussistono, allo stato, le condizioni per adottare un provvedimento generale di carattere autorizzativo ai sensi dell'art. 124, comma 5, del Codice rivolto ai fornitori di servizi di comunicazione elettronica accessibili al pubblico che abbiano abilitato i propri utenti a effettuare comunicazioni e a richiedere servizi mediante l'utilizzo delle predette modalità alternative;

Tenuto conto che i dati contenuti nelle fatture dettagliate attengono ad aspetti della vita privata che riguardano il chiamante, l'abbonato e il chiamato; rilevato che è necessario contemperare i rispettivi diritti e che si rende, quindi, necessario adottare il presente provvedimento di carattere autorizzativo ai sensi dell'art. 124, comma 5, del Codice;

Ritenuto che i fornitori di servizi di comunicazione elettronica accessibili al pubblico che intendano avvalersi della facoltà prevista per legge e dal presente provvedimento dovranno informare preventivamente della decisione di esercitare tale facoltà tutti i rispettivi abbonati mediante un'idonea informativa da inserire all'interno di almeno due fatture e nel proprio sito *web*;

Considerato che la società che si avvale della presente autorizzazione è tenuta, in ogni caso, a offrire ai propri abbonati che lo richiedano la possibilità di ricevere la fatturazione con le ultime tre cifre *"mascherate"*;

Considerato che l'informativa dei fornitori dovrà specificare agli abbonati che abbiano richiesto o intendano richiedere la fatturazione dettagliata che la riceveranno *"in chiaro"*; che in tale informativa il fornitore dovrà inserire un invito agli abbonati a informare coloro che utilizzano l'utenza che la fatturazione perverrà completa dei numeri chiamati relativi alle comunicazioni documentate nella fatturazione dettagliata; che dovrà essere altresì indicato agli abbonati, che su loro specifica richiesta, essi potranno ricevere la fatturazione con le ultime tre cifre *"mascherate"*;

Ritenuto che, in ragione della richiesta di Assotelecomunicazioni-Asstel di stabilire una data unica per gli operatori, appare congruo indicare nel 1° luglio 2008 la data a partire dalla quale tutti i fornitori di comunicazione elettronica accessibili al pubblico, sempreché essi abbiano abilitato i propri utenti a effettuare chiamate e a richiedere servizi nei termini sopra indicati, potranno indicare i numeri completi delle comunicazioni nella fatturazione dettagliata;

Visto che copia del presente provvedimento verrà trasmessa al Ministero della giustizia, anche ai fini della sua pubblicazione sulla *Gazzetta Ufficiale* della Repubblica italiana a cura dell'Ufficio pubblicazione leggi e decreti, nonché, per opportuna conoscenza, all'Autorità per le garanzie nelle comunicazioni.

Vista la documentazione in atti;

Viste le osservazioni dell'Ufficio, formulate dal segretario generale ai sensi dell'art. 15 del regolamento del Garante n. 1/2000 del 28 giugno 2000;

Relatore il prof. Francesco Pizzetti;

TUTTO CIÒ PREMESSO IL GARANTE

a) autorizza, ai sensi dell'art. 124, comma 5, del Codice, a partire dal 1° luglio 2008, tutti i fornitori di servizi di comunicazione elettronica accessibili al pubblico, sempreché essi abbiano abilitato i propri utenti a effettuare comunicazioni e a richiedere servizi da qualsiasi terminale avvalendosi per il pagamento di modalità alternative alla fatturazione, a indicare nella fatturazione dettagliata richiesta dagli abbonati, i numeri completi delle comunicazioni, a condizione che essi forniscano a tutti i propri abbonati un'idonea informativa da inserire all'interno di almeno due fatture e nel proprio sito *web*. L'informativa dovrà:
   - menzionare la decisione del fornitore di avvalersi della presente autorizzazione, specificando che tutti gli abbonati che abbiano chiesto o chiederanno la fatturazione dettagliata la riceveranno "in chiaro", salvo che non richiedano il mascheramento delle ultime tre cifre;
   - contenere l'invito, rivolto a tutti gli abbonati, che abbiano chiesto o chiederanno la fatturazione dettagliata "in chiaro", a informare coloro che utilizzino l'utenza che la fatturazione perverrà completa di tutti i numeri chiamati relativi alle comunicazioni documentate nella fatturazione dettagliata;

b) dispone, ai sensi dell'art. 143, comma 2, del Codice, che copia del presente provvedimento sia trasmessa al Ministero della giustizia anche ai fini della sua pubblicazione sulla *Gazzetta Ufficiale* della Repubblica italiana a cura dell'Ufficio pubblicazione leggi e decreti, nonché, per opportuna conoscenza, all'Autorità per le garanzie nelle comunicazioni.

Roma, 13 marzo 2008

IL PRESIDENTE
Pizzetti

IL RELATORE
Pizzetti

IL SEGRETARIO GENERALE
Buttarelli

39 Schema preliminare del codice di deontologia e di buona condotta per il trattamento dei dati personali effettuato per svolgere investigazioni difensive o per far valere o difendere un diritto in sede giudiziaria (*)

20 marzo 2008

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Nella riunione odierna, in presenza del prof. Francesco Pizzetti, del dott. Giuseppe Chiaravalloti, vice presidente, del dott. Mauro Paissan e del dott. Giuseppe Fortunato, componenti, e del dott. Giovanni Buttarelli, segretario generale;

Visto l'art. 135 del Codice con il quale è stato demandato al Garante il compito di promuovere, ai sensi dell'art. 12 del medesimo Codice, la sottoscrizione di un codice di deontologia e di buona condotta per il trattamento dei dati personali effettuato per lo svolgimento delle investigazioni difensive di cui alla legge 7 dicembre 2000, n. 397, o per far valere o difendere un diritto in sede giudiziaria, in particolare da liberi professionisti o da soggetti che esercitano un'attività di investigazione privata autorizzata in conformità alla legge;

Visto il provvedimento del 16 febbraio 2006 (in G.U. 1° marzo 2006, n. 50) con il quale il Garante ha promosso il predetto codice di deontologia e di buona condotta;

Rilevato che i soggetti menzionati nel verbale della riunione del 17 marzo 2008, conclusiva della prima fase dei lavori per la redazione del codice, hanno convenuto uno schema preliminare di codice che hanno sottoposto all'esame dell'Autorità;

Visto il provvedimento del Garante del 20 luglio 2006 (in G.U. 8 agosto 2006, n. 183) con il quale è stato adottato il regolamento n. 2/2006, recante la procedura per la sottoscrizione dei codici di deontologia e di buona condotta;

VISTI gli atti d'ufficio e rilevata, sulla base di una prima verifica, la non manifesta sussistenza di profili di non conformità del codice alla normativa vigente e la conseguente esigenza di darne notizia e diffusione nei modi previsti dall'art. 6, comma 2, del menzionato regolamento n. 2/2006;

Relatore il dott. Giuseppe Chiaravalloti;

TUTTO CIÓ PREMESSO IL GARANTE

a) dispone la pubblicazione sul sito Internet dell'Autorità www.garanteprivacy.it dello schema preliminare del codice di deontologia e di buona condotta per il trattamento dei dati personali effettuato per svolgere investigazioni difensive o per far valere o difendere un diritto in sede giudiziaria;
b) invita in applicazione dell'art. 6, comma 2, del regolamento n. 2/2006 del Garante i soggetti interessati ai sensi dell'art. 12 del Codice a formulare eventuali osservazioni che dovranno pervenire all'Autorità per posta elettronica entro il 30 aprile 2008, all'indirizzo: *codiceforense@garanteprivacy.it*;
c) invita, altresì, i soggetti rappresentativi o interessati a dare ampia pubblicità al predetto schema preliminare;
d) dispone la trasmissione all'Ufficio pubblicazioni leggi e decreti del Ministero della

(*) [doc. *web* n. 1503511]

giustizia di un avviso da pubblicare nella *Gazzetta Ufficiale* della Repubblica italiana, volto a rendere nota l'inserzione del medesimo schema preliminare sul predetto sito Internet.

Roma, 20 marzo 2008

IL PRESIDENTE
Pizzetti

IL RELATORE
Chiaravalloti

IL SEGRETARIO GENERALE
Buttarelli

SCHEMA PRELIMINARE DEL CODICE DI DEONTOLOGIA E DI BUONA CONDOTTA
PER IL TRATTAMENTO DEI DATI PERSONALI
EFFETTUATO PER SVOLGERE INVESTIGAZIONI DIFENSIVE
O PER FAR VALERE O DIFENDERE UN DIRITTO IN SEDE GIUDIZIARIA
17 marzo 2008

Preambolo

I sottoindicati soggetti sottoscrivono il presente codice di deontologia e di buona condotta sulla base delle seguenti premesse:

1. diversi soggetti, in particolare gli avvocati e i praticanti avvocati iscritti nei relativi albi e registri e chi esercita un'attività di investigazione privata autorizzata in conformità alla legge, utilizzano dati di carattere personale per svolgere investigazioni difensive collegate a un procedimento penale (l. 7 dicembre 2000, n. 397) o, comunque, per far valere o difendere un diritto in sede giudiziaria. L'utilizzo di questi dati è imprescindibile per garantire una tutela piena ed effettiva dei diritti, con particolare riguardo al diritto di difesa e al diritto alla prova: un'efficace tutela di questi due diritti non è pregiudicata, ed è anzi rafforzata, dal principio secondo cui il trattamento dei dati personali deve rispettare i diritti, le libertà fondamentali e la dignità delle persone interessate, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali (artt. 1 e 2 del Codice);

2. gli specifici adattamenti e cautele previsti dalla legge o dal presente codice deontologico non possono trovare applicazione se i dati sono trattati per finalità diverse da quelle di cui all'art. 1 del presente codice;

3. consapevoli del primario interesse al legittimo esercizio del diritto di difesa e alla tutela del segreto professionale, i predetti soggetti avvertono l'esigenza di individuare aspetti specifici delle loro attività professionali, in particolare rispetto alle informazioni personali di carattere sensibile o giudiziario. Ciò, al fine di valorizzare le peculiarità delle attività di ricerca, di acquisizione, di utilizzo e di conservazione dei dati, delle dichiarazioni e dei documenti a fini difensivi, specie in sede giudiziaria, e di prevenire talune incertezze applicative che si sono a volte sviluppate e che hanno portato anche a ipotizzare inutili misure protettive non previste da alcuna disposizione e anzi contrastanti con ordinarie esigenze di funzionalità. Il primario interesse al legittimo esercizio del diritto di difesa deve essere rispettato in ogni sede, anche in occasione di accertamenti ispettivi, tenendo altresì conto dei limiti normativi all'esercizio dei diritti dell'interessato (artt. 7, 8 e 9 del Codice) previsti per finalità di tutela del diritto di difesa;

4. il trattamento dei dati per l'attività di difesa concorre alla formazione permanente del professionista e contribuisce alla realizzazione di un patrimonio di precedenti giuridici che perdura nel tempo, per ipotizzabili necessità di difesa, anche dopo l'estinzione del rapporto di mandato, oltre a essere espressione della propria attività professionale;

5. norme di legge e provvedimenti attuativi prevedono già garanzie e accorgimenti da osservare per la protezione dei dati personali utilizzati per far valere o difendere un diritto in sede giudiziaria o per svolgere investigazioni difensive. Tali cautele, che non vanno osservate se i dati sono anonimi, hanno già permesso di chiarire, ad esempio, a quali condizioni

sia lecito raccogliere informazioni personali senza consenso e senza una specifica informativa, e che è legittimo utilizzarle in modo proporzionato per esigenze di difesa anche quando il procedimento civile o penale di riferimento non sia ancora instaurato. I predetti accorgimenti e garanzie possono comportare, se non sono rispettati, l'inutilizzabilità dei dati trattati (art. 11, comma 2, del Codice). Essi riguardano, in particolare:

a) l'informativa agli interessati, che può non comprendere gli elementi già noti alla persona che fornisce i dati e può essere caratterizzata da uno stile colloquiale e da formule sintetiche adatte al rapporto fiduciario con la persona assistita o, comunque, alla prestazione professionale; essa può essere fornita, anche solo oralmente e, comunque, *una tantum* rispetto al complesso dei dati raccolti sia presso l'interessato, sia presso terzi. Ciò, con possibilità di omettere l'informativa stessa per i dati raccolti presso terzi, qualora gli stessi siano trattati solo per il periodo strettamente necessario per far valere o difendere un diritto in sede giudiziaria o per svolgere investigazioni difensive, tenendo presente che non sono raccolti presso l'interessato i dati provenienti da un rilevamento lecito a distanza, ossia tale da non interagire direttamente con l'interessato (art. 13, comma 5, lett. *b*) del Codice);

b) il consenso dell'interessato, che non va richiesto per adempiere a obblighi di legge e che non occorre, altresì, per i dati anche di natura sensibile utilizzati per perseguire finalità di difesa di un diritto anche mediante investigazioni difensive. Ciò, sia per i dati trattati nel corso di un procedimento, anche in sede amministrativa, di arbitrato o di conciliazione, sia nella fase propedeutica all'instaurazione di un eventuale giudizio, anche al fine di verificare con le parti se vi sia un diritto da tutelare utilmente in sede giudiziaria, sia nella fase successiva alla risoluzione, giudiziale o stragiudiziale della lite. Occorre peraltro avere cura di rispettare, se si tratta di dati idonei a rivelare lo stato di salute e la vita sessuale, il principio del "pari rango", il quale giustifica il loro trattamento quando il diritto che si intende tutelare, anche derivante da atto o fatto illecito, è "di rango pari a quello dell'interessato, ovvero consistente in un diritto della personalità o in altro diritto o libertà fondamentale e inviolabile" (artt. 24, comma 1, lett. *f*) e 26, comma 4, lett. *c*) del Codice; aut. gen. nn. 2/2007, 4/2007 e 6/2007; *Provv.* 9 luglio 2003 [doc. *web* n. 29832]);

c) l'accesso ai dati personali e l'esercizio degli altri diritti da parte dell'interessato rispetto al trattamento dei dati stessi; diritti per i quali è previsto, per legge, un possibile differimento nel periodo durante il quale, dal loro esercizio, può derivare un pregiudizio effettivo e concreto per lo svolgimento delle investigazioni difensive o per l'esercizio del diritto in sede giudiziaria (art. 8, comma 2, lett. *e*) del Codice);

d) il flusso verso l'estero dei dati trasferiti solo per finalità di svolgimento di investigazioni difensive o, comunque, per far valere o difendere un diritto in sede giudiziaria, per il tempo a ciò strettamente necessario, trasferimento che non è pregiudicato né verso Paesi dell'Unione europea, né verso Paesi terzi (artt. 42 e 43, comma 1, lett. *e*) del Codice);

e) la notificazione dei trattamenti, che non è richiesta per innumerevoli trattamenti di dati effettuati per far valere o difendere un diritto in sede giudiziaria, o per svolgere investigazioni difensive (art. 37, comma 1, del Codice; *Prov.* 31 marzo 2004, n. 1 [doc. *web* n. 852561] e nota di chiarimenti n. 9654/33365 del 23 aprile 2004 [doc. *web* n. 993385]);

f) la designazione di incaricati e di eventuali responsabili del trattamento, considerata la facoltà di avvalersi di soggetti che possono utilizzare legittimamente i dati (colleghi, collaboratori, corrispondenti, domiciliatari, sostituti, periti, ausiliari e consulenti che non rivestano la qualità di autonomi titolari del trattamento: artt. 29 e 30 del Codice);

g) i dati particolari quali quelli genetici, per i quali sono previste già alcune cautele in particolare per ciò che riguarda il principio di proporzionalità, le misure di sicurezza, il contenuto dell'informativa agli interessati e la manifestazione del consenso (art. 90 del Codice; aut. gen. del Garante del 22 febbraio 2007);

h) l'informatica giuridica, per la quale apposite disposizioni di legge hanno individuato opportune cautele per tutelare gli interessati senza pregiudicare l'informazione scientifico-giuridica (artt. 51 e 52 del Codice);

i) l'utilizzazione di dati pubblici e di altri dati e documenti contenuti in pubblici registri, elenchi, albi, atti o documenti conoscibili da chiunque, nonché in banche

di dati, archivi ed elenchi, ivi compresi gli atti dello stato civile, dai quali possono essere estratte lecitamente informazioni personali riportate in certificazioni e attestazioni utilizzabili a fini difensivi;

6. rispetto a questo quadro, il presente codice individua alcune regole complementari di comportamento le quali costituiscono una condizione essenziale per la liceità e la correttezza del trattamento dei dati, ma non hanno diretta rilevanza sul piano degli illeciti disciplinari; esse non pregiudicano, quindi, la distinta e autonoma valenza delle norme deontologiche professionali e le scelte adottate al riguardo dai competenti organismi di settore, in particolare rispetto al codice deontologico forense. Peraltro, l'inosservanza di quest'ultimo può assumere rilievo ai fini della valutazione della liceità e correttezza del trattamento dei dati personali;

7. utile supporto alla protezione dei dati proviene anche da ulteriori princìpi già riconosciuti, in materia, dal codice di procedura penale e dallo stesso codice deontologico forense (in particolare, per quanto riguarda il dovere di segretezza e riservatezza, anche nei confronti di *ex* clienti, la rivelazione di notizie riservate o coperte dal segreto professionale, la rivelazione al pubblico del nominativo di clienti, la registrazione di colloqui tra avvocati e la corrispondenza tra colleghi), nonché da altre regole di comportamento individuate dall'Unione delle camere penali italiane o da ulteriori organismi sottoscrittori del presente codice deontologico.

CAPO I - PRINCIPI GENERALI

Art. 1 - Ambito di applicazione

1. Le disposizioni del presente codice devono essere rispettate nel trattamento di dati personali per svolgere investigazioni difensive o per far valere o difendere un diritto in sede giudiziaria, sia nel corso di un procedimento, anche in sede amministrativa, di arbitrato o di conciliazione, sia nella fase propedeutica all'instaurazione di un eventuale giudizio, sia nella fase successiva alla sua definizione, da parte di:

a) avvocati o praticanti avvocati iscritti ad albi territoriali o ai relativi registri, sezioni ed elenchi, i quali esercitino l'attività in forma individuale, associata o societaria svolgendo, anche su mandato, un'attività in sede giurisdizionale o di consulenza o di assistenza stragiudiziale, anche avvalendosi di collaboratori, dipendenti o ausiliari, nonché da avvocati stranieri esercenti legalmente la professione sul territorio dello Stato;

b) soggetti che, sulla base di uno specifico incarico anche da parte di un difensore (aut. gen. n. 6/2007, punto n. 2), svolgano in conformità alla legge attività di investigazione privata (art. 134 r.d. 18 giugno 1931, n. 773; art. 222 norme di coordinamento del c.p.p.).

2. Le disposizioni del presente codice si applicano, altresì, a chiunque tratti dati personali per le finalità di cui al comma 1, in particolare a altri liberi professionisti o soggetti che in conformità alla legge prestino, su mandato, attività di consulenza per le medesime finalità.

CAPO II - TRATTAMENTI DA PARTE DI AVVOCATI

Art. 2 - Modalità di trattamento

1. L'avvocato organizza il trattamento anche non automatizzato dei dati personali secondo le modalità che risultino più adeguate, caso per caso, a favorire in concreto l'effettivo rispetto dei diritti, delle libertà e della dignità degli interessati, applicando i princìpi di finalità, necessità, proporzionalità e non eccedenza sulla base di un'attenta valutazione sostanziale e non formalistica delle garanzie previste, nonché di un'analisi della quantità e qualità delle informazioni che utilizza e dei possibili rischi.

2. Le decisioni relativamente a quanto previsto dal comma 1 sono adottate dal titolare del trattamento il quale resta individuato, a seconda dei casi, in:

a) un singolo professionista;

b) una pluralità di professionisti, codifensori della medesima parte assistita o che, anche al di fuori del mandato di difesa, siano stati comunque interessati a concorrere all'opera professionale quali consulenti o domiciliatari;

c) un'associazione tra professionisti o una società di professionisti.

3. Nel quadro delle adeguate istruzioni da impartire per iscritto agli incaricati del tratta-

mento da designare e ai responsabili del trattamento prescelti facoltativamente (artt. 29 e 30 del Codice), sono formulate concrete indicazioni in ordine alle modalità che tali soggetti devono osservare, a seconda del loro ruolo di sostituto processuale, di praticante avvocato con o senza abilitazione al patrocinio, di consulente tecnico di parte, perito, investigatore privato o altro ausiliario che non rivesta la qualità di autonomo titolare del trattamento, nonché di tirocinante, stagista o di persona addetta a compiti di collaborazione amministrativa.

4. Specifica attenzione è prestata all'adozione di idonee cautele per prevenire l'ingiustificata raccolta, utilizzazione o conoscenza di dati in caso di:

a) acquisizione anche informale di notizie, dati e documenti connotati da un alto grado di confidenzialità o che possono comportare, comunque, rischi specifici per gli interessati;
b) scambio di corrispondenza, specie per via telematica;
c) esercizio contiguo di attività autonome all'interno di uno studio;
d) utilizzo di dati di cui è dubbio l'impiego lecito, anche per effetto del ricorso a tecniche invasive;
e) utilizzo e distruzione di dati riportati su particolari dispositivi o supporti, specie elettronici (ivi comprese registrazioni audio/video), o documenti (tabulati di flussi telefonici e informatici, consulenze tecniche e perizie, relazioni redatte da investigatori privati);
f) custodia di materiale documentato, ma non utilizzato in un procedimento e ricerche su banche dati a uso interno, specie se consultabili anche telematicamente da uffici dello stesso titolare del trattamento situati altrove;
g) acquisizione di dati e documenti da terzi, verificando che si abbia titolo per ottenerli;
h) conservazione di atti relativi ad affari definiti.

5. Se i dati sono trattati per esercitare il diritto di difesa in sede giurisdizionale, ciò può avvenire anche prima della pendenza di un procedimento, sempreché i dati medesimi risultino strettamente funzionali all'esercizio del diritto di difesa, in conformità ai princìpi di proporzionalità, di pertinenza, di completezza e di non eccedenza rispetto alle finalità difensive (art. 11 del Codice).

6. Sono utilizzati lecitamente e secondo correttezza:

a) i dati personali contenuti in pubblici registri, elenchi, albi, atti o documenti conoscibili da chiunque, nonché in banche di dati, archivi ed elenchi, ivi compresi gli atti dello stato civile, dai quali possono essere estratte lecitamente informazioni personali riportate in certificazioni e attestazioni utilizzabili a fini difensivi;
b) atti, annotazioni, dichiarazioni e informazioni acquisite nell'ambito di indagini difensive, in particolare ai sensi degli articoli 391-*bis*, 391-*ter* e 391-*quater* del codice di procedura penale, evitando l'ingiustificato rilascio di copie eventualmente richieste. Se per effetto di un conferimento accidentale, anche in sede di acquisizione di dichiarazioni e informazioni ai sensi dei medesimi articoli 391-*bis*, 391-*ter* e 391-*quater*, sono raccolti dati eccedenti e non pertinenti rispetto alle finalità difensive, tali dati, qualora non possano essere estrapolati o distrutti, formano un unico contesto, unitariamente agli altri dati raccolti.

Art. 3 - Informativa unica

1. L'avvocato può fornire in un unico contesto, anche mediante affissione nei locali dello studio o pubblicazione sul proprio sito Internet e anche utilizzando formule sintetiche e colloquiali, l'informativa sul trattamento dei dati personali (art. 13 del Codice) e le notizie che deve indicare ai sensi della disciplina sulle indagini difensive.

Art. 4 - Conservazione e cancellazione dei dati

1. La definizione di un grado di giudizio o la cessazione dello svolgimento di un incarico non comportano un'automatica dismissione dei dati. Una volta estinto il procedimento o il relativo rapporto di mandato, atti e documenti attinenti all'oggetto della difesa o delle investigazioni difensive possono essere conservati, in originale o in copia e anche in formato elettronico, qualora risulti necessario in relazione a ipotizzabili altre esigenze difensive della parte assistita o del titolare del trattamento, ferma restando la loro utilizzazione in forma anonima per finalità scientifiche. La valutazione è effettuata tenendo conto della tipologia dei dati. Se è prevista una conservazione per adempiere a un obbligo normativo, anche in

materia fiscale e di contrasto della criminalità, sono custoditi i soli dati personali effettivamente necessari per adempiere al medesimo obbligo.

2. Fermo restando quanto previsto dal codice deontologico forense in ordine alla restituzione al cliente dell'originale degli atti da questi ricevuti, e salvo quanto diversamente stabilito dalla legge, è consentito, previa comunicazione alla parte assistita, distruggere, cancellare o consegnare all'avente diritto o ai suoi eredi o aventi causa la documentazione integrale dei fascicoli degli affari trattati e le relative copie.

3. In caso di revoca o di rinuncia al mandato fiduciario o del patrocinio, la documentazione acquisita è rimessa, in originale ove detenuta in tale forma, al difensore che subentra formalmente nella difesa.

4. La titolarità del trattamento non cessa per il solo fatto della sospensione o cessazione dell'esercizio della professione. In caso di cessazione anche per sopravvenuta incapacità e qualora manchi un altro difensore anche succeduto nella difesa o nella cura dell'affare, la documentazione dei fascicoli degli affari trattati, decorso un congruo termine dalla comunicazione all'assistito, è consegnata al Consiglio dell'ordine di appartenenza ai fini della conservazione per finalità difensive.

Art. 5 - Comunicazione e diffusione di dati

1. Nei rapporti con i terzi e con la stampa possono essere rilasciate informazioni non coperte da segreto qualora sia necessario per finalità di tutela dell'assistito, ancorché non concordato con l'assistito medesimo, nel rispetto dei princìpi di finalità, liceità, correttezza, indispensabilità, pertinenza e non eccedenza di cui al Codice (art. 11), nonché dei diritti e della dignità dell'interessato e di terzi, di eventuali divieti di legge e del codice deontologico forense.

Art. 6 - Accertamenti riguardanti documentazione detenuta dal difensore

1. In occasione di accertamenti ispettivi che lo riguardano l'avvocato ha diritto ai sensi dell'articolo 159, comma 3, del Codice che vi assista il presidente del competente Consiglio dell'ordine forense o un consigliere da questo delegato. Allo stesso, se interviene e ne fa richiesta, è consegnata copia del provvedimento.

2. In sede di istanza di accesso o richiesta di comunicazione dei dati di traffico relativi a comunicazioni telefoniche in entrata ai sensi degli artt. 8, comma 2, lett. *f*) e 24, comma 1, lett. *f*) del Codice, l'avvocato attesta al fornitore di servizi di comunicazione elettronica accessibili al pubblico la sussistenza del pregiudizio effettivo e concreto che deriverebbe per lo svolgimento delle investigazioni difensive dalla mancata disponibilità dei dati, senza menzionare necessariamente il numero di repertorio di un procedimento penale.

CAPO III - TRATTAMENTI DA PARTE DI ALTRI LIBERI PROFESSIONISTI E ULTERIORI SOGGETTI

Art. 7 - Applicazione di disposizioni riguardanti gli avvocati

1. Le disposizioni di cui agli articoli 2 e 5 si applicano, salvo quanto applicabile per legge unicamente all'avvocato:

a) a liberi professionisti che prestino o su mandato dell'avvocato o unitamente a esso o, comunque, nei casi e nella misura consentita dalla legge, attività di consulenza e assistenza per far valere o difendere un diritto in sede giudiziaria o per lo svolgimento delle investigazioni difensive;

b) agli altri soggetti, di cui all'art. 1, comma 2, salvo quanto risulti obiettivamente incompatibile in relazione alla figura soggettiva o alla funzione svolta.

CAPO IV - TRATTAMENTI DA PARTE DI INVESTIGATORI PRIVATI

Art. 8 - Modalità di trattamento

1. L'investigatore privato organizza il trattamento anche non automatizzato dei dati personali secondo le modalità di cui all'articolo 2, comma 1.

2. L'investigatore privato non può intraprendere di propria iniziativa investigazioni, ricerche o altre forme di raccolta dei dati. Tali attività possono essere eseguite esclusivamente sulla base di apposito incarico conferito per iscritto e solo per le finalità di cui al presente codice.

3. L'atto d'incarico deve menzionare in maniera specifica il diritto che si intende esercitare in sede giudiziaria, ovvero il procedimento penale al quale l'investigazione è collegata, nonché i principali elementi di fatto che giustificano l'investigazione e il termine ragionevole entro cui questa deve essere conclusa.

4. L'investigatore privato deve eseguire personalmente l'incarico ricevuto e può avvalersi solo di altri investigatori privati indicati nominativamente all'atto del conferimento dell'incarico, oppure successivamente in calce a esso qualora tale possibilità sia stata prevista nell'atto di incarico e non siano trattati dati sensibili.

5. Nel caso in cui si avvalga di collaboratori interni designati quali responsabili o incaricati del trattamento in conformità a quanto previsto dagli artt. 29 e 30 del Codice, l'investigatore privato formula concrete indicazioni in ordine alle modalità da osservare e vigila, con cadenza almeno settimanale, sulla puntuale osservanza delle norme di legge e delle istruzioni impartite. Tali soggetti possono avere accesso ai soli dati strettamente pertinenti alla collaborazione a essi richiesta.

6. Il difensore o il soggetto che ha conferito l'incarico devono essere informati periodicamente dell'andamento dell'investigazione, anche al fine di permettere loro una valutazione tempestiva circa le determinazioni da adottare riguardo all'esercizio del diritto in sede giudiziaria o al diritto alla prova.

Art. 9 - Altre regole di comportamento

1. L'investigatore privato si astiene dal porre in essere prassi elusive di obblighi e di limiti di legge e, in particolare, conforma ai princìpi di liceità e correttezza del trattamento sanciti dal Codice:

a) l'acquisizione di dati personali presso altri titolari del trattamento, anche mediante mera consultazione, verificando che si abbia titolo per ottenerli;

b) il ricorso ad attività lecite di rilevamento, specie a distanza, e di audio/videoripresa;

c) la raccolta di dati biometrici.

2. L'investigatore privato rispetta nel trattamento dei dati le disposizioni di cui all'articolo 2, commi 4, 5 e 6 del presente codice.

Art. 10 - Conservazione e cancellazione dei dati

1. Nel rispetto dell'art. 11, comma 1, lett. *e)* del Codice i dati personali trattati dall'investigatore privato possono essere conservati per un periodo non superiore a quello strettamente necessario per eseguire l'incarico ricevuto. A tal fine deve essere verificata costantemente, anche mediante controlli periodici, la stretta pertinenza, non eccedenza e indispensabilità dei dati rispetto alle finalità perseguite e all'incarico conferito.

2. Una volta conclusa la specifica attività investigativa, il trattamento deve cessare in ogni sua forma, fatta eccezione per l'immediata comunicazione al difensore o al soggetto che ha conferito l'incarico, i quali possono consentire, anche in sede di mandato, l'eventuale conservazione temporanea di materiale strettamente personale di chi ha curato l'attività svolta, ai soli fini dell'eventuale dimostrazione della liceità e correttezza del proprio operato. Se è stato contestato il trattamento il difensore o il soggetto che ha conferito l'incarico possono anche fornire all'investigatore il materiale necessario per dimostrare la liceità e correttezza del proprio operato, per il tempo a ciò strettamente necessario.

3. La sola pendenza del procedimento al quale l'investigazione è collegata, ovvero il passaggio ad altre fasi di giudizio in attesa della formazione del giudicato, non costituiscono, di per se stessi, una giustificazione valida per la conservazione dei dati da parte dell'investigatore privato.

Art. 11 - Informativa

1. L'investigatore privato può fornire l'informativa in un unico contesto ai sensi dell'articolo 3 del presente codice, ponendo in particolare evidenza l'identità e la qualità professionale dell'investigatore, nonché la natura facoltativa del conferimento dei dati.

CAPO V - DISPOSIZIONI FINALI

Art. 12 - Monitoraggio dell'attuazione del codice

1. Ai sensi della art. 135 del Codice, i soggetti che sottoscrivono il presente codice avviano forme di collaborazione per verificare periodicamente la sua attuazione anche ai fini di un eventuale adeguamento alla luce del progresso tecnologico, dell'esperienza acquisita o di novità normative.

Art. 13 - Entrata in vigore

1. Il presente codice si applica a decorrere dal ... 2008.

40 Linee-guida in materia di trattamento di dati personali di lavoratori per finalità di gestione del rapporto di lavoro in ambito pubblico (*) *14 giugno 2007*

Registro delle deliberazioni
n. 23 del 14 giugno 2007

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Nella riunione odierna, in presenza del prof. Francesco Pizzetti, presidente, del dott. Giuseppe Chiaravalloti, vice presidente, del dott. Mauro Paissan e del dott. Giuseppe Fortunato, componenti, e del dott. Giovanni Buttarelli, segretario generale;

Visto il Codice in materia di protezione dei dati personali (d.lg. 30 giugno 2003, n. 196), anche in riferimento all'art. 154, comma 1, lett. *h*);

Esaminate le istanze (segnalazioni e quesiti) pervenute riguardo al trattamento di dati personali di lavoratori per finalità di gestione del rapporto di lavoro in ambito pubblico;

Ritenuta l'opportunità di individuare un quadro unitario di misure e di accorgimenti necessari e opportuni, volti a fornire orientamenti utili per cittadini e amministrazioni interessate;

Visto il testo unico delle leggi sull'ordinamento degli enti locali (d.lg. 18 agosto 2000, n. 267);

Vista la documentazione in atti;

Viste le osservazioni dell'Ufficio, formulate dal segretario generale ai sensi dell'art. 15 del regolamento del Garante, n. 1/2000;

Relatore il dott. Mauro Paissan;

DELIBERA

1. di adottare le *"Linee-guida in materia di trattamento di dati personali di lavoratori per finalità di gestione del rapporto di lavoro in ambito pubblico"* contenute nel documento allegato quale parte integrante della presente deliberazione (Allegato 1);

2. che copia del presente provvedimento sia trasmessa al Ministero della giustizia-Ufficio pubblicazione leggi e decreti, per la sua pubblicazione sulla *Gazzetta Ufficiale* della Repubblica italiana ai sensi dell'art. 143, comma 2, del Codice.

Roma, 14 giugno 2007

IL PRESIDENTE
Pizzetti

IL RELATORE
Paissan

IL SEGRETARIO GENERALE
Buttarelli

(*) *G.U.* 13 luglio 2007, n. 161
[doc. *web* n. 1417809]

LINEE-GUIDA IN MATERIA DI TRATTAMENTO DI DATI PERSONALI DI LAVORATORI PER FINALITÀ DI GESTIONE DEL RAPPORTO DI LAVORO IN AMBITO PUBBLICO (*)

(Deliberazione n. 23 del 14 giugno 2007)

Sommario

1. Premessa

1.1. *Scopo delle linee-guida.* Per fornire indicazioni e raccomandazioni riguardo alle operazioni di trattamento effettuate con dati personali (anche sensibili) di lavoratori alle dipendenze di datori di lavoro pubblici, il Garante ravvisa l'esigenza di adottare le presenti linee-guida, suscettibili di periodico aggiornamento, nelle quali si tiene conto di precedenti decisioni dell'Autorità.

Le presenti linee-guida seguono quelle adottate rispetto agli analoghi trattamenti effettuati da datori di lavoro privati [1], con le quali coincidono per molteplici aspetti che sono comunque riprodotti nel presente documento.

L'adozione di distinte linee-guida per il settore pubblico deriva dall'esigenza di evidenziare, nel quadro della tendenziale uniformità dei princìpi applicabili al rapporto di lavoro [2], alcune specificità che si pongono per i soggetti pubblici datori di lavoro (taluni presupposti del trattamento; speciali disposizioni che prevedono casi di necessaria comunicazione o diffusione di dati; situazioni particolari).

Come per il settore privato, le indicazioni fornite non pregiudicano l'applicazione delle disposizioni di legge o di regolamento che stabiliscono particolari divieti o limiti in relazione a taluni settori o a specifici casi di trattamento (artt. 113, 114 e 184, comma 3, del Codice).

(*) *Le note sono in calce al testo*

1.2. *Ambiti considerati.* Le tematiche prese in considerazione si riferiscono, in particolare, alla comunicazione e alla diffusione di dati e al trattamento delle informazioni sensibili (in specie, di quelli idonei a rivelare lo stato di salute e le convinzioni religiose) o di dati biometrici relativi a lavoratori alle dipendenze di pubbliche amministrazioni.

2. Il rispetto dei princìpi di protezione dei dati personali

2.1. *Considerazioni generali.* Anche per i datori di lavoro pubblici il trattamento dei dati personali è disciplinato assicurando un livello elevato di tutela dei diritti e delle libertà fondamentali e conformando il medesimo trattamento ai princìpi di semplificazione, armonizzazione ed efficacia, sia per le modalità di esercizio dei diritti, sia per l'adempimento degli obblighi da parte dei titolari del trattamento [3].

I lavoratori, nel rapporto con il proprio datore di lavoro pubblico, hanno diritto di ottenere che il trattamento dei dati effettuato mediante l'uso di tecnologie telematiche sia conformato al rispetto dei predetti diritti e libertà [4].

Assume quindi particolare rilievo la necessità che i soggetti pubblici colgano l'occasione della progressiva introduzione di nuove tecniche rispetto alle modalità tradizionali di trattamento dei dati su base cartacea per valutare preventivamente come rendere efficienti i propri sistemi informativi, individuando forme adeguate di trattamento che tutelino appieno i lavoratori.

Le cautele e gli accorgimenti devono essere opportunamente graduati tenendo conto anche delle diverse forme del trattamento e della differente natura dei dati comuni e sensibili.

2.2. *Liceità, pertinenza, trasparenza.* Il datore di lavoro pubblico può lecitamente trattare dati personali dei lavoratori nella misura in cui ciò sia necessario per la corretta gestione del rapporto di lavoro, avendo cura di applicare le previsioni che riguardano le proprie funzioni istituzionali o il rapporto di lavoro, contenute in leggi, regolamenti, contratti e in accordi collettivi, in modo da avvalersi di informazioni personali e modalità di trattamento proporzionate ai singoli scopi.

Il Codice in materia di protezione dei dati personali, anche in attuazione di direttive comunitarie (nn. 95/46/Ce e 2002/58/Ce), prescrive che il trattamento di dati personali per la gestione del rapporto di lavoro avvenga, in particolare:

- rispettando i princìpi di necessità, di liceità e di qualità dei dati (artt. 3 e 11 del Codice);
- attenendosi alle funzioni istituzionali e applicando i presupposti e i limiti previsti da leggi e regolamenti rilevanti per il trattamento, in particolare in materia di pubblico impiego (art. 18 del Codice);
- dando applicazione effettiva e concreta al principio di indispensabilità nel trattamento dei dati sensibili e giudiziari, il quale vieta di trattare informazioni o di effettuare operazioni che non siano realmente indispensabili per raggiungere determinate finalità previste specificamente (artt. 4, comma 1, lett. *d*) ed *e*), 22, commi 3, 5 e 9, e 112 del Codice);
- limitando il trattamento di dati sensibili e giudiziari alle sole informazioni ed operazioni di trattamento individuate e rese pubbliche con l'atto regolamentare adottato in conformità al parere del Garante (artt. 20, 21, 112 e 154 del Codice);
- informando preventivamente e adeguatamente gli interessati (art. 13 del Codice);
- adottando adeguate misure di sicurezza, idonee a preservare i dati da alcuni eventi tra cui accessi ed utilizzazioni indebiti, rispetto ai quali l'amministrazione può essere chiamata a rispondere anche civilmente e penalmente (artt. 15 e 31 e ss. del Codice).

2.3. *Finalità.* Il trattamento dei dati personali, anche sensibili, riferibili ai lavoratori deve essere orientato in concreto all'esclusivo o prevalente scopo di adempiere agli obblighi e ai compiti in materia di rapporto di lavoro e di impiego alle dipendenze delle amministrazioni pubbliche.

Oltre alle leggi e ai regolamenti, anche i contratti collettivi (nazionali e integrativi) contengono alcune previsioni che permettono di trattare lecitamente informazioni di natura personale anche per ciò che attiene all'attività sindacale (ad esempio, per determinare il trattamento economico fondamentale ed accessorio, per fruire di permessi o di aspettative sindacali, per accedere a qualifiche, per la mobilità o per la responsabilità disciplinare).

Il trattamento effettuato dal soggetto pubblico deve attenersi in concreto a queste disposizioni e restare compatibile con le finalità per le quali i dati sono stati inizialmente raccolti o già trattati (art. 11, comma 1, lett. *b*), del Codice).

Particolare attenzione deve essere posta alle disposizioni dei contratti collettivi che prevedono la conoscenza di dati da parte di organizzazioni sindacali, avendo cura che il doveroso rispetto degli obblighi di informativa, consultazione, concertazione e contrattazione che comportano la comunicazione di informazioni alle medesime organizzazioni avvenga nel rispetto dei princìpi di necessità e proporzionalità.

I soggetti pubblici potrebbero peraltro cogliere l'occasione dei rinnovi dei contratti collettivi per verificare l'attualità e la chiarezza di tali previsioni contrattuali, verificando anche la loro adeguatezza rispetto a casi che si verificano in concreto (si pensi al problema della contestuale iscrizione dei lavoratori a più organizzazioni sindacali contestata da alcuna di esse).

In questo quadro occorre anche mantenere distinti i casi in cui è prevista specificamente la comunicazione solo di dati numerici aggregati da quelli in cui, in un'ottica di trasparenza e graduazione dell'accesso delle organizzazioni sindacali ad informazioni personali che risultino necessarie per verificare in conformità alla legge la concreta applicazione delle disposizioni del contratto collettivo da parte del datore di lavoro, è invece consentita (ed è giustificata in rapporto al caso concreto) la conoscenza di dati riferiti a singoli lavoratori.

In tale ottica, nell'ambito della disciplina contrattuale, si potrebbe pertanto prevedere di regola un accesso preliminare del sindacato a dati aggregati, riferiti all'intera struttura lavorativa o a singole unità organizzative ovvero a gruppi di lavoratori e, soltanto in presenza di successive anomalie o di specifiche esigenze di verifica, consentire (in casi espressamente previsti e circostanziati) all'organizzazione sindacale di conoscere anche informazioni personali relative a singoli o a gruppi di lavoratori. Ciò sempreché, nel caso concreto, sia effettivamente necessario per dimostrare la corretta applicazione dei criteri pattuiti e la comunicazione sia limitata alle informazioni pertinenti e non eccedenti rispetto a tale scopo. Resta fermo che l'eventuale successivo trattamento illecito o non corretto delle informazioni acquisite da parte dell'organizzazione sindacale si svolge nella sfera di responsabilità della medesima organizzazione [5].

3. Titolare, responsabile e incaricati del trattamento

3.1. Corretta individuazione delle figure. Resta importante individuare correttamente i soggetti che, a diverso titolo, possono trattare i dati nell'ambito della pubblica amministrazione "titolare" del trattamento ("incaricati"; eventuali "responsabili"), definendo chiaramente le rispettive attribuzioni (artt. 4, comma 1, lett. *f*), *g*) e *h*), 28, 29 e 30 del Codice).

Rinviando per brevità di esposizione ai numerosi pronunciamenti del Garante sul tema, giova ricordare che in linea di principio, per individuare il titolare del trattamento, occorre far riferimento all'amministrazione o ente centrale o locale nel suo complesso, anziché a singole articolazioni interne o alle persone fisiche che l'amministrano o la rappresentano (ad esempio, il ministro, il direttore generale o il presidente) [6].

Nelle amministrazioni più articolate, specie di grandi dimensioni o ramificate sul territorio, è possibile che alcune figure o unità organizzative siano dotate in conformità alla legge di poteri decisionali effettivamente del tutto autonomi riguardo ai trattamenti di dati personali. In tal caso, rispettando in concreto quanto previsto dal Codice (art. 28), tali articolazioni possono essere considerate lecitamente quali "titolari" autonomi o eventuali "contitolari del trattamento" (si pensi, ad esempio, ad una singola direzione generale o area geografica di un'amministrazione ministeriale di particolare complessità organizzativa [7]).

Nel rispetto dei princìpi generali sopra richiamati in materia di trattamento di dati personali (*cfr.* punto 2), le amministrazioni devono disciplinare le modalità del trattamento, designando gli eventuali soggetti responsabili e, in ogni caso, le persone fisiche incaricate, che possono acquisire lecitamente conoscenza dei dati inerenti alla gestione del rapporto di lavoro, attenendosi alle funzioni svolte e a idonee istruzioni scritte (artt. 4, comma 1, lett. *g*) e *h*), 29 e 30).

È, infatti, facoltà delle amministrazioni designare alcuni soggetti (persone fisiche o giuridiche, enti od organismi) quali "responsabili" del trattamento, delineandone analiticamente e per iscritto i compiti attribuiti, e individuando al loro interno, se del caso, ulteriori livelli di responsabilità in base all'organizzazione delle divisioni e degli uffici o alle tipologie di trattamenti, di archivi e di dati, sempreché ciascuno di questi dimostri l'esperienza, la capacità e l'affidabilità richieste dalla legge (art. 29 del Codice).

È necessario invece che ogni lavoratore sia preposto per iscritto, in qualità di "incaricato", alle operazioni di trattamento e sia debitamente istruito in ordine all'accesso e all'utilizzo delle informazioni personali di cui può venire a conoscenza nello svolgimento della propria prestazione lavorativa. La designazione degli incaricati può essere effettuata nominativamente o, specie nell'ambito di strutture organizzative complesse, mediante atti di preposizione del lavoratore a unità organizzative per le quali venga altresì previamente individuato, per iscritto, l'ambito del trattamento consentito (art. 30 del Codice).

3.2. *Medico competente.* Anche il datore di lavoro pubblico deve svolgere alcuni trattamenti di dati in applicazione della disciplina in materia di igiene e sicurezza del lavoro (art. 1, commi 1 e 2, d.lg. n. 626/1994 e successive modificazioni e integrazioni).

Tale disciplina, che attua anche alcune direttive comunitarie e si colloca nella cornice più ampia delle misure necessarie a tutelare l'integrità psico-fisica dei lavoratori, pone direttamente in capo al medico competente in materia di igiene e sicurezza nei luoghi di lavoro la sorveglianza sanitaria obbligatoria (e, ai sensi degli artt. 16 e 17 del d.lg. n. 626/1994, il correlato trattamento dei dati contenuti in cartelle cliniche).

In questo ambito il medico competente effettua accertamenti preventivi e periodici sui lavoratori (art. 33 d.P.R. n. 303/1956; art. 16 d.lg. n. 626/1994) e istituisce (curandone l'aggiornamento) una cartella sanitaria e di rischio (in conformità alle prescrizioni contenute negli artt. 17, 59-*quinquiesdecies*, comma 2, lett. b), 59-*sexiesdecies*, 70, 72-*undecies* e 87 d.lg. n. 626/1994).

Detta cartella è custodita presso l'amministrazione "con salvaguardia del segreto professionale, e consegnata in copia al lavoratore stesso al momento della risoluzione del rapporto di lavoro, ovvero quando lo stesso ne fa richiesta" (artt. 4, comma 8, e 17, comma 1, lett. d), d.lg. n. 626/1994); in caso di cessazione del rapporto di lavoro le cartelle sono trasmesse all'Istituto superiore prevenzione e sicurezza sul lavoro-Ispesl (artt. 59-*sexiesdecies*, comma 4, 70, comma 4, 72-*undecies*, comma 3 e 87, comma 3, lett c), d.lg. n. 626/1994), in originale e in busta chiusa [8].

In relazione a tali disposizioni, al medico competente è consentito trattare dati sanitari dei lavoratori anche mediante annotazione nelle cartelle sanitarie e di rischio, e curando le opportune misure di sicurezza per salvaguardare la segretezza delle informazioni trattate. Ciò, quale che sia il titolare del trattamento effettuato a cura del medico.

Alle predette cartelle il datore di lavoro non può accedere, dovendo soltanto concorrere ad assicurarne un'efficace custodia nei locali dell'amministrazione (anche in vista di possibili accertamenti ispettivi da parte dei soggetti istituzionalmente competenti) ma, come detto, "con salvaguardia del segreto professionale" [9].

Il datore di lavoro pubblico è tenuto, su parere del medico competente (o qualora quest'ultimo lo informi di anomalie imputabili all'esposizione a rischio), ad adottare le misure preventive e protettive per i lavoratori interessati; in questo specifico contesto il datore di lavoro può accedere al giudizio di idoneità del lavoratore allo svolgimento di date mansioni, anziché alle specifiche patologie accertate [10].

Il medico può farsi assistere da personale sanitario, anche dipendente dello stesso datore di lavoro pubblico, che deve essere designato quale incaricato del trattamento dei dati personali impartendo ad esso specifiche istruzioni per salvaguardare la segretezza delle informazioni trattate (art. 30 del Codice). In tal caso, a prescindere da quale sia il titolare del trattamento e dagli eventuali obblighi in tema di segreto d'ufficio, il medico competente deve predisporre misure idonee a garantire il rispetto del segreto professionale da parte dei propri collaboratori che non siano tenuti per legge al segreto professionale, mettendoli ad esempio a conoscenza di tali disposizioni e delle relative sanzioni (art. 10 del codice di deontologia medica del 16 dicembre 2006; art. 4 del codice deontologico per gli infermieri del maggio del 1999) [11].

4. Dati sensibili e rapporto di lavoro

Le pubbliche amministrazioni devono adottare maggiori cautele se le informazioni personali sono idonee a rivelare profili particolarmente delicati della vita privata dei propri dipendenti quali la salute, le abitudini sessuali, le convinzioni politiche, sindacali, religiose, filosofiche o d'altro genere e l'origine razziale ed etnica (art. 4, comma 1, lett. *d*), del Codice).

In linea generale il datore di lavoro pubblico può utilizzare informazioni sensibili relative al proprio personale in attuazione della normativa in materia di instaurazione e gestione di rapporti di lavoro di qualunque tipo, per finalità di formazione, nonché per concedere benefici economici e altre agevolazioni (artt. 112, 95 e 68 del Codice).

Come sopra ricordato, il datore di lavoro pubblico deve limitare il trattamento dei dati sensibili e giudiziari alle sole informazioni ed operazioni individuate e rese pubbliche con l'atto regolamentare adottato in conformità al parere del Garante (artt. 20, 21, 112 e 154 del Codice) [12].

Nel perseguire tali finalità occorre comunque rispettare i princìpi di necessità e di indispensabilità che impongono di ridurre al minimo l'utilizzo di dati personali e, quando non si possa prescindere dall'uso di informazioni personali sensibili o giudiziarie, di trattare dati solo in riferimento ai tipi di dati e di operazioni indispensabili in relazione alla specifica finalità di gestione del rapporto di lavoro (artt. 3 e 22 del Codice).

Scaduto il termine transitorio del 28 febbraio 2007, il trattamento da parte di un soggetto pubblico che non sia previsto da tali fonti normative è ora illecito e, oltre all'inutilizzabilità dei dati trattati, può comportare l'adozione di provvedimenti anche giudiziari di blocco o di divieto del trattamento (art. 154 del Codice; art. 3 d.l. 24 giugno 2004, n. 158, come modificato dalla l. 27 luglio 2004, n. 188; art. 11, commi 1, lett. a) e 2, del Codice) [13].

Resta ferma la possibilità per le amministrazioni che non abbiano eventualmente adottato i necessari atti regolamentari entro il suddetto termine, di provvedervi comunque con sollecitudine, al fine rendere leciti i trattamenti dei dati sensibili e giudiziari.

5. Comunicazione di dati personali

5.1. *Comunicazione.* Specifiche disposizioni legislative o regolamentari individuano i casi in cui l'amministrazione pubblica è legittimata a comunicare informazioni che riguardano i lavoratori a terzi, soggetti pubblici o privati (art. 19 del Codice).

Quando manca una tale previsione specifica non possono essere quindi comunicati dati personali del dipendente (ad esempio, quelli inerenti alla circostanza di un'avvenuta assunzione, allo status o alla qualifica ricoperta, all'irrogazione di sanzioni disciplinari, a trasferimenti del lavoratore come pure altre informazioni contenute nei contratti individuali di lavoro) a terzi quali associazioni (anche di categoria), conoscenti, familiari e parenti.

Devono ritenersi in linea generale lecite le comunicazioni a terzi di informazioni di carattere sensibile relative ad uno o più dipendenti, quando esse siano realmente indispensabili per perseguire le finalità di rilevante interesse pubblico connesse all'instaurazione e alla gestione di rapporti di lavoro da parte di soggetti pubblici di cui all'art. 112 del Codice. Tali comunicazioni possono avere ad oggetto dati individuati nei pertinenti atti regolamentari

dell'amministrazione e che siano in concreto indispensabili, pertinenti e non eccedenti in rapporto ai compiti e agli adempimenti che incombono al soggetto pubblico in qualità di datore di lavoro in base alla normativa sull'ordinamento del lavoro alle dipendenze delle amministrazioni pubbliche (artt. 20 e 22 del Codice) [14].

La disciplina di protezione dei dati consente inoltre al datore di lavoro pubblico di rendere conoscibili a terzi dati personali del dipendente in attuazione delle disposizioni che definiscono presupposti, modalità e limiti per l'esercizio del diritto d'accesso a documenti amministrativi (contenenti dati personali) [15] o che prevedono un determinato regime di conoscibilità per talune informazioni [16], ovvero in virtù di una delega conferita dall'interessato.

Oltre a designare i soggetti che possono venire lecitamente a conoscenza dei dati inerenti alla gestione del rapporto di lavoro, quali incaricati o responsabili del trattamento, il datore di lavoro deve adottare particolari cautele anche nelle trasmissioni di informazioni personali che possono intervenire tra i medesimi incaricati o responsabili nelle correnti attività di organizzazione e gestione del personale. In tali flussi di dati occorre evitare, in linea di principio, di fare superflui riferimenti puntuali a particolari condizioni personali riferite a singoli dipendenti, specie se riguardanti le condizioni di salute, selezionando le informazioni di volta in volta indispensabili, pertinenti e non eccedenti (artt. 11 e 22 del Codice) [17].

A tal fine, può risultare utile esplicitare delicate situazioni di disagio personale solo sulla base di espressioni generiche e utilizzando, in casi appropriati, codici numerici, come pure riportare tali informazioni -quale presupposto degli atti adottati- solo nei provvedimenti messi a disposizione presso gli uffici per eventuali interessati e controinteressati (limitandosi quindi a richiamarli anche nelle comunicazioni interne e indicando gli estremi o un estratto del loro contenuto) [18].

5.2 *Rapporti con le organizzazioni sindacali.* Le pubbliche amministrazioni possono comunicare a terzi in forma realmente anonima dati ricavati dalle informazioni relative a singoli o a gruppi di lavoratori: si pensi al numero complessivo di ore di lavoro straordinario prestate o di ore non lavorate nelle varie articolazioni organizzative, agli importi di trattamenti stipendiali o accessori individuati per fasce o qualifiche/livelli professionali, anche nell'ambito di singole funzioni o unità organizzative.

Sulla base delle disposizioni dei contratti collettivi, i criteri generali e le modalità inerenti a determinati profili in materia di gestione del rapporto di lavoro sono oggetto di specifici diritti di informazione sindacale preventiva o successiva.

Ad esclusione dei casi in cui il contratto collettivo applicabile preveda espressamente che l'informazione sindacale abbia ad oggetto anche dati nominativi del personale per verificare la corretta attuazione di taluni atti organizzativi [19], l'amministrazione può fornire alle organizzazioni sindacali dati numerici o aggregati e non anche quelli riferibili ad uno o più lavoratori individuabili [20]. É il caso, ad esempio, delle informazioni inerenti ai sistemi di valutazione dell'attività dei dirigenti, alla ripartizione delle ore di straordinario e alle relative prestazioni, nonché all'erogazione dei trattamenti accessori [21].

Resta disponibile per l'organizzazione sindacale anche la possibilità di presentare istanze di accesso a dati personali attinenti ad uno o più lavoratori su delega o procura (art. 9, comma 2, del Codice), come pure la facoltà di esercitare il diritto d'accesso a documenti amministrativi in materia di gestione del personale, nel rispetto delle condizioni, dei limiti e delle modalità previsti dalle norme vigenti e per salvaguardare un interesse giuridicamente rilevante di cui sia portatore il medesimo sindacato (artt. 59 e 60 del Codice) [22]. Il rifiuto, anche tacito, dell'accesso ai documenti amministrativi, è impugnabile presso il tribunale amministrativo regionale, la Commissione per l'accesso presso la Presidenza del Consiglio dei ministri o il difensore civico (artt. 25 e ss. l. 7 agosto 1990, n. 241; art. 6 d.P.R. 12 aprile 2006, n. 184).

L'amministrazione può anche rendere note alle organizzazioni sindacali informazioni personali relative alle ritenute effettuate a carico dei relativi iscritti, in conformità alle pertinenti disposizioni del contratto applicabile [23] e alle misure di sicurezza previste dal Codice (artt. 31-35).

5.3. *Modalità di comunicazione.* Fuori dei casi in cui forme e modalità di divulgazione di dati personali siano regolate specificamente da puntuali previsioni (*cfr.* art. 174, comma 12, del Codice), l'amministrazione deve utilizzare forme di comunicazione individualizzata con il lavoratore, adottando le misure più opportune per prevenire la conoscibilità ingiustificata di dati personali, in particolare se sensibili, da parte di soggetti diversi dal destinatario, ancorché incaricati di talune operazioni di trattamento (ad esempio, inoltrando le comunicazioni in plico chiuso o spillato; invitando l'interessato a ritirare personalmente la documentazione presso l'ufficio competente; ricorrendo a comunicazioni telematiche individuali).

L'utilizzo del *telefax* come mezzo di comunicazione è consentito sebbene, in taluni casi, specifiche disposizioni prevedano apposite modalità di inoltro delle comunicazioni, come, ad esempio, nell'ambito di procedimenti disciplinari [24]. Anche per il *telefax* si devono comunque adottare opportune cautele che favoriscano la conoscenza dei documenti da parte delle sole persone a ciò legittimate.

6. Diffusione di dati personali

La diffusione di dati personali riferiti ai lavoratori può avvenire quando è prevista espressamente da disposizioni di legge o di regolamento (artt. 4, comma 1, lett. *m*) e 19, comma 3, del Codice), anche mediante l'uso delle tecnologie telematiche (art. 3 d.lg. 7 marzo 2005, n. 82, recante il *"Codice dell'amministrazione digitale"*).

A parte quanto eventualmente previsto sul piano normativo per specifiche categorie di atti, l'amministrazione, sulla base di apposite disposizioni regolamentari può, infatti, valorizzare anche l'utilizzo di reti telematiche per mettere a disposizione atti e documenti contenenti dati personali (es. concorsi o a selezioni pubbliche) nel rispetto dei princìpi di necessità, pertinenza e non eccedenza (artt. 3 e 11, comma 1, lett. *d*), del Codice).

Occorre, poi, una specifica valutazione per selezionare le informazioni eventualmente idonee a rivelare lo stato di salute degli interessati, la cui diffusione è vietata (artt. 22, comma 8, del Codice). A tale divieto non è consentito derogare invocando generiche esigenze di pubblicità connesse alla trasparenza delle procedure in materia di organizzazione del personale e degli uffici, come quelle relative alla mobilità dei dipendenti pubblici [25]. Non è ad esempio consentito diffondere i nominativi degli aventi diritto al collocamento obbligatorio contenuti in elenchi e graduatorie, atteso che il divieto di diffusione dei dati idonei a rivelare lo stato di salute è ribadito espressamente dal Codice anche in relazione allo svolgimento delle attività di concessione di benefici ed agevolazioni previste dalla legge e dai regolamenti (art. 68, comma 3, del Codice) [26].

6.1 *Dati relativi a concorsi e selezioni.* Nel quadro delle attività delle pubbliche amministrazioni si procede comunque, di regola, alla pubblicazione di graduatorie e di esiti di concorsi e selezioni pubbliche.

Ad esempio, le graduatorie dei vincitori di concorsi per accedere agli impieghi nelle pubbliche amministrazioni o per attribuire specifici incarichi professionali devono essere pubblicate nel bollettino ufficiale della Presidenza del Consiglio dei ministri o dell'amministrazione interessata, dandone, se previsto, contestuale avviso sulla Gazzetta Ufficiale [27]. Un analogo regime di conoscibilità è previsto per le procedure di reclutamento dei professori universitari di ruolo e dei ricercatori, con riferimento alle informazioni contenute nelle relazioni riassuntive dei lavori svolti dalle commissioni giudicatrici per le valutazioni comparative e negli annessi giudizi individuali e collegiali espressi sui candidati [28].

La diffusione, che l'amministrazione può lecitamente porre in essere in base a specifiche previsioni legislative o regolamentari, deve avere ad oggetto solo i dati personali pertinenti e non eccedenti ai fini del corretto espletamento della procedura concorsuale e della sua rispondenza ai parametri stabiliti nel bando (elenchi nominativi ai quali vengano abbinati i risultati di prove intermedie, elenchi degli ammessi alle prove scritte o orali, punteggi riferiti a singoli argomenti di esame; punteggi totali ottenuti).

Non risulta lecito riportare negli atti delle graduatorie da pubblicare altre tipologie di informazioni non pertinenti quali, ad esempio, recapiti di telefonia fissa o mobile o il codice fiscale [29].

Anche in tale ambito i soggetti pubblici possono avvalersi di nuove tecnologie per facilitare le comunicazioni con gli interessati riguardanti concorsi o selezioni pubbliche, mediante, ad esempio, la ricezione *on-line* di domande di partecipazione a concorsi e selezioni, corredate di diversi dati personali. A tale proposito va rilevato che le previsioni normative che disciplinano la pubblicazione di graduatorie, esiti e giudizi concorsuali rendono, in linea generale, lecita l'operazione di diffusione dei relativi dati personali a prescindere dal mezzo utilizzato.

La disciplina sulla protezione dei dati personali regola (v. art. 19, c. 3, del Codice) la diffusione di tali informazioni in maniera tendenzialmente uniforme, sia che essa avvenga attraverso una pubblicazione cartacea, sia attraverso la messa a disposizione su Internet mediante una pagina *web* [30].

Va tuttavia evidenziato che le caratteristiche di Internet consentono a chiunque, per effetto dei comuni motori di ricerca esterni ai siti, reperire indiscriminatamente e in tempo reale un insieme consistente di informazioni personali rese disponibili in rete, più o meno aggiornate e di natura differente [31].

Nell'utilizzare tale strumento di diffusione occorre, quindi, prevedere forme adeguate di selezione delle informazioni che potrebbero essere altrimenti aggregate massivamente mediante un comune motore di ricerca esterno ai siti. Si pensi alle pagine *web* contenenti dati relativi a esiti, graduatorie e giudizi di valutazione, che in termini generali dovrebbero essere conosciute più appropriatamente solo consultando un determinato sito Internet, oppure attribuendo solo alle persone interessate una chiave personale di accesso (a vari dati relativi alla procedura, oppure solo a quelli che li riguardano), o predisponendo, nei siti istituzionali, aree ad accesso parimenti selezionato nelle quali possono essere riportate ulteriori informazioni accessibili anche ai controinteressati [32].

Ancorché, talvolta, la disciplina normativa di settore preveda espressamente forme specifiche e circoscritte di divulgazione (mediante, ad esempio, la sola messa a disposizione di documenti presso gli uffici o la sola affissione di atti in bacheche nei locali dell'amministrazione, ovvero mediante materiale affissione all'albo pretorio [33]),tali forme di pubblicazione non autorizzano, di per sé, a trasporre tutti i documenti contenenti dati personali così pubblicati in una sezione del sito Internet dell'amministrazione liberamente consultabile. Al tempo stesso, ciò non preclude all'amministrazione di riprodurre in rete alcuni dei predetti documenti, sulla base di una valutazione responsabile e attenta ai limiti posti dai princìpi di pertinenza e non eccedenza.

In ogni caso, è ovviamente consentita la diffusione in Internet di un avviso che indichi il periodo durante il quale determinati documenti sono consultabili presso l'amministrazione [34].

6.2 *Dati relativi all'organizzazione degli uffici, alla retribuzione e ai titolari di cariche e incarichi pubblici.* Alcuni specifici obblighi normativi -taluni dei quali si richiamano di seguito a titolo meramente esemplificativo- impongono ad amministrazioni pubbliche di rendere noti, attraverso i propri siti Internet, determinati dati personali concernenti i propri dipendenti (es. organigramma degli uffici con l'elenco dei nominativi dei dirigenti; elenco delle caselle di posta elettronica istituzionali attive). [35]

Tali dati, sebbene siano di fatto disponibili in Internet, sono utilizzabili da terzi (in particolare, gli indirizzi di posta elettronica) solo in relazione ad eventi, comunicazioni e scopi correlati alle funzioni istituzionali e al ruolo ricoperto dall'interessato all'interno dell'amministrazione. I medesimi dati non sono quindi utilizzabili liberamente da chiunque per inviare, ad esempio, comunicazioni elettroniche a contenuto commerciale o pubblicitario [36].

In virtù della disciplina sul riordino della dirigenza statale le amministrazioni dello Stato possono altresì diffondere in Internet i dati personali dei dirigenti inquadrati nei ruoli istituiti da ciascuna amministrazione (art. 23 d.lg. 30 marzo 2001, n. 165), nel rispetto dei princìpi di completezza, esattezza, aggiornamento, pertinenza e non eccedenza dei dati (art. 11 del Codice) [37].

Altre disposizioni di settore prevedono, inoltre, specifici regimi di pubblicità per talune informazioni personali concernenti le retribuzioni, i livelli stipendiali o le situazioni patrimoniali di titolari di cariche e incarichi pubblici.

A titolo meramente esemplificativo, si menziona il caso delle amministrazioni e degli organismi tenuti a pubblicare sui propri siti Internet i compensi e le retribuzioni degli amministratori delle società partecipate direttamente o indirettamente dallo Stato, dei dirigenti con determinato incarico (conferito ai sensi dell'art. 19, comma 6, del d.lg. 30 marzo 2001, n. 165), nonché dei consulenti, dei membri di commissioni e di collegi e dei titolari di qualsivoglia incarico corrisposto dallo Stato, da enti pubblici o da società a prevalente partecipazione pubblica non quotate in borsa [38].

Un ampio regime di conoscibilità è previsto da specifiche disposizioni legislative anche per i livelli stipendiali e le situazioni patrimoniali di parlamentari e consiglieri di enti locali, seppure mediante differenti modalità di diffusione [39]. Alcune disposizioni permettono inoltre al datore di lavoro pubblico di acquisire, ma non di pubblicare, taluni dati personali relativi alla situazione patrimoniale dei propri dirigenti e, se vi consentono, del coniuge e dei figli conviventi, previa idonea informativa sul trattamento che ne verrà effettuato (art. 13 del Codice). Le medesime disposizioni non consentono, tuttavia, alle amministrazioni di conoscere l'integrale contenuto delle dichiarazioni dei redditi, nelle quali possono essere contenute informazioni eccedenti rispetto alla ricostruzione della situazione patrimoniale degli interessati, alcune delle quali aventi –peraltro- anche natura "sensibile" (si pensi, ad esempio, ad alcune particolari tipologie di spese per le quali sono riconosciute apposite detrazioni d'imposta) [40].

6.3. *Atti in materia di organizzazione degli uffici.* Salvo che ricorra una delle ipotesi sopra richiamate o previste da specifiche disposizioni legislative o regolamentari, non è di regola lecito diffondere informazioni personali riferite a singoli lavoratori attraverso la loro pubblicazione in comunicazioni e documenti interni affissi nei luoghi di lavoro o atti e circolari destinati alla collettività dei lavoratori, come nelle ipotesi di informazioni riguardanti contratti individuali di lavoro, trattamenti stipendiali o accessori percepiti, assenze dal lavoro per malattia, ferie, permessi, iscrizione e/o adesione di singoli dipendenti ad associazioni.

In presenza di disposizioni legislative o regolamentari che prevedono forme di pubblicazione obbligatoria delle deliberazioni adottate dall'amministrazione [41] o degli atti conclusivi di taluni procedimenti amministrativi occorre, poi, valutare con attenzione le stesse tecniche di redazione dei provvedimenti e delle deliberazioni in materia di organizzazione del personale. Nel rispetto dell'obbligo di adeguata motivazione degli atti amministrativi [42] vanno pertanto selezionate le informazioni da diffondere alla luce dei princìpi di pertinenza e indispensabilità rispetto alle finalità perseguite dai singoli provvedimenti, anche in relazione al divieto di diffusione dei dati idonei a rivelare lo stato di salute (artt. 11 e 22 del Codice). Un'attenta valutazione, nei termini sopra richiamati, è indispensabile soprattutto quando vengono in considerazione informazioni sensibili o di carattere giudiziario: si pensi, ad esempio, agli atti in materia di concessione dei benefici previsti dalla legge 5 febbraio 1992, n. 104 e ai provvedimenti di irrogazione di sanzioni disciplinari o relativi a controversie giudiziarie nelle quali siano coinvolti singoli dipendenti [43].

Con specifico riferimento alle finalità di applicazione della disciplina in materia di concessione di benefici economici o di abilitazioni, ad esempio, il trattamento può comprendere la diffusione dei dati sensibili nei soli casi in cui ciò sia indispensabile per la trasparenza delle attività medesime, in conformità alle leggi, e per finalità di vigilanza e di controllo conseguenti alle attività medesime, fermo restando, comunque, il divieto di diffusione dei dati idonei a rivelare lo stato di salute (art. 68, comma 3, del Codice).

Ove costituiscano presupposto dei provvedimenti adottati, tali informazioni vanno riportate solo negli atti a disposizione negli uffici consultabili esclusivamente da interessati e controinteressati, omettendo quindi di dettagliarle nel corpo degli atti da pubblicare e richiamandone soltanto gli estremi e/o un estratto dei relativi atti d'ufficio.

6.4. *Cartellini identificativi.* Analogamente, determina un'ipotesi di diffusione dei dati personali l'esibizione degli stessi su cartellini identificativi, appuntati, ad esempio, sull'abito o sulla divisa del personale di alcune strutture della pubblica amministrazione o di concessionari pubblici, in attuazione di taluni atti amministrativi di natura organizzativa, a livello sia nazionale, sia locale [44].

Nell'ambito del lavoro alle dipendenze delle pubbliche amministrazioni i cartellini identificativi possono rappresentare un valido strumento per garantire trasparenza ed efficacia dell'azione amministrativa [45], nonché per migliorare il rapporto fra operatori ed utenti.

Nel selezionare i dati personali destinati ad essere diffusi attraverso i cartellini identificativi, le amministrazioni sono tenute a rispettare i princìpi di pertinenza e non eccedenza dei dati in rapporto alle finalità perseguite (art. 11 del Codice), specie in assenza di necessarie disposizioni di legge o regolamento che prescrivano l'adozione per determinati dipendenti di cartellini identificativi e ne individuino eventualmente anche il relativo contenuto.

In tali ipotesi, alla luce di specifiche esigenze di personalizzazione e di umanizzazione del servizio e/o di collaborazione da parte dell'utente può risultare giustificato, in casi particolari e con riferimento a determinate categorie di dipendenti, riportare nei cartellini elementi identificativi ulteriori rispetto alla qualifica, al ruolo professionale, alla fotografia o ad un codice identificativo quali, ad esempio, le loro generalità (si pensi alle prestazioni sanitarie in regime di ricovero ospedaliero e al rapporto fiduciario che si instaura tra il paziente e gli operatori sanitari coinvolti).

7. Impronte digitali e accesso al luogo di lavoro

Anche nell'ambito del pubblico impiego [46], non è consentito utilizzare in modo generalizzato sistemi di rilevazione automatica delle presenze dei dipendenti mediante la raccolta di dati biometrici, specie se ricavati dalle impronte digitali. I dati biometrici, per la loro peculiare natura, richiedono l'adozione di elevate cautele per prevenire possibili pregiudizi a danno degli interessati, con particolare riguardo a condotte illecite che determinino l'abusiva "ricostruzione" dell'impronta digitale, partendo dal modello di riferimento (*template*), e la sua ulteriore "utilizzazione" a loro insaputa.

7.1. *Princìpi generali.* Il trattamento dei dati personali relativi alla rilevazione dell'orario di lavoro è riconducibile alle finalità perseguite dai soggetti pubblici quali datori di lavoro legittimati ad accertare il rispetto dell'orario di lavoro mediante "forme di controlli obiettivi e di tipo automatizzato" [47] (e in taluni casi a garantire speciali livelli di sicurezza), ma deve essere effettuato nel pieno rispetto della disciplina in materia di protezione dei dati personali.

Il principio di necessità impone a ciascuna amministrazione titolare del trattamento di accertare se la finalità perseguita possa essere realizzata senza dati biometrici o evitando ogni eccesso nel loro utilizzo che ne comporti un trattamento sproporzionato (artt. 3 e 11 del Codice). Devono essere quindi valutati preventivamente altri sistemi, dispositivi e misure di sicurezza fisiche e logicistiche che possano assicurare una puntuale e attendibile verifica delle presenze e degli ingressi sul luogo di lavoro.

Resta in particolare privo di giuridico fondamento l'utilizzo di sistemi di rilevazione delle impronte digitali per verificare l'esatto adempimento di prestazioni lavorative, ove siano attivabili misure "convenzionali" non lesive dei diritti della persona quali, ad esempio, apposizioni di firme anche in presenza di eventuale personale incaricato, fogli di presenza o sistemi di timbratura mediante *badge* magnetico.

Di regola, non è pertanto consentito il trattamento di dati relativi alle impronte digitali per accertare le ore di lavoro prestate effettivamente dal personale dislocato anche in sedi distaccate o addetto a servizi esterni, con riferimento, ad esempio, all'esigenza di computare con sistemi oggettivi le turnazioni, l'orario flessibile, il recupero, i permessi, il lavoro straordinario, i buoni pasto, nonché di prevenire eventuali usi abusivi o dimenticanze del *badge*.

Non può desumersi alcuna approvazione implicita dal semplice inoltro al Garante di note relative a progetti di installazione di impianti di rilevazione di impronte digitali, cui eventualmente non segua un esplicito riscontro dell'Autorità.

7.2. *Casi particolari.* Di regola, sistemi di rilevazione di impronte digitali nel luogo di lavoro possono essere quindi attivati soltanto per particolari esigenze di controllo dell'accesso a speciali aree dei luoghi di lavoro in cui si debbano assicurare elevati e specifici livelli di sicurezza, in relazione a specifiche necessità quali, ad esempio, la destinazione dell'area interessata:

- allo svolgimento di attività aventi particolare carattere di segretezza, ovvero prestate da personale selezionato e impiegato in attività che comportano la necessità di trattare informazioni rigorosamente riservate (es. accesso a sale operative ove confluiscono segnalazioni afferenti alla sicurezza anticrimine; aree adibite ad attività inerenti alla difesa e alla sicurezza dello Stato; ambienti di torri di controllo aeroportuali);
- alla conservazione di oggetti di particolare valore o la cui disponibilità deve essere ristretta ad un numero circoscritto di dipendenti in quanto un loro utilizzo improprio può determinare una grave e concreta situazione di rischio per la salute e l'incolumità degli stessi o di terzi (es. ambienti ove sono custodite sostanze stupefacenti o psicotrope).

Nelle ipotesi sopramenzionate il trattamento di dati relativi alle impronte digitali è ammesso a condizione che:

- sia sottoposto con esito positivo –di regole, a seguito di un interpello del titolare [48] – alla verifica preliminare, che l'Autorità si riserva di effettuare ai sensi dell'art. 17 del Codice anche per determinate categorie di titolari o di trattamenti;
- venga effettuata preventivamente la notificazione al Garante (artt. 37, comma 1, lett. *a*) e 38 del Codice);
- non sia comunque registrata l'immagine integrale dell'impronta digitale, bensì solo il modello di riferimento da essa ricavato (*template*);
- tale modello non sia archiviato in una memoria centralizzata, bensì in un supporto posto nell'esclusiva disponibilità dell'interessato (*smart card* o dispositivo analogo) e privo di indicazioni nominative riferibili a quest'ultimo (essendo sufficiente attribuire a ciascun dipendente un codice individuale);
- sia fornita ai dipendenti interessati un'informativa specifica per il trattamento in questione (art. 13 del Codice).

8. Dati idonei a rivelare lo stato di salute

8.1. *Dati sanitari.* Il datore di lavoro pubblico deve osservare cautele particolari anche per il trattamento dei dati sensibili (artt. 4, comma 1, lett. *d*), 20 e 112 del Codice) e, segnatamente, di quelli idonei a rivelare lo stato di salute.

Nel trattamento di queste informazioni l'amministrazione deve rispettare anzitutto i princìpi di necessità e di indispensabilità, valutando specificamente il rapporto tra i dati sensibili e gli adempimenti derivanti da compiti e obblighi di volta in volta previsti dalla legge (artt. 20 e 22 del Codice). È importante valorizzare tali princìpi nell'applicare disposizioni di servizio e regolamenti interni precedenti alla disciplina in materia di protezione dei dati personali.

In tale quadro non risultano, ad esempio, lecite le modalità –utilizzate da amministrazioni militari e forze di polizia, a fini di organizzazione del lavoro e/o di turni di servizio– che prevedono la redazione di un elenco nominativo di ufficiali o agenti in licenza, recante:

- l'indicazione "per convalescenza" o "in aspettativa", per regolare l'accesso alla caserma del personale assente dal servizio [49];
- l'indicazione, su ordini di servizio o altri atti affissi nei luoghi di lavoro, i motivi giustificativi delle assenze del personale (utilizzando, ad esempio, diciture quali "a riposo medico").

Particolari accorgimenti per la gestione dei dati sensibili possono essere previsti anche da norme estranee al Codice in materia di protezione dei dati personali, ma volte comunque a contenere, nei limiti dell'indispensabile, i dati dei quali il datore di lavoro può venire a conoscenza

per instaurare e gestire il rapporto di lavoro [50]. La disciplina contenuta nel Codice deve essere quindi coordinata e integrata (*cfr.* punto 3.2.) con altre regole settoriali [51] o speciali [52].

8.2. *Assenze per ragioni di salute.* Riguardo al trattamento di dati idonei a rivelare lo stato di salute, la normativa sul rapporto di lavoro e le disposizioni contenute in contratti collettivi possono giustificare il trattamento dei dati relativi a casi di infermità che determinano un'incapacità lavorativa (temporanea o definitiva), con conseguente accertamento di condizioni di salute del lavoratore da parte dell'amministrazione di appartenenza [53], anche al fine di accertare l'idoneità al servizio, alle mansioni o allo svolgimento di un proficuo lavoro [54].

Tra questi ultimi può rientrare anche una informazione relativa all'assenza dal servizio per malattia, indipendentemente dalla circostanza che sia contestualmente indicata esplicitamente la diagnosi [55].

Non diversamente, il datore di lavoro può in vari casi trattare legittimamente dati sensibili relativi all'invalidità o all'appartenenza a categorie protette, nei modi e per le finalità prescritte dalla vigente normativa in materia (art. 112, comma 2, lett. *a*) del Codice) [56].

A tale riguardo va rilevata la sussistenza di specifici obblighi normativi nei riguardi del lavoratore per consentire al datore di lavoro di verificare le sue reali condizioni di salute nelle forme di legge [57]. Per attuare tali obblighi è ad esempio previsto che venga fornita all'amministrazione di appartenenza un'apposita documentazione a giustificazione dell'assenza, consistente in un certificato medico contenente la sola indicazione dell'inizio e della durata presunta dell'infermità: *cd.* "prognosi" [58]. In assenza di speciali disposizioni di natura normativa, che dispongano diversamente per specifiche figure professionali [59], il datore di lavoro pubblico non è legittimato a raccogliere certificazioni mediche contenenti anche l'indicazione della diagnosi [60].

Anche nei casi in cui la raccolta dei dati relativi alla diagnosi sia effettuata lecitamente sulla base di tali disposizioni, in conformità ai princìpi di proporzionalità e indispensabilità, non è consentito all'amministrazione di appartenenza trascrivere nei documenti caratteristici o matricolari del personale le indicazioni sulla prognosi e la diagnosi contenute nei certificati prodotti dall'interessato per giustificare le assenze dal servizio (artt. 11, comma 1, lett. *e*) e 22, comma 9, del Codice) [61]. A tale riguardo, va anzi rilevato che, qualora il lavoratore produca documentazione medica recante anche l'indicazione della diagnosi insieme a quella della prognosi, l'amministrazione (salvi gli speciali casi eventualmente previsti nei termini sopra indicati) deve astenersi dall'utilizzare ulteriormente tali informazioni (art. 11, comma 2, del Codice) invitando anche il personale a non produrne altri con le medesime caratteristiche [62].

In linea generale, all'esito delle visite di controllo sullo stato di infermità –effettuate da medici dei servizi sanitari pubblici (art. 5 l. 20 maggio 1970, n. 300) [63]–, il datore di lavoro pubblico è legittimato a conoscere i dati personali dei lavoratori riguardanti la capacità o l'incapacità al lavoro e la prognosi riscontrata, con esclusione di qualsiasi informazione attinente alla diagnosi [64].

In tale quadro, il datore di lavoro può, al fine di far valere i propri diritti in relazione a fenomeni di ritenuto assenteismo e di eventuale non veritiera certificazione sanitaria, redigere note informative, segnalazioni o denunce contenenti anche riferimenti circostanziati alle ragioni e alle modalità delle singole assenze e individuandone i destinatari nel rispetto dei princìpi di indispensabilità, pertinenza e non eccedenza [65].

Sulla base degli elementi acquisiti da segnalazioni e quesiti pervenuti all'Autorità, risulta giustificata, alla luce delle disposizioni contenute nei contratti collettivi, la conoscenza da parte dell'amministrazione di appartenenza di informazioni personali relative all'effettuazione di visite mediche, prestazioni specialistiche o accertamenti clinici, nonché alla presenza di patologie che richiedono terapie invalidanti [66], quando il dipendente richiede di usufruire del trattamento di malattia o di permessi retribuiti per le assenze correlate a tali esigenze.

8.3. *Denuncia all'Inail.* Per dare esecuzione ad obblighi di comunicazione relativi a dati sanitari, in taluni casi il datore di lavoro può anche venire a conoscenza delle condizioni di salute del lavoratore.

Tra le fattispecie più ricorrenti deve essere annoverata la denuncia all'istituto assicuratore (Inail) avente ad oggetto infortuni e malattie professionali occorsi ai lavoratori; essa, infatti, per espressa previsione normativa, deve essere corredata da specifica certificazione medica (artt. 13 e 53 d.P.R. n. 1124/1965).

In tali casi l'amministrazione, pur potendo conoscere la diagnosi, deve comunicare all'ente assicurativo solo le informazioni sanitarie relative o collegate alla patologia denunciata, anziché dati sulla salute relativi ad altre assenze che si siano verificate nel corso del rapporto di lavoro, la cui eventuale comunicazione sia eccedente e non pertinente –con la conseguente loro inutilizzabilità–, trattandosi di dati non rilevanti nel caso oggetto di denuncia (art. 11, commi 1 e 2, del Codice) [67].

8.4. *Visite medico-legali.* Le pubbliche amministrazioni possono trattare legittimamente dati idonei a rivelare lo stato di salute dei propri dipendenti, non solo per accertare, anche d'ufficio, attraverso le strutture sanitarie pubbliche competenti, la persistente idoneità al servizio, alle mansioni o allo svolgimento di un proficuo lavoro [68], ma anche per riconoscere la dipendenza da causa di servizio, per concedere trattamenti pensionistici di privilegio o l'equo indennizzo [69] ovvero per accertare, sempre per fini pensionistici, la sussistenza di stati invalidanti al servizio o di inabilità non dipendenti da causa di servizio (artt. 20 e 112, comma 2, lett. *d*) del Codice) [70].

Nel disporre tali accertamenti le amministrazioni possono comunicare ai collegi medici competenti i dati personali sensibili del dipendente dei quali dispongano, nel rispetto del principio di indispensabilità (art. 22, commi 1, 5 e 9) [71]; devono inoltre conformare il trattamento dei dati sanitari del lavoratore secondo modalità volte a prevenire violazioni dei diritti, delle libertà fondamentali e della dignità dell'interessato, anche in riferimento al diritto alla protezione dei dati personali (*cfr. par.* 4.3) [72].

Analoghi accorgimenti devono essere adottati dagli organismi di accertamento sanitario all'atto sia della convocazione dell'interessato a visita medico-collegiale, sia della comunicazione dell'esito degli accertamenti effettuati all'amministrazione di appartenenza del lavoratore, ed eventualmente all'interessato medesimo. In particolare, nel caso di accertamenti sanitari finalizzati ad accertare l'idoneità al servizio, alle mansioni o a proficuo lavoro del dipendente, alla luce del principio di indispensabilità, i collegi medici devono trasmettere all'amministrazione di appartenenza dell'interessato il relativo verbale di visita con la sola indicazione del giudizio medico-legale di idoneità, inidoneità o di altre forme di inabilità [73].

Qualora siano trasmessi dagli organismi di accertamento sanitario verbali recanti l'indicazione della diagnosi dell'infermità o della lesione che determinano un'incapacità lavorativa, i datori di lavoro non possono, comunque, utilizzare ulteriormente tali informazioni (art. 11, comma 2, del Codice).

8.5. *Abilitazioni al porto d'armi e alla guida.* In conformità alle norme sulle autorizzazioni di polizia per la detenzione ed il porto d'armi, le amministrazioni possono di regola trattare i dati relativi agli esiti delle visite medico-legali cui sottopongono i propri dipendenti per consentire l'adozione da parte degli uffici competenti dei provvedimenti sull'arma di servizio, ove si tratti di agenti di pubblica sicurezza, abilitati al porto di pistola [74].

La normativa di settore e le disposizioni contenute nei contratti collettivi non autorizzano, invece, le pubbliche amministrazioni a comunicare agli uffici competenti del Dipartimento per i trasporti terrestri informazioni idonee a rivelare lo stato di salute dei propri dipendenti, ancorché acquisite legittimamente, per consentire di verificare la persistenza in capo a questi ultimi dei requisiti fisici e psichici previsti dalla legge per il conseguimento della patente di guida [75]. Allo stato dell'attuale normativa tale attività comporta, infatti, un flusso di dati personali sensibili verso l'amministrazione dei trasporti che non risulta trovare una base di legittimazione in un'idonea disposizione normativa [76], né risulta altrimenti riconducibile alle finalità di rilevante interesse pubblico connesse alla gestione di rapporti di lavoro da parte dell'amministrazione di appartenenza dell'interessato (art. 112 del Codice) [77].

Siffatte operazioni di comunicazione non possono ritenersi lecite anche se effettuate da

forze armate e di polizia che, in base al Codice della strada, provvedano direttamente nei riguardi del personale in servizio all'individuazione e all'accertamento dei requisiti necessari alla guida dei veicoli in loro dotazione e al rilascio del relativo titolo abilitativo [78], attesa la diversità dei presupposti per il conferimento (o l'eventuale sospensione o ritiro) della patente militare rispetto a quella civile e la sfera di discrezionalità ad esse conferite [79].

8.6. *Altre informazioni relative alla salute.* Devono essere presi in considerazione altri casi nei quali può effettuarsi un trattamento di dati relativi alla salute del lavoratore (e anche di suoi congiunti), al fine di permettergli di godere dei benefici di legge: si pensi, ad esempio, alle agevolazioni previste per l'assistenza a familiari disabili, ai permessi retribuiti e ai congedi per gravi motivi familiari.

In attuazione dei princìpi di indispensabilità, pertinenza e non eccedenza, in occasione di istanze volte ad usufruire dei congedi a favore dei lavoratori con familiari disabili in situazione di gravità, l'amministrazione di appartenenza non deve venire a conoscenza di dati personali del congiunto portatore di handicap relativi alla diagnosi o all'anamnesi accertate dalle commissioni mediche indicate dall'art. 4 della l. 5 febbraio 1992, n. 104 [80]. A tal fine, infatti, il lavoratore deve presentare al datore di lavoro una certificazione dalla quale risulti esclusivamente l'accertata condizione di handicap grave per opera delle commissioni mediche di cui all'art. 1 della legge 15 ottobre 1990, n. 295 [81].

Diversamente, per usufruire di permessi o congedi per gravi infermità o altri gravi motivi familiari, il lavoratore è tenuto per legge a produrre alla propria amministrazione idonea documentazione medica attestante le gravi infermità o le gravi patologie da cui risultano affetti i propri familiari [82].

Allo stesso modo, il datore di lavoro può venire a conoscenza dello stato di tossicodipendenza di un proprio dipendente o di un familiare di questi, in caso di richieste di accesso o concorso a programmi riabilitativi o terapeutici con conservazione del posto di lavoro (senza retribuzione), atteso l'onere di presentare (nei termini prescritti dai contratti collettivi e dagli accordi di lavoro per il pubblico impiego) specifica documentazione medica al datore di lavoro [83].

9. Dati idonei a rivelare le convinzioni religiose

Analoghe cautele devono essere osservate nel trattamento di altre tipologie di informazioni sensibili relative al lavoratore, quali quelle idonee a rivelarne le convinzioni religiose. Il trattamento di queste informazioni deve ritenersi in via generale lecito soltanto ove risulti indispensabile per la gestione da parte dei soggetti pubblici del rapporto di lavoro e di impiego, e, in particolare, per consentire l'esercizio delle libertà religiose riconosciute ai lavoratori appartenenti a determinate confessioni, in conformità alle disposizioni di legge e di regolamento che regolano i rapporti tra lo Stato e le medesime confessioni.

Ad esempio, i dati sulle convinzioni religiose possono venire in considerazione per la concessione dei permessi per festività religiose su specifica richiesta dell'interessato motivata per ragioni di appartenenza a una determinata confessione [84]. Le convinzioni religiose potrebbero emergere, inoltre, in relazione al contesto in cui sono trattate o al tipo di trattamento effettuato, da alcune particolari scelte del lavoratore, rispondenti a determinati dettami religiosi, per il servizio di mensa eventualmente apprestato presso il luogo di lavoro.

Inoltre, in base alle specifiche norme sull'accesso agli impieghi nelle pubbliche amministrazioni e le modalità di svolgimento dei concorsi, dei concorsi unici e delle altre forme di assunzione nei pubblici impieghi, le prove del concorso scritte e orali non possono aver luogo, ai sensi della legge 8 marzo 1989, n. 101, nei giorni di festività religiose ebraiche rese note con decreto del Ministro dell'interno mediante pubblicazione nella *Gazzetta Ufficiale* della Repubblica, nonché nei giorni di festività religiose valdesi [85].

In tale quadro, pertanto, nel fissare il diario delle prove concorsuali per l'accesso ai pubblici impieghi, non risulta giustificata la raccolta sistematica e preventiva dei dati relativi alle convinzioni religiose dei predetti candidati [86] essendo sufficiente fissare le prove in giorni non coincidenti con dette festività.

(1) *Provv.* 23 novembre 2006, n. 53, in *www.garanteprivacy.it*, doc. *web* n. 1364099, e in *G.U.* 7 dicembre 2006, n. 285.

(2) Anche per le presenti linee-guida si è tenuto conto della Raccomandazione n. R (89) 2 del Consiglio d'Europa relativa alla protezione dei dati a carattere personale utilizzati ai fini dell'occupazione, del Parere n. 8/2001 sul trattamento dei dati personali nel contesto dell'occupazione, reso il 13 settembre 2001 dal Gruppo Art. 29 dei Garanti europei (in *http://ec.europa.eu*), nonché del Code of practice, *"Protection of workers' personal data"*, approvato dall'Organizzazione internazionale del lavoro (Ilo).

(3) Art. 2, comma 2, del Codice.

(4) Art. 2, comma 5, del Codice dell'amministrazione digitale (d.lg. 7 marzo 2005, n. 82 così come modificato dal d.lg. 4 aprile 2006, n. 159).

(5) L'organizzazione sindacale potrà a sua volta comunicare a terzi o diffondere i dati personali ottenuti dall'amministrazione soltanto previa acquisizione del consenso informato dei dipendenti interessati o di altro presupposto equipollente (art. 24 del Codice).

(6) *Provv.* 30 dicembre 2003, in *www.garanteprivacy.it*, doc. *web* n. 1085621.

(7) Note 9 dicembre 1997, ivi, doc. *web* nn. 30915 e 39785.

(8) *Cfr.* circolare Ispesl 3 marzo 2003, n. 2260.

(9) Art. 4, comma 8, d.lg. 19 settembre 1994, n. 626.

(10) *Provv.* 23 novembre 2006, in *www.garanteprivacy.it*, doc. *web* n. 1364099.

(11) *Provv.* 9 novembre 2005, in *www.garanteprivacy.it*, doc. *web* n. 1191411.

(12) A titolo di esempio, oltre ad alcuni regolamenti concernenti amministrazioni centrali (Ministero della difesa, d.m. 13 aprile 2006, n. 203, in *G.U.* 1° giugno 2006, n. 126; Ministero dell'interno, d.m. 21 giugno 2006, n. 244, in *G.U.* 9 agosto 2006, n. 184, S.O.; Ministero della pubblica istruzione, d.m. 7 dicembre 2006, n. 305, in *G.U.* 15 gennaio 2007, n. 11; Ministero delle infrastrutture, d.m. 9 febbraio 2007, n. 21, in *G.U.* 16 marzo 2007, n. 63; Ministero della giustizia, d.m. 12 dicembre 2006, n. 306, in *G.U.* 15 gennaio 2007, n. 11; Ministero dell'università e della ricerca, d.m. 28 febbraio 2007, n. 54, in *G.U.* 26 aprile 2007, n. 96), si segnalano taluni schemi tipo di regolamento relativi ad enti locali (in *www.garanteprivacy.it*, doc. *web* n. 1174532), comunità montane (doc. *web* n. 1182195) e province (doc. *web* n. 1175684).

(13) *Provv.* 30 giugno 2005, in *www.garanteprivacy.it*, doc. *web* n. 1144445.

(14) Art. 50 d.lg. 30 marzo 2001, n. 165 con riferimento alla trasmissione alla Presidenza del Consiglio dei ministri di informazioni nominative relative al personale che ha fruito di distacchi, permessi cumulativi sotto forma di distacco, aspettative e permessi per attività sindacale o per funzioni pubbliche elettive, al fine del contenimento, della trasparenza e della razionalizzazione delle aspettative e dei permessi sindacali nel settore pubblico.

(15) Artt. 59 e 60 del Codice. Si vedano anche gli artt. 22 e ss. l. 7 agosto 1990, n. 241; d.P.R. 12 aprile 2006, n. 184; art. 8 d.P.R. 27 giugno 1992, n. 352; artt. 10 e 43 d.lg. 18 agosto 2000, n. 267.

(16) *Cfr. par.* 5.1 e 5.2 delle presenti linee-guida.

(17) Relazione annuale per il 2004 del Garante, p. 81.

(18) *Provv.* 12 maggio 2005, in *www.garanteprivacy.it*, doc. *web* n. 1137798.

(19) *Cfr.* art. 6 Ccnl relativo al personale del comparto scuola del 24 luglio 2003.

(20) *Cfr.* art. 40, comma 4, d.lg. n. 165/2001 e art. 28 l. 20 maggio 1970, n. 300. Si vedano anche Corte cass. 17 aprile 2004, n. 7347; Corte d'appello Torino 16 luglio 2003 in Rivista giuridica del lavoro e della previdenza sociale, 2002, parte I, p. 116; *par.* 7 Raccomandazione del Consiglio d'Europa n. R (89)2; *par.* 10.10. del Code of practice dell'Ilo.

(21) Si veda, *ad es.*, art. 37 Ccnl del personale del comparto "ministeri" del 16 maggio 1995; art. 48 del Ccnl del personale del comparto "sanità" del 1° settembre 1995; art. 6 del Ccnl del personale del comparto "università" del 9 agosto 2000; art. 6, Ccnl del personale del comparto enti art. 70 d.lg. 165/2001 del 14 febbraio 2001; art. 37 Ccnl del personale del comparto delle "Istituzioni e degli enti di ricerca e sperimentazione" del 21 febbraio 2002; art. 7 Ccnl del personale del comparto delle regioni-autonomie locali del 6 luglio 1995; art. 7 Ccnl del personale del comparto regioni ed autonomie locali personale non dirigente del 1°aprile 1999.

(22) Si veda, *ad es.*, Consiglio di Stato sez. IV, 5 maggio 1998, n. 752; Tar Lombardia Milano, sez. I, 31 luglio 2002, n. 3261; Tar Emilia-Romagna 10 gennaio 2003, n. 16; Tar Calabria, sez. II, 11 luglio 2005, n. 1165; Commissione per l'accesso ai documenti amministrativi, pareri 6 luglio 2004, n. 8 e 28 giugno 2006, n. 51.

(23) Si vedano *ad es.*, art. 12 Ccnl del personale dirigente dell'area 1 del 5 aprile 2001; art. 11, Ccnl segretari comunali e provinciali del 16 maggio 2001; art. 13 Ccnl relativo al quadriennio normativo 1998-2001 del personale del comparto università.

(24) Artt. 111 e 104 d.P.R. 10 gennaio 1957, n. 3.

(25) *Cfr. Provv.* 27 febbraio 2002 (doc. *web* n. 1063639), con il quale il Garante ha vietato la diffusione di dati idonei a rivelare lo stato di salute riportati in una graduatoria dei trasferimenti affissa nella bacheca di un provveditorato agli studi.

(26) *Cfr.* Relazione annuale del Garante 2004, p. 83.

(27) Art. 15 d.P.R. 9 maggio 1994, n. 487; *v.* anche art. 4 d.P.R. 21 settembre 2001, n. 446; art. 18, comma 6, d.P.R. 27 marzo 2001, n. 220; art. 8 d.P.R. 28 luglio 2000, n. 271; art. 2 d.P.R. 28 luglio 2000, n. 272; art. 2 d.P.R. 28 luglio 2000, n. 270; art. 52, comma 2, r.d. 12 ottobre 1933, n. 1364.

(28) *Cfr.* art. 6 d.P.R. 23 marzo 2000, n. 117.

(29) *Provv.* 19 aprile 2007 recante *"Linee-guida in materia di trattamento di dati personali per finalità di pubblicazione e diffusione di atti e documenti di enti locali"*.

(30) *Cfr.* Comunicato stampa del Garante del 14 giugno 1999.

(31) *Cfr. Provv. 10* novembre 2004, doc. *web* n. 1116068; *cfr.* anche *Newsletter* 21-27 marzo 2005.

(32) *Cfr. Provv.* 19 aprile 2007, *cit.*

(33) *Cfr., ad es.*, art. 6, comma 6, d.P.R. n. 487/1994 con riferimento agli esiti delle prove intermedie dei concorsi per accedere agli impieghi nelle pubbliche amministrazioni e art. 25, comma 3, r.d. 22 gennaio 1934, n. 37, con riferimento all'elenco degli ammessi alla prove orali per l'abilitazione alla professione di avvocato.

(34) *Cfr. Provv.* 19 aprile 2007, *cit.*

(35) Art. 54 d.lg. 7 marzo 2005, n. 82.

(36) *Cfr. Provv.* 19 dicembre 2002, doc. *web* n. 1067231.

(37) *Cfr.* art. 23 d.lg. n. 165/ 2001 e artt. 1, comma 7 e 2, comma 4, d.P.R. 23 aprile 2004, n. 108.

(38) Art. 1, comma 593, l. 27 dicembre 2006, n. 296.

(39) *Cfr.* l. 5 luglio 1982, n. 441. Si veda anche *Newsletter* del Garante 4-10 giugno 2001 e Corte di giustizia delle Comunità europee, 20 maggio 2003, causa C-465/2000.

(40) *Cfr.* art. 17, comma 22, l. 15 maggio 1997, n. 127. Si veda anche Parere 8 giugno 1999, doc. *web* n. 40369. Analoga disciplina vige anche per magistrati, avvocati dello Stato e procuratori, professori e ricercatori universitari di livello dirigenziale od equiparato.

(41) *Cfr.* art. 10 e 124 d.lg. n. 267/2000.

(42) Art. 3, comma 3, l. n. 241/1990.

(43) *Cfr. Provv.* 27 febbraio 2002, doc. *web* 1063639, *Provv.* 9 dicembre 2003 e *Provv.* 17 aprile 2003, doc. *web* n. 1054640. Si vedano anche, con particolare riferimento alle deliberazioni degli enti locali, *Provv.* 19 aprile 2007 *cit.* e *Provv.* 25 gennaio 2007, doc. *web* n. 1386836.

(44) *Cfr.* parte seconda, 2.3.1, b.3), d.P.C.M. 21 dicembre 1992; art. 1.1. e all. n. 8 art. 61 d.P.C.M. 19 maggio 1995; parte seconda, 2.5.1, d.P.C.M. 30 dicembre 1998 art. 4.2.2, *provv.* Conferenza permanente per i rapporti tra lo Stato, le Regioni e le Province autonome di Trento e Bolzano 5 agosto 1999.

(45) Art.1 l. n. 241/1990.

(46) Per i dipendenti del settore privato *v. Provv.* 23 novembre 2006, doc. *web* n. 1364939.

(47) *Cfr.* art. 18 del Codice; art. 4 dell'accordo riguardante le tipologie degli orari di lavoro ai sensi dell'art. 19, comma 5, del Ccnl comparto ministeri del 16 maggio 1995, confermato dall'art. 26 del Ccnl del 12 giugno 2003. Si veda anche l'art. 17 Ccnl del comparto del personale delle regioni-autonomie locali del 6 luglio 1995, confermato dall'art. 45 del Ccnl del 22 gennaio 2004.

(48) Nell'interpello al Garante vanno specificate le caratteristiche tecnologiche delle apparecchiature utilizzate e le ragioni in base alle quali non si ritengono idonei, rispetto alle finalità da perseguire, altri sistemi o procedure che pongono minori pericoli o rischi per i diritti e le libertà fondamentali degli interessati.

(49) *Cfr. Provv.* 7 luglio 2004, doc. *web* n. 1068839.

(50) *Cfr.* artt. 8 e 38 l. n. 300/1970 e artt. 113 e 171 del Codice.

(51) Tra le quali, ad esempio, la richiamata disciplina contenuta nel d.lg. n. 626/1994 o nell'art. 5 della l. n. 300/1970 sugli accertamenti sanitari facoltativi.

(52) Si pensi ai divieti contenuti negli artt. 5 e 6 l. 5 giugno 1990, n. 135, in materia di Aids.

(53) *Cfr.* art. 5 l. n. 300/1970; si vedano anche le pertinenti disposizioni dei contratti collettivi relativi ai differenti comparti (art. 21, comma 10, Ccnl Comparto ministeri del 16 mag-

gio 1995; art. 17, comma 12, Ccnl relativo al personale del comparto scuola del 24 luglio 2003, già art. 49, lettera g) del Ccnl del 26 maggio 1999 e art. 23, comma 12, del Ccnl del 4 agosto 1995; art. 34, comma 10, Ccnl del personale non dirigente del comparto università, del 9 agosto 2000; art. 17, comma 11, Ccnl relativo al personale del comparto delle istituzioni e degli enti di ricerca e sperimentazione del 21 febbraio 2002; art. 11, comma 12, Ccnl relativo al personale del comparto delle istituzioni di alta formazione e specializzazione artistica e musicale del 16 febbraio 2005).

(54) *Cfr.* art. 5, comma 3, l. n. 300/1970, art. 15, d.P.R. n. 461/2001, art. 21, comma 3, Ccnl Comparto ministeri del 16 maggio 1995; art. 17, comma 3, Ccnl relativo al personale del comparto scuola del 24 luglio 2003, già art. 23, comma 3, del Ccnl del 4 agosto 1995; art. 34, comma 3, Ccnl del personale non dirigente del comparto università, del 9 agosto 2000; art. 17, comma 4, Ccnl relativo al personale del comparto delle istituzioni e degli enti di ricerca e sperimentazione del 21 febbraio 2002; art. 11, comma 3, Ccnl relativo al personale del comparto delle istituzioni di alta formazione e specializzazione artistica e musicale del 16 febbraio 2005. Dall'accertamento in questione può, inoltre, conseguire l'attribuzione all'interessato di altri incarichi o mansioni, oppure la risoluzione del rapporto di lavoro e la conseguente adozione degli atti necessari per riconoscere trattamenti pensionistici alle condizioni previste dalle disposizioni di settore. *Cfr.* art. 8 d.P.R. 27 febbraio 1991 n. 132 (Corpo forestale dello Stato); art. 129 d.lg. 30 ottobre 1992, n. 443 (Corpo di polizia penitenziaria); art. 15 d.P.R. 29 ottobre 2001, n. 461; art. 99 l. 22 dicembre 1975, n. 685; tossicodipendenza; art 5 d.P.R. 20 febbraio 2001, n. 114 (carriera diplomatica); art. 5 d.P.R. 23 maggio 2001, n. 316 (carriera prefettizia); art. 2 d.m. 30 giugno 2003, n. 198 (Polizia di Stato).

(55) *Cfr. Provv.* 7 luglio 2004, doc. *web* n. 1068839. *V.* pure il punto 50 della sentenza della Corte di giustizia delle Comunità europee 6 novembre 2003 C-101/01, Lindqvist.

(56) *Cfr.* l. n. 68/1999 citata e l. 29 marzo 1985, n. 113.

(57) *Provv.* 15 aprile 2004, doc. *web* n. 1092564; *Cfr.* art. 5 l. n. 300/1970; si vedano anche le pertinenti disposizioni dei contratti collettivi di lavoro applicabili ai diversi comparti come, ad esempio, l'art. 21 Ccnl comparto ministeri personale non dirigente del 16 maggio 1995.

(58) *Cfr.* art. 2 d.l. 30 dicembre 1979, n. 663, conv. in l., con mod., con l'art. 1 l. 29 febbraio 1980, n. 33, successivamente modificato dal comma 149 dell'art. 1 l. 30 dicembre 2004, n. 311.

(59) *Cfr.* art. 61 d.P.R. 28 ottobre 1985, n. 782 per il personale della Polizia di Stato.

(60) In tal senso si veda art. 17, comma 11, Ccnl relativo al personale del comparto scuola del 24 luglio 2003, già art. 49, lettera f) del Ccnl del 26 maggio 1999 e art. 23, comma 10, del Ccnl del 4 agosto 1995; art. 34,comma 9, Ccnl del personale non dirigente del comparto Università, del 9 agosto 2000; art. 17, comma 10, Ccnl relativo al personale del comparto delle istituzioni e degli enti di ricerca e sperimentazione del 21 febbraio 2002; art. 11, comma 11, Ccnl relativo al personale del comparto delle istituzioni di alta formazione e specializzazione artistica e musicale del 16 febbraio 2005.

(61) *Cfr.* art. 55 d.P.R. d.P.R. 10 gennaio 1957, n. 3 e art. 24 d.P.R. 3 maggio 1957 n. 686. Si veda anche *Provv.* 19 ottobre 2005, doc. *web* n. 1185148 con riferimento al servizio matricolare del Corpo della Guardia di finanza.

(62) *Cfr. par.* 1.1 delle presenti linee-guida.

(63) *Cfr.* art. 2 d.l. 30 dicembre 1979, n. 663, conv. in l., con mod., con l'art. 1, l. 29 febbraio 1980, n. 33 e mod. dal comma 149 dell'art. 1 l. 30 dicembre 2004, n. 311. Si veda anche art. 14, lett. q), l. 23 dicembre 1978, n. 833.

(64) Art. 5 d.l. 12 settembre 1983, n. 463 conv., con mod., in l. 11 novembre 1983, n. 638 e art. 6, comma 3, d.m. 15 luglio 1986.

(65) *Cfr. Provv.* 24 settembre 2001, doc. *web* n. 39460 e 28 settembre 2001, doc. *web* n. 41103.

(66) *Cfr.* art. 17 Ccnl del personale del comparto scuola stipulato il 24 luglio 2003; art. 17 Ccnl del personale del comparto delle istituzioni e degli enti di ricerca e sperimentazione stipulato il 21 febbraio 2002; art. 34 Ccnl del personale non dirigente del comparto Università stipulato il 9 agosto 2000; art. 23 Ccnl del personale del comparto sanità stipulato il 1° settembre 1995 e art. 11 Ccnl integrativo stipulato il 20 settembre 2001; art. 21 Ccnl del personale del comparto ministeri stipulato il 16 maggio 1995 e art. 6 Ccnl integrativo stipulato il 16 maggio 2001. Si vedano anche i chiarimenti forniti dall'Aran in data 20 gennaio 2003 in relazione ai quesiti B14 e B16, in *www.aranagenzia.it.*

(67) In tal senso *v.* il *Provv.* 15 aprile 2004, doc. *web* n. 1092564.

(68) Art. 5, comma 3, l. n. 300/1970; art. 15 d.P.R. 29 ottobre 2001, n. 461.

(69) *Cfr.* d.P.R. 29 dicembre 1973, n.1092 e d.P.R. 29 ottobre 2001, n. 461.

(70) *Cfr.* art. 2, comma 12, l. 8 agosto 1995, n. 335; art. 13, l. 8 agosto 1991, n. 274; d.P.R. 29 ottobre 2001, n. 461.
(71) Artt. 7, 9, comma 2 e 15, comma 1, d.P.R. n. 461/2001.
(72) *Cfr. Provv.* 23 luglio 2004, doc. *web* n. 1099216.
(73) Art. 4, commi 3 e 4, d.P.R. n. 461/2001.
(74) *Cfr. Provv.* 22 gennaio 2004, doc. *web* n. 1086280; *v.* anche, per altri profili, *Provv.* 15 gennaio 2004, doc. *web* n. 1054663 e Trib. Venezia 14 luglio 2004, n. 340.
(75) *Cfr.* artt. 119 e 128–130 d.lg. 30 aprile 1992, n. 285.
(76) *Cfr.* d.lg. 30 aprile 1992, n. 285 e d.P.R. 16 dicembre 1992, n. 495.
(77) *Cfr.* artt. 119 e 128–130 d.lg. 30 aprile 1992, n. 285. In merito, poi, alle comunicazioni di dati personali sensibili da parte delle aziende sanitarie alle commissioni mediche locali per le patenti di guida si guardi il *Provv.* del Garante del 28 giugno 2006, doc. *web* n. 1322833.
(78) Art. 138 d.lg. n. 285/1992.
(79) *Cfr.* art. 138, commi 4 e 12, d.lg. n. 285/1992. Si veda anche Cons. Stato sez. IV, 14 maggio 2001, n. 2648.
(80) *Cfr. Provv.* 21 marzo 2007, doc. *web* n. 1395821.
(81) *Cfr.* art. 33 l. 5 febbraio 1992, n. 104; art. 4, comma 2, l. 8 marzo 2000, n. 53 e artt. 33 e 42 d.lg. 26 marzo 2001, n. 151; si veda anche Cass. civ., 17 agosto 1998, n. 8068.
(82) Art. 4, l. 8 marzo 2000, n. 53 e d.m. 21 luglio 2000, n. 278.
(83) Art. 124, commi 1 e 2, d.P.R. n. 309/1990.
(84) Art. 4, comma 2, l. 8 marzo 1989, n. 101 recante "Norme per la regolazione dei rapporti tra lo Stato e l'Unione delle Comunità ebraiche italiane"; art. 17, comma 2, l. 22 novembre 1988, n. 516 recante *"Norme per la regolazione dei rapporti tra lo Stato e l'Unione italiana delle Chiese cristiane avventiste del 7° giorno"*.
(85) Art. 6, comma 2, d.P.R. 9 maggio 1994, n. 487 "Regolamento recante norme sull'accesso agli impieghi nelle pubbliche amministrazioni e le modalità di svolgimento dei concorsi, dei concorsi unici e delle altre forme di assunzione nei pubblici impieghi".
(86) *Cfr.* artt. 4, comma 2 e 5, l. n. 101/1989 e art. 17, comma 2, l. n. 516/1988 *cit.*

41 Linee-guida per trattamenti di dati relativi al rapporto banca-clientela (*) *25 ottobre 2007*

Registro delle deliberazioni
n. 53 del 25 ottobre 2007

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Nella riunione odierna, in presenza del prof. Francesco Pizzetti, presidente, del dott. Giuseppe Chiaravalloti, vice presidente, del dott. Mauro Paissan e del dott. Giuseppe Fortunato, componenti, e del dott. Giovanni Buttarelli, segretario generale;

Visto il d.lg. 30 giugno 2003, n. 196 (Codice in materia di protezione dei dati personali), anche in riferimento agli artt. 13, comma 5 e 154, comma 1, lett. *h*);

Esaminate le istanze (segnalazioni, reclami e quesiti) di clienti, associazioni di tutela dei consumatori e banche, pervenute in tema di trattamento di dati personali della clientela nell'ambito di rapporti bancari;

Viste le pronunce adottate in proposito dall'Autorità anche a seguito di ricorso di interessati;

Ritenuta l'opportunità di definire, in tale contesto, un quadro unitario di misure e di accorgimenti necessari e opportuni in grado di fornire ulteriori orientamenti utili per gli operatori economici e i clienti in ordine alle operazioni di trattamento di dati personali connesse all'attività bancaria, individuando, a tal fine, i comportamenti più appropriati da adottare;

Rilevata l'esigenza che tale quadro sia riassunto in alcune linee-guida, suscettibili di periodico aggiornamento, di cui verrà curata la pubblicità anche attraverso il sito Internet dell'Autorità (*www.garanteprivacy.it*);

Viste le osservazioni formulate dal segretario generale ai sensi dell'art. 15 del regolamento del Garante n. 1/2000;

Relatore il dott. Giuseppe Fortunato;

DELIBERA

1. di adottare le *"Linee-guida in materia di trattamento di dati personali della clientela in ambito bancario"*, di cui al documento che è allegato quale parte integrante della presente deliberazione (Allegato 1);
2. ai sensi dell'art. 13, comma 5, lett. *c*), del Codice che i titolari del trattamento che si rendano cessionari di sportelli bancari possano effettuare l'informativa prevista dal medesimo art. 13 secondo le modalità indicate al punto 3.7. delle allegate "Linee-guida", ovvero:
   a. mediante pubblicazione nella *Gazzetta Ufficiale* della Repubblica italiana dell'informativa avente le caratteristiche di cui all'art. 13, commi 1 e 2 del Codice;
   b. inoltre, mediante la successiva comunicazione agli interessati, alla prima occasione utile, degli elementi contenuti nello stesso art. 13, commi 1 e 2;
3. ai sensi dell'art. 143, comma 2, del Codice, di trasmettere al Ministero della Giustizia-Ufficio pubblicazione leggi e decreti copia del presente provvedimento,

(*) ***G.U.*** **23 novembre 2007, n. 273**
[doc. *web* n. 1457247]

unitamente alle menzionate "Linee-guida", per la loro pubblicazione sulla *Gazzetta Ufficiale* della Repubblica italiana.

Roma, 25 ottobre 2007

IL PRESIDENTE
Pizzetti

IL RELATORE
Fortunato

IL SEGRETARIO GENERALE
Buttarelli

LINEE-GUIDA IN MATERIA DI TRATTAMENTO DI DATI PERSONALI DELLA CLIENTELA IN AMBITO BANCARIO (*)

(Deliberazione n. 53 del 25 ottobre 2007)

Sommario

1. Premessa

1.1. *Scopo delle linee-guida.* Le presenti linee-guida, redatte tenendo conto di segnalazioni, reclami e quesiti pervenuti, nonché di precedenti decisioni adottate dall'Autorità, e suscettibili di periodico aggiornamento, mirano a fornire indicazioni di natura generale in relazione al trattamento di dati personali della clientela effettuato dalle banche al fine di garantire il rispetto dei princìpi in materia di protezione dei dai personali ai sensi del d.lg. 30 giugno 2003, n. 196 (Codice in materia di protezione dei dati personali).

(*) Le note sono in calce al testo

1.2. *Ambiti considerati.* Le presenti linee-guida trovano applicazione, nella misura compatibile con eventuali specificità del settore, anche alla corrispondente attività che, in base alla legge, può essere svolta da operatori postali nell'ambito dei servizi bancari e finanziari [1].

2. Il rispetto dei princìpi di protezione dei dati personali

2.1. *Liceità, pertinenza, trasparenza.* I dati personali, sempre che siano pertinenti e non eccedenti, possono essere trattati dalla banca solo per perseguire finalità legittime (quali, ad esempio, quella di dare esecuzione al rapporto contrattuale o soddisfare obblighi derivanti dalla legge) [2], osservando tutte le disposizioni della vigente disciplina in materia di protezione dei dati personali.

Il Codice prescrive, in particolare, che il trattamento avvenga:

- solo da parte di incaricati (nonché, se designati, dei responsabili) del trattamento e limitatamente alle istruzioni loro impartite [3];
- nel rispetto dei princìpi di necessità e di qualità dei dati, con riferimento all'esattezza e all'aggiornamento (artt. 3 e 11);
- informando preventivamente e adeguatamente gli interessati (art. 13) [4];
- chiedendo il loro consenso solo quando, tenendo anche conto della natura dei dati, non sia possibile avvalersi di uno dei presupposti equipollenti al consenso (artt. 23, 24, 26 e 43 del Codice);
- osservando, se si trattano dati sensibili o giudiziari, le prescrizioni contenute nelle autorizzazioni anche di carattere generale rilasciate dal Garante (artt. 26 e 27 del Codice);
- adottando le misure di sicurezza idonee a prevenire alcuni eventi (in particolare accessi e utilizzazioni indebite), in relazione ai quali la banca può essere chiamata a rispondere anche civilmente e penalmente (artt. 15, 31 ss., 167 e 169 del Codice).

2.2. *Principio di pertinenza e non eccedenza: dati identificativi della clientela.* Il principio di pertinenza dei dati deve essere osservato anche in relazione al trattamento di informazioni finalizzate a identificare i clienti in occasione dell'instaurazione del rapporto contrattuale o in sede di esecuzione di operazioni bancarie (quali, ad esempio, versamenti, pagamenti, altre disposizioni impartite dalla clientela e presentazioni per il pagamento di assegni o vaglia postali).

L'identificazione della clientela –che avviene, di regola, a seguito dell'esibizione di un documento di riconoscimento e, talvolta, anche acquisendone copia fotostatica (specie nei confronti di chi non sia cliente o comunque conosciuto dal personale della banca)– rappresenta un obbligo posto in capo agli istituti di credito da diverse norme e, in particolare, da quelle in materia di riciclaggio [5], nonché da quella secondo cui [6] *"le banche, la società Poste italiane Spa, gli intermediari finanziari, le imprese di investimento, gli organismi di investimento collettivo del risparmio, le società di gestione del risparmio, nonché ogni altro operatore finanziario, fatto salvo quanto disposto [...] per i soggetti non residenti, sono tenuti a rilevare e a tenere in evidenza i dati identificativi, compreso il codice fiscale, di ogni soggetto che intrattenga con loro qualsiasi rapporto o effettui, per conto proprio ovvero per conto o a nome di terzi, qualsiasi operazione di natura finanziaria ad esclusione di quelle effettuate tramite bollettino di conto corrente postale per un importo unitario inferiore a 1.500 euro".*

L'onere di identificare l'interessato ricade sugli istituti di credito anche in caso di presentazione all'incasso di assegni; in tale circostanza possono essere utilizzati, oltre a idonei elementi di valutazione (quali la conoscenza personale o un'eventuale documentazione previamente acquisita, per esempio all'atto dell'instaurazione del rapporto), i dati personali degli interessati contenuti in un documento di riconoscimento la cui esibizione può essere richiesta e i cui estremi possono essere annotati sul titolo medesimo o sulla documentazione interna relativa all'operazione [7].

Per tale trattamento, fatta salva l'osservanza dell'obbligo di informativa (fornita anche *una tantum* al cliente [8]), non è necessario richiedere il consenso dal momento che i dati sono trattati in base a un obbligo di legge o, comunque, per eseguire obblighi derivanti dal contratto o per adempiere a specifiche richieste dell'interessato (art. 24, comma 1, lett. *a*) e *b*), del Codice).

2.3. *Principio di pertinenza e non eccedenza: servizi resi telefonicamente e registrazione del contenuto delle chiamate.* Per particolari ordini e istruzioni della clientela la banca può registrare il contenuto di conversazioni telefoniche intercorse, anche per eventuali profili di prova e di tutela di diritti in caso di controversia. In tal senso provvedono anche specifiche discipline di settore, con particolare riferimento agli ordini di borsa.

Fuori di questi specifici casi può risultare altresì giustificato procedere ad analoghe registrazioni in relazione a concrete esigenze, come ad esempio per servizi di *telephone banking*.

In tutti questi casi, l'interessato deve essere informato in ordine a tali registrazioni ai sensi dell'art. 13 del Codice, in sede di conclusione del contratto o, al più tardi, all'inizio della prima conversazione telefonica.

Per le registrazioni e gli eventuali dati personali connessi, se conservati, devono essere adottate le misure di sicurezza volte a prevenirne l'accesso, l'alterazione o l'uso non consentito da parte di soggetti non legittimati; il contenuto delle conversazioni, al quale l'interessato può accedere ai sensi dell'art. 7 del Codice (v. infra punto 5.1.), non deve essere conservato per un tempo superiore a quello necessario per conseguire le finalità per le quali la registrazione è stata effettuata [9].

2.4. Principio di qualità dei dati e pagamenti mediante la procedura "rapporti interbancari diretti" (Rid). Nell'eseguire gli ordini di pagamento impartiti dal cliente nell'ambito di rapporti interbancari diretti (*cd.* procedura Rid) [10], la banca del debitore/interessato (*cd.* banca domiciliataria) deve verificare la completezza e l'esattezza dei dati trattati.

Posto che le informazioni necessarie a eseguire l'operazione (con particolare riferimento alle coordinate bancarie e al conto corrente sul quale effettuare l'addebito) possono essere raccolte presso il debitore anche a cura del creditore (ad esempio, il fornitore di un servizio) [11] e essere inviati successivamente alla banca domiciliataria tramite la banca di quest'ultimo (*cd.* banca assuntrice o di allineamento) [12], in tali fasi potrebbero verificarsi errori od omissioni.

È pertanto necessario che, in caso di discordanze o incongruenze nei dati trasmessi, vengano effettuati (a cura della banca domiciliataria o con la cooperazione del creditore) appropriati controlli preventivi, se necessario contattando il cliente prima di dare esecuzione all'ordine, al fine di garantire l'esattezza dei dati trattati e di prevenire l'eventuale addebito su conti diversi da quello individuato dal debitore.

3. Comunicazione dei dati personali

3.1. *Regole di protezione dei dati e cd. segreto bancario.* La comunicazione a terzi di dati personali relativi a un cliente è ammessa se lo stesso vi acconsente (art. 23 del Codice) o se ricorre uno dei casi in cui il trattamento può essere effettuato senza il consenso (art. 24 del Codice) [13].

Fuori dei casi di operazioni di comunicazione dei dati strumentali alle prestazioni richieste e ai servizi erogati (per le quali non è necessario ottenere il consenso degli interessati: art. 24, comma 1, lett. *b*), del Codice), gli istituti di credito e il personale incaricato dell'esecuzione delle operazioni bancarie di volta in volta richieste devono mantenere il riserbo sulle informazioni utilizzate.

3.2. *Comunicazioni indebite.* La comunicazione indebita di dati a terzi (che comporta gravi conseguenze anche sul piano della responsabilità civile e penale, alla luce degli artt. 15 e 167 del Codice) può avvenire per una pluralità di ragioni. Ciò può avvenire, a titolo meramente esemplificativo e tenendo in considerazione le tipologie di segnalazioni e ricorsi pervenuti all'Autorità, nei seguenti casi:

- per la mancata predisposizione di misure idonee a prevenire l'indebita conoscenza di informazioni personali da parte di terzi, ivi comprese le "distanze di cortesia" nei luoghi dedicati all'esecuzione di operazioni bancarie [14];
- per l'inosservanza delle istruzioni impartite agli incaricati del trattamento, come nel caso di telefonate o colloqui effettuati indebitamente ad alta voce in presenza di terzi [15];

- a seguito della comunicazione di informazioni bancarie a terzi che non siano in alcun modo autorizzati dall'interessato a porre in essere operazioni per suo conto o a conoscere il contenuto della relazione contrattuale in essere con la banca, come, ad esempio, nei confronti:
- del coniuge, cui venga consegnata documentazione bancaria riferita esclusivamente all'altro [16];
- di familiari, contattati talora telefonicamente per comunicazioni dirette ai clienti, ma il cui contenuto venga invece rivelato ingiustificatamente ai primi;
- di professionisti [17] o soggetti legati da un rapporto di lavoro con l'interessato;
- di terzi che, per errore nell'imbustamento o nella spedizione della corrispondenza, divengano destinatari di comunicazioni scritte aventi ad oggetto informazioni bancarie (ad esempio, di estratti conto);
- a seguito della comunicazione di informazioni bancarie presso recapiti non autorizzati, in modo da consentire a terzi di venire a conoscenza di dati riferiti all'interessato (ad esempio, in caso di comunicazioni via *fax*) [18];
- più in generale, per l'inosservanza di misure di sicurezza [19].

3.3. *Comunicazioni dovute o autorizzate.* In numerosi casi è possibile comunicare dati relativi alla clientela senza violare le rilevanti disposizioni in materia di protezione dei dati personali; altre comunicazioni sono anzi doverose in quanto richieste dalla legge. A titolo meramente esemplificativo possono menzionarsi i casi di:

- comunicazioni di informazioni personali per attuare la disciplina in materia di contrasto del riciclaggio [20]. A questo proposito merita rilevare che possono formare oggetto di trattamento da parte della banca non solo informazioni relative a singole transazioni economiche effettuate, ma un novero più ampio di dati personali necessari a rilevare l'anomalia di un'operazione in rapporto alle caratteristiche del cliente [21];
- comunicazioni, per finalità di contrasto finanziario al terrorismo [22] e alla commercializzazione di materiale pedopornografico [23], attualmente nei riguardi dell'Ufficio italiano dei cambi;
- comunicazioni di informazioni personali per l'accertamento e la repressione di violazioni tributarie, nei limiti previsti dalla legge [24]. In quest'ambito, possono essere ricomprese alcune ipotesi quali quelle contenute:
  - nell'ultima parte del menzionato art. 7, comma 6, d.P.R. n. 605/1973, secondo cui *"l'esistenza dei rapporti, nonché la natura degli stessi sono comunicate all'anagrafe tributaria, ed archiviate in apposita sezione, con l'indicazione dei dati anagrafici dei titolari, compreso il codice fiscale"*;
  - nell'art. 32, comma 7, del d.P.R. 29 settembre 1973, n. 600, in materia di disposizioni comuni sull'accertamento delle imposte sui redditi;
  - nella disciplina concernente le comunicazioni verso la *cd.* "anagrafe dei rapporti di conto e di deposito" [25];
- comunicazioni di informazioni, in conformità alla disciplina che regola la materia, alla Centrale rischi della Banca d'Italia [26] e al Servizio centralizzato di rilevazione dei rischi di importo contenuto (Cric) [27] e alla Centrale d'allarme interbancaria (in merito, *v.* infra punto 3.4.);
- comunicazioni (nelle forme previste dalla legge) nei confronti dell'autorità giudiziaria [28] e, nell'ambito di una procedura esecutiva, al creditore procedente (nel rispetto delle vigenti disposizioni in materia di pignoramento presso terzi: artt. 543 ss. c.p.c., come modificati dalla l. 24 febbraio 2006, n. 52) [29];
- comunicazioni a seguito di istanza di accesso alla documentazione bancaria ai sensi dell'art. 119 del testo unico delle leggi in materia bancaria e creditizia (Tub: d.lg. 1° settembre 1993, n. 385; *v.* infra punto 5.2.).

Possono, poi, formare oggetto di comunicazione ai gestori di sistemi (privati) di informazione creditizie, in conformità alla deliberazione del Garante n. 9 del 16 novembre 2004 [30], i dati personali (di contenuto *"negativo"*) necessari per effettuare i trattamenti in conformità al *"codice di deontologia e di buona condotta per i sistemi informativi gestiti da soggetti privati in tema di credito al consumo, affidabilità e puntualità nei pagamenti"* [31], se preceduti dal preavviso previsto (art. 4, comma 7, del codice di deontologia medesimo) [32].

Possono essere altresì comunicate lecitamente al soggetto garante alcune informazioni personali relative al debitore garantito, nella misura in cui le medesime siano pertinenti rispetto al rapporto di garanzia in essere [33].

3.4. Comunicazioni di dati personali alla Centrale d'allarme interbancaria. L'art. 36 del decreto legislativo n. 507/1999 concernente la depenalizzazione di alcuni reati minori, che ha introdotto nella legge 15 novembre 1990, n. 386 il nuovo art. 10-bis, ha previsto l'istituzione di un archivio informatizzato degli assegni bancari e postali e delle carte di pagamento (la *cd.* Centrale d'allarme interbancaria, di seguito Cai), la cui disciplina di dettaglio è contenuta nel d.m. 7 novembre 2001, n. 458 [34] e nel regolamento del Governatore della Banca d'Italia del 29 gennaio 2002 [35].

Dall'esame delle fattispecie presentate al Garante, anche a seguito dell'esercizio dei diritti previsti dall'art. 7 del Codice (nei confronti sia degli intermediari segnalanti, sia della Banca d'Italia, in qualità di titolari del trattamento) [36], emerge la necessità che gli enti segnalanti prestino la massima cautela nell'accertare l'esattezza e la completezza dei dati personali trattati prima di procedere alla segnalazione (art. 3, comma 2, d.m. n. 458/2001). Ciò, al fine di prevenire l'inserimento nella Cai di nominativi di vittime di furto d'identità (e, comunque, provvedendo con tempestività alle necessarie verifiche e alle eventuali cancellazioni, anche a seguito dell'esercizio del diritto d'accesso da parte dell'interessato) [37], come pure di soggetti che, pur avendo comunicato correttamente alla banca il furto o lo smarrimento di assegni (che devono formare oggetto di successiva e tempestiva segnalazione a cura degli enti segnalanti nel segmento "Pass" della Cai), vengano segnalati in tale archivio a seguito di un'abusiva negoziazione dei medesimi titoli (ad esempio, per mancanza di provvista o per emissione degli assegni in difetto di autorizzazione) [38].

Gli enti segnalanti, oltre a dover effettuare le operazioni di trattamento in modo lecito (osservando quindi anche la disciplina di settore che regola il complessivo funzionamento dell'archivio), devono comportarsi secondo correttezza (art. 11, comma 1, lett. a), del Codice) [39].

La segnalazione è lecita anche in caso di "richiamo" dell'assegno da parte della banca negoziatrice atteso che, nel caso di assegni emessi senza autorizzazione, l'illecito si perfeziona all'atto dell'emissione e, nel caso di assegni emessi senza provvista, al momento della presentazione al pagamento [40].

Limitatamente ai casi di mancato pagamento di un assegno per difetto di provvista (art. 9-*bis* legge n. 386/1990) [41], la segnalazione alla Cai non può essere effettuata se il debitore pone tempestivamente in essere i comportamenti analiticamente indicati all'art. 8 della legge n. 386/1990 [42]. Nel caso in esame, inoltre, l'iscrizione del traente nella Cai non può avvenire se la banca segnalante non ha inviato preventivamente un preavviso di revoca (ai sensi dell'art. 9-bis della legge n. 386/1990), dal ricevimento del quale devono decorrere almeno dieci giorni prima di provvedere all'iscrizione medesima.

Tali presupposti non ricorrono, invece, per quanto riguarda le revoche delle carte di pagamento nella Cai: alla luce della vigente disciplina, infatti, nessuno specifico rilievo è assegnato alla circostanza che l'obbligazione pecuniaria nascente dall'utilizzo di una carta di pagamento sia stata o meno successivamente adempiuta [43].

Le banche sono altresì tenute a segnalare nella Cai i casi di revoca delle carte di pagamento utilizzate per l'acquisto di materiale pedopornografico sulla rete Internet o su altre reti di comunicazioni [44].

3.5. *Benefondi.* Il *cd.* benefondi fa riferimento a una prassi interbancaria che prevede, nell'ambito della negoziazione di assegni tra banche per la realizzazione del credito portato dal titolo, la comunicazione dell'esistenza di una provvista sufficiente in relazione al pagamento di assegni da addebitare sul conto corrente del traente [45]. Le informazioni possono essere fornite dagli istituti di credito nel rispetto dei princìpi generali che la legge prevede per tutti i trattamenti di dati personali svolti dalle banche e secondo le indicazioni riportate nei modelli di informativa distribuiti alla clientela, nei quali può rientrare anche questo tipo di comunicazione alla banca mandataria per l'incasso.

La prassi del benefondi, tuttavia, deve trovare corretta attuazione: le informazioni devono essere fornite ai soli soggetti legittimati all'incasso o alla negoziazione dell'assegno, anziché a terzi non autorizzati; inoltre, le informazioni fornite dalla banca devono essere esatte, aggiornate e non eccedenti rispetto allo scopo per il quale il benefondi è utilizzato, che è relativo alla semplice informazione dell'esistenza o meno sul conto corrente del cliente della banca trattaria dei fondi necessari al pagamento dell'assegno [46].

3.6. *Comunicazione dei dati relativi alla clientela e cessione di sportelli bancari: esonero dall'obbligo di rendere l'informativa.* Un esame più approfondito, sotto i profili della comunicazione dei dati e dell'informativa da rendere alla clientela, merita la fattispecie della cessione di sportelli bancari: essa implica, di regola, limitatamente agli sportelli ceduti, il trasferimento dell'intero compendio di beni, rapporti giuridici attivi e passivi, oltre che dei rapporti contrattuali esistenti a favore della banca cessionaria.

In tale contesto sussistono, come analiticamente indicato di seguito, i presupposti per l'esonero dall'obbligo di rendere l'informativa per la banca cessionaria, la quale potrà pertanto utilizzare modalità più snelle per rendere edotta la clientela in ordine al trattamento dei dati personali correlato alla cessione degli sportelli;

a) *presupposti del trattamento*: bilanciamento degli interessi. La cessione di sportelli bancari, infatti, non esaurisce i propri effetti sul solo piano negoziale, ma determina in pari tempo la comunicazione di dati personali (riferibili, ad esempio, alla clientela, a fornitori, o connessi all'esecuzione del rapporto di lavoro del personale dipendente) dalla banca cedente alla cessionaria, con conseguente applicazione del Codice.
   In relazione a tali operazioni la banca cedente (titolare del trattamento) non provvede, di regola, ad acquisire il consenso degli interessati; deve pertanto verificarsi se sussista un altro fondamento per porre in essere la comunicazione.
   Come è noto, la cessione di innumerevoli rapporti attivi e passivi in corrispondenza del mutamento del centro di imputazione soggettiva dei medesimi (dalla banca cedente a quella cessionaria) trova una disciplina apposita e articolata nell'art. 58 del menzionato Tub, della quale è necessario tener conto in ragione dei riflessi che la stessa può spiegare rispetto ai profili di protezione dei dati personali [47].
   Detta disciplina, infatti, introduce modalità atte ad agevolare, snellendone gli adempimenti, la cessione in blocco di rapporti giuridici, riducendone i costi e preservando in pari tempo i legittimi interessi dei soggetti coinvolti, a vario titolo, nella cessione [48].
   Il *favor* che l'ordinamento riserva alle cessioni "in blocco" di rapporti giuridici in materia bancaria spiega effetti anche sul profilo accessorio della comunicazione dei dati personali che le medesime implicano. Stante la peculiare disciplina approntata dall'ordinamento all'art. 58 del Tub e attesa la natura dei dati trattati (di regola anagrafici o relativi a transazioni di natura economica), i diritti e il legittimo interesse dei soggetti ceduti in ordine al trattamento dei dati che li riguardano non risultano nel caso di specie prevalenti rispetto al legittimo interesse alla comunicazione della banca cedente. Ciò, anche in ragione dell'immutata finalità del trattamento dei dati oggetto della cessione.
   Deve quindi ritenersi integrata la fattispecie prevista nell'art. 24, comma 1, lett. *g*), del Codice sì che, per effetto del presente provvedimento, la comunicazione dei dati personali oggetto della cessione degli sportelli bancari deve ora ritenersi lecita (per le sole finalità sopra menzionate), limitatamente ai dati diversi da quelli sensibili, anche in assenza del consenso degli interessati;
b) *esonero dall'obbligo di rendere l'informativa.* Rispetto alle ipotesi di cessione di sportelli bancari regolata dall'art. 58 del Tub, il cessionario che raccoglie i dati presso il terzo (banca cedente) è comunque tenuto a rendere, al momento della registrazione dei dati, ai soggetti ceduti l'informativa sul trattamento (art. 13, comma 4, del Codice).
   L'informativa, se resa singolarmente a ciascun interessato con la tempistica richiesta dal menzionato art. 13, comma 4 (stante l'elevato numero di soggetti ceduti nelle menzionate operazioni), potrebbe risultare impossibile e, comunque, risulta comportare costi e oneri amministrativi manifestamente sproporzio-

nati rispetto al diritto tutelato, anche perché deve essere fornita in un contesto temporale circoscritto a innumerevoli soggetti, individuati ovvero individuabili per *relationem* grazie alla ricognizione degli sportelli oggetto dell'operazione.
Alla luce di ciò, in via generale e in relazione a ciascuna delle operazioni di cessione di sportelli bancari, il Garante, ai sensi dell'art. 13, comma 5, lett. *c*), del Codice, dichiara che l'impiego dei mezzi necessari a rendere l'informativa singolarmente a ciascuno degli interessati coinvolti nell'operazione risulta sproporzionato rispetto all'interesse che il precetto contenuto nel menzionato art. 13, comma 4, del Codice intende tutelare.
Per queste ragioni l'informativa può essere quindi resa nelle medesime forme previste, seppur a diverso fine, dall'art. 58 del Tub;

c) *misure appropriate.* Tuttavia, come già disposto in passato dall'Autorità [49], è necessario che venga assicurata comunque un'adeguata informativa a vantaggio degli interessati. Occorrono, quindi, misure appropriate a cura delle banche cessionarie che siano parte delle operazioni di cessione di sportelli bancari.

Ciò, dovrà essere assicurato mediante la pubblicazione dell'informativa contenente gli elementi previsti dall'art. 13, commi 1 e 2, del Codice sulla *Gazzetta Ufficiale* della Repubblica italiana, contestualmente alla pubblicazione dell'avviso previsto dal menzionato art. 58.

In applicazione del principio di semplificazione (art. 2 del Codice), i titolari del trattamento non dovranno presentare al Garante una richiesta preventiva di esonero dall'informativa. L'elevato livello di tutela degli interessati (art. 2 *cit.*) dovrà essere, comunque, garantito adottando anche l'ulteriore misura che risulta appropriata (art. 13, comma 5, lett. *c*), del Codice), di seguito indicata: i cessionari dovranno in ogni caso fornire direttamente ai soggetti ceduti gli elementi contenuti nell'art. 13, commi 1 e 2, del Codice, alla prima occasione utile successiva all'avvenuta cessione in blocco (ad esempio, in sede di invio dell'estratto conto). Tale modalità aggiuntiva favorisce una maggiore conoscibilità dell'avvenuta raccolta dei dati presso terzi ad opera della cessionaria [50].

4. Tutela dei propri diritti da parte della banca

L'istituto di credito può utilizzare in sede giudiziaria informazioni relative ai rapporti intrattenuti con la clientela per tutelare i propri diritti nelle controversie con gli interessati, non assumendo valore ostativo, in questa ipotesi, l'impegno di riservatezza assunto in relazione ai servizi prestati, che non può tradursi in un vincolo tale da produrre effetti lesivi nella sfera giuridica della stessa banca e in un limite all'esigenza di difesa giudiziaria dei propri diritti (*cfr.*, al riguardo, art. 24, comma 1, lett. *f*), del Codice).

Il cliente non può infatti pretendere dalla banca un comportamento che si risolva in una lesione dei propri interessi giuridicamente rilevanti e del proprio diritto di difesa.

Tuttavia, i dati che possono essere prodotti in giudizio devono essere solo quelli pertinenti all'esigenza di far valere o difendere un diritto dell'istituto di credito; si deve evitare, ad esempio, l'ingiustificata produzione di interi tabulati (*ad es.*, interi estratti conto) contenenti dati personali (a volte anche riferiti a terzi) non rilevanti per le citate finalità di difesa [51].

5. Esercizio dei diritti previsti dall'art. 7 del Codice

5.1. *Accesso ai dati.* L'art. 7 del Codice obbliga la banca (in qualità di titolare del trattamento) a fornire idoneo riscontro alle richieste di accesso avanzate dagli interessati con riferimento ai dati personali che li riguardano [52].

Tra questi devono essere annoverate anche tutte le informazioni personali relative alle operazioni effettuate dagli interessati, nonché quelle relative alle registrazioni telefoniche degli ordini di negoziazione dagli stessi impartiti [53], come pure le informazioni di carattere personale, eventualmente raccolte dalla banca nell'eseguire ordini di investimento della clientela e idonee a manifestarne obiettivi e propensione al rischio.

L'istanza presentata ai sensi degli artt. 7 e 8 del Codice comporta l'obbligo per la banca di estrapolare dai propri archivi e dai documenti effettivamente conservati i dati personali relativi all'interessato oggetto della richiesta, e di comunicarli allo stesso in modo intelligibile nei modi di cui all'art. 10 del Codice, fornendo se necessario i criteri e i parametri per la comprensione del significato di eventuali codici associati alle informazioni riferite all'interessato medesimo (art. 10, comma 6, del Codice) [54].

In particolare, nel caso in cui l'estrazione dei dati risulti particolarmente difficoltosa, la banca può fornire riscontro alla richiesta dell'interessato anche *"attraverso l'esibizione o la consegna in copia di atti e documenti contenenti i dati personali richiesti"* (art. 10, comma 4, del Codice) [55], ancorché la disciplina di protezione dei dati non preveda l'obbligo per il titolare del trattamento di esibire o di allegare copia di ogni singolo documento contenente i dati personali dell'interessato [56].

Il diritto di ottenere la comunicazione in forma intelligibile dei dati non riguarda dati personali relativi a terzi; tali dati, quindi, nel caso di consegna di copia di documentazione che li contenga, debbono essere oscurati [57].

L'esercizio da parte dell'interessato del diritto di accesso ai dati personali che lo riguardano e degli altri diritti previsti dall'art. 7 del Codice è gratuito, salva la previsione contenuta nell'art. 10, commi 7 e 8, del Codice che prevede la possibilità di chiedere all'interessato un contributo spese quando "si determina un notevole impiego di mezzi in relazione alla complessità o all'entità della richiesta" (art. 10, comma 8, del Codice).

5.2. *Accesso ai dati personali ex art. 7 del Codice e accesso alla documentazione bancaria ai sensi dell'art. 119 Tub.* Il diritto di accedere ai dati personali previsto dall'art. 7 del Codice deve essere distinto dal diritto di accesso alla documentazione bancaria previsto dall'art. 119 del Tub [58].

Va al riguardo considerato che quest'ultimo, a differenza di quanto previsto dagli artt. 7 ss. del Codice, riconosce al cliente, a colui che gli succede a qualunque titolo e a chi subentra nell'amministrazione dei suoi beni, il diritto di ottenere copia di atti o documenti bancari (sia che essi contengano dati personali relativi all'interessato, sia nel caso in cui ciò non accada) [59].

Tale diritto non prevede limitazioni rispetto all'ostensibilità delle informazioni contenute nella documentazione richiesta (ivi compresi dati personali relativi a terzi che dovessero esservi contenuti), neanche nelle forme di un parziale oscuramento delle informazioni stesse; il suo esercizio prevede il pagamento delle spese a carico del cliente.

5.3. *Accesso ai dati di defunti (art. 9 del Codice).* La disciplina in materia di protezione dei dati personali prevede che il diritto di accesso ai dati riferiti a persone decedute possa essere esercitato "da chi ha un interesse proprio, o agisce a tutela dell'interessato o per ragioni familiari meritevoli di protezione" (art. 9, comma 3, del Codice) legittimando i soggetti che si trovino in tali condizioni ad esercitare tale diritto in rapporto a dati personali (inclusi rapporti bancari e finanziari) riferibili al defunto.

L'istituto di credito è quindi tenuto a comunicare ai soggetti indicati al menzionato art. 9, comma 3, in modo chiaro e comprensibile informazioni riguardanti la consistenza patrimoniale del defunto, le movimentazioni bancarie, i saldi riferiti ai depositi "al portatore", anche se estinti da terzi successivamente al decesso, nonché la data in cui è stata disposta l'estinzione del conto o il trasferimento del saldo ad altro conto.

Non possono, invece, formare oggetto di comunicazione ai sensi degli artt. 7 e 9, comma 3, del Codice informazioni che siano dati personali riferibili non all'interessato, ma a terzi [60]. Ad esempio, non è conoscibile in base alle norme appena richiamate il nominativo del percettore del saldo di deposito, pur intestato al *de cuius*, in quanto tale informazione riguarda non il cliente deceduto, ma un terzo [61]; ciò, salvo che ricorra un'ipotesi di cointestazione con il defunto [62]. In base, poi, a tale disciplina non può essere accolta la differente richiesta di accesso a dati personali trattati da una banca e riferiti ad una persona

deceduta, se volta a conoscere specificamente e direttamente l'identità della persona delegata dal defunto ad effettuare determinate operazioni bancarie [63].

5.4. *Accesso ai dati personali ex art. 7 del Codice e fallito.* Il diritto d'accesso previsto dall'art. 7 del Codice può essere esercitato dal fallito il quale, per effetto del fallimento, è privato esclusivamente dell'amministrazione e della disponibilità dei suoi beni. A tale proposito, l'amministrazione del patrimonio fallimentare, rimessa al curatore, non riguarda i diritti di natura strettamente personale esercitabili senza autorizzazione o sostituzione del curatore [64].

(1) Allo stato, in base al d.P.R. 14 marzo 2001, n. 144 (Regolamento recante norme sui servizi di bancoposta), adottato in attuazione della delega contenuta nell'art. 40 della l. 23 dicembre 1998, n. 448.

(2) Così, al fine di elevare il grado di sicurezza di beni e persone (segnatamente, del personale dipendente degli istituti di credito e della clientela), le banche possono effettuare trattamenti di dati personali della clientela, nella forma della rilevazione di impronte digitali e di immagini, nei limiti e in conformità alle misure e agli accorgimenti stabiliti nel *Provv.* 27 ottobre 2005, in *www.garanteprivacy.it*, doc. *web* n. 1246675 (pubblicato in *G.U.* 22 marzo 2006, n. 68).

(3) *Cfr. Provv.* 8 marzo 2007, doc. *web* n. 1390872, relativo all'accesso per finalità personali (e non istituzionali) da parte di un funzionario di banca alla Centrale dei rischi della Banca d'Italia e al sistema centralizzato di rilevazione dei rischi di importo contenuto.

(4) In merito, vigente la l. n. 675/1996, l'Autorità (anche a seguito del *Provv.* 28 maggio 1997, doc. *web* n. 40425) si era espressa in termini generali in ordine al rispetto della disciplina relativa all'informativa da rendere alla clientela e alle modalità per raccogliere, ove necessario, il consenso degli interessati: *cfr. Newsletter* 10 maggio 1999.

(5) Allo stato, *v.* art. 2 d.l. 3 maggio 1991, n. 143 (Provvedimenti urgenti per limitare l'uso del contante e dei titoli al portatore nelle transazioni e prevenire l'utilizzazione del sistema finanziario a scopo di riciclaggio), convertito con modificazioni dalla l. 5 luglio 1991, n. 197 e successivamente modificato dal d.lg. 26 maggio 1997, n. 153. In merito *v.* pure Comitato di Basilea per la vigilanza bancaria (Dovere di diligenza delle banche nell'identificazione della clientela), ottobre 2001.

(6) Art. 7, comma 6, del d.P.R. 29 settembre 1973, n. 605, come sostituito, a far data dal 1° gennaio 2006, dal comma 332 dell'art. 1 l. 30 dicembre 2004, n. 311 e, infine, così modificato dal d.l. 30 settembre 2005, n. 203.

(7) *Cfr. Provv.* 27 ottobre 2005, doc. *web* n. 1189435, relativo all'identificazione della clientela.

(8) *Provv.* 28 maggio 1997, doc. *web* n. 40425, in materia di informativa e consenso della clientela nell'ambito dei servizi bancari.

(9) In merito *v.* le prescrizioni contenute nel regolamento Consob 1° luglio 1998 n. 11522 (Regolamento di attuazione del decreto legislativo 24 febbraio 1998, n. 58, concernente la disciplina degli intermediari), con particolare riguardo all'art. 69.

(10) In particolare, la prassi conosce tre tipologie di tale procedura corrispondenti a diverse esigenze commerciali: Rid utenze, Rid commerciale e Rid veloce. In merito *cfr.* circolare Abi n. 45, serie tecnica O del 6 giugno 1983; *v.* altresì le circolari Abi Prot. SP6014 del 22 dicembre 2004; prot. SP1453 del 29 marzo 2005; prot. SP/003076 del 17 giugno 2005.

(11) *Cfr.* circolari *citt.*

(12) Nel Rid utenze si consente al debitore che vuole avvalersi della procedura per il pagamento del servizio reso da una società di ricevere da quest'ultima il modulo di autorizzazione permanente all'addebito in conto corrente, consegnandolo poi alla banca presso la quale intrattiene il rapporto di conto corrente, ovvero al medesimo creditore; in quest'ultimo caso è essenziale che i moduli riportino *"la indicazione degli estremi completi dell'azienda di credito presso la quale è intrattenuto il conto da addebitare (intestazione e numero filiale, numero dell'agenzia, indirizzo)"*: *cfr.* punto 2.2.1 della menzionata circolare Abi del 6 giugno 1983.

(13) Ciò, è in armonia con il *cd.* segreto bancario che si sostanzia nel dovere della banca di mantenere il riserbo in ordine alle notizie riguardanti i clienti nell'esercizio dell'attività bancaria, rispetto alle quali sussiste un interesse, meritevole di tutela, a che non siano divulgate o comunicate a terzi. Peraltro, come è noto, la Corte costituzionale (sentenza 18 febbraio

1992, n. 51) ha precisato che la tutela del *cd.* segreto bancario, talora desunto dalla clausola generale di correttezza e di buona fede tra banca e cliente (artt. 1175 e 1375 c.c.), non può spingersi "fino al punto di fare di questo ultimo un ostacolo all'adempimento di doveri inderogabili di solidarietà, prima fra tutti quella di concorrere alle spese pubbliche in ragione della propria capacità contributiva (art. 53 della Costituzione), ovvero fino al punto di farne derivare il benché minimo intralcio all'attuazione di esigenze costituzionali primarie, come quelle connesse all'amministrazione della giustizia e, in particolare, alla persecuzione dei reati". *V.* altresì *Provv.* 23 maggio 2001, doc. *web* n. 39821.

(14) *V.* pure art. 1 del codice di comportamento del settore bancario e finanziario adottato dall'Abi.

(15) *Cfr. Provv.* 6 febbraio 2001, doc. *web* n. 40879.

(16) *Cfr. Provv.* 17 settembre 2002, doc. *web* n. 1066132.

(17) Tale è il caso in cui il dipendente aveva divulgato dati su rapporti di conto corrente e di deposito titoli ad un legale esterno il quale, a sua volta, li aveva utilizzati in una controversia tra il cliente e un terzo (si trattava, in concreto, di una controversia relativa all'aumento dell'assegno di divorzio): *Provv.* 23 maggio 2001, doc. *web* n. 39821.

(18) *Cfr. Provv.* 8 marzo 2007, doc. *web* n. 1390910.

(19) *Cfr.* con particolare riguardo allo svolgimento dell'attività di *e-banking*, il *Provv.* 11 novembre 2002, doc. *web* n. 1067296.

(20) *Cfr.* l. 5 luglio 1991, n. 197, con particolare riferimento all'art. 3, comma 7; si prendano pure in considerazione i successivi decreti ministeriali attuativi del 19 dicembre 1991, 26 giugno 1992, 7 luglio 1992 e 7 agosto 1992.

(21) Già nelle *"Indicazioni operative per la segnalazione di operazioni sospette"* (*cd.* "Decalogo"), impartite dalla Banca d'Italia il 12 gennaio 2001 ai sensi dell'art. 3 bis, comma 4, l. 5 luglio 1991, n. 197, punto 2.1. (*cd. know your customer rule*), si precisava che *"il dato oggettivo va integrato con le informazioni sul cliente in possesso dell'intermediario, nel valutare la coerenza e la compatibilità dell'operazione con il profilo economico-finanziario che deve essere dichiarato dal cliente medesimo; particolare attenzione è richiesta qualora risulti che il cliente non svolge attività con rilievo economico. Ingiustificate incongruenze rispetto alle caratteristiche soggettive del cliente e alla sua normale operatività -sia sotto il profilo quantitativo, sia sotto quello degli schemi contrattuali utilizzati- richiedono l'attivazione della procedura di segnalazione"* [...] *"Gli accertamenti bancari e gli ulteriori provvedimenti disposti dall'autorità giudiziaria (misure di prevenzione, rinvii a giudizio, ecc.) sono utilizzati per la valutazione sulla qualità dei clienti così come le notizie di stampa, specie se relative a operazioni finanziarie internazionali irregolari, le comunicazioni pubblicate nella Gazzetta Ufficiale e tutte le altre informazioni desumibili sulla piazza"*.

(22) *V.*, allo stato, il *Provv.* del 9 novembre 2001 dell'Ufficio italiano dei cambi (Istruzioni in materia di contrasto finanziario al terrorismo), pubblicato sulla *G.U.* 15 novembre 2001, n. 266; *v.* anche, in particolare, l'art. 10, d.lg. 22 giugno 2007, n. 109, recante *Misure per prevenire, contrastare e reprimere il finanziamento del terrorismo e l'attività dei Paesi che minacciano la pace e la sicurezza internazionale, in attuazione della direttiva 2005/60/Ce*, in *G.U.* 26 luglio 2007, n. 172 (disciplina che, tra l'altro, ha abrogato le previgenti pertinenti disposizioni del d.l. 12 ottobre 2001, n. 369, recante *"Misure urgenti per reprimere e contrastare il finanziamento del terrorismo internazionale"*).

(23) *Cfr.* art. 14-*quinquies*, comma 2, della l. 3 agosto 1998, n. 296 come novellata dall'art. 19 l. 6 febbraio 2006, n. 38, recante *Disposizioni in materia di lotta contro lo sfruttamento sessuale dei bambini e la pedopornografia anche a mezzo Internet.*

(24) *Cfr.*, ad esempio, art. 7, comma 6, d.P.R. 29 settembre 1973, n. 605 (*Disposizioni relative all'anagrafe tributaria e al codice fiscale dei contribuenti*) e art. 1, comma 3, d.l. 28 giugno 1990 n. 167 (*Rilevazione a fini fiscali di taluni trasferimenti da e per l'estero di denaro, titoli e valori*), in *G.U.* 30 giugno 1990, n. 151 (e convertito in legge, con modificazioni, dall'art. 1, comma 1, l. 4 agosto 1990, n. 227).

(25) Detta "anagrafe" è stata a suo tempo prevista dall'art. 20, comma 4, della l. 30 dicembre 1991, n. 413 e successivamente regolata con il d.m. 4 agosto 2000, n. 269; *v.* ora d.l. 4 luglio 2006, n. 223, conv., con mod., dalla legge 4 agosto 2006, n. 248); *Provv.* Agenzia delle entrate del 19 gennaio 2007 *"Modalità e termini di comunicazione dei dati all'Anagrafe Tributaria da parte degli operatori finanziari di cui all'art. 7, sesto comma, del decreto del Presidente della Repubblica 29 settembre 1973, n. 605, e successive modificazioni"*.

(26) *Cfr.* del. Cicr 29 marzo 1994; *Provv.* Banca d'Italia 10 agosto 1995; Circ. Banca d'Italia 11 febbraio 1991, n. 139 e successivi aggiornamenti.

(27) *V.*, in particolare, la del. Cicr 3 maggio 1999 (*Istituzione di un archivio accentrato per la rilevazione dei rischi di importo contenuto*) e le Istruzioni della Banca d'Italia (*Sistema centralizzato di rilevazione dei rischi di importo contenuto*), in G.U. 21 novembre 2000, n. 272.

(28) *Cfr.* Cass. 7 agosto 1990, n. 7953; Cass. 27 settembre 2001, n. 12093; Corte app. Milano, 22 luglio 1997, in Giust. civ. 1998, I, 246.

(29) L'art. 547 c.p.c. (come modificato dall'art. 12, l. n. 52/2006) dispone che il terzo pignorato (nel caso in esame, la banca) debba "specificare di quali cose o di quali somme è debitore o si trova in possesso", dandone comunicazione al creditore procedente in conformità alla previsione contenuta nell'art. 543, comma 2, n. 4 c.p.c.

(30) Del. 16 novembre 2004, n. 9 (Bilanciamento di interessi), in *G.U.* 23 dicembre 2004, n. 300 e doc. *web* n. 1070779.

(31) *V.* Del. 16 novembre 2004, n. 8, in *G.U.* 23 dicembre 2004, n. 300, come modificato dall'*errata corrige* pubblicata in *G.U.* 9 marzo 2005, n. 56 e doc. *web* n. 1070713.

(32) In tal senso *v. Provv.* 1° febbraio 2007, doc. *web* n. 1388576; *Provv.* 18 gennaio 2007, doc. *web* n. 1386384; *Provv.* 21 dicembre 2006, doc. *web* n. 1381657; *Provv.* 21 dicembre 2006, doc. *web* n. 1378189; *Provv.* 7 dicembre 2006, doc. *web* n. 1375058; *Provv.* 7 dicembre 2006, doc. *web* n. 1375085; *Provv.* 7 dicembre 2006, doc. *web* n. 1375133; *Provv.* 7 dicembre 2006, doc. *web* n. 1375150; *Provv.* 20 aprile 2006, doc. *web* n. 1289957.

(33) *Cfr. Provv.* 8 ottobre 2003, doc. *web* n. 1132740.

(34) *"Regolamento sul funzionamento dell'archivio informatizzato degli assegni bancari e postali e delle carte di pagamento"*, pubblicato nella *G.U.* 4 gennaio 2002, n. 3.

(35) Relativo al *"Funzionamento dell'archivio informatizzato degli assegni bancari e postali e delle carte di pagamento"*, pubblicato in *G.U.* 1° febbraio 2002, n. 27 e successive modificazioni.

(36) *Cfr.* art. 11 d.m. n. 458/2001 e art. 13 del regolamento della Banca d'Italia che (in conformità ai princìpi contenuti nell'art. 7 del Codice) prevede che l'interessato possa accedere "ai dati contenuti nell'archivio che lo riguardano tramite gli enti segnalanti privati o tramite le filiali della Banca d'Italia".

(37) *Cfr. Provv.* 25 gennaio 2007, doc. *web* n. 1387164, in relazione all'inserimento nella Cai di dati personali, solo in parte veritieri, connessi all'emissione di una carta di pagamento non richiesta, né ricevuta dall'interessato.

(38) *V.* in merito *Provv.* 21 dicembre 2006, doc. *web* n. 1378399 (e, in ordine alla medesima vicenda, il successivo *Provv.* 22 febbraio 2007, doc. *web* n. 1391891).

(39) Tenendo in considerazione le circostanze del tutto particolari che in concreto si erano presentate il Garante ha disposto la cancellazione dei dati dall'archivio Cai con *Provv.* 27 settembre 2004, doc. *web* n. 1069074.

(40) *Provv.* 15 febbraio 2005, doc. *web* n. 1148524, che richiama in tal senso le Istruzioni della Banca d'Italia del 21 novembre 2002 e dell'11 luglio 2003.

(41) *Provv.* 17 marzo 2005, doc. *web* n. 1152149.

(42) In particolare il debitore, entro sessanta giorni dalla data di scadenza del termine di presentazione del titolo (dall'art. 9-*bis*, l. n. 386/1990), deve provvedere tempestivamente al pagamento dell'assegno, degli interessi, della penale e delle eventuali spese per il protesto o per la constatazione equivalente e documentare, altresì, l'avvenuto pagamento nelle forme puntualmente previste dal menzionato art. 8: *cfr.* in merito *Provv.* 22 febbraio 2007, doc. *web* n. 1391942; *Provv.* 26 luglio 2005, doc. *web* n. 1157986; *Provv.* 3 marzo 2005, doc. *web* n. 1149190; sulla tempestività delle attività rimesse al debitore *cfr. Provv.* 26 ottobre 2006, doc. *web* n. 1367653.

(43) *Provv.* 19 ottobre 2005, doc. *web* n. 1192373; *Provv.* 4 ottobre 2004, doc. *web* n. 1102353; *v.* ora, d.m. 30 aprile 2007, n. 112 di attuazione della legge 17 agosto 2005, n. 166, recante *"Istituzioni di un sistema di prevenzione delle frodi sulle carte di pagamento"*.

(44) *Cfr.* art. 14-*quinquies*, commi 5 e 6, l. n. 296/1998, *cit.*

(45) In ordine a tale prassi la disciplina in materia di protezione dei dati personali non prevede alcun divieto: *cfr.* Parere del 30 novembre 1998 (in Bollettino n. 6, p. 85 e) doc. *web* n. 39416. In ordine alla legittimità del *cd.* benefondi *v.* pure Cass., 27 novembre 2003, n. 18118; Cass. 10 marzo 2000, n. 2742.

(46) *Cfr.* Cass. 6 giugno 2003, n. 9103; Cass. 7 febbraio 1979, n. 820.

(47) Banca d'Italia, Istruzioni di vigilanza per le banche, tit. III, cap. 5, assume che nella dizione "ramo di azienda", utilizzata dall'art. 58 Tub, possano comprendersi "le succursali e, in genere, ogni insieme omogeneo di attività operative, a cui siano riferibili rapporti contrattuali e di lavoro dipendente nell'ambito di una specifica struttura organizzativa".

(48) Ciò, è stato reso possibile con la previsione di modalità semplificate per notificare la cessione,

consentendo comunque al contraente ceduto di recedere entro tre mesi (dall'avvenuta cessione) dal contratto in presenza di giusta causa (analogamente alla disciplina relativa alla cessione d'azienda di cui all'art. 2558 c.c. e distaccandosi, invece, dai princìpi di diritto comune relativi alla cessione del contratto di cui all'art. 1406 c.c.).

(49) In materia di cessione in blocco e cartolarizzazione dei crediti: *Provv.* 18 gennaio 2007, doc. *web* n. 1392461.

(50) Analoga prescrizione è stata impartita dalla Banca d'Italia, seppure a diverso fine, in relazione alle operazioni di cessione in blocco di rapporti giuridici ai sensi dell'art. 58 del Tub: *cfr.* Banca d'Italia, *Istruzioni di vigilanza per le banche*, tit. III, cap. 5, sez. II.

(51) Restano comunque ferme, ai sensi dell'art. 160, comma 6, del Codice, le autonome determinazioni che l'autorità giudiziaria riterrà di adottare in ordine all'efficacia e all'utilizzabilità di atti e documenti nel procedimento giudiziario.

(52) A tal proposito si vedano altresì le indicazioni già fornite in termini generali dal Garante con le *"Linee-guida in materia di trattamento di dati personali di lavoratori per finalità di gestione del rapporto di lavoro alle dipendenze di datori di lavoro privati"* (Del. n. 53 del 23 novembre 2006), punto 9.

(53) *Cfr. Provv.* 23 luglio 2004, doc. *web* n. 1099411; *v.* pure, in relazione all'accesso a registrazioni di conversazioni aventi ad oggetto l'acquisto di pacchetti azionari, *Provv.* 19 giugno 2002, doc. *web* n. 1065269; *v.* pure *Provv.* 19 maggio 2005, doc. *web* n. 1151188.

(54) *Cfr. Provv.* 12 marzo 2004, doc. *web* n. 1090100.

(55) *Cfr.* tra gli altri *Provv.* 29 ottobre 2003, doc. *web* n. 1144061; *Provv.* 13 luglio 2006, doc. *web* n. 1321296; *Provv.* 20 dicembre 2006, doc. *web* n. 1376382; *Provv.* 16 marzo 2007, doc. *web* n. 1399446.

(56) *Provv.* 13 luglio 2006, doc. *web* n. 1320699; *Provv.* 23 marzo 2006, doc. n. 1285350.

(57) *Cfr. Provv.* 9 novembre 2006, doc. *web* n. 1366189; *Provv.* 10 dicembre 2003, doc. *web* n. 1053648; *Provv.* 27 dicembre 2001, doc. *web* n. 40987.

(58) *Provv.* 20 luglio 2006, doc. *web* n. 1322844.

(59) *Provv.* 28 settembre 2006, doc. *web* n. 1349798; *Provv.* 1° giugno 2005, doc. *web* n. 1139982; *Provv.* 1° giugno 2005, doc. *web* n. 1139991.

(60) In tal senso *cfr. Provv.* 20 maggio 2004, doc. *web* n. 1098787; Cass., 12 maggio 2006, n. 11004; Circ. n. 229 del 21 aprile 1999, p. 18 e ss.

(61) *Provv.* 27 aprile 2000, doc. *web* n. 1113611.

(62) In tal caso, con *Provv.* 3 aprile 2002, doc. *web* n. 1065256, si è affermato che *"il diritto di accesso ai dati personali conferisce* [...] l*a possibilità di acquisire piena cognizione di tutte le informazioni personali detenute dalla Cassa, permettendo allo stesso di comprendere il loro contenuto, anche attraverso il chiaro richiamo alle generalità dei cointestatari predetti (dati che lo stesso de cuius avrebbe avuto a suo tempo il diritto di conoscere)"*; *v.* pure *Provv.* 8 ottobre 2003, doc. *web* n. 1053855.

(63) *Provv.* 13 novembre 2003, doc. *web* n. 1053654.

(64) Per precedenti in materia *v. Provv.* 9 marzo 2006, doc. *web* n. 1268821, con richiami ulteriori a Cass., 23 luglio 1994, n. 6873 e Cass. 21 aprile 1997, n. 3400; *v.* pure artt. 31, 42 e ss. r.d. n. 267/1942, come modificato, allo stato, dal d.lg. 9 gennaio 2006, n. 5.

42 Linee-guida del Garante per posta elettronica e Internet nel rapporto di lavoro (*)
1 marzo 2007

Registro delle deliberazioni
n. 13 del 1 marzo 2007

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

In data odierna, in presenza del prof. Francesco Pizzetti, presidente, del dott. Giuseppe Chiaravalloti, vice presidente, del dott. Giuseppe Fortunato e del dott. Mauro Paissan, componenti, e del dott. Giovanni Buttarelli, segretario generale;

Visti i reclami, le segnalazioni e i quesiti pervenuti riguardo ai trattamenti di dati personali effettuati da datori di lavoro riguardo all'uso, da parte di lavoratori, di strumenti informatici e telematici;

Vista la documentazione in atti;

Visti gli artt. 24 e 154, comma 1, lett. *b*) e *c*) del Codice in materia di protezione dei dati personali (d.lg. 30 giugno 2003, n. 196);

Viste le osservazioni formulate dal segretario generale ai sensi dell'art. 15 del regolamento del Garante n. 1/2000;

Relatore il dott. Mauro Paissan;

PREMESSO

1. Utilizzo della posta elettronica e della rete Internet nel rapporto di lavoro

1.1. *Premessa*

Dall'esame di diversi reclami, segnalazioni e quesiti è emersa l'esigenza di prescrivere ai datori di lavoro alcune misure, necessarie o opportune, per conformare alle disposizioni vigenti il trattamento di dati personali effettuato per verificare il corretto utilizzo nel rapporto di lavoro della posta elettronica e della rete Internet.

Occorre muovere da alcune premesse:

a) compete ai datori di lavoro assicurare la funzionalità e il corretto impiego di tali mezzi da parte dei lavoratori, definendone le modalità d'uso nell'organizzazione dell'attività lavorativa, tenendo conto della disciplina in tema di diritti e relazioni sindacali;

b) spetta ad essi adottare idonee misure di sicurezza per assicurare la disponibilità e l'integrità di sistemi informativi e di dati, anche per prevenire utilizzi indebiti che possono essere fonte di responsabilità (artt. 15, 31 ss., 167 e 169 del Codice);

c) emerge l'esigenza di tutelare i lavoratori interessati anche perché l'utilizzazione dei predetti mezzi, già ampiamente diffusi nel contesto lavorativo, è destinata ad un rapido incremento in numerose attività svolte anche fuori della sede lavorativa;

d) l'utilizzo di Internet da parte dei lavoratori può infatti formare oggetto di analisi, profilazione e integrale ricostruzione mediante elaborazione di log file della navigazione *web* ottenuti, ad esempio, da un *proxy server* o da un altro strumento di registrazione delle informazioni. I servizi di posta elettronica sono parimenti suscettibili (anche attraverso la tenuta di *log file* di traffico *e-mail* e l'archiviazione di messaggi) di controlli che possono giungere fino alla conoscenza da parte del datore di lavoro (titolare del trattamento) del contenuto della corrispondenza;

e) le informazioni così trattate contengono dati personali anche sensibili riguardanti lavoratori o terzi, identificati o identificabili. [1]

(*) *G.U.* 10 marzo 2007, n. 58
[doc. *web* n. 1387522]
Le note sono in calce al testo

1.2. *Tutela del lavoratore*

Le informazioni di carattere personale trattate possono riguardare, oltre all'attività lavorativa, la sfera personale e la vita privata di lavoratori e di terzi. La linea di confine tra questi ambiti, come affermato dalla Corte europea dei diritti dell'uomo, può essere tracciata a volte solo con difficoltà [2].

Il luogo di lavoro è una formazione sociale nella quale va assicurata la tutela dei diritti, delle libertà fondamentali e della dignità degli interessati garantendo che, in una cornice di reciproci diritti e doveri, sia assicurata l'esplicazione della personalità del lavoratore e una ragionevole protezione della sua sfera di riservatezza nelle relazioni personali e professionali (artt. 2 e 41, secondo comma, Cost.; art. 2087 cod. civ.; *cfr.* altresì l'art. 2, comma 5, Codice dell'amministrazione digitale (d.lg. 7 marzo 2005, n. 82), riguardo al diritto ad ottenere che il trattamento dei dati effettuato mediante l'uso di tecnologie telematiche sia conformato al rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato) [3].

Non a caso, nell'organizzare l'attività lavorativa e gli strumenti utilizzati, diversi datori di lavoro hanno prefigurato modalità d'uso che, tenendo conto del crescente lavoro in rete e di nuove tariffe di traffico forfettarie, assegnano aree di lavoro riservate per appunti strettamente personali, ovvero consentono usi moderati di strumenti per finalità private.

2. Codice in materia di protezione dei dati e discipline di settore

2.1. *Principi generali*

Nell'impartire le seguenti prescrizioni il Garante tiene conto del diritto alla protezione dei dati personali, della necessità che il trattamento sia disciplinato assicurando un elevato livello di tutela delle persone, nonché dei principi di semplificazione, armonizzazione ed efficacia (artt. 1 e 2 del Codice). Le prescrizioni potranno essere aggiornate alla luce dell'esperienza e dell'innovazione tecnologica.

2.2. *Discipline di settore*

Alcune disposizioni di settore, fatte salve dal Codice, prevedono specifici divieti o limiti, come quelli posti dallo Statuto dei lavoratori sul controllo a distanza (artt. 113, 114 e 184, comma 3, del Codice; artt. 4 e 8 l. 20 maggio 1970, n. 300).

La disciplina di protezione dei dati va coordinata con regole di settore riguardanti il rapporto di lavoro e il connesso utilizzo di tecnologie, nelle quali è fatta salva o richiamata espressamente (art. 47, comma 3, lett. *b*) Codice dell'amministrazione digitale) [4].

2.3. *Princìpi del Codice*

I trattamenti devono rispettare le garanzie in materia di protezione dei dati e svolgersi nell'osservanza di alcuni cogenti princìpi:

a) il principio di necessità, secondo cui i sistemi informativi e i programmi informatici devono essere configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi in relazione alle finalità perseguite (art. 3 del Codice; *par.* 5.2);

b) il principio di correttezza, secondo cui le caratteristiche essenziali dei trattamenti devono essere rese note ai lavoratori (art. 11, comma 1, lett. *a*), del Codice). Le tecnologie dell'informazione (in modo più marcato rispetto ad apparecchiature tradizionali) permettono di svolgere trattamenti ulteriori rispetto a quelli connessi ordinariamente all'attività lavorativa. Ciò, all'insaputa o senza la piena consapevolezza dei lavoratori, considerate anche le potenziali applicazioni di regola non adeguatamente conosciute dagli interessati (*v. par.* 3);

c) i trattamenti devono essere effettuati per finalità determinate, esplicite e legittime (art. 11, comma 1, lett. *b*), del Codice: *par.* 4 e 5), osservando il principio di pertinenza e non eccedenza (*par.* 6). Il datore di lavoro deve trattare i dati *"nella misura meno invasiva possibile"*; le attività di monitoraggio devono essere svolte solo da soggetti preposti (*par.* 8) ed essere *"mirate sull'area di rischio, tenendo conto della normativa sulla protezione dei dati e, se pertinente, del principio di segretezza della corrispondenza"* (*Parere* n. 8/2001, *cit.*, punti 5 e 12).

3. Controlli e correttezza nel trattamento

3.1. *Disciplina interna*

In base al richiamato principio di correttezza, l'eventuale trattamento deve essere ispirato ad un canone di trasparenza, come prevede anche la disciplina di settore (art. 4, secondo comma, Statuto dei lavoratori; allegato VII, *par.* 3 d.lg. n. 626/1994 e successive integrazioni e modificazioni in materia di *"uso di attrezzature munite di videoterminali"*, il quale esclude la possibilità del controllo informatico *"all'insaputa dei lavoratori"*) [5].

Grava quindi sul datore di lavoro l'onere di indicare in ogni caso, chiaramente e in modo particolareggiato, quali siano le modalità di utilizzo degli strumenti messi a disposizione ritenute corrette e se, in che misura e con quali modalità vengano effettuati controlli. Ciò, tenendo conto della pertinente disciplina applicabile in tema di informazione, concertazione e consultazione delle organizzazioni sindacali.

Per la predetta indicazione il datore ha a disposizione vari mezzi, a seconda del genere e della complessità delle attività svolte, e informando il personale con modalità diverse anche a seconda delle dimensioni della struttura, tenendo conto, ad esempio, di piccole realtà dove vi è una continua condivisione interpersonale di risorse informative.

3.2. *Linee-guida*

In questo quadro, può risultare opportuno adottare un disciplinare interno redatto in modo chiaro e senza formule generiche, da pubblicizzare adeguatamente (verso i singoli lavoratori, nella rete interna, mediante affissioni sui luoghi di lavoro con modalità analoghe a quelle previste dall'art. 7 dello Statuto dei lavoratori, *ecc.*) e da sottoporre ad aggiornamento periodico.

A seconda dei casi andrebbe ad esempio specificato:

- se determinati comportamenti non sono tollerati rispetto alla "navigazione" in Internet (*ad es.*, il *download* di *software* o di *file* musicali), oppure alla tenuta di *file* nella rete interna;
- in quale misura è consentito utilizzare anche per ragioni personali servizi di posta elettronica o di rete, anche solo da determinate postazioni di lavoro o caselle oppure ricorrendo a sistemi di *webmail*, indicandone le modalità e l'arco temporale di utilizzo (*ad es.*, fuori dall'orario di lavoro o durante le pause, o consentendone un uso moderato anche nel tempo di lavoro);
- quali informazioni sono memorizzate temporaneamente (*ad es.*, le componenti di *file* di *log* eventualmente registrati) e chi (anche all'esterno) vi può accedere legittimamente;
- se e quali informazioni sono eventualmente conservate per un periodo più lungo, in forma centralizzata o meno (anche per effetto di copie di *back up*, della gestione tecnica della rete o di *file* di *log*);
- se, e in quale misura, il datore di lavoro si riserva di effettuare controlli in conformità alla legge, anche saltuari o occasionali, indicando le ragioni legittime –specifiche e non generiche– per cui verrebbero effettuati (anche per verifiche sulla funzionalità e sicurezza del sistema) e le relative modalità (precisando se, in caso di abusi singoli o reiterati, vengono inoltrati preventivi avvisi collettivi o individuali ed effettuati controlli nominativi o su singoli dispositivi e postazioni);
- quali conseguenze, anche di tipo disciplinare, il datore di lavoro si riserva di trarre qualora constati che la posta elettronica e la rete Internet sono utilizzate indebitamente;
- le soluzioni prefigurate per garantire, con la cooperazione del lavoratore, la continuità dell'attività lavorativa in caso di assenza del lavoratore stesso (specie se programmata), con particolare riferimento all'attivazione di sistemi di risposta automatica ai messaggi di posta elettronica ricevuti;
- se sono utilizzabili modalità di uso personale di mezzi con pagamento o fatturazione a carico dell'interessato;
- quali misure sono adottate per particolari realtà lavorative nelle quali debba essere rispettato l'eventuale segreto professionale cui siano tenute specifiche figure professionali;
- le prescrizioni interne sulla sicurezza dei dati e dei sistemi (art. 34 del Codice, nonché Allegato B), in particolare regole 4, 9, 10).

3.3. *Informativa (art. 13 del Codice)*

All'onere del datore di lavoro di prefigurare e pubblicizzare una *policy* interna rispetto al corretto uso dei mezzi e agli eventuali controlli, si affianca il dovere di informare comunque gli interessati ai sensi dell'art. 13 del Codice, anche unitamente agli elementi indicati ai punti 3.1. e 3.2..

Rispetto a eventuali controlli gli interessati hanno infatti il diritto di essere informati preventivamente, e in modo chiaro, sui trattamenti di dati che possono riguardarli.

Le finalità da indicare possono essere connesse a specifiche esigenze organizzative, produttive e di sicurezza del lavoro, quando comportano un trattamento lecito di dati (art. 4, secondo comma, l. n. 300/1970); possono anche riguardare l'esercizio di un diritto in sede giudiziaria.

Devono essere tra l'altro indicate le principali caratteristiche dei trattamenti, nonché il soggetto o l'unità organizzativa ai quali i lavoratori possono rivolgersi per esercitare i propri diritti.

4. Apparecchiature preordinate al controllo a distanza

Con riguardo al principio secondo cui occorre perseguire finalità determinate, esplicite e legittime (art. 11, comma 1, lett. *b*), del Codice), il datore di lavoro può riservarsi di controllare (direttamente o attraverso la propria struttura) l'effettivo adempimento della prestazione lavorativa e, se necessario, il corretto utilizzo degli strumenti di lavoro (*cfr.* artt. 2086, 2087 e 2104 cod. civ.).

Nell'esercizio di tale prerogativa occorre rispettare la libertà e la dignità dei lavoratori, in particolare per ciò che attiene al divieto di installare *"apparecchiature per finalità di controllo a distanza dell'attività dei lavoratori"* (art. 4, primo comma, l. n. 300/1970), tra cui sono certamente comprese strumentazioni *hardware* e *software* mirate al controllo dell'utente di un sistema di comunicazione elettronica.

Il trattamento dei dati che ne consegue è illecito, a prescindere dall'illiceità dell'installazione stessa. Ciò, anche quando i singoli lavoratori ne siano consapevoli [6].

In particolare non può ritenersi consentito il trattamento effettuato mediante sistemi *hardware* e *software* preordinati al controllo a distanza, grazie ai quali sia possibile ricostruire –a volte anche minuziosamente– l'attività di lavoratori. È il caso, ad esempio:

- della lettura e della registrazione sistematica dei messaggi di posta elettronica ovvero dei relativi dati esteriori, al di là di quanto tecnicamente necessario per svolgere il servizio *e-mail*;
- della riproduzione ed eventuale memorizzazione sistematica delle pagine *web* visualizzate dal lavoratore;
- della lettura e della registrazione dei caratteri inseriti tramite la tastiera o analogo dispositivo;
- dell'analisi occulta di *computer* portatili affidati in uso.

Il controllo a distanza vietato dalla legge riguarda l'attività lavorativa in senso stretto e altre condotte personali poste in essere nel luogo di lavoro [7]. A parte eventuali responsabilità civili e penali, i dati trattati illecitamente non sono utilizzabili (art. 11, comma 2, del Codice) [8].

5. Programmi che consentono controlli "indiretti"

5.1. Il datore di lavoro, utilizzando sistemi informativi per esigenze produttive o organizzative (*ad es.*, per rilevare anomalie o per manutenzioni) o, comunque, quando gli stessi si rivelano necessari per la sicurezza sul lavoro, può avvalersi legittimamente, nel rispetto dello Statuto dei lavoratori (art. 4, comma 2), di sistemi che consentono indirettamente un controllo a distanza (*cd.* controllo preterintenzionale) e determinano un trattamento di dati personali riferiti o riferibili ai lavoratori [9]. Ciò, anche in presenza di attività di controllo discontinue [10].

Il trattamento di dati che ne consegue può risultare lecito. Resta ferma la necessità di rispettare le procedure di informazione e di consultazione di lavoratori e sindacati in rela-

zione all'introduzione o alla modifica di sistemi automatizzati per la raccolta e l'utilizzazione dei dati [11], nonché in caso di introduzione o di modificazione di procedimenti tecnici destinati a controllare i movimenti o la produttività dei lavoratori [12].

5.2. *Principio di necessità*

In applicazione del menzionato principio di necessità il datore di lavoro è chiamato a promuovere ogni opportuna misura, organizzativa e tecnologica volta a prevenire il rischio di utilizzi impropri (da preferire rispetto all'adozione di misure "repressive") e, comunque, a "minimizzare" l'uso di dati riferibili ai lavoratori (artt. 3, 11, comma 1, lett. *d*) e 22, commi 3 e 5, del Codice; aut. gen. al trattamento dei dati sensibili n. 1/2005, punto 4).

Dal punto di vista organizzativo è quindi opportuno che:

- si valuti attentamente l'impatto sui diritti dei lavoratori (prima dell'installazione di apparecchiature suscettibili di consentire il controllo a distanza e dell'eventuale trattamento);
- si individui preventivamente (anche per tipologie) a quali lavoratori è accordato l'utilizzo della posta elettronica e l'accesso a Internet [13];
- si determini quale ubicazione è riservata alle postazioni di lavoro per ridurre il rischio di un loro impiego abusivo.

Il datore di lavoro ha inoltre l'onere di adottare tutte le misure tecnologiche volte a minimizzare l'uso di dati identificativi (*cd. privacy enhancing technologies* - PETs). Le misure possono essere differenziate a seconda della tecnologia impiegata (*ad es.*, posta elettronica o navigazione in Internet).

a) Internet: la navigazione web

Il datore di lavoro, per ridurre il rischio di usi impropri della "navigazione" in Internet (consistenti in attività non correlate alla prestazione lavorativa quali la visione di siti non pertinenti, l'*upload* o il *download* di *file*, l'uso di servizi di rete con finalità ludiche o estranee all'attività), deve adottare opportune misure che possono, così, prevenire controlli successivi sul lavoratore. Tali controlli, leciti o meno a seconda dei casi, possono determinare il trattamento di informazioni personali, anche non pertinenti o idonei a rivelare convinzioni religiose, filosofiche o di altro genere, opinioni politiche, lo stato di salute o la vita sessuale (art. 8 l. n. 300/1970; artt. 26 e 113 del Codice; *Provv.* 2 febbraio 2006, *cit.*).

In particolare, il datore di lavoro può adottare una o più delle seguenti misure opportune, tenendo conto delle peculiarità proprie di ciascuna organizzazione produttiva e dei diversi profili professionali:

- individuazione di categorie di siti considerati correlati o meno con la prestazione lavorativa;
- configurazione di sistemi o utilizzo di filtri che prevengano determinate operazioni –reputate inconferenti con l'attività lavorativa– quali l'*upload* o l'accesso a determinati siti (inseriti in una sorta di *black list*) e/o il *download* di *file* o *software* aventi particolari caratteristiche (dimensionali o di tipologia di dato);
- trattamento di dati in forma anonima o tale da precludere l'immediata identificazione di utenti mediante loro opportune aggregazioni (*ad es.*, con riguardo ai *file* di *log* riferiti al traffico *web*, su base collettiva o per gruppi sufficientemente ampi di lavoratori);
- eventuale conservazione nel tempo dei dati strettamente limitata al perseguimento di finalità organizzative, produttive e di sicurezza.

b) *Posta elettronica*

Il contenuto dei messaggi di posta elettronica –come pure i dati esteriori delle comunicazioni e i *file* allegati– riguardano forme di corrispondenza assistite da garanzie di segretezza tutelate anche costituzionalmente, la cui *ratio* risiede nel proteggere il nucleo essenziale della dignità umana e il pieno sviluppo della personalità nelle formazioni sociali; un'ulteriore protezione deriva dalle norme penali a tutela dell'inviolabilità dei segreti (artt. 2 e 15 Cost.; Corte cost. 17 luglio 1998, n. 281 e 11 marzo 1993, n. 81; art. 616, quarto comma, c.p.; art. 49 Codice dell'amministrazione digitale) [14].

Tuttavia, con specifico riferimento all'impiego della posta elettronica nel contesto lavorativo e in ragione della veste esteriore attribuita all'indirizzo di posta elettronica nei singoli casi, può risultare dubbio se il lavoratore, in qualità di destinatario o mittente, utilizzi la posta elettronica operando quale espressione dell'organizzazione datoriale o ne faccia un uso personale pur operando in una struttura lavorativa.

La mancata esplicitazione di una *policy* al riguardo può determinare anche una legittima aspettativa del lavoratore, o di terzi, di confidenzialità rispetto ad alcune forme di comunicazione.

Tali incertezze si riverberano sulla qualificazione, in termini di liceità, del comportamento del datore di lavoro che intenda apprendere il contenuto di messaggi inviati all'indirizzo di posta elettronica usato dal lavoratore (posta *"in entrata"*) o di quelli inviati da quest'ultimo (posta *"in uscita"*).

É quindi particolarmente opportuno che si adottino accorgimenti anche per prevenire eventuali trattamenti in violazione dei principi di pertinenza e non eccedenza. Si tratta di soluzioni che possono risultare utili per contemperare le esigenze di ordinato svolgimento dell'attività lavorativa con la prevenzione di inutili intrusioni nella sfera personale dei lavoratori, nonché violazioni della disciplina sull'eventuale segretezza della corrispondenza.

In questo quadro è opportuno che:

- il datore di lavoro renda disponibili indirizzi di posta elettronica condivisi tra più lavoratori (*ad es.*, *info@ente.it*, *ufficiovendite@ente.it*, *ufficioreclami@società.com*, *urp@ente.it*, *etc.*), eventualmente affiancandoli a quelli individuali (*ad es.*, *m.rossi@ente.it*, *rossi@società.com*, *mario.rossi@società.it*);
- il datore di lavoro valuti la possibilità di attribuire al lavoratore un diverso indirizzo destinato ad uso privato del lavoratore; [15]
- il datore di lavoro metta a disposizione di ciascun lavoratore apposite funzionalità di sistema, di agevole utilizzo, che consentano di inviare automaticamente, in caso di assenze (*ad es.*, per ferie o attività di lavoro fuori sede), messaggi di risposta contenenti le "coordinate" (anche elettroniche o telefoniche) di un altro soggetto o altre utili modalità di contatto della struttura. È parimenti opportuno prescrivere ai lavoratori di avvalersi di tali modalità, prevenendo così l'apertura della posta elettronica [16]. In caso di eventuali assenze non programmate (*ad es.*, per malattia), qualora il lavoratore non possa attivare la procedura descritta (anche avvalendosi di servizi *webmail*), il titolare del trattamento, perdurando l'assenza oltre un determinato limite temporale, potrebbe disporre lecitamente, sempre che sia necessario e mediante personale appositamente incaricato (*ad es.*, l'amministratore di sistema oppure, se presente, un incaricato aziendale per la protezione dei dati), l'attivazione di un analogo accorgimento, avvertendo gli interessati;
- in previsione della possibilità che, in caso di assenza improvvisa o prolungata e per improrogabili necessità legate all'attività lavorativa, si debba conoscere il contenuto dei messaggi di posta elettronica, l'interessato sia messo in grado di delegare un altro lavoratore (fiduciario) a verificare il contenuto di messaggi e a inoltrare al titolare del trattamento quelli ritenuti rilevanti per lo svolgimento dell'attività lavorativa. A cura del titolare del trattamento, di tale attività dovrebbe essere redatto apposito verbale e informato il lavoratore interessato alla prima occasione utile;
- i messaggi di posta elettronica contengano un avvertimento ai destinatari nel quale sia dichiarata l'eventuale natura non personale dei messaggi stessi, precisando se le risposte potranno essere conosciute nell'organizzazione di appartenenza del mittente e con eventuale rinvio alla predetta *policy* datoriale.

6. Pertinenza e non eccedenza

6.1. *Graduazione dei controlli*

Nell'effettuare controlli sull'uso degli strumenti elettronici deve essere evitata un'interferenza ingiustificata sui diritti e sulle libertà fondamentali di lavoratori, come pure di soggetti esterni che ricevono o inviano comunicazioni elettroniche di natura personale o privata.

L'eventuale controllo è lecito solo se sono rispettati i princìpi di pertinenza e non eccedenza.

Nel caso in cui un evento dannoso o una situazione di pericolo non sia stato impedito con preventivi accorgimenti tecnici, il datore di lavoro può adottare eventuali misure che consentano la verifica di comportamenti anomali.

Deve essere per quanto possibile preferito un controllo preliminare su dati aggregati, riferiti all'intera struttura lavorativa o a sue aree.

Il controllo anonimo può concludersi con un avviso generalizzato relativo ad un rilevato utilizzo anomalo degli strumenti aziendali e con l'invito ad attenersi scrupolosamente a compiti assegnati e istruzioni impartite. L'avviso può essere circoscritto a dipendenti afferenti all'area o settore in cui è stata rilevata l'anomalia. In assenza di successive anomalie non è di regola giustificato effettuare controlli su base individuale.

Va esclusa l'ammissibilità di controlli prolungati, costanti o indiscriminati.

6.2. *Conservazione*

I sistemi *software* devono essere programmati e configurati in modo da cancellare periodicamente ed automaticamente (attraverso procedure di sovraregistrazione come, ad esempio, la *cd.* rotazione dei *log file*) i dati personali relativi agli accessi ad Internet e al traffico telematico, la cui conservazione non sia necessaria.

In assenza di particolari esigenze tecniche o di sicurezza, la conservazione temporanea dei dati relativi all'uso degli strumenti elettronici deve essere giustificata da una finalità specifica e comprovata e limitata al tempo necessario –e predeterminato– a raggiungerla (*v.* art. 11, comma 1, lett. *e*), del Codice).

Un eventuale prolungamento dei tempi di conservazione va valutato come eccezionale e può aver luogo solo in relazione:

- ad esigenze tecniche o di sicurezza del tutto particolari;
- all'indispensabilità del dato rispetto all'esercizio o alla difesa di un diritto in sede giudiziaria;
- all'obbligo di custodire o consegnare i dati per ottemperare ad una specifica richiesta dell'autorità giudiziaria o della polizia giudiziaria.

In questi casi, il trattamento dei dati personali (tenendo conto, con riguardo ai dati sensibili, delle prescrizioni contenute nelle autorizzazioni generali nn. 1/2005 e 5/2005 adottate dal Garante) deve essere limitato alle sole informazioni indispensabili per perseguire finalità preventivamente determinate ed essere effettuato con logiche e forme di organizzazione strettamente correlate agli obblighi, compiti e finalità già esplicitati.

7. Presupposti di liceità del trattamento: bilanciamento di interessi

7.1. *Datori di lavoro privati*

I datori di lavoro privati e gli enti pubblici economici, se ricorrono i presupposti sopra indicati (v., in particolare, art. 4, secondo comma, dello Statuto), possono effettuare lecitamente il trattamento dei dati personali diversi da quelli sensibili.

Ciò, può avvenire:

a) se ricorrono gli estremi del legittimo esercizio di un diritto in sede giudiziaria (art. 24, comma 1, lett. *f*) del Codice);
b) in caso di valida manifestazione di un libero consenso;
c) anche in assenza del consenso, ma per effetto del presente provvedimento che individua un legittimo interesse al trattamento in applicazione della disciplina sul *cd.* bilanciamento di interessi (art. 24, comma 1, lett. *g*), del Codice).

Per tale bilanciamento si è tenuto conto delle garanzie che lo Statuto prevede per il controllo "indiretto" a distanza presupponendo non il consenso degli interessati, ma un accordo

con le rappresentanze sindacali (o, in difetto, l'autorizzazione di un organo periferico dell'amministrazione del lavoro).

L'eventuale trattamento di dati sensibili è consentito con il consenso degli interessati o, senza il consenso, nei casi previsti dal Codice (in particolare, esercizio di un diritto in sede giudiziaria, salvaguardia della vita o incolumità fisica; specifici obblighi di legge anche in caso di indagine giudiziaria: art. 26).

7.2. *Datori di lavoro pubblici*

Per quanto riguarda i soggetti pubblici restano fermi i differenti presupposti previsti dal Codice a seconda della natura dei dati, sensibili o meno (artt. 18-22 e 112).

In tutti i casi predetti resta impregiudicata la facoltà del lavoratore di opporsi al trattamento per motivi legittimi (art. 7, comma 4, lett. *a*), del Codice).

8. Individuazione dei soggetti preposti

Il datore di lavoro può ritenere utile la designazione (facoltativa), specie in strutture articolate, di uno o più responsabili del trattamento cui impartire precise istruzioni sul tipo di controlli ammessi e sulle relative modalità (art. 29 del Codice).

Nel caso di eventuali interventi per esigenze di manutenzione del sistema, va posta opportuna cura nel prevenire l'accesso a dati personali presenti in cartelle o spazi di memoria assegnati a dipendenti.

Resta fermo l'obbligo dei soggetti preposti al connesso trattamento dei dati (in particolare, gli incaricati della manutenzione) di svolgere solo operazioni strettamente necessarie al perseguimento delle relative finalità, senza realizzare attività di controllo a distanza, anche di propria iniziativa.

Resta parimenti ferma la necessità che, nell'individuare regole di condotta dei soggetti che operano quali amministratori di sistema o figure analoghe cui siano rimesse operazioni connesse al regolare funzionamento dei sistemi, sia svolta un'attività formativa sui profili tecnico-gestionali e di sicurezza delle reti, sui principi di protezione dei dati personali e sul segreto nelle comunicazioni (*cfr.* Allegato B) al Codice, regola n. 19.6; Parere n. 8/2001 *cit.*, punto 9).

TUTTO CIÒ PREMESSO IL GARANTE

1) prescrive ai datori di lavoro privati e pubblici, ai sensi dell'art. 154, comma 1, lett. *c*), del Codice, di adottare la misura necessaria a garanzia degli interessati, nei termini di cui in motivazione, riguardante l'onere di specificare le modalità di utilizzo della posta elettronica e della rete Internet da parte dei lavoratori (punto 3.1.), indicando chiaramente le modalità di uso degli strumenti messi a disposizione e se, in che misura e con quali modalità vengano effettuati controlli;

2) indica inoltre, ai medesimi datori di lavoro, le seguenti linee-guida a garanzia degli interessati, nei termini di cui in motivazione, per ciò che riguarda:

a) l'adozione e la pubblicizzazione di un disciplinare interno (punto 3.2.);

b) l'adozione di misure di tipo organizzativo (punto 5.2.) affinché, segnatamente:
- si proceda ad un'attenta valutazione dell'impatto sui diritti dei lavoratori;
- si individui preventivamente (anche per tipologie) a quali lavoratori è accordato l'utilizzo della posta elettronica e dell'accesso a Internet;
- si individui quale ubicazione è riservata alle postazioni di lavoro per ridurre il rischio di impieghi abusivi;

c) l'adozione di misure di tipo tecnologico, e segnatamente:

I. rispetto alla "navigazione" in Internet (punto 5.2., a):
- l'individuazione di categorie di siti considerati correlati o non correlati con la prestazione lavorativa;
- la configurazione di sistemi o l'utilizzo di filtri che prevengano determinate operazioni;
- il trattamento di dati in forma anonima o tale da precludere l'imme-

diata identificazione degli utenti mediante opportune aggregazioni;
- l'eventuale conservazione di dati per il tempo strettamente limitato al perseguimento di finalità organizzative, produttive e di sicurezza;
- la graduazione dei controlli (punto 6.1.);

II. rispetto all'utilizzo della posta elettronica (punto 5.2., b):
- la messa a disposizione di indirizzi di posta elettronica condivisi tra più lavoratori, eventualmente affiancandoli a quelli individuali;
- l'eventuale attribuzione al lavoratore di un diverso indirizzo destinato ad uso privato;
- la messa a disposizione di ciascun lavoratore, con modalità di agevole esecuzione, di apposite funzionalità di sistema che consentano di inviare automaticamente, in caso di assenze programmate, messaggi di risposta che contengano le "coordinate" di altro soggetto o altre utili modalità di contatto dell'istituzione presso la quale opera il lavoratore assente;
- consentire che, qualora si debba conoscere il contenuto dei messaggi di posta elettronica in caso di assenza improvvisa o prolungata e per improrogabili necessità legate all'attività lavorativa, l'interessato sia messo in grado di delegare un altro lavoratore (fiduciario) a verificare il contenuto di messaggi e a inoltrare al titolare del trattamento quelli ritenuti rilevanti per lo svolgimento dell'attività lavorativa. Di tale attività dovrebbe essere redatto apposito verbale e informato il lavoratore interessato alla prima occasione utile;
- l'inserzione nei messaggi di un avvertimento ai destinatari nel quale sia dichiarata l'eventuale natura non personale del messaggio e sia specificato se le risposte potranno essere conosciute nell'organizzazione di appartenenza del mittente;
- la graduazione dei controlli (punto 6.1.);

3) vieta ai datori di lavoro privati e pubblici, ai sensi dell'art. 154, comma 1, lett. *d*), del Codice, di effettuare trattamenti di dati personali mediante sistemi *hardware* e *software* che mirano al controllo a distanza di lavoratori (punto 4), svolti in particolare mediante:

a) la lettura e la registrazione sistematica dei messaggi di posta elettronica ovvero dei relativi dati esteriori, al di là di quanto tecnicamente necessario per svolgere il servizio *e-mail*;
b) la riproduzione e l'eventuale memorizzazione sistematica delle pagine *web* visualizzate dal lavoratore;
c) la lettura e la registrazione dei caratteri inseriti tramite la tastiera o analogo dispositivo;
d) l'analisi occulta di *computer* portatili affidati in uso;

4) individua, ai sensi dell'art. 24, comma 1, lett. *g*), del Codice, nei termini di cui in motivazione (punto 7), i casi nei quali il trattamento dei dati personali di natura non sensibile possono essere effettuati per perseguire un legittimo interesse del datore di lavoro anche senza il consenso degli interessati;

5) dispone che copia del presente provvedimento sia trasmessa al Ministero della giustizia-Ufficio pubblicazione leggi e decreti, per la sua pubblicazione sulla *Gazzetta Ufficiale* della Repubblica italiana ai sensi dell'art. 143, comma 2, del Codice.

Roma, 1 marzo 2007

IL PRESIDENTE
Pizzetti

IL RELATORE
Paissan

IL SEGRETARIO GENERALE
Buttarelli

(1) *Cfr.* Gruppo Art. 29 sulla protezione dei dati, Parere n. 8/2001 sul trattamento dei dati personali nel contesto dell'occupazione, 13 settembre 2001, punti 5 e 12, in *http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2001/wp48en.pdf*.

(2) *Cfr.* Niemitz *v.* Germany, 23 novembre 1992, *par.* 29; *v.* pure Halford *v.* United Kingdom, 25 giugno 1997, parr. 44-46.

(3) *V.* pure Gruppo Art. 29 *cit.*, Documento di lavoro riguardante la vigilanza sulle comunicazioni elettroniche sul posto di lavoro, Wp 55, 29 maggio 2002, p. 4, in *http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2002/wp55_it.pdf*.

(4) *V.* pure la Direttiva per l'impiego della posta elettronica nelle pubbliche amministrazioni del 27 novembre 2003; Raccomandazione n. R(89)2 del Consiglio d'Europa in materia di protezione dei dati personali nel contesto del rapporto di lavoro, in *http://cm.coe.int/ta/rec/1989/word/89r2.doc*); Parere n. 8/2001, *cit.*, punto 5.

(5) *V.* altresì la Raccomandazione n. R(89)2, *cit.*, punto 3; Parere n. 8/2001, *cit.*, punto 9.1 e Wp 55, *cit.*, punto 3.1.3.

(6) Cass. 18 febbraio 1983, n. 1236 e 16 settembre 1997, n. 9211.

(7) *Cfr.* Cass. 11 marzo 1986, n. 1490.

(8) *Cfr.* anche Cass., 17 giugno 2000, n. 8250 rispetto all'uso probatorio.

(9) Cass. 18 febbraio 1983, n. 1236 e 16 settembre 1997, n. 9211.

(10) Cass. 11 marzo 1986, n. 1490 *cit.*

(11) Raccomandazione n. R (89)2, *cit.*, art. 3, comma 1.

(12) Art. 3, comma 2; disposizione in base alla quale, in presenza di rischi *"per il diritto al rispetto della vita privata e della dignità umana dei lavoratori, dovrà essere ricercato l'accordo dei lavoratori o dei loro rappresentanti prima dell'introduzione o della modifica di tali sistemi o procedimenti, a meno che altre garanzie specifiche non siano previste dalla legislazione nazionale"*: art. 3, comma 3.

(13) *Cfr. Provv.* 2 febbraio 2006 , in *www.garanteprivacy.it*, doc. *web* n. 1229854.

(14) *Cfr.* nota del Garante 16 giugno 1999, Boll. n. 9, giugno 1999, p. 96; Tar Lazio, Sez. I ter, 15 novembre 2001, n. 9425.

(15) *Cfr.* il documento Wp 55, *cit.*, p. 23.

(16) *Cfr.* il documento Wp 55, *cit.*, p. 5.

43 Consultazione pubblica in tema di trattamenti di dati personali nell'ambito delle sperimentazioni cliniche di medicinali (*)
29 novembre 2007

Registro delle deliberazioni
n. 62 del 29 novembre 2007

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Nella riunione odierna, in presenza del prof. Francesco Pizzetti, presidente, del dott. Giuseppe Chiaravalloti, vice presidente, del dott. Mauro Paissan e del dott. Giuseppe Fortunato, componenti, e del dott. Giovanni Buttarelli, segretario generale;

Considerato che l'Autorità ha concluso i primi approfondimenti istruttori inerenti ai trattamenti di dati personali effettuati per promuovere studi clinici, con particolare riferimento alla sperimentazione dei medicinali, a seguito degli accertamenti eseguiti presso alcune società farmaceutiche e altri soggetti coinvolti in attuazione del programma ispettivo deliberato dall'Autorità nel gennaio del 2006 riguardante anche la sperimentazione;

Considerato che detti approfondimenti hanno evidenziato una situazione di non compiuta osservanza della disciplina sulla protezione dei dati personali specie da parte delle società farmaceutiche che hanno ritenuto, erroneamente, di non applicare la disciplina di protezione dei dati a informazioni che, diversamente da quanto sostenuto dalle medesime società, risultano riconducibili all'identità dei pazienti partecipanti agli studi clinici;

Rilevata l'esigenza di individuare misure e accorgimenti necessari e opportuni da porre, a garanzia dei pazienti interessati, in relazione ai trattamenti di dati che li riguardano a fini di sperimentazione clinica di medicinali;

Rilevata l'opportunità che la prescrizione di tali misure e accorgimenti, che sono allo stato individuati dal Garante nell'unito documento, sia preceduta da una consultazione pubblica dei soggetti e delle categorie interessate, in particolare delle società farmaceutiche e delle organizzazioni di ricerca che operano nel settore della sperimentazione, nonché di strutture ospedaliere o universitarie e istituti pubblici o privati autorizzati, di organismi rappresentativi di operatori sanitari e associazioni di pazienti interessati, di comitati etici, del Ministero della salute, dell'Istituto superiore di sanità, dell'Agenzia italiana del farmaco e della Conferenza Stato-Regioni, anche al fine di acquisire eventuali riscontri e osservazioni circa gli accorgimenti e le misure previsti e le relative modalità attuative;

Visto il Codice in materia di protezione dei dati personali (d.lg. 30 giugno 2003, n. 196);

Viste le osservazioni dell'Ufficio formulate dal segretario generale ai sensi dell'art. 15 del regolamento del Garante n. 1/2000;

Relatore il dott. Giuseppe Chiaravalloti;

DELIBERA

a) di adottare l'unito documento che forma parte integrante della presente deliberazione (*"Linee-guida per i trattamenti di dati personali nell'ambito delle sperimentazioni cliniche di medicinali"*);
b) di avviare una consultazione pubblica sul documento di cui alla lettera a).

L'obiettivo della consultazione è acquisire osservazioni e commenti, in particolare da parte di società farmaceutiche e organizzazioni di ricerca che operano nel settore della spe-

(*) *G.U.* 15 dicembre 2007, n. 291
[doc. *web* n. 1468981]

rimentazione, nonché di strutture ospedaliere o universitarie e istituti pubblici o privati autorizzati, di organismi rappresentativi di operatori sanitari e associazioni di pazienti interessati, di comitati etici, del Ministero della salute, dell'Istituto superiore di sanità, dell'Agenzia italiana del farmaco e della Conferenza Stato-Regioni.

Osservazioni e commenti potranno pervenire entro il 15 febbraio 2008 all'indirizzo dell'Autorità di Piazza di Monte Citorio n. 121, 00186 Roma, ovvero all'indirizzo di posta elettronica: *sperimentazionefarmaci@garanteprivacy.it*

La presente deliberazione verrà pubblicata sul sito *web* del Garante *www.garanteprivacy.it* e verrà inviato un avviso all'Ufficio pubblicazione leggi e decreti del Ministero della giustizia affinché sia riportato sulla *Gazzetta ufficiale* della Repubblica italiana.

Roma, 29 novembre 2007

IL PRESIDENTE
Pizzetti

IL RELATORE
Chiaravalloti

IL SEGRETARIO GENERALE
Buttarelli

ALLEGATO N. 1

LINEE-GUIDA PER I TRATTAMENTI DI DATI
NELL'AMBITO DELLE SPERIMENTAZIONI CLINICHE DI MEDICINALI

Sommario

1. Considerazioni preliminari

Gli studi condotti su esseri umani nell'ambito della sperimentazione clinica mirano a scoprire o verificare gli effetti di medicinali sperimentali, compresa qualsiasi reazione avversa, al fine di accertarne la sicurezza e l'efficacia. Tali studi vengono non di rado promossi da società farmaceutiche (promotore, committente, *sponsor*) a livello nazionale e (specie a cura di società facenti parte di gruppi multinazionali) internazionale.

A tal fine dette società, dopo aver predisposto un protocollo che descrive la progettazione, gli obiettivi e la metodologia della sperimentazione, curano la presentazione alle autorità competenti e ai comitati etici interessati della documentazione necessaria all'attivazione della sperimentazione.

Le attività collegate allo studio vengono eseguite presso una o più strutture ospedaliere o universitarie o istituti di ricerca pubblici o privati autorizzati (centri di sperimentazione).

Vengono pertanto raccolte, in conformità al protocollo e a più riprese nel corso dello studio, varie informazioni di carattere medico/clinico e i campioni biologici dei pazienti che accettano di far parte dello studio tramite visite mediche e accertamenti diagnostici effettuati da medici sperimentatori.

A queste informazioni non ha accesso soltanto il personale sanitario operante presso i centri. Il promotore supervisiona, infatti, l'andamento dello studio, per garantire che esso venga effettuato in osservanza del protocollo. Ciò, avvalendosi di propri collaboratori (*clinical study monitor*) i quali visitano i centri di sperimentazione per effettuare il monitoraggio e, se necessario, esaminano la documentazione medica originale dei pazienti messa a loro disposizione dai medici (*ad es.*, cartelle ospedaliere, registri clinici, note di laboratorio, referti, *ecc.*).

Le informazioni raccolte presso ciascun centro di sperimentazione vengono trasmesse alla società farmaceutica promotrice; ciò, a più riprese nel corso dello studio, ovvero al termine della sperimentazione presso il centro. Conclusa la fase della sperimentazione presso il centro, le medesime informazioni sono normalmente inserite dalle società farmaceutiche *sponsor*, direttamente o tramite soggetti esterni di cui si avvalgono, su un *database* unico attraverso il quale viene effettuato il controllo e la validazione dei dati e, successivamente, l'elaborazione statistica, con l'obiettivo di conseguire i risultati dello studio da documentare poi in un rapporto.

Negli studi promossi da società farmaceutiche che operano nell'ambito di gruppi multinazionali, il destinatario dei dati riferiti ai pazienti partecipanti alla sperimentazione è solitamente la società capogruppo che può avere sede al di fuori del territorio nazionale. Inoltre, le società committenti si avvalgono sovente di soggetti esterni (*clinical study monitor*, organizzazioni di ricerca a contratto, laboratori di analisi, *ecc.*), che possono risiedere in Paesi anche al di fuori dell'Unione europea, per svolgere uno o più compiti relativi all'esecuzione della sperimentazione (*ad es.*, il monitoraggio dello studio, l'inserimento, la validazione e l'analisi statistica dei dati, la farmacovigilanza, l'esecuzione degli esami clinici e di laboratorio previsti dal protocollo). Ciò comporta che numerose informazioni o campioni biologici vengano condivisi tra diverse categorie di soggetti aventi sede anche in Paesi terzi, i quali possono accedervi o averne la disponibilità (il promotore; gli addetti al monitoraggio dello studio; i soggetti esterni che collaborano con il promotore per l'inserimento dei dati e il loro trattamento statistico; il laboratorio di analisi, *ecc.*).

Al fine di confermare la validità della conduzione dello studio e l'integrità dei dati raccolti anche in occasione di eventuali verifiche da parte delle autorità dotate di poteri ispettivi, le informazioni ottenute nel corso dello studio sono oggetto di conservazione per un periodo di tempo considerevole dopo il completamento della sperimentazione.

In base agli approfondimenti svolti, la raccolta, la circolazione e la conservazione massiva, anche in Paesi terzi, di molteplici informazioni attinenti alla salute delle persone che partecipano alle sperimentazioni cliniche presentano vari aspetti di criticità con riferimento alla protezione dei dati personali e necessitano, pertanto, dell'adozione di elevate cautele volte a prevenire rischi specifici per gli interessati.

In relazione ad alcune circostanze che sembrano emergere dai primi accertamenti svolti presso talune società, l'Autorità ritiene necessario richiamare il quadro normativo di base al quale le società stesse devono fare riferimento per un trattamento lecito e corretto dei dati. Il Garante si riserva di verificare in separata sede eventuali violazioni riguardanti singole società; si riserva, altresì, di apportare alle presenti "Linee-guida" eventuali integrazioni riguardanti le concrete modalità di trattamento dei dati e l'impiego di nuove tecnologie, anche alla luce dell'esperienza maturata e dell'applicazione delle stesse.

2. Normativa applicabile

Gli studi condotti nell'ambito della sperimentazione clinica devono essere gestiti nel rispetto dei princìpi etici i quali traggono origine dalla Dichiarazione di Helsinki (fatta nel giugno 1964 e successive modificazioni), dei requisiti previsti dagli *standard* internazionali di buona pratica clinica (Gcp) adottati anche dall'Unione europea (e recepiti nell'ordina-

mento italiano, *v.* d.lg. 6 novembre 2007, n. 200; d.lg. 24 giugno 2003, n. 211; d.m. 15 luglio 1997) e delle procedure operative *standard* delle società promotrici (Sop). Il centro di sperimentazione deve condurre lo studio in conformità al protocollo e alle procedure operative *standard* del promotore e non può discostarsi in alcun modo da essi, né apportarvi modifiche, senza accordo con il promotore stesso. Ciò, eccetto casi eccezionali correlati al sorgere di rischi immediati per i pazienti o a cambiamenti implicanti solo aspetti marginali dello studio (art. 10, comma 1, lettera a), d.lg. n. 211/2003; d.m. 15 luglio 1997, all. 1/1B punto 1.38, all. 1/4A punto 4.5.1. e 4.5.2, all. 1/5A punto 5.1 e all. 1/5B punto 5.20).

La normativa applicabile prevede diverse ipotesi in cui le informazioni medico/cliniche raccolte dal centro devono essere comunicate al promotore dello studio. Si tratta in primo luogo dei dati medico/clinici riferiti a ciascun partecipante allo studio i quali devono essere registrati dal medico su schede raccolta dati (Crf) trasmesse al promotore della sperimentazione (d.m. 15 luglio 1997, all. 1/1A punto 1.11). I centri sono tenuti poi a notificare al promotore le reazioni e gli eventi avversi (Ae e Adr), correlabili alla somministrazione ai pazienti del medicinale in sperimentazione o comunque al suo svolgimento, insieme ad ogni altra informazione pertinente di *follow-up* (artt. 16, 17 e 18 d.lg. 24 giugno 2003, n. 211).

Al fine di tutelare l'identità dei pazienti la medesima normativa prevede che il centro partecipante alla sperimentazione debba assegnare a ciascun interessato un codice di identificazione e utilizzarlo al posto del relativo nominativo in ciascuna comunicazione al promotore di dati collegati allo studio (d.m. 15 luglio 1997, all. 1/1B punto 1.58 e all. 1/4B punto 4.11.1, *v.* anche art. 16, comma 5, d.lg. n. 211/2003). Una lista cartacea, che consente di associare ai codici i dati nominativi dei pazienti, è detenuta esclusivamente da ciascun centro di sperimentazione che la custodisce come documento riservato essenziale alla conduzione dello studio clinico (d.m. 15 luglio 1997, all. 1/1A punto 1.21, all. 1/4B punto 4.9.4 e 4.9.5, all. 1/5A punto 5.5.12, all. 1/8 punto 8.1 e 8.4.3).

Anche le schede raccolta dati, le segnalazioni e i rapporti relativi agli eventi e alle reazioni avversi, in quanto documenti essenziali alla conduzione dello studio, devono essere conservati, in base alla citata normativa, sia presso il promotore, sia presso i singoli centri, per un periodo di tempo non inferiore a sette anni dal completamento della sperimentazione, ovvero per un periodo più lungo richiesto da altre disposizioni applicabili o da un accordo tra il promotore e detti centri (art. 18 d.lg. n. 200/2007; d.lg. n. 219/2006, all. 1, punto 5.2, lett. c); d.m. 15 luglio 1997, all. 1/4B, punto 4.9.4, 4.9.5, 5.5.11 e 5.5.12).

3. Natura dei dati trattati

Le società farmaceutiche hanno sviluppato in genere specifiche procedure interne per codificare i dati medico/clinici dei pazienti ad opera dei centri di sperimentazione: solitamente, si utilizzano codici numerici che consentono di identificare univocamente i singoli interessati all'interno dello stesso studio clinico, senza utilizzare il nominativo, l'indirizzo o numeri di identificazione personale.

Tuttavia, alcune società farmaceutiche richiedono ai centri di registrare sulle schede raccolta dati e sulle segnalazioni di reazioni e eventi avversi -da trasmettere alle prime- le iniziali del nome e cognome dei singoli pazienti, oltre ai rispettivi codici identificativi. Inoltre i protocolli prevedono, di regola, che i centri debbano raccogliere sulle schede informazioni ulteriori rispetto ai dati medico/clinici riferiti agli interessati, quali dati di carattere demografico (data di nascita e/o età, sesso, origine etica, origine razziale, peso e statura) e, a seconda delle finalità della ricerca, informazioni relative alla storia medica dei soggetti o agli stili di vita. Queste informazioni, riportate sui documenti essenziali alla conduzione dello studio, sono conservate dai centri partecipanti e dalla società promotrice per un periodo di tempo che, a seconda della disciplina applicabile, può essere collegato all'intera durata dell'autorizzazione del medicinale nei diversi Paesi.

Sebbene sia previsto che soltanto ciascun centro abbia la disponibilità della lista che consente di associare il nominativo del paziente al relativo codice identificativo e che il committente dello studio non debba venire a conoscenza della sua identità, quest'ultimo, tramite propri collaboratori addetti al monitoraggio, ha tuttavia accesso, come detto, presso il cen-

tro di sperimentazione e sotto il controllo dei medici, alla documentazione sanitaria originale dei pazienti per verificare l'accuratezza e la completezza dei dati raccolti, nonché alla lista contenente i dati nominativi dei pazienti nell'ambito delle verifiche relative alle procedure riguardanti l'acquisizione del consenso informato.

Alla luce delle indicazioni formulate dal Gruppo dei garanti europei nel Parere n. 4/2007 (Wp 136) sulla definizione di dato personale, va rilevato che tra le informazioni raccolte nel corso degli studi in esame compaiono, in genere, uno o più elementi specifici caratteristici dell'identità del paziente (ivi compresa la statura o particolari patologie). La combinazione di tali elementi è suscettibile di consentire il riconoscimento dell'interessato (ad esempio, mediante combinazione delle iniziali del nome e del cognome del paziente con la data di nascita o con la sua collocazione geografica desumibile dai dati identificativi del centro di sperimentazione e del medico sperimentatore).

Le modalità di codificazione utilizzate dalle società *sponsor* rappresentano una specifica misura di sicurezza adottata in applicazione delle disposizioni normative vigenti a tutela della riservatezza dei pazienti che però non è, di per sé, tale da rendere anonimi i dati oggetto di trattamento nell'ambito della sperimentazione (art. 16, comma 5, d.lg. n. 211/2003; d.m. 15 luglio 1997, all. 1/1B punto 1.58 e all. 1/4B punto 4.11.1; *v.* anche autorizzazione del Garante n. 2/2007 al trattamento dei dati idonei a rivelare lo stato di salute e la vita sessuale, specie punto 1.2, lett. *a*), disponibile sul sito Internet dell'Autorità, doc. *web* n. 1429775). Le predette modalità di utilizzo del codice identificativo mirano, del resto, a consentire, in base alla specifica disciplina applicabile, l'identificabilità del singolo paziente in casi determinati; ad esempio, per consentire al medico sperimentatore, che è il solo ad avere un contatto diretto con il paziente, di modificare o interrompere la terapia farmacologica somministrata in caso di eventi o reazioni avversi; oppure, per permettere agli addetti al monitoraggio di verificare, per conto della società farmaceutica, la corrispondenza delle informazioni raccolte nel corso studio con quelle contenute nella documentazione medica originale dei pazienti; o, ancora, per consentire alla società farmaceutica di utilizzare le informazioni conseguite nell'ambito dello studio al fine di difendere i propri diritti nell'ambito di eventuali azioni legali. Analogamente, ai fini delle valutazioni da fare sull'identificabilità, vanno tenuti in considerazione il tempo di conservazione della lista di identificazione, gli eventuali rischi di disfunzione o malfunzionamento delle misure tecnico-organizzative eventualmente adottate per la custodia e la sicurezza dei dati e quelli di violazione delle regole di riservatezza e confidenzialità previste dalle disposizioni normative applicabili (artt. 3, comma 1, lett. *c*) e 11, comma 3, d.lg. n. 211/2003), nonché le precauzioni che gli addetti al monitoraggio sono tenuti ad utilizzare per mantenere riservata l'identità degli interessati (d.m. 15 luglio 1997, all. 1/1A punto 1.21 e all. 1/2, punto 2.11).

La quantità e la tipologia di informazioni fornite al promotore, le modalità di trattamento previste e le diverse categorie di soggetti che possono accedere ai dati della sperimentazione comportano, quindi, la possibilità di identificare gli interessati, sia pure indirettamente, mediante il riferimento ad altre informazioni detenute dallo *sponsor* o a qualsiasi altra informazione non necessariamente nella disponibilità di quest'ultimo, ma detenuta da terzi. Ciò, considerando, in conformità alla disciplina comunitaria, l'insieme dei mezzi che possono essere ragionevolmente utilizzati dal primo, come pure da soggetti terzi, per identificare gli interessati (considerando 26 della direttiva 95/46/Ce).

Pertanto, le informazioni collegate al codice identificativo di ciascun paziente sono da ritenere dati personali sulla salute riconducibili al singolo interessato (artt. 2, all. 1, lett. *a*) e 8 direttiva 95/46/Ce; art. 4, comma 1, lett. *b*) e *d*), del Codice). La loro acquisizione da parte delle società committenti nell'ambito delle sperimentazioni cliniche e le successive attività svolte su questi ultimi configurano un trattamento di dati al quale è applicabile la disciplina del Codice sulle informazioni idonee a rivelare lo stato di salute (art. 26), nonché le ulteriori cautele poste a tutela dei diritti e della riservatezza degli interessati dall'autorizzazione del Garante n. 2/2007 al trattamento dei dati sulla salute e sulla vita sessuale (deliberazione n. 25 del 28 giugno 2007, doc. *web* n. 1429775) e, ove applicabile, dall'autorizzazione del Garante al trattamento dei dati genetici (deliberazione del 22 febbraio 2007, doc. *web* n. 1389918).

4. Titolarità dei trattamenti finalizzati alla sperimentazione

Risulta essenziale verificare quale rapporto intercorre tra le società farmaceutiche che promuovono sperimentazioni cliniche e i centri di sperimentazione, per ciò che riguarda il trattamento dei dati personali. In questo quadro, occorre approfondire il ruolo effettivamente svolto da tali società per ciò che concerne l'individuazione delle finalità e delle modalità del trattamento, anche alla luce delle delucidazioni fornite dal Garante a proposito della figura del "titolare" e del "responsabile del trattamento" (*cfr.* Parere del 18 maggio 2000, doc. *web* n. 30935).

Al riguardo, va evidenziato che il promotore, prima dell'avvio della sperimentazione, identifica i possibili centri partecipanti verificandone l'idoneità e il relativo interesse; predispone poi il protocollo da osservare nel corso dello studio; quindi, impartisce ai centri le necessarie direttive sul trattamento dei dati, ivi compresi i profili relativi alla loro custodia e sicurezza, nonché le istruzioni relative alle modalità di utilizzo dei sistemi informativi eventualmente previsti, e, se necessario, forniti al centro; verifica poi, a mezzo di propri collaboratori, l'osservanza del protocollo e delle proprie procedure interne da parte del centro; predispone i documenti da impiegare per informare i pazienti e per ottenerne il consenso anche per ciò che riguarda il trattamento dei dati che li riguardano; infine, avverte i centri quando non è più necessario conservare la documentazione relativa allo studio.

Lo *sponsor* non effettua quindi alcuna attività di raccolta diretta dei dati, né può interloquire con i pazienti inclusi nella sperimentazione; compiti, questi, spettanti ai medici sperimentatori. Tuttavia lo *sponsor* acquisisce, come detto, in diverse ipotesi i dati dei pazienti raccolti dai centri e sugli stessi effettua diverse operazioni di trattamento; tramite i propri collaboratori addetti al monitoraggio esamina, infatti, presso i centri le informazioni contenute nella documentazione medica originale e nella lista di identificazione dei pazienti; è destinatario dei dati registrati da ciascun centro sulle schede raccolta dati e sulle segnalazioni di reazioni e eventi avversi; ne cura direttamente, ovvero tramite soggetti esterni ai quali può demandare alcuni o tutti i compiti in materia di sperimentazione, il loro inserimento sul *database*, nonché il controllo, la validazione e la successiva elaborazione statistica dei dati al fine di conseguire i risultati dello studio.

D'altra parte, va rilevato che il centro non è assoggettato a vincoli di subordinazione nei confronti del promotore: accetta il protocollo concordandone con il promotore alcuni aspetti, compresi quelli relativi alla formulazione del consenso informato dei pazienti in ottemperanza al parere del comitato etico di riferimento; esegue la sperimentazione con propria autonomia organizzativa, sebbene nel rispetto del protocollo, delle procedure operative standard e delle direttive del promotore; per l'esecuzione della sperimentazione si avvale inoltre di collaboratori che ritiene idonei ed è responsabile del loro operato; fornisce ai pazienti l'informativa e raccoglie il loro consenso anche per ciò che riguarda il trattamento dei dati che li riguardano; permette che i collaboratori del promotore accedano alla documentazione medica originale dei pazienti per svolgere le attività di monitoraggio; gestisce e custodisce sotto la propria responsabilità tale documentazione.

Dalla ricostruzione delle attività svolte anche nell'ambito degli accertamenti ispettivi effettuati, i singoli centri di sperimentazione e le società *sponsor* hanno in genere responsabilità distinte nell'ambito degli studi clinici e si configurano, quindi, quali autonomi titolari, ovvero contitolari del trattamento (art. 28 del Codice). Per poter effettuare lecitamente il trattamento dei dati relativi alle sperimentazioni, tali società sono pertanto tenute al rispetto delle disposizioni del Codice e delle prescrizioni della citata autorizzazione generale del Garante con particolare riferimento ai profili relativi alle modalità di trattamento e ai requisiti dei dati, alla designazione degli incaricati e di eventuali responsabili, nonché alla custodia e sicurezza delle medesime informazioni (artt. 11, 29, 30, 31 e ss. del Codice; *v.* anche autorizzazione n. 2/2007, specie punto 1.2). La trasmissione dei dati della sperimentazione da parte dei centri di sperimentazione alle società committenti configura inoltre una vera e propria "comunicazione" di dati e un trattamento di dati da parte di terzi, i quali vanno indicati nominativamente e distintamente nell'informativa agli interessati e nel modello di consenso, anche per ciò che riguarda l'esercizio del diritto di accesso e degli altri diritti previsti dagli artt. 7 e 8 del Codice (artt. 13, 23 e 26 del Codice).

5. Altri soggetti che intervengono nella sperimentazione dei farmaci

Il promotore può stipulare un contratto con soggetti esterni (organizzazioni di ricerca a contratto, laboratori di analisi, *ecc.*) ai quali può demandare alcuni, o tutti i compiti e le funzioni di sua competenza inerenti alle sperimentazioni di farmaci, specificandoli per iscritto (d.m. 15 luglio 1997, all. 1/5A, punto 5.2). In tal caso questi soggetti, i quali possono essere singole persone fisiche ovvero società, istituzioni e altri organismi, possono svolgere nell'ambito degli studi clinici attività che, a seconda delle mansioni di volta in volta affidate, comportano il trattamento di dati personali riferiti ai singoli pazienti inclusi nelle sperimentazioni, come accade nelle ipotesi in cui essi vengano incaricati del monitoraggio degli studi, dell'inserimento, della validazione o dell'analisi statistica dei dati, ovvero della farmacovigilanza.

Questi soggetti eseguono generalmente tali attività per conto e, in alcuni casi, anche in nome del promotore, nel rispetto delle procedure operative *standard* di quest'ultimo, o di proprie procedure visionate e approvate dal promotore stesso, ovvero di puntuali direttive di volta in volta impartite per iscritto da quest'ultimo. A tal fine, il promotore espleta spesso un'attività di formazione specifica nei confronti di tali collaboratori e, talvolta, si riserva il diritto di esprimere il proprio gradimento sui singoli. I medesimi soggetti possono inoltre utilizzare le informazioni e i documenti eventualmente ottenuti dai centri di sperimentazione nell'ambito dello studio soltanto in funzione dell'espletamento delle mansioni loro delegate; a conclusione della loro collaborazione, consegnano di regola al promotore tutte le informazioni e la documentazione conseguita.

Con specifico riferimento alle attività di monitoraggio, le società farmaceutiche promotrici di studi clinici possono avvalersi, come detto, non solo di personale interno all'azienda, ma anche di collaboratori esterni. In entrambi i casi gli addetti al monitoraggio (*clinical study monitor*) vengono selezionati, nominati e addestrati in modo specifico dal promotore che stabilisce l'estensione e il tipo di monitoraggio da effettuare. Nello svolgimento della loro attività sono inoltre tenuti ad osservare le procedure del promotore e le specifiche istruzioni impartite da quest'ultimo, nonché soggetti al controllo del promotore al quale devono sottoporre un rapporto scritto dopo ogni visita ai centri di sperimentazione o dopo ogni comunicazione riguardante la sperimentazione stessa (d.m. 15 luglio 1997, all. 1/5 punto 5.18).

La relazione fra le società *sponsor*, da un lato, e, dall'altro, i soggetti esterni ai quali queste delegano alcune o tutte le mansioni riguardanti gli studi clinici (ivi compresi gli addetti al monitoraggio) possono essere pertanto utilmente inquadrate nell'ambito di un rapporto fra "titolare" e "incaricati" (unicamente persone fisiche) o, eventualmente, in base al grado di autonomia da osservare nel trattamento dei dati, "responsabili del trattamento" (persone fisiche o giuridiche). Tali soggetti devono quindi essere designati, in conformità alle disposizioni del Codice sugli incaricati e sui responsabili, e ricevere idonee istruzioni alle quali attenersi nel trattamento dei dati della sperimentazione (artt. 29 e 30).

I medesimi soggetti che, in quanto collaboratori delle società committenti, accedono ai dati personali dei pazienti per le finalità della sperimentazione, devono essere inoltre menzionati, anche per categorie, nell'informativa da fornire agli interessati e, qualora vengano designati più responsabili, occorre indicare anche gli estremi identificativi di almeno uno di essi, nonché le modalità per reperire, anche *on-line* sul sito del rispettivo committente, il loro elenco aggiornato (art. 13 del Codice). Diversamente, qualora le società farmaceutiche non ritengano poter designare in base alla legge i soggetti di cui si avvalgano quali "incaricati" o "responsabili" ai sensi del Codice, questi potrebbero trattare i dati illecitamente e configurarsi anche come autonomi "titolari" del trattamento. In quest'ultimo caso, il flusso delle informazioni riferite ai pazienti eventualmente ottenuti dai centri di sperimentazione costituirebbe una comunicazione di dati personali che potrebbe essere effettuata lecitamente soltanto in presenza del consenso specifico e informato degli interessati (artt. 11, comma 1, lett. *a*), 13, 23 e 26 del Codice).

A tutela della riservatezza dei dati personali relativi alla salute e, in qualche caso direttamente identificativi dei pazienti, oggetto di trattamento, gli addetti al monitoraggio devono essere, altresì, sottoposti a regole di condotta analoghe al segreto professionale. Il loro processo di designazione deve poi prevedere la frequenza di una specifica attività formativa concernente l'illustrazione dei rischi e delle responsabilità derivanti dal trattamento di queste

informazioni, le istruzioni da rispettare per la loro custodia e sicurezza, nonché le regole di riservatezza e confidenzialità previste dalle disposizioni normative applicabili (artt. 3, comma 1, lett. c) e 11, comma 3, d.lg. n. 211/2003) e le specifiche precauzioni da utilizzare per tutelare l'identità delle persone partecipanti alla sperimentazione anche nei riguardi dello stesso promotore (d.m. 15 luglio 1997, all. 1/1A punto 1.21 e all. 1/2, punto 2.11).

6. Informativa ai pazienti

Le società committenti di regola individuano le informazioni da comunicare ai pazienti e la procedura da seguire per raccogliere il consenso degli interessati tramite i centri di sperimentazione, anche per ciò che riguarda il trattamento dei dati che li riguardano, per consentirne l'esame da parte dei comitati etici interessati (artt. 6, 7, 8 e 11 d.lg. n. 211/2003).

Tuttavia, ritenendo erroneamente di non dover applicare la disciplina di protezione dei dati a informazioni riconducibili ai pazienti coinvolti nella sperimentazione, i promotori invitano, in genere, i centri ad informare i pazienti interessati che i dati che li riguardano saranno trasmessi dal medico dello studio alla società che lo ha commissionato esclusivamente in forma anonima. Ciò non consente di far comprendere ai pazienti interessati, riguardo al trattamento dei dati, quali siano i ruoli effettivamente svolti dallo *sponsor* e dagli altri soggetti, della cui collaborazione queste eventualmente si avvalgano.

Così formulata, l'informativa ai pazienti inclusi nelle sperimentazioni è, quindi, inidonea ai sensi del Codice (art. 13), in quanto non permette agli interessati di esprimere una volontà consapevole riguardo al fatto che i trattamenti effettuati presso lo *sponsor* o i soggetti che eventualmente collaborano con il primo (anche al di fuori del territorio nazionale) concernono informazioni che, seppure codificate, sono in realtà riconducibili ai medesimi interessati.

L'informativa da fornire agli interessati tramite i centri di sperimentazione deve pertanto comprendere indicazioni specifiche relative a:

a. la natura dei dati trattati dal promotore e la circostanza che tali dati vengono trasmessi all'estero;
b. il ruolo effettivamente svolto dal promotore riguardo al trattamento dei dati e le finalità e modalità di quest'ultimo;
c. i soggetti o le categorie di soggetti ai quali i dati possono essere comunicati o che possono venirne a conoscenza in qualità di incaricati o di responsabili;
d. l'esercizio del diritto d'accesso e gli altri diritti in materia di dati personali nei confronti del promotore e degli altri soggetti eventualmente destinatari dei dati (artt. 7 e 8 del Codice);

7. Consenso al trattamento dei dati

Anche il modello che i centri di sperimentazione sono tenuti a sottoporre agli interessati per raccogliere le dichiarazioni di consenso al trattamento dei dati che li riguardano viene di regola predisposto dalle società committenti e sottoposto all'esame dei comitati etici interessati (artt. 6, 7, 8 e 11 d.lg. n. 211/2003).

Le formule solitamente utilizzate per la manifestazione del consenso si limitano ad autorizzare il medico a far esaminare la documentazione medica originale dei pazienti da parte del personale dello *sponsor* addetto al monitoraggio (o da personale esterno da questi delegato), dei componenti del comitato etico e delle autorità sanitarie competenti al fine di verificare le procedure dello studio e/o l'accuratezza dei dati raccolti (d.m. 15 luglio 1997, all. 1/4B punto 4.8.10). Tali formule non consentono, invece, agli interessati di esprimere la propria volontà circa gli ulteriori trattamenti di dati effettuati presso lo *sponsor* e/o i soggetti che, anche all'estero, collaborano eventualmente con il primo nell'ambito della sperimentazione.

Lo *sponsor* e i suoi eventuali collaboratori non possono utilizzare lecitamente i dati personali dei pazienti inclusi negli studi clinici se non provvedono ad acquisire previamente dagli interessati, tramite i centri di sperimentazione, idonee e specifiche manifestazioni di consenso riguardo ai trattamenti di dati da essi effettuati (artt. 23 e 26 del Codice).

8. Trasferimento di dati all'estero

Nelle sperimentazioni cliniche dei medicinali accade, frequentemente, che le informazioni e i campioni biologici dei pazienti, raccolti dai medici sperimentatori in un Paese, vengano trasferiti a soggetti ubicati in altri Paesi, anche al di fuori dell'Unione europea, o siano resi accessibili a diverse categorie di soggetti aventi sede in tali Paesi. Ciò, avviene specialmente negli studi promossi da società farmaceutiche che operano nell'ambito di gruppi multinazionali nei quali gli stessi promotori, gli addetti al monitoraggio dello studio, il laboratorio di analisi e gli altri soggetti esterni che collaborano con il promotore, possono avere sede in Paesi terzi.

Tali informazioni, in quanto riconducibili ai singoli pazienti interessati, possono essere trasferite lecitamente in Paesi extra-Ue che non garantiscono un livello adeguato di protezione dei dati personali a condizione che i pazienti interessati ne siano stati previamente informati e abbiano manifestato per iscritto un consenso specifico (art. 43, comma 1, lettera *a)* del Codice), ovvero vengano adottate garanzie equipollenti e adeguate per i diritti degli interessati (art. 44, comma 1, lett. *b)* del Codice). In particolare, costituiscono garanzie sufficienti per la tutela della vita privata e dei diritti degli interessati le clausole contrattuali *standard* per il trasferimento di dati personali a "responsabili del trattamento" residenti in Paesi terzi (*cfr.* decisione della Commissione europea del 27 dicembre 2001, n. 2002/16/Ce e deliberazione del Garante n. 3 del 10 aprile 2002, doc. *web* n. 1065361), nonché quelle previste per il trasferimento di dati effettuati da un "titolare del trattamento" avente sede nell'Unione europea a un diverso "titolare" residente al di fuori del territorio europeo (*cfr.* decisione della Commissione europea del 15 giugno 2001, n. 2001/497/Ce e deliberazione del Garante del 10 ottobre 2001, doc. *web* n. 42156; decisione del 27 dicembre 2004, n. 2004/915/Ce e autorizzazione del Garante del 9 giugno 2005, doc. *web* n. 1151949). Ai fini dell'utilizzazione delle citate clausole è comunque necessario definire preventivamente, con chiarezza e precisione, i ruoli svolti dai soggetti nell'ambito del trasferimento dei dati e delle operazioni di trattamento effettuate in conformità ai parametri indicati (l'esportatore deve effettivamente risultare "titolare" del trattamento e, l'importatore, deve essere l'effettivo "responsabile" o "titolare" autonomo del trattamento), nonché specificare le attività principali di trattamento cui sottoporre le informazioni personali oggetto di trasferimento.

Per ciò che concerne il trasferimento di dati verso organizzazioni stabilite negli Stati Uniti d'America fornisce parimenti adeguate garanzie per l'interessato l'adesione ai princìpi in materia di riservatezza contenuti nel *cd.* accordo del *"Safe Harbor"* (*cfr.* decisione della Commissione europea del 26 luglio 2000 n. 2000/520/Ce e autorizzazione del Garante del 10 ottobre 2001, doc. *web* n. 30939).

9. Periodo di conservazione e trattamento di dati per ulteriori fini di ricerca

I dati e i campioni biologici dei pazienti partecipanti alle sperimentazioni devono essere conservati per un arco di tempo non superiore a quello necessario per conseguire le finalità per le quali sono stati raccolti e trattati (art. 11, comma 1, lett. *e)* del Codice, autorizzazione del Garante al trattamento dei dati genetici del 22 febbraio 2007, doc. *web* n. 1389918).

Al riguardo, la normativa applicabile alle sperimentazioni cliniche prevede che i documenti essenziali relativi allo studio (compresa la documentazione medica riferita ai singoli pazienti) debbano essere conservati presso lo *sponsor* e i centri partecipanti per almeno sette anni dopo il completamento della sperimentazione, ovvero per un periodo di tempo considerevolmente più lungo in conformità alla disciplina applicabile o agli accordi intervenuti tra *sponsor* e centri partecipanti (art. 18 d.lg. n. 200/2007; d.lg. n. 219/2006, all. 1, punto 5.2, lett. c); d.m. 15 luglio 1997, all. 1/4B, punti 4.9.4 e 4.9.5 e all. 1/5A, punti 5.5.11 e 5.5.12).

Le società che hanno commissionato uno studio clinico possono utilizzare lecitamente in future attività di studio e di ricerca i dati e i campioni biologici riconducibili ai singoli interessati, anche avvalendosi dei soggetti esterni che hanno collaborato con le prime per l'esecuzione della sperimentazione, a condizione che i pazienti ne siano stati previamente e adeguatamente informati e abbiano manifestato per iscritto un consenso specifico e distinto (artt. 11, comma 1, lett. *e)*, 13, 26 e 99 del Codice; aut. *cit.* del 22 febbraio 2007, doc. *web* n. 1389918).

10. Custodia e sicurezza dei dati

A seguito dei primi approfondimenti, anche tecnici, svolti nell'ambito degli accertamenti ispettivi effettuati presso alcune società *sponsor* e altri soggetti coinvolti nelle sperimentazioni sono stati individuati idonei accorgimenti e misure da porre a garanzia degli interessati nei trattamenti di dati effettuati per l'esecuzione di tali studi. La particolare delicatezza dei dati trattati nella sperimentazione impone, infatti, l'adozione di specifici accorgimenti tecnici per incrementare il livello di sicurezza dei dati (art. 31 del Codice) senza pregiudizio di ogni altra misura minima che ciascun titolare del trattamento deve adottare ai sensi del Codice (art. 33 e ss.). Ciò, con particolare riferimento alle operazioni di registrazione con strumenti elettronici dei dati dei pazienti coinvolti nello studio presso i centri di sperimentazione, al loro trasferimento in via telematica verso un unico *database* presso la società committente o gli altri soggetti che svolgono, per conto di quest'ultima, la validazione e l'elaborazione statistica dei dati, nonché alla gestione della medesima banca dati.

In relazione a tali operazioni di trattamento deve ritenersi che le società *sponsor* di sperimentazioni cliniche di medicinali, le organizzazioni di ricerca a contratto e i centri di sperimentazione, ciascuno per la parte di propria competenza, debbano adottare, per effetto del provvedimento che il Garante si accinge a deliberare:

a. procedure di autenticazione forte (*strong authentication*) per l'accesso individuale ai sistemi di elaborazione elettronici per la registrazione dei dati;
b. sistemi di memorizzazione e archiviazione dei dati (*file system* o *database system*) con funzioni crittografiche avanzate basate su algoritmi robusti in grado di proteggere i dati registrati dai rischi di accesso abusivo, furto o smarrimento parziali o integrali di supporti di memorizzazione o di sistemi di elaborazione portatili e fissi;
c. protocolli di comunicazione sicuri basati sull'utilizzo di *standard* crittografici per la trasmissione elettronica dei dati raccolti dai centri di sperimentazione al *database* centralizzato presso la società farmaceutica o gli altri soggetti che effettuano la successiva validazione ed elaborazione statistica dei dati;
d. con specifico riferimento al menzionato *database*:
   - procedure di autenticazione forte (*strong authentication*) per l'accesso individuale ai sistemi centralizzati con cui è realizzato il *database*;
   - idonei profili di autorizzazione per gli incaricati del trattamento in funzione dei ruoli e delle esigenze di accesso e trattamento;
   - verifiche periodiche sulla qualità e coerenza delle credenziali di autenticazione e dei profili di autorizzazione assegnati agli incaricati del trattamento;
   - sistemi di *audit log* per il controllo degli accessi al *database* e per il rilevamento di eventuali anomalie.

Il Garante si riserva di stabilire il termine entro il quale le prescrizioni che saranno impartite dall'Autorità dovranno essere attuate dalle società *sponsor* di sperimentazioni cliniche di medicinali, dalle organizzazioni di ricerca a contratto e dai centri di sperimentazione. Il Garante si riserva altresì di individuare alcuni trattamenti da notificare all'Autorità ai sensi dell'art. 37, comma 2, del Codice.

44 Guida pratica e misure di semplificazione per le piccole e medie imprese (*) *24 maggio 2007*

Registro delle deliberazioni
n. 21 del 24 maggio 2007

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Nella riunione odierna, in presenza del prof. Francesco Pizzetti, presidente, del dott. Giuseppe Chiaravalloti, vice presidente, del dott. Mauro Paissan e del dott. Giuseppe Fortunato, componenti, e del dott. Giovanni Buttarelli, segretario generale;

Visto il d.lg. 30 giugno 2003, n. 196 (Codice in materia di protezione dei dati personali) con particolare riferimento all'art. 154, comma 1, lett. *h*);

Esaminate le istanze provenienti da associazioni di categoria, con particolare riferimento alle piccole e medie imprese, ivi compresi gli artigiani, in materia di adempimenti derivanti dalla disciplina di protezione dei dati personali;

Ritenuta l'opportunità di indicare, a tal proposito, linee di comportamento conformi al Codice e misure di semplificazione da questo previste in grado di fornire orientamenti utili per gli operatori economici nel rispetto dei diritti degli interessati;

Rilevata l'esigenza che tale quadro sia riassunto in una guida pratica, suscettibile di aggiornamento periodico e di cui verrà curata la più ampia pubblicità anche attraverso il sito Internet dell'Autorità (*www.garanteprivacy.it*);

Viste le osservazioni formulate dal segretario generale ai sensi dell'art. 15 del regolamento del Garante n. 1/2000;

Relatore il dott. Giuseppe Fortunato;

DELIBERA

1. ai sensi dell'art. 154, comma 1, lett. *h*), del Codice, di adottare il documento *"Guida pratica e misure di semplificazione per le piccole e medie imprese"*, allegato quale parte integrante della presente deliberazione (Allegato 1);
2. ai sensi dell'art. 143, comma 2, del Codice, di trasmettere copia del presente provvedimento al Ministero della giustizia-Ufficio pubblicazione leggi e decreti, unitamente alle menzionata "Guida pratica", per la pubblicazione sulla *Gazzetta Ufficiale* della Repubblica italiana.

Roma, 24 maggio 2007

IL PRESIDENTE
Pizzetti

IL RELATORE
Fortunato

IL SEGRETARIO GENERALE
Buttarelli

(*) ***G.U.*** **21 giugno 2007, n. 142**
[doc. *web* n. 1412271]

GUIDA PRATICA E MISURE DI SEMPLIFICAZIONE
PER LE PICCOLE E MEDIE IMPRESE (*)

Sommario

Con la disciplina contenuta nel decreto legislativo n. 196 del 2003 *(Codice in materia di protezione dei dati personali)* l'ordinamento italiano si è dotato di un quadro organico per attuare obblighi internazionali nascenti dalla Convenzione del Consiglio d'Europa sulla protezione delle persone rispetto al trattamento automatizzato di dati di carattere personale (Strasburgo, 28 gennaio 1981) e per recepire direttive comunitarie (95/46/Ce e 2002/58/Ce).

Specie nello svolgimento delle ordinarie attività d'impresa, e in particolare per le realtà produttive di piccole dimensioni, alcuni adempimenti contenuti nella disciplina di protezione dei dati personali vengono reputati talvolta onerosi. Una giusta protezione dei dati personali e della riservatezza può in verità rappresentare una risorsa per l'impresa, rendendone più efficiente l'attività in modo da incrementare la fiducia di consumatori e utenti.

Questa guida intende fornire a chi opera nella realtà delle medie e piccole imprese uno strumento utile per curare gli adempimenti derivanti dalla normativa vigente, indicando le soluzioni semplificate a disposizione.

La guida, integrata da una *check list* e pubblicata sul sito *web* dell'Autorità, potrà subire aggiornamenti nel tempo[1].

1. I soggetti che effettuano il trattamento

Nello svolgimento dell'attività di impresa è normale che vengano trattati dati personali, vale a dire informazioni riferibili a soggetti identificati o identificabili (ad esempio, dipendenti [2], clienti e fornitori). I dati devono essere pertinenti e non eccedenti rispetto a finalità legittime, esatti e aggiornati (art. 11 del Codice). Le operazioni di trattamento (quali la raccolta, comunicazione o diffusione di dati personali) sono effettuate anche a cura del responsabile (se designato) e degli incaricati del trattamento.

1.1. *Chi è il titolare del trattamento?*

Il *"titolare del trattamento"*, è la "[...] *entità che esercita un potere decisionale del tutto autonomo sulle finalità e sulle modalità del trattamento, ivi compreso il profilo della sicurezza"* (art. 28 del Codice). In particolare, nell'ambito dello svolgimento dell'attività economica, *"titolare del trattamento"* può essere la persona fisica (si pensi all'imprenditore individuale) o giuridica (ad esempio, la società) che tratta i dati (con la raccolta, la registrazione, la comunicazione o la diffusione).

Il *"titolare del trattamento"* è chiamato ad attuare gli obblighi in materia (riassunti nella presente *Guida*) e, se ritiene di designare uno o più responsabili del trattamento, è tenuto a vigilare sulla puntuale osservanza delle istruzioni da impartire loro.

1.2. *Chi sono i responsabili del trattamento?*

Il *"responsabile del trattamento"* (possono essere più d'uno), è una figura che può essere designata a propria discrezione dal titolare del trattamento con un atto scritto nel quale

(*) *Le note sono in calce al testo*

vanno indicati i compiti affidati. Occorre scegliere persone fisiche od organismi 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 (**art. 29** del Codice).

Tale figura, la cui designazione da parte del "titolare del trattamento" è quindi facoltativa, ricorre frequentemente in presenza di articolazioni interne delle realtà produttive dotate di una certa autonomia (*ad es.*, possono essere designati responsabili del trattamento i dirigenti di funzioni aziendali, quali quelle del personale o del settore *marketing*) o, rispetto a soggetti esterni all'impresa, per svariate forme di *outsourcing* che comportino un trattamento di dati personali (*ad es.*, per i centri di elaborazione dati contabili, per i servizi di postalizzazione, per le società di recupero crediti [3]).

1.3. *Chi sono gli incaricati del trattamento?*

Gli "incaricati del trattamento" sono soggetti (solo persone fisiche) che effettuano materialmente le operazioni di trattamento dei dati personali e operano sotto la diretta autorità del titolare (o del responsabile) attenendosi a istruzioni scritte (**art. 30** del Codice). Il "titolare del trattamento" è tenuto a designarli.

È sufficiente assegnare un dipendente ad una unità organizzativa, a condizione che risultino per iscritto le categorie di dati cui può avere accesso e gli ambiti del trattamento [4].

2. La notifica del trattamento

La notificazione è una dichiarazione con la quale il titolare del trattamento, prima di iniziarlo, rende nota al Garante (che la inserisce nel registro pubblico dei trattamenti consultabile da chiunque sul sito *web* dell'Autorità) l'esistenza di un'attività di raccolta e di utilizzazione dei dati personali.

2.1. *È sempre necessario notificare il trattamento dei dati al Garante?*

In linea di principio i trattamenti ordinari svolti presso piccole realtà produttive non vanno notificati: si pensi ai trattamenti di dati relativi ai dipendenti, ai fornitori o alla clientela [5]. In particolare, **non devono essere notificati i dati relativi agli inadempimenti dei propri clienti tenuti da ciascuna impresa.**

In questo quadro la notificazione deve essere effettuata in ipotesi particolari (indicate all'**art.** 37 del Codice). Con specifico riguardo all'attività di impresa, i trattamenti soggetti a notificazione sono quelli relativi a:

- 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; come detto, **non rientrano in quest'ambito, i dati relativi agli inadempimenti dei propri clienti tenuti da ciascuna impresa.**
- dati genetici [6], biometrici o dati che indicano la posizione geografica di persone od oggetti mediante una rete di comunicazione elettronica (ad esempio, dati trattati mediante sistemi di geolocalizzazione installati su veicoli al fine di individuarne la posizione);
- 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 (*cd.* profilazione), ovvero a monitorare l'utilizzo di servizi di comunicazione elettronica con esclusione dei trattamenti tecnicamente indispensabili per fornire i servizi medesimi agli utenti;
- dati sensibili registrati in banche di dati a fini di selezione del personale per conto terzi (non, quindi, quelli trattati direttamente dall'imprenditore), nonché dati sensibili utilizzati per sondaggi di opinione, ricerche di mercato e altre ricerche campionarie.

2.2. *Come si effettua la notificazione al Garante?*

Solo utilizzando l'interfaccia disponibile sul sito *web* dell'Autorità e seguendo le istruzioni ivi indicate (*v.* art. 38 del Codice).

2.3. *Quando occorre fare una nuova notificazione?*

Solo in caso di cessazione del trattamento o di mutamento di alcuni elementi dell'originaria notificazione.

3. L'informativa

Chi effettua operazioni di trattamento di dati personali deve rappresentare agli interessati le caratteristiche essenziali dei trattamenti effettuati. L'informativa deve essere resa per i dati raccolti presso l'interessato e per quelli reperiti presso terzi. La disciplina prevede alcune ipotesi di semplificazione e di esonero.

3.1. *Cosa è l'informativa?*

L'informativa, da rendersi con **chiarezza e senza inutili formalità, anche in modo sintetico e colloquiale**, contiene i seguenti elementi (**art. 13** del Codice):

- finalità e modalità del trattamento;
- natura obbligatoria o facoltativa del conferimento dei dati e conseguenze di un eventuale rifiuto di rispondere;
- soggetti o categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza;
- diritti riconosciuti all'interessato dall'articolo 7 del Codice;
- estremi identificativi del titolare e, se designato, del responsabile del trattamento.

Se taluno di questi elementi è già noto all'interessato, non è necessario farlo presente nuovamente.

3.2. *Quando deve essere resa l'informativa?*

In caso di dati raccolti presso l'interessato, l'informativa deve essere resa, anche in forma orale, prima delle operazioni del trattamento. Nel rapporto con fornitori, clienti, dipendenti e collaboratori **non è necessario ripeterla in occasione di ogni contatto:** è sufficiente fornirla con una formula generale *una tantum*, all'inizio delle operazioni di trattamento (che potranno anche protrarsi nel tempo).

L'informativa deve essere resa anche nel caso in cui i dati personali sono raccolti presso terzi; in tal caso, deve essere fornita al momento della registrazione dei dati o, se è prevista la comunicazione a terzi da parte del titolare, non oltre la prima comunicazione. Vanno indicate anche le categorie dei dati trattati.

3.3. *È possibile rendere l'informativa in una forma semplificata?*

È possibile fornire l'informativa anche oralmente, in modo sintetico e colloquiale, senza includere elementi già noti all'interessato (art. 13, comma 2, del Codice). Si può utilizzare anche uno spazio all'interno dell'ordinario materiale cartaceo e della corrispondenza.

Inoltre la disciplina prevede margini ulteriori di semplificazione (art. 13, comma 3, del Codice), tenendo conto delle circostanze concrete da rappresentare al Garante, formulando apposita **istanza**, anche tramite associazioni di categoria.

3.4. *In quali casi non è necessario rendere l'informativa agli interessati?*

In relazione ai dati raccolti presso terzi, tenuto conto delle circostanze concrete, si può omettere di fornire l'informativa se i dati sono trattati (art. 13, comma 5, lett. *c*), del Codice):

- in base ad un obbligo previsto dalla legge, da un regolamento o dalla normativa comunitaria;
- ai fini dello svolgimento delle investigazioni difensive (legge 7 dicembre 2000, n. 397) o per far valere o difendere un diritto in sede giudiziaria.

Inoltre, è prevista la possibilità di esonero totale o parziale dall'obbligo di fornire l'informativa:

- nei casi in cui renderla, a giudizio del Garante –cui può essere inviata apposita **istanza**–, risulti impossibile o manifestamente sproporzionato rispetto al diritto fatto valere.

4. Il consenso dell'interessato

Talora il soggetto privato che effettua operazioni di trattamento è tenuto a raccogliere il consenso dell'interessato per effettuare un trattamento di dati lecito (**art. 23** del Codice). Più spesso, però, nello svolgimento dell'ordinaria attività d'impresa, il consenso dell'interessato non è necessario (**art. 24** del Codice).

4.1. *Nello svolgimento dell'attività d'impresa è necessario acquisire il consenso degli interessati?*

Con particolare riferimento ai trattamenti di dati personali (non sensibili) nell'ordinaria attività d'impresa, non è necessario il consenso nei casi in cui (*cfr.* art. 24 del Codice):

- i dati vengono trattati nell'esecuzione di un contratto o in fase pre-contrattuale (art. 24, comma 1, lett. *b*), del Codice);
- il trattamento viene posto in essere per dare esecuzione a un obbligo legale (art. 24, comma 1, lett. *a*) del Codice);
- i dati provengono da registri ed elenchi pubblici (art. 24, comma 1, lett. *c*), del Codice);
- i dati sono relativi allo svolgimento di attività economiche da parte dell'interessato (art. 24, comma 1, lett. d), del Codice).

A queste macro-categorie, che comprendono larga parte dei trattamenti effettuati ordinariamente da un'impresa, devono essere aggiunte le ulteriori ipotesi di esonero enumerate all'art. 24 del Codice [7].

Nei casi restanti, l'interessato deve aver manifestato un consenso libero, specifico e informato in relazione al trattamento effettuato. Il consenso deve essere documentato per iscritto (art. 23 del Codice).

4.2. *Quali sono gli adempimenti da osservare per trattare dati sensibili?*

Cautele maggiori devono essere osservate nel trattamento dei **dati sensibili**: tali sono considerate le informazioni idonee 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 dei dati personali idonei a rivelare lo stato di salute e la vita sessuale (**art. 4, comma 1, lett. *d*)**, del Codice).

Per il trattamento dei dati sensibili di regola è necessario il consenso scritto, oltre l'autorizzazione del Garante.

Il Garante ha rilasciato **sette autorizzazioni generali** che comprendono tutti i trattamenti abitualmente effettuati nell'ordinaria attività di impresa. Non vi è quindi bisogno di rivolgere una richiesta al Garante, che va presentata solo per casi del tutto eccezionali non contemplati dalle medesime autorizzazioni già rilasciate (questa ipotesi si è sinora verificata in casi rari) [8].

Inoltre, per i dati sensibili il Codice non richiede il consenso dell'interessato se:

- il trattamento è necessario per svolgere le investigazioni difensive di cui alla legge 7 dicembre 2000, n. 397 o per far valere o difendere in sede giudiziaria un diritto. I dati vanno trattati solo per tali finalità e per il periodo strettamente necessario al loro perseguimento (art. 26, comma 4, lett. *c*) del Codice) [9];
- il trattamento è necessario per adempiere a specifici obblighi o compiti previsti dalla legge oppure da un regolamento o dalla normativa comunitaria per la gestione del rapporto di lavoro, anche in materia di igiene e sicurezza del lavoro e della popolazione e di previdenza e assistenza. Occorre rispettare i limiti previsti dall'autorizzazione generale del Garante (art. 26, comma 4, lett. *d*) del Codice).

5. La sicurezza dei sistemi

Il profilo della sicurezza e dell'integrità delle informazioni oggetto di legittimo trattamento è un elemento qualificante delle discipline di protezione dei dati personali (**artt. 31 ss.** del Codice e disciplinare tecnico di cui all'All. B al Codice).

5.1. *Chi deve adottare le misure di sicurezza*

L'obbligo generale di adottare idonee misure di sicurezza è posto dal Codice. Il titolare del trattamento può adempiervi avvalendosi anche di un responsabile (art. 29, comma 2, del Codice).

5.2. *Quali misure di sicurezza devono essere adottate?*

Il titolare del trattamento è tenuto ad adottare tutte le misure idonee, valutate alla luce delle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle caratteristiche del trattamento, a ridurre i rischi di distruzione o di perdita anche accidentale dei dati o di accesso non autorizzato o non consentito ai dati (**art. 31** del Codice).

In questo quadro vanno anche attuate le misure minime, applicabili a piccole e medie imprese (**artt. 33-35** e all. B del Codice [10]).

5.3. *Come e quando deve essere redatto il Dps?*

In base alla vigente disciplina, in caso di trattamento di dati sensibili e giudiziari attraverso sistemi informatici deve essere redatto il documento programmatico sulla sicurezza (art. 34, comma 1, lett. *g*) e **regola 19 dell'Allegato B** al Codice). Si può tener conto dei suggerimenti già formulati dal Garante che –recependo le esigenze e le istanze peculiari di professionisti e piccoli operatori, con particolare riguardo alle piccole e medie imprese– ha già reso disponibile *on-line*, a far data dal 11 giugno 2004, una *"Guida operativa"*.

Il Dps:

- va redatto o aggiornato entro il 31 marzo di ciascun anno;
- non deve essere comunicato al Garante, ma semplicemente conservato dal titolare presso la propria struttura per essere esibito in occasione di eventuali accertamenti ispettivi (**art. 34**, comma 1, lett. *g*) del Codice e regola 19 dell'Allegato B) al Codice);
- deve essere redatto dal "[...] titolare di un trattamento di dati sensibili o giudiziari anche attraverso il responsabile, se designato [...]" (regola 19 dell'All. B) *cit.*).

6. Il trasferimento di dati personali in Paesi terzi

Nello svolgimento dell'attività di impresa può risultare necessario trasferire dati personali fuori dell'Unione europea (ad esempio relativi alla clientela o ai dipendenti). Il Codice prevede specifiche regole al riguardo.

6.1. *Quando si applica la disciplina del Codice in materia di trasferimento di dati fuori dall'Unione europea?*

La disciplina in materia di trasferimento di dati fuori dall'Unione europea (Ue) riguarda principalmente i flussi di dati personali verso i *cd.* Paesi terzi, considerato che i Paesi situati all'interno dell'Ue hanno attuato, nei rispettivi ambiti, la direttiva 95/46/Ce, adottando specifiche normative in materia di protezione dei dati personali. Il loro rispetto è considerato idoneo per trasferire dati nell'Ue (**art. 42** del Codice).

6.2. *In quali casi è consentito il trasferimento dei dati fuori dall'Unione europea?*

Il trasferimento è sempre consentito in varie ipotesi (**art. 43** del Codice), tra le quali, con particolare riferimento alle attività d'impresa, possono ricordarsi i casi in cui:

- l'interessato ha manifestato il proprio consenso espresso e, se si tratta di dati sensibili, in forma scritta;
- il trasferimento è necessario 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, ovvero per la conclusione o per l'esecuzione di un contratto stipulato a favore dell'interessato;
- il trasferimento è necessario per la salvaguardia di un interesse pubblico rilevante individuato con legge o con regolamento;
- è necessario ai fini dello svolgimento delle investigazioni difensive (legge 7 dicembre 2000, n. 397), o, comunque, per far valere o difendere un diritto in sede giudiziaria;
- il trattamento concerne dati riguardanti persone giuridiche, enti o associazioni.

6.3. *Qualora non sussistano i presupposti sopra indicati, in quali circostanze il trasferimento è comunque autorizzato?*

Il trasferimento è consentito anche quando è autorizzato dal Garante in presenza di adeguate garanzie per i diritti dell'interessato:

- individuate dal Garante;
- in base alle decisioni di adeguatezza adottate dalla Commissione europea in ordine al livello di protezione dei dati garantito dall'ordinamento del Paese destinatario (artt. 25, *par.* 6, e 26, *par.* 4, della direttiva 95/46/Ce) [11];
- in base alla decisione di adeguatezza delle garanzie contenute nel *Safe Harbor* per il trasferimento verso organizzazioni stabilite negli Stati Uniti d'America che ad esso aderiscono [12];
- in base all'adozione di clausole contrattuali *standard* tra "esportatore" e "importatore" di dati, il cui contenuto è stato ritenuto idoneo dalla Commissione europea (artt. 25, *par.* 6, e 26, *par.* 4, della direttiva 95/46/Ce) [13] .

7. I doveri del titolare del trattamento in caso di esercizio dei diritti degli interessati ai sensi dell'art. 7 del Codice

La disciplina di protezione dei dati personali attribuisce a ciascun interessato il diritto di accedere ai dati personali a sé riferiti e di esercitare gli altri diritti previsti dall'art. 7 del Codice [14].

7.1. *Cosa si deve fare quando l'interessato esercita il diritto d'accesso?*

Se l'interessato esercita il proprio diritto d'accesso ai dati che lo riguardano o uno degli altri diritti che gli sono riconosciuti, il titolare del trattamento (o il responsabile) deve fornire riscontro (di regola) entro quindici giorni dal ricevimento dell'istanza (**art. 146** del Codice).

7.2. *Quali sono le conseguenze nel caso in cui non venga fornito il riscontro all'interessato?*

In caso di omesso o incompleto riscontro, i predetti diritti possono essere fatti valere dinanzi all'autorità giudiziaria o con ricorso al Garante (**art. 145** del Codice).

8. *Check list*

La seguente lista di controllo è predisposta per i "titolari del trattamento"; mira a riassumere, in forma interrogativa, i punti sopra riassunti. La risposta negativa ad uno dei quesiti, denota un possibile profilo critico dal punto di vista della protezione dei dati personali.

Quesito	SI	NO
1. I soggetti che effettuano il trattamento		
È stata effettuata una valutazione circa le operazioni di trattamento di dati personali, anche sensibili, effettuate dall'impresa?		
I dati trattati sono pertinenti e non eccedenti rispetto alle legittime finalità del trattamento, oltre che esatti e aggiornati?		
Le persone fisiche che all'interno dell'impresa trattano dati personali sono state designate tutte quali "incaricate del trattamento"?		
Sono state fornite a tutti gli "incaricati del trattamento" istruzioni scritte circa i propri compiti?		
Se all'interno dell'impresa sono stati individuati soggetti che hanno ambiti di autonomia nel trattamento dei dati personali, sono stati designati per iscritto "responsabili del trattamento"?		
Se fuori dell'impresa enti o persone fisiche trattano dati personali nel suo interesse, obbligati a seguirne le istruzioni (come accade per i casi di *outsourcing*), sono stati designati per iscritto quali "responsabili del trattamento"?		

Quesito	SI	NO
2. La notificazione del trattamento		
Si è verificato, prima di intraprendere operazioni di trattamento, se l'impresa effettua i trattamenti da notificare al Garante?		
Se sono intervenute modificazioni relativamente ai trattamenti già eventualmente notificati, è stato curato il loro aggiornamento in una nuova notificazione?		
Se cessano i trattamenti, ciò ha formato oggetto di specifica notificazione?		

Quesito	SI	NO
3. L'informativa		
È stata fornita l'informativa agli interessati in caso di dati raccolti presso di essi?		
È stata fornita l'informativa agli interessati in caso di dati raccolti presso soggetti diversi dagli interessati stessi?		

Quesito	SI	NO
4. Il consenso dell'interessato		
Il trattamento dei dati personali viene effettuato in presenza di uno dei presupposti di liceità indicati all'art. 24 del Codice?		
Se non ricorre uno dei presupposti di liceità indicati all'art. 24 del Codice, è stato raccolto il consenso dell'interessato?		
Se sono trattati dati sensibili è stato raccolto il consenso scritto degli interessati?		
Se sono trattati dati sensibili, è stato verificato se il trattamento rientra tra quelli già autorizzati dal Garante con le autorizzazioni generali?		
Se il trattamento di dati sensibili non rientra tra quelli previsti dalle autorizzazioni generali, è stata richiesta al Garante un'autorizzazione *ad hoc*?		

Quesito	SI	NO
5. La sicurezza dei dati		
Sono state adottate idonee misure di sicurezza per proteggere i dati personali?		
Sono state adottate le misure minime di sicurezza previste per proteggere i dati personali?		
Se sono trattati dati sensibili e giudiziari, è stato redatto, quando è necessario, il documento programmatico per la sicurezza e ne vengono osservate le previsioni?		
Periodicamente, e comunque entro il 31 marzo di ciascun anno, formano oggetto di rinnovata valutazione le misure di sicurezza individuate con il documento programmatico per la sicurezza?		

Quesito	SI	NO
6. Il trasferimento dei dati in Paesi terzi		
Se i dati personali trattati dall'impresa sono soggetti a trasferimento verso Paesi terzi (esterni all'Unione europea e all'area economica europea), il trasferimento avviene: - in presenza di una delle condizioni previste dall'art. 43 del Codice? oppure - verso uno dei paesi che assicurano un livello adeguato di protezione (Svizzera, Argentina, Isola di Man, Baliato di Guernsey)? oppure - verso un'impresa statunitense che aderisce al *Safe Harbor*? oppure - in presenza di clausole contrattuali *standard* tra esportatore e importatore? oppure - in presenza di un'autorizzazione *ad hoc* da parte del Garante?		

Quesito	SI	NO
7. I doveri del titolare del trattamento in caso di esercizio dei diritti degli interessati ai sensi dell'art. 7 del Codice		
In presenza dell'esercizio del diritto d'accesso, viene dato riscontro all'interessato secondo le modalità previste dalla legge?		

(1) La guida ha mero valore indicativo ed esemplificativo rispetto al contenuto delle disposizioni normative, alla cui osservanza chiunque resta vincolato.

(2) In relazione al trattamento dei dati personali dei dipendenti si vedano altresì le *"Linee-guida in materia di trattamento di dati personali di lavoratori per finalità di gestione del rapporto di lavoro alle dipendenze di datori di lavoro privati"*, doc. *web* n. 1364099.

(3) In materia *v.* il *Provvedimento* generale del 30 novembre 2005, doc. *web* n. 1213644.

(4) Così, in un'azienda nella quale ad una unità organizzativa sono stati assegnati un determinato numero di dipendenti, si potrà ovviare ad una formale designazione (*ad esempio*, mediante consegna di apposita comunicazione scritta), qualora si individuino gli ambiti di competenza (in ordine ai trattamenti di dati consentiti) di quella unità mediante una previsione scritta (*ad es.* nell'organigramma, nel contratto, nei mansionari, *ecc.*) e risulti inoltre che tali dipendenti sono stati assegnati stabilmente a tale unità.

(5) Specifiche indicazioni sono contenute anche nel provvedimento del Garante del 31 marzo 2004 *Provvedimento* relativo ai casi da sottrarre all'obbligo di notificazione, in *G.U.* del 6 aprile 2004, n. 81 e in *www.garanteprivacy.it*, doc. *web* n. 852561. *V.* pure, Chiarimenti sui trattamenti da notificare al Garante, 23 aprile 2004, doc. *web.* n. 993385.

(6) *V.* in materia *Provv.* 22 febbraio 2007, doc. *web* n. 1389918.

(7) Art. 24. *Casi nei quali può essere effettuato il trattamento senza consenso*

1. Il consenso non è richiesto, oltre che nei casi previsti nella Parte II, quando il trattamento:

a) è necessario per adempiere ad un obbligo previsto dalla legge, da un regolamento o dalla normativa comunitaria;

b) è necessario 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) riguarda dati provenienti da pubblici registri, elenchi, atti o documenti conoscibili da chiunque, fermi restando i limiti e le modalità che le leggi, i regolamenti o la normativa comunitaria stabiliscono per la conoscibilità e pubblicità dei dati;

d) riguarda dati relativi allo svolgimento di attività economiche, trattati nel rispetto della vigente normativa in materia di segreto aziendale e industriale;

e) è necessario per la salvaguardia della vita o dell'incolumità fisica di un terzo. Se la medesima finalità riguarda l'interessato e quest'ultimo non può prestare il proprio consenso per impossibilità fisica, per incapacità di agire o per incapacità di intendere o di volere, il consenso è manifestato da chi esercita legalmente la potestà, ovvero da un prossimo congiunto, da un familiare, da un convivente o, in loro assenza, dal responsabile della struttura presso cui dimora l'interessato. Si applica la disposizione di cui all'articolo 82, comma 2;

f) con esclusione della diffusione, è necessario 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, nel rispetto della vigente normativa in materia di segreto aziendale e industriale;

g) con esclusione della diffusione, è necessario, nei casi individuati dal Garante sulla base dei princìpi sanciti dalla legge, per perseguire un legittimo interesse del titolare o di un terzo destinatario dei dati, anche in riferimento all'attività di gruppi bancari e di società controllate o collegate, qualora non prevalgano i diritti e le libertà fondamentali, la dignità o un legittimo interesse dell'interessato;

h) 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;

i) è necessario, in conformità ai rispettivi codici di deontologia di cui all'allegato A), per esclusivi scopi scientifici o statistici, ovvero per esclusivi scopi storici presso archivi privati dichiarati di notevole interesse storico ai sensi dell'articolo 6, comma 2, del decreto legislativo 29 ottobre 1999, n. 490, di approvazione del testo unico in materia di beni culturali e ambientali o, secondo quanto previsto dai medesimi codici, presso altri archivi privati.

(8) *V.*, allo stato, l'Autorizzazione n. 1/2005 al trattamento dei dati sensibili nei rapporti di lavoro - 21 dicembre 2005, in *G.U.* n. 2 del 3 gennaio 2006 Suppl. Ordinario n. 1 e doc. *web* n. 1203930; Autorizzazione n. 2/2005 al trattamento dei dati idonei a rivelare lo stato di salute e la vita sessuale - 21 dicembre 2005, in *G.U.* n. 2 del 3 gennaio 2006 Suppl. Ordinario n. 1 e doc. *web* n. 1203946; Autorizzazione n. 3/2005 al trattamento dei dati sensibili da parte degli organismi di tipo associativo e delle fondazioni - 21 dicembre 2005, in *G.U.* n. 2 del 3 gennaio 2006 Suppl. Ordinario n. 1 e doc. *web* n. 1203934; Autorizzazione n. 4/2005 al trattamento dei dati sensibili da parte dei liberi professionisti - 21 dicembre 2005, in *G.U.* n. 2 del 3 gennaio 2006 Suppl. Ordinario n. 1 e doc. *web* n. 1203954; Autorizzazione n. 5/2005 al trattamento dei dati sensibili da parte di diverse categorie di titolari - 21 dicembre 2005, in *G.U.* n. 2 del 3 gennaio 2006 Suppl. Ordinario n. 1 e doc. *web* n. 1203938; Autorizzazione n. 6/2005 al trattamento dei dati sensibili da parte degli investigatori privati - 21 dicembre 2005, in *G.U.* n. 2 del 3 gennaio 2006 Suppl. Ordinario n. 1 e doc. *web* n. 1203950; Autorizzazione n. 7/2005 al trattamento dei dati a carattere giudiziario da parte di privati, di enti pubblici economici e di soggetti pubblici - 21 dicembre 2005, in *G.U.* n. 2 del 3 gennaio 2006 Suppl. Ordinario n. 1 e doc. *web* n. 1203942.

(9) Tuttavia *"se i dati sono idonei a rivelare lo stato di salute e la vita sessuale, il diritto deve essere di rango pari a quello dell'interessato, ovvero consistente in un diritto della personalità o in un altro diritto o libertà fondamentale e inviolabile"*.

(10) Le misure minime di sicurezza contenute nell'allegato B) del Codice riguardano anzitutto i trattamenti effettuati con strumenti elettronici: esse comprendono un sistema di autenticazione informatica con credenziali di autenticazione (cioè, un codice per l'identificazione dell'incaricato associato a una parola chiave), programmi per elaboratore volti a prevenirne la vulnerabilità (*ad es.*, antivirus), procedure per realizzare il salvataggio periodico dei dati (*cd.* procedure di *back up*) e la redazione di un documento programmatico sulla sicurezza in caso di trattamento di dati sensibili. Per i trattamenti effettuati senza l'ausilio di strumenti elettronici rientrano tra le misure minime le istruzioni scritte finalizzate al controllo ed alla custodia dei dati impartite agli incaricati e l'uso di contenitori o locali con idonea serratura per custodire i dati personali.

(11) Per l'Argentina, Decisione della Commissione del 30 giugno 2003, n. 2003/490/Ce; per il Canada, Decisione della Commissione del 20 dicembre 2001, n. 2002/2/Ce; per il Baliato di Guernsey, Decisione della Commissione del 21 novembre 2003, n. 2003/821/Ce; per l'Isola di Man, Decisione della Commissione del 28 aprile 2004, n. 2004/411/Ce; per la Svizzera, Decisione della Commissione del 26 luglio 2000, n. 2000/518/Ce. In relazione ad esse *v.*, nell'ordine, le autorizzazioni rilasciate dal Garante: Autorizzazione del 9 giugno 2005 in *G.U.* del 25 luglio 2005, n. 171, doc. *web* n. 1151846; Autorizzazione del 30 aprile 2003 in *G.U.* n. 191 del 19 agosto 2003, doc. *web* n. 1075324; Autorizzazione del 7 settembre 2004 in *G.U.* del 22 luglio 2005, n. 169, doc. *web* n. 1139333; Autorizzazione del 9 giugno 2005 in *G.U.* del 25 luglio 2005, n. 171, doc. *web* n. 1151889; Autorizzazione del 17 ottobre 2001 in *G.U.* del 26 novembre 2001 n. 275 - Suppl. Ordinario n. 250, doc. *web* n. 39428.

(12) *Cfr.* Decisione della Commissione europea del 26 luglio 2000 n. 2000/520/Ce e la correlativa l'Autorizzazione del 10 ottobre 2001 (in *G.U.* 26 novembre 2001), doc. *web* n. 39939. Le organizzazioni aderenti al *Safe Harbor* sono pubblicate sul sito *web*: *www.export.gov/safeharbor/* .

(13) *Cfr.* Decisione della Commissione europea del 27 dicembre 2001, n. 2002/16/Ce, relativa alle clausole contrattuali tipo per il trasferimento di dati personali a "incaricati" del trattamento residenti in paesi terzi, a norma della direttiva 95/46/Ce (e correlativa deliberazione del Garante n. 3 del 10 aprile 2002, doc. *web* n. 1065361); Decisione della Commissione europea del 15 giugno 2001, n. 2001/497/Ce, relativa alle clausole contrattuali tipo per il trasferimento di dati a carattere personale verso paesi terzi a norma della direttiva 95/46/Ce (e correlativa deliberazione del Garante del 10 ottobre 2001, doc. *web* n. 42156). La Commissione ha altresì individuato un modello alternativo di clausole contrattuali tipo (definito Insieme II) con la decisione del 27 dicembre 2004, n. 2004/915/Ce (e la correlativa autorizzazione del Garante del 9 giugno 2005, doc. *web* n. 1151949).

(14) 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.

45 Linee-guida sulla pubblicazione di atti da parte di enti locali (*)
19 aprile 2007

Registro delle deliberazioni
n. 17 del 19 aprile 2007

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Nella riunione odierna, in presenza del prof. Francesco Pizzetti, presidente, del dott. Giuseppe Chiaravalloti, vice presidente, del dott. Mauro Paissan e del dott. Giuseppe Fortunato, componenti, e del dott. Giovanni Buttarelli, segretario generale;

Visto il Codice in materia di protezione dei dati personali (d.lg. 30 giugno 2003, n. 196), anche in riferimento all'art. 154, comma 1, lett. *h*);

Esaminate le istanze (segnalazioni e quesiti) pervenute da cittadini e soggetti pubblici riguardo al trattamento di dati personali effettuato nelle attività connesse alla pubblicazione e diffusione di atti e documenti di enti locali;

Ritenuta l'opportunità di individuare un quadro unitario di misure e di accorgimenti necessari e opportuni, volti a fornire orientamenti utili per cittadini e amministrazioni interessate;

Visto il testo unico delle leggi sull'ordinamento degli enti locali (d.lg. 18 agosto 2000, n. 267);

Vista la documentazione in atti;

Viste le osservazioni dell'Ufficio, formulate dal segretario generale ai sensi dell'art. 15 del regolamento del Garante, n. 1/2000;

Relatore il dott. Mauro Paissan;

DELIBERA

1. di adottare le *"Linee-guida in materia di trattamento di dati personali per finalità di pubblicazione e diffusione di atti e documenti di enti locali"* contenute nel documento allegato quale parte integrante della presente deliberazione (Allegato 1);
2. che copia del presente provvedimento sia trasmessa al Ministero della giustizia-Ufficio pubblicazione leggi e decreti, per la sua pubblicazione sulla *Gazzetta Ufficiale* della Repubblica italiana ai sensi dell'art. 143, comma 2, del Codice.

Roma, 19 aprile 2007

IL PRESIDENTE
Pizzetti

IL RELATORE
Paissan

IL SEGRETARIO GENERALE
Buttarelli

(*) *G.U.* 25 maggio 2007
n. 120
[doc. *web* n. 1407101]

ALLEGATO 1

LINEE-GUIDA IN MATERIA DI TRATTAMENTO DI DATI PERSONALI PER FINALITÀ DI PUBBLICAZIONE E DIFFUSIONE DI ATTI E DOCUMENTI DI ENTI LOCALI (*)

Sommario

1. Premessa

Diversi cittadini e amministrazioni si sono rivolti a questa Autorità prospettando alcune problematiche relative alle modalità con le quali gli enti locali danno pubblicità alla propria attività istituzionale, anche di vigilanza e controllo, in rapporto alla protezione dei dati personali contenuti in atti e documenti resi accessibili ai cittadini.

Considerato anche il rilevante numero di tali interessati il Garante ravvisa l'esigenza di adottare le presenti linee-guida, suscettibili di periodico aggiornamento e nelle quali si tiene conto di precedenti decisioni dell'Autorità. (1)

In questa sede vengono prese in specifica considerazione solo questioni riguardanti la pubblicazione e diffusione di atti e documenti tenendo presente che, accanto alle forme di pubblicità scelte dagli enti locali o imposte per legge, restano vigenti gli obblighi per i medesimi enti di attuare la disciplina sul diritto di accesso ai documenti amministrativi e sul distinto diritto di accesso ai dati personali, che sono stati oggetto di numerosi provvedimenti del Garante. (2)

2. Protezione dati e trasparenza: considerazioni generali

La necessità di garantire un livello elevato di tutela dei diritti e delle libertà fondamentali rispetto al trattamento dei dati personali (art. 2, comma 1, del Codice) non ostacola una piena trasparenza dell'attività amministrativa.

(*) *Le note sono in calce al testo*

Tale tutela non preclude la valorizzazione delle attività di comunicazione istituzionale e la partecipazione dei cittadini alla vita democratica, favorite dall'impiego di nuove tecnologie che sono già utilizzate nell'ambito di proficue esperienze avviate nell'e-government e nelle reti civiche. Tuttavia, la presenza di dati personali negli atti e nei documenti conoscibili o diffusi dagli enti locali richiede, da parte di questi ultimi, alcune doverose valutazioni affinché siano rispettati i diritti degli interessati.

In presenza di taluni dati personali o di determinate forme di diffusione vanno inoltre individuate specifiche soluzioni e modalità per attuare la trasparenza in modo ponderato e secondo correttezza.

3. Princìpi generali relativi al trattamento dati da parte degli enti locali

Gli enti locali, in quanto soggetti pubblici, possono trattare dati di carattere personale anche sensibile e giudiziario solo per svolgere le rispettive funzioni istituzionali (art. 18, comma 2, del Codice).

Oltre alle garanzie previste dal Codice e da altre disposizioni normative in materia di protezione dei dati, l'ente locale deve osservare i presupposti e i limiti previsti da ogni altra disposizione di legge o di regolamento che rilevi ai fini del trattamento (art. 18, comma 3, del Codice).

Gli enti locali devono astenersi dal richiedere il consenso al trattamento dei dati da parte degli interessati (art. 18, comma 4, del Codice). Il consenso è infatti richiesto solo nei riguardi di soggetti privati ed enti pubblici economici, nonché in ambito sanitario (rispetto ad organismi sanitari pubblici ed esercenti le professioni sanitarie: artt. 18, comma 4, 23, 76 e ss. del Codice).

La pubblicazione e la divulgazione di atti e documenti determinano una "diffusione" di dati personali, comportando la conoscenza di dati da parte di un numero indeterminato di cittadini. L'interferenza nella sfera personale degli interessati che ne consegue è legittima, solo se la diffusione è prevista da una norma di legge o di regolamento (artt. 4, comma 1, lett. *m*), e 19, comma 3, del Codice).

Prima di intraprendere un'attività che comporta una diffusione di dati personali, l'ente locale deve valutare se la finalità di trasparenza e di comunicazione può essere perseguita senza divulgare tali dati, oppure rendendo pubblici atti e documenti senza indicare dati identificativi adottando modalità che permettano di identificare gli interessati solo quando è necessario: lo impone il principio di necessità, il quale comporta un obbligo di attenta configurazione di sistemi informativi e di programmi informatici per ridurre al minimo l'utilizzazione di dati personali (art. 3 del Codice).

Se questa valutazione preliminare porta a constatare che gli atti e i documenti resi conoscibili o pubblici devono contenere dati di carattere personale, l'ente deve rispettare anche l'ulteriore principio di proporzionalità: i tipi di dati e il genere di operazioni svolte per pubblicarli e diffonderli devono essere infatti pertinenti e non eccedenti rispetto alle finalità perseguite (art. 11, comma 1, lett. *d*), del Codice).

L'ente può trovarsi di fronte all'interrogativo se pubblicare e diffondere anche dati sensibili o giudiziari. La loro particolare delicatezza ne rende lecita la diffusione solo se:

- è realmente indispensabile (artt. 3, 4, comma 1, lett. *d*) ed *e*), 22, commi 3, 8 e 9, del Codice);
- l'ente ha adottato il regolamento in materia previsto dal Codice su parere conforme del Garante (artt. 20, comma 2, 21, comma 2 e 181, comma 1, lett. *a*)). L'ente, salvi casi del tutto particolari che può rappresentare al Garante, non deve rivolgere specifiche richieste di parere a questa Autorità qualora abbia utilizzato, per il proprio regolamento, gli schemi tipo su cui il Garante ha espresso parere favorevole, predisposti per i comuni, le comunità montane e le province, rispettivamente dall'Associazione nazionale dei comuni italiani (Anci), dall'Unione nazionale comuni comunità enti montani (Uncem) e dall'Unione delle province d'Italia (Upi). [3]

Possono avvalersi di tali schemi tipo anche altri enti locali (ad es. unioni di comuni, comunità isolane o di arcipelago), in relazione alle finalità di rilevante interesse pubblico che essi perseguono nei limiti di legge, direttamente o per conto di amministrazioni di riferimento.

4. Forme di pubblicità dei dati personali contenuti in atti e provvedimenti

"Pubblicità", "accessibilità" e "diffusione" non esprimono sempre un'identica situazione. Le forme da osservare per rendere accessibili e per divulgare atti e documenti possono variare a seconda dei casi e comportare quindi modalità e ambiti di conoscenza di tipo differente; conseguentemente, possono rendere necessario o opportuno predisporre accorgimenti di tipo diverso per rispettare i diritti degli interessati.

Per i comuni e le province è prevista per legge una modalità specifica per pubblicare atti e documenti, fermi restando i diritti di accesso a dati personali e a documenti amministrativi.

Tutti gli atti dell'amministrazione comunale e provinciale sono infatti pubblici, ad eccezione di quelli che siano considerati "riservati" per espressa indicazione di legge, oppure per effetto di una dichiarazione del sindaco o del presidente della provincia che ne vieti l'esibizione poiché la loro diffusione può pregiudicare il diritto alla riservatezza di persone, gruppi o imprese (art. 10 d.lg. 18 agosto 2000, n. 267, recante il "Testo unico delle leggi sull'ordinamento degli enti locali").

Spetta all'amministrazione interessata disciplinare il rilascio di questa dichiarazione, sulla base di un apposito regolamento che deve anche dettare norme necessarie per assicurare ai cittadini, tra l'altro, il diritto *"di accedere, in generale, alle informazioni di cui è in possesso l'amministrazione"* (art. 10 d.lg. n. 267/2000 citato).

5. Impiego di tecniche informatiche e telematiche

In questo quadro, l'ente locale deve prevedere le diverse forme di accessibilità ad atti e documenti evitando, per quanto possibile, di applicare modalità indifferenziate che non tengano conto delle finalità sottostanti alla trasparenza, nonché delle diverse situazioni personali. Mentre alcuni documenti possono essere forniti agevolmente ai cittadini solo a richiesta, altri possono essere pubblicati, anche in rete, integralmente o per estratto.

Con un approccio equilibrato e meditato, l'ente locale dovrebbe fare, opportunamente, largo uso di nuove tecnologie che facilitino la conoscenza da parte dei cittadini, tenuto conto anche del diritto all'utilizzo nei loro confronti delle tecnologie telematiche (art. 3 d.lg. 7 marzo 2005, n. 82, recante il "Codice dell'amministrazione digitale").

A parte quanto eventualmente previsto sul piano normativo per specifiche categorie di atti, il regolamento dell'ente locale può valorizzare l'utilizzo di reti civiche e telematiche per mettere a disposizione dei cittadini atti e documenti contenenti dati personali e che attengano, ad esempio, a concorsi o a selezioni pubbliche.

Laddove la finalità da perseguire riguardi prevalentemente solo una o alcune categorie di persone, andrebbero previste forme di accesso in rete selezionato, attribuendo agli interessati una chiave personale (*username* e *password*; n. di protocollo o altri estremi identificativi di una pratica forniti dall'ente agli aventi diritto). Ad esempio, la pubblicità tramite siti *web* su talune procedure concorsuali può essere perseguita divulgando integralmente alcuni atti (*ad es.*, deliberazioni che indicono concorsi o approvano graduatorie), indicando invece in sezioni dei siti ad accesso selezionato alcuni dettagli conoscibili da interessati e controinteressati (elaborati, verbali, valutazioni, documentazione personale comprovante titoli). [4]

Accorgimenti analoghi andrebbero previsti, a seconda dei casi, con riferimento alle graduatorie relative al riconoscimento di autorizzazioni, agevolazioni, benefici ed iniziative a vantaggio di categorie di cittadini (es., procedure per ammettere minori ad asili nido, per assegnare alloggi di edilizia residenziale pubblica, per valutare domande di mobilità o rilasciare autorizzazioni e concessioni edilizie).

In questi casi occorre evitare, nuovamente, di considerare la protezione dei dati come un ostacolo alla trasparenza, prevenendo al tempo stesso la superflua e ingiustificata diffusione indifferenziata di specifiche informazioni e dettagli ininfluenti (che restano conoscibili, in base alla legge, dai soli soggetti legittimati nel caso concreto).

6. Pubblicità assicurata mediante affissione all'albo pretorio

Nell'articolare in modo equilibrato le diverse situazioni prima sintetizzate, l'ente locale deve anche tenere presente che, per assicurare determinati effetti dichiarativi, il predetto Testo unico delle leggi sull'ordinamento degli enti locali prevede che la pubblicazione di tutte le deliberazioni del comune e della provincia debba avvenire non in rete, ma mediante materiale affissione all'albo pretorio nella sede dell'ente, per quindici giorni consecutivi, salvo quanto previsto da specifiche disposizioni di legge (art. 124 d.lg n. 267/2000 citato [5]).

La pubblicazione delle deliberazioni nell'albo pretorio è quindi lecita e non contrasta, per ciò stesso, con la protezione dei dati personali, sempreché sia effettuata osservando gli accorgimenti di seguito indicati.

Peraltro, questa forma di pubblicazione obbligatoria non autorizza, di per sé, a trasporre tutte le deliberazioni così pubblicate in una sezione del sito Internet dell'ente liberamente consultabile. Al tempo stesso, la previsione normativa in questione non preclude neanche all'ente di riprodurre in rete alcuni dei predetti documenti, sulla base di una valutazione responsabile e attenta ai richiamati princìpi e limiti.

É ovviamente consentita la diffusione in Internet di un avviso che indichi il periodo durante il quale determinati documenti sono consultabili presso l'albo pretorio.

Riguardo alla diretta indicazione di dati personali nelle deliberazioni da pubblicare presso l'albo pretorio, va rispettato il richiamato principio di pertinenza e non eccedenza (o, se i dati sono sensibili o giudiziari, di indispensabilità) rispetto alle finalità perseguite con i singoli atti. [6] Si pensi, ad esempio, al dettaglio di dati che possono essere indicati nella redazione di verbali e di resoconti dell'attività degli organi collegiali o assembleari, in rapporto al fine di rispettare il principio di pubblicità dell'attività istituzionale. [7]

La circostanza secondo la quale tutte le deliberazioni sono pubblicate deve indurre l'amministrazione comunale a valutare con estrema attenzione le stesse tecniche di redazione delle deliberazioni e dei loro allegati. Ciò, soprattutto quando vengono in considerazione informazioni sensibili (si pensi ad esempio agli atti adottati nel quadro dell'attività di assistenza e beneficenza, che comportano spesso la valutazione di circostanze e requisiti personali che attengono a situazioni di particolare disagio).

Può risultare ad esempio utile menzionare tali dati solo negli atti a disposizione negli uffici (richiamati quale presupposto della deliberazione e consultabili solo da interessati e controinteressati), come pure menzionare delicate situazioni di disagio personale solo sulla base di espressioni di carattere più generale o, se del caso, di codici numerici.

Occorre, poi, una specifica valutazione per selezionare le informazioni sensibili o a carattere giudiziario che possono essere diffuse. Resta salvo il divieto di diffondere dati idonei a rivelare lo stato di salute degli interessati (artt. 22, comma 8, 65, comma 5, e 68, comma 3, del Codice): è il caso, ad esempio, dell'indicazione di specifici elementi identificativi dello stato di diversamente abile. [8]

7. Materiale a stampa, pubblicazioni e volumi anche per scopi storici

Oltre alle norme in materia di comunicazione istituzionale [9], agli enti locali sono applicabili anche le disposizioni del Codice che riguardano i trattamenti di dati personali finalizzati alla pubblicazione o alla diffusione occasionale di articoli, saggi o altre manifestazioni del pensiero. É parimenti applicabile il codice di deontologia per l'attività giornalistica (art. 136, comma 1, lett. *c*); *Provv.* del 29 luglio 1998, in *G.U.* 3 agosto 1998, n. 179, allegato A.1 al Codice).

Si pensi al caso in cui gli enti locali pubblichino riviste e notiziari anche telematici a sfondo giornalistico o intendano riprodurre all'interno di volumi editi da loro stessi informazioni riferite a particolari eventi verificatisi sul proprio territorio. In tali casi può essere valutata l'opportunità di utilizzare a fini di pubblicazione anche dati personali che sono stati oggetto di autorizzazioni e di deliberazioni già rese conoscibili a chiunque tramite il locale albo pretorio.

Una distinta possibilità di divulgare dati personali può derivare dall'intento dell'ente locale di intraprendere un'attività di studio, indagine, ricerca e documentazione di figure, fatti e circostanze del passato. Questa finalità di tipo storico è oggetto di specifiche disposizioni e garanzie contenute anche in un apposito codice di deontologia e di buona condotta che riguarda, altresì, la consultazione degli archivi storici di enti pubblici, allegato al Codice. [10]

8. Casi specifici che possono essere menzionati nel regolamento locale

Nell'ambito del regolamento che deve assicurare il diritto dei cittadini all'accesso alle informazioni di cui è in possesso l'amministrazione (art. 10 d.lg. n. 267/2000 *cit.*), l'ente locale dovrebbe cogliere l'occasione per definire organicamente la propria politica in tema di trasparenza, in rapporto alle diverse procedure amministrative, alle distinte esigenze di trasparenza da perseguire e al genere di mezzi di diffusione utilizzati, anche in Internet. [11]

Tale regolamento non può rendere inefficaci eventuali limiti, cautele e modalità previsti da norme di settore, quali quelle che regolano la conoscibilità di atti e documenti concernenti:

a) gli atti anagrafici

Mentre i certificati concernenti la residenza e lo stato di famiglia sono rilasciati a chiunque ne faccia richiesta, faone residente sono rilasciati solo ad amministrazioni pubbliche che ne facciano motivata richiesta, per esclusivo uso di pubblica utilità (artt. 33 e 34 d.P.R. 30 maggio 1989, n. 223, recante "Approvazione del nuovo regolamento anagrafico della popolazione residente"); [12]

b) gli estratti degli atti dello stato civile

Anche tali certificazioni sono rilasciate per riassunto, o per copia integrale, soltanto quando ne è fatta espressa richiesta da chi vi ha interesse e qualora il rilascio non sia vietato dalla legge (artt. 106 e ss. d.P.R. 3 novembre 2000, n. 396, recante il "Regolamento per la revisione e la semplificazione dell'ordinamento dello stato civile, a norma dell'articolo 2, comma 12, della l. 15 maggio 1997, n. 127");

c) le pubblicazioni matrimoniali

Tali atti devono restare infatti affissi solo presso la porta della casa comunale, almeno per otto giorni (artt. 55 e ss. d.P.R n. 396/2000 citato);

d) l'organizzazione degli uffici

L'organigramma, l'articolazione degli uffici, le attribuzioni e l'organizzazione di ciascuna unità, corredati dai nominativi dei dirigenti responsabili, nonché l'elenco completo delle caselle di posta elettronica istituzionali attive, devono essere riportati necessariamente "nei siti delle pubbliche amministrazioni" (art. 54 d.lg. 7 marzo 2005, n. 82);

e) dati reddituali

Gli elenchi nominativi dei contribuenti che hanno presentato la dichiarazione dei redditi, o che esercitano imprese commerciali, arti e professioni, sono depositati per la durata di un anno, ai fini della consultazione da parte di chiunque, presso i comuni interessati; l'amministrazione finanziaria stabilisce annualmente con apposito decreto i termini e le modalità per la loro formazione (art. 69 d.P.R. 29 settembre 1973, n. 600, recante "Disposizioni comuni in materia di accertamento delle imposte sui redditi"); con il decreto del 29 settembre 2004 il Direttore dell'Agenzia delle entrate ha previsto, in relazione ai redditi del 2001 e 2002, che gli elenchi nominativi dei soggetti che hanno presentato la dichiarazione ai fini Irpef contengano cognome, nome e data di nascita; categoria di reddito; attività esercitata (se trattasi di soggetto esercente imprese commerciali, arti e professioni); [13]

f) retribuzioni, compensi ed emolumenti

I compensi e le retribuzioni degli amministratori delle società partecipate direttamente o indirettamente dallo Stato, dei dirigenti con incarico conferito ai sensi dell'art. 19, comma 6, del d.lg. 30 marzo 2001, n. 165, nonché dei consulenti, mem-

bri di commissioni e di collegi e dei titolari di qualsivoglia incarico corrisposto dallo Stato, da enti pubblici o da società a prevalente partecipazione pubblica non quotate in borsa devono essere resi noti attraverso la pubblicazione sul sito *web* dell'amministrazione o del soggetto interessato (art. 1, comma 593, l. 27 dicembre 2006, n. 296, recante "Disposizioni per la formazione del bilancio annuale e pluriennale dello Stato (legge finanziaria 2007));

g) autorizzazioni e concessioni edilizie

Il rilascio del permesso di costruire; i dati relativi agli immobili e alle opere realizzati abusivamente, oggetto dei rapporti degli ufficiali ed agenti di polizia giudiziaria e delle relative ordinanze di sospensione; i provvedimenti di sospensione dei lavori e di annullamento del permesso di costruire sono resi noti al pubblico mediante affissione all'albo pretorio del comune (artt. 20, comma 7, 31, comma 7, e 39 comma 5, d.P.R. 6 giugno 2001, n. 380, recante il "Testo unico delle disposizioni legislative e regolamentari in materia edilizia").

9. La diffusione di dati personali su Internet tramite pagina *web*

In termini generali, le disposizioni ed i princìpi sopra richiamati si applicano in relazione a tutte le modalità tecniche utilizzate per divulgare i dati personali.

Rispetto alla diffusione in rete, i dati delle pubbliche amministrazioni vanno resi disponibili e accessibili con l'uso delle tecnologie dell'informazione alle condizioni fissate dall'ordinamento (artt. 50 e ss. d.lg. n. 82/2005 citato). Occorre pertanto verificare, caso per caso, il quadro normativo di riferimento relativo allo specifico regime di pubblicità dei singoli documenti.

Alcune disposizioni di legge o di regolamento dispongono la necessaria messa a disposizione di determinati atti e documenti sul sito *web* dell'ente locale.

Ad esempio, l'ente locale è soggetto ai predetti obblighi di rendere noti, attraverso il proprio sito *web*, l'organigramma degli uffici corredato dal nominativo dei dirigenti responsabili, nonché il nominativo e l'ammontare della retribuzione dei dirigenti con incarico conferito ai sensi dell'art. 19, comma 6, del d.lg. 30 marzo 2001, n. 165, dei consulenti, e dei titolari di incarichi corrisposti (art. 54 d.lg. n. 82/2005 citato; art. 1, comma 593, l. n. 296/2006 citato).

La diffusione in Internet di dati personali pone specifiche valutazioni in rapporto ai diritti degli interessati. I dati così messi a disposizione di un numero indefinito di persone sono consultabili da molteplici luoghi e in qualsiasi momento. Il loro "carattere ubiquitario" è valorizzato dal crescente accesso ad Internet. Attraverso i motori interni ed esterni di ricerca può essere ricostruito unitariamente un numero ingente di dati riferiti a soggetti individuati, più o meno aggiornati e di natura differente. [14]

Decorsi determinati periodi di tempo, la diffusione tramite siti *web* di tali dati può comportare un sacrificio sproporzionato dei diritti degli interessati specie se si tratta di provvedimenti risalenti nel tempo e che hanno raggiunto le loro finalità. L'ente locale, oltre ad assicurare l'esattezza, l'aggiornamento e la pertinenza e non eccedenza dei dati, deve garantire il rispetto del diritto all'oblìo dell'interessato una volta perseguite le finalità poste alla base del trattamento (art. 11, comma 1, lett. *c*), *d*) ed *e*), del Codice).

Nel rispetto di eventuali (e, allo stato, rare) disposizioni di legge o di regolamento che impongano specificamente la messa a disposizione su Internet di dati personali per puntuali periodi, l'ente può trovarsi di fronte all'esigenza di stabilire in via amministrativa per quali congrui periodi di tempo mantenere in rete documenti contenenti dati personali. In tal caso l'ente, dopo aver valutato se è giustificato includere i documenti diffusi in eventuali sezioni del sito che li rendano direttamente individuabili in rete a partire anche da motori di ricerca esterni al sito stesso, deve individuare –opportunamente, con regolamento– periodi di tempo congrui rispetto alle finalità perseguite. Decorsi tali periodi, determinati documenti o sezioni del sito dovrebbero rimanere in rete, ma essere consultabili solo a partire dal sito stesso. [15]

10. Altri casi particolari

A garanzia degli interessati si rendono necessari particolari accorgimenti in determinate situazioni che comportano specifiche esigenze di trasparenza dell'attività amministrativa locale.

10.1. *Albo dei beneficiari di provvidenze di natura economica*

Gli enti locali sono tenuti ad istituire l'albo dei soggetti (ivi comprese le persone fisiche) cui sono stati erogati contributi, sovvenzioni, crediti, sussidi e benefici di natura economica, favorendo accesso e pubblicità, anche per via telematica (artt. 1 e 2 d.P.R. 7 aprile 2000, n. 118, recante il "Regolamento recante norme per la semplificazione del procedimento per la disciplina degli albi dei beneficiari di provvidenze di natura economica, a norma dell'articolo 20, comma 8, della L. 15 marzo 1997, n. 59").

Tale disposizione costituisce un presupposto idoneo per diffondere in modo proporzionato dati di carattere personale (art. 19, comma 3, del Codice). È quindi lecito favorire l'ampia conoscibilità di dati personali necessari per attuare il principio di pubblicità e trasparenza dell'attività amministrativa pubblicando dati (quali i nominativi dei beneficiari e la relativa data di nascita) unitamente all'indicazione della normativa che autorizza l'erogazione (art. 1, comma 2, d.P.R. n. 118/2000 citato).

Resta ferma l'esigenza di non diffondere ulteriori dettagli eccedenti, a seconda dei casi, rispetto alle finalità perseguite (quali, ad esempio, indirizzi, codici fiscali, coordinate bancarie, ripartizioni di assegnatari secondo le fasce dell'Isee-indicatore della situazione economica equivalente (d.lg. 31 marzo 1998, n. 109, recante "Definizioni di criteri unificati di valutazione della situazione economica dei soggetti che richiedono prestazioni sociali agevolate, a norma dell'articolo 59, comma 51, della L. 27 dicembre 1997, n. 449").

Analoga considerazione va formulata con riferimento a dati personali la cui diffusione possa creare imbarazzo, disagio o esporre l'interessato a conseguenze indesiderate (*ad es.*, indicando fuori dei casi previsti analitiche situazioni reddituali o particolari condizioni di bisogno o peculiari situazioni abitative), specie in riferimento a fasce deboli della popolazione (minori di età, anziani, soggetti inseriti in programmi di recupero e di reinserimento sociale).

Nei limiti già illustrati, specie per ciò che riguarda il divieto di diffondere dati sulla salute, gli enti locali possono trattare lecitamente anche dati sensibili e giudiziari indispensabili per applicare la disciplina in materia di concessione, liquidazione, modifica e revoca di benefici economici, agevolazioni, elargizioni e di altri emolumenti ed abilitazioni, individuati nei citati schemi tipo di regolamento (art. 68 del Codice; schede n. 20 per i comuni e n. 8 per le province degli schemi tipo di regolamento citati). [16]

10.2. *Procedure concorsuali e graduatorie*

Nel quadro delle attività delle pubbliche amministrazioni, è prevista la diffusione di esiti concorsuali. In particolare, le graduatorie dei vincitori di concorsi per accedere agli impieghi nelle pubbliche amministrazioni locali sono pubblicate nell'albo pretorio del relativo ente (art. 15 d.P.R. 9 maggio 1994, n. 487, recante il "Regolamento recante norme sull'accesso agli impieghi nelle pubbliche amministrazioni e le modalità di svolgimento dei concorsi, dei concorsi unici e delle altre forme di assunzione nei pubblici impieghi"). Tale operazione, nel caso di graduatorie selettive degli enti locali, trova fondamento nella disposizione di cui al citato art. 10 del d.lg. n. 267/2000.

Indipendentemente dalla forma di diffusione adottata, è necessario richiamare nuovamente l'obbligo di rispettare il principio di pertinenza e non eccedenza nel trattamento dei dati, risultando divulgabili solo i dati strettamente necessari per rendere conoscibile l'esito o la graduatoria di un concorso o di una selezione.

10.2.1. *Concorsi pubblici*

Sulla base degli elementi acquisiti in base alle segnalazioni e ai quesiti pervenuti, non risulta lecito, negli atti delle graduatorie concorsuali da pubblicare, inserire dati superflui quali recapiti di telefonia fissa o mobile, titoli di studio, codice fiscale.

Vanno pubblicati solo i dati personali pertinenti e non eccedenti ai fini del corretto espletamento della procedura concorsuale e della sua rispondenza ai parametri stabiliti nel bando di concorso, in particolare elenchi nominativi ai quali vengano abbinati i risultati di prove intermedie; elenchi di ammessi a prove orali; punteggi riferiti a singoli argomenti di esame; punteggi totali ottenuti.

10.2.2. *Asili nido*

Le amministrazioni locali devono selezionare con particolare attenzione i dati personali da includere nelle deliberazioni diffuse contenenti le graduatorie per ammettere minori agli asili nido, verificando quali tra le informazioni sulla cui base sono stati attribuiti singoli punteggi debbano essere necessariamente inserite anche nell'atto deliberativo.

La graduatoria da affiggere all'albo pretorio deve essere parimenti priva dei dati non necessari ad assicurare il rispetto del principio di pubblicità e trasparenza dell'attività amministrativa tramite la relativa pubblicazione (condizione reddituale del nucleo familiare; ripartizione dei richiedenti secondo le fasce dell'Isee; indirizzi, domicili o residenze del minore), nonché di dati idonei a rivelare lo stato di salute degli interessati (art. 22, comma 8, del Codice).

Non risulta inoltre lecito diffondere indifferenziatamente i punteggi parziali attribuiti a ciascun richiedente sulla base della documentazione presentata, laddove gli stessi siano idonei a rivelare informazioni particolarmente delicate per la dignità e la riservatezza dell'interessato. Ci si riferisce in particolare ai punteggi parziali conferiti in base alle specifiche condizioni soggettive ed oggettive del minore (ad esempio in affidamento familiare) e del suo nucleo familiare (posizione lavorativa dei genitori, presenza di persone diversamente abili), anche alla luce del richiamato divieto di diffondere dati idonei a rivelare lo stato di salute.

10.2.3. *Alienazione e assegnazione di alloggi di edilizia agevolata*

Analoghe valutazioni in termini di pertinenza e non eccedenza devono essere effettuate dall'ente locale in relazione alla diffusione di graduatorie riguardanti l'assegnazione degli alloggi di edilizia agevolata, le quali sono predisposte sulla base di punteggi e di criteri di priorità prescritti nei bandi di concorso e direttamente correlati a particolari situazioni di disagio degli interessati.

Sulla base degli elementi acquisiti in base alle segnalazioni e ai quesiti pervenuti non risulta lecito diffondere indifferenziamente tutti i presupposti oggettivi e soggettivi che hanno determinato l'assegnazione degli alloggi di edilizia agevolata e riguardanti sia il richiedente, sia le persone appartenenti al medesimo nucleo familiare. Si pensi, ad esempio, a specifiche informazioni sullo stato di salute o condizione reddituale, a situazioni di grave disagio abitativo sofferte, alla presenza nel nucleo familiare di anziani o di persone diversamente abili, alla condizione di gestante o di genitore solo con figli minori a carico, alla situazione lavorativa del richiedente, all'indicazione del codice fiscale, alla fascia Isee di appartenenza.

La relativa graduatoria, oltre ai nominativi degli assegnatari corredati dalle informazioni necessarie a renderli identificabili (data di nascita, punteggio finale per l'assegnazione), non deve quindi contenere ulteriori dati personali contrastanti con il richiamato principio di pertinenza e non eccedenza, fermo restando il divieto di pubblicare dati idonei a rivelare lo stato di salute.

10.2.4. *Graduatorie delle domande di mobilità*

Nell'ambito delle procedure di trasferimento tra amministrazioni pubbliche, gli interessati possono fruire di benefici e titoli di preferenza attribuiti in base alla legge 5 febbraio 1992, n. 104 (recante la "Legge-quadro per l'assistenza, l'integrazione sociale e i diritti delle persone handicappate").

Generiche esigenze di pubblicità connesse alla trasparenza della relativa procedura non possono in alcun caso consentire di derogare allo specifico divieto di diffusione dei dati personali idonei a rivelare lo stato di salute (art. 22, comma 8, del Codice).

Alla luce delle segnalazioni e dei quesiti pervenuti, va rilevato che le graduatorie da pubblicare non devono riportare, accanto ai nominativi dei soggetti che hanno presentato domanda di trasferimento, riferimenti riguardanti condizioni di salute che, nella varia casistica esistente, potrebbero giustificare una precedenza degli interessati.

Applicate alle persone diversamente abili, tali cautele rafforzano il principio del rispetto della dignità delle persone interessate, garantito dall'art. 2 del Codice e dall'art. 1 della citata l. n. 104/1992.

11. Altri adempimenti da rispettare

Gli enti locali titolari di trattamenti di dati personali restano infine tenuti a rispettare gli obblighi di trasparenza e di sicurezza che attengono:

a) alla predisposizione di adeguate informative sul trattamento dei dati da fornire ai relativi interessati (art. 13 del Codice);

b) alle necessarie misure anche minime volte ad assicurare l'integrità di dati e sistemi (artt. 31-36 e Allegato B recante il *"Disciplinare tecnico in materia di misure di sicurezza"* del Codice).

(1) *Cfr.* note del Garante pubblicate in *www.garanteprivacy.it*, in data 29 maggio 1998 (doc. *web* n. 41055), 26 ottobre 1998 (doc. *web* n. 30951), 2 agosto 1999 (doc. *web* n. 1096700), 2 settembre 1999 (doc. *web* n. 1092322), 17 febbraio 2000 (doc. *web* n. 38969) e 23 maggio 2000 (doc. *web* n. 40229); *v.* anche, ivi, i *Provv.* 17 gennaio 2001 (doc. *web* n. 41031), 27 febbraio 2002 (doc. *web* n. 1063639), 9 dicembre 2003 (doc. *web* n. 1054649), 10 novembre 2004 (doc. *web* n. 1116068) e 6 aprile 2006 (doc. *web* n. 1269403).

(2) Art. 10 d.lg. 18 agosto 2000, n. 267; artt. 22 e ss. l. 7 agosto 1990, n. 241, modificati dalla l. n. 15/2005; *v.* anche artt. 59 e 60 del Codice per ciò che riguarda il diritto di accesso a documenti amministrativi contenenti dati personali sensibili o giudiziari, in particolare di quelli idonei a rivelare lo stato di salute o la sfera sessuale (*cfr. Provv.* 9 luglio 2003, doc. *web* n. 29832, sul principio del "pari rango"); *v.* anche gli artt. 7 e ss. del Codice sul diritto di accesso ai dati personali.

(3) *V.* i relativi schemi tipo di regolamento (doc. *web* nn. 1174532, 1182195 e 1175684); *v.* anche, per il termine ultimo del 28 febbraio 2007 entro il quale i regolamenti dei soggetti pubblici in materia di dati sensibili e giudiziari dovevano essere adottati, l'art. 6, comma 1, d.l. 28 dicembre 2006, n. 300, conv., con mod., dalla l. 26 febbraio 2007, n. 17.

(4) *Cfr. Provv.* 6 aprile 2006 (doc. *web* n. 1269403), *cit.*, concernente l'inserimento in Internet di dati personali relativi ad una graduatoria di merito per accedere a taluni corsi di laurea.

(5) Analoghe forme di pubblicità sono state considerate applicabili alle determinazioni dirigenziali: *cfr.* Cons. Stato, Sez. V, 15 marzo 2006, n. 1370.

(6) *Cfr.* nota del Garante 26 ottobre 1998 (doc. *web* n. 30951), *cit.*, con cui gli enti locali sono stati richiamati a selezionare con rinnovata attenzione i dati personali, specie sensibili, la cui inclusione nelle deliberazioni da pubblicare sia realmente necessaria per le finalità conseguite dai singoli provvedimenti.

(7) Art. 65, comma 4, del Codice; schede n. 33 per i comuni, n. 19 per le comunità montane e n. 4 per le province, degli schemi tipo di regolamento citati.

(8) *Cfr. Provv.* 27 febbraio 2002 (doc. *web* n. 1063639), *cit.*, con il quale il Garante ha vietato la diffusione di dati idonei a rivelare lo stato di salute riportati in una graduatoria dei trasferimenti affissa nella bacheca di un provveditorato agli studi.

(9) L. 7 giugno 2000, n. 150.

(10) Artt. 4, comma 4, lett. *a*), 101 e ss. del Codice; d.lg. 29 ottobre 1999, n. 490, modificato dal d.lg. 22 gennaio 2004, n. 42, richiamato dall'art. 103 del Codice; *Provv.* n. 8/P/2001 del 14 marzo 2001, in *G.U.* 5 aprile 2001, n. 80, allegato A.2 al Codice.

(11) *Cfr. Nota* 23 maggio 2000 (doc. *web* n. 40229), *cit.*, con la quale sono stati forniti chiarimenti in ordine all'applicazione, da parte dei comuni, della disciplina in materia di protezione dei dati personali.

(12) *Cfr. Provv.* 6 ottobre 2005, in *G.U.* 24 ottobre 2005, n. 248 (doc. *web* n. 1179484), contenente prescrizioni del Garante nei confronti di tutti i comuni riguardo alle anagrafi della popolazione residente.

(13) *Cfr. Nota* 6 maggio 2004 (doc. *web* n. 1007634), con cui il Garante ha evidenziato che, fatte salve le valutazioni che seguiranno in ordine alla loro possibile diffusione, il giornalista può chiedere di acquisire o venire legittimamente a conoscenza delle informazioni concernenti, tra l'altro, l'ammontare complessivo dei dati reddituali dei contribuenti, presso i comuni.

(14) *Cfr.* Corte di giustizia delle Comunità europee, sentenza 6 novembre 2003, Bodil Lindqvist, C-101/01, Racc. 2003, p. I-12971.

(15) *Cfr. Provv.* 10 novembre 2004 (doc. *web* n. 1116068), *cit.*, concernente le modalità di diffusione, tramite Internet, di dati personali e le misure necessarie a garantire il diritto all'oblìo.

(16) *Cfr.* nota del Garante 2 novembre 2004, in Relazione del Garante per la protezione dei dati personali 2004, p. 18, riguardante la compatibilità dello specifico regime di pubblicità dell'albo dei beneficiari di provvidenze economiche con le disposizioni in materia di protezione dei dati personali.

46 Semplificazione dell'obbligo di informativa in ambito assicurativo (*) *26 aprile 2007*

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

In data odierna, in presenza del prof. Francesco Pizzetti, presidente, del dott. Giuseppe Chiaravalloti, vice presidente, del dott. Giuseppe Fortunato, componente, e del dott. Giovanni Buttarelli, segretario generale;

Visto il Codice in materia di protezione dei dati personali (d.lg. 30 giugno 2003, n. 196);

Vista la Raccomandazione del Consiglio d'Europa Rec(2002)9, del 18 settembre 2002;

Esaminate le comunicazioni del 5 febbraio 2002, 31 luglio 2002, 18 febbraio 2004 e 9 maggio 2006 provenienti dall'Associazione nazionale per le imprese assicuratrici (Ania) e contenenti, fra l'altro, richieste volte ad ottenere la semplificazione e l'esonero dall'obbligo di rendere l'informativa agli interessati nell'ambito dello svolgimento dell'attività assicurativa (art. 13, commi 3 e 5, del Codice);

Vista la documentazione in atti, acquisita anche a seguito degli incontri avvenuti presso la sede dell'Autorità in data 11 maggio 2006 e 20 giugno 2006;

Viste le osservazioni formulate dal segretario generale ai sensi dell'art. 15 del regolamento del Garante n. 1/2000;

Relatore il dott. Giuseppe Chiaravalloti;

PREMESSO

1. Il trattamento di dati personali nell'ambito della *cd.* "catena assicurativa"

1.1. L'Associazione nazionale per le imprese assicuratrici (Ania) ha rappresentato alcune problematiche affrontate dalle imprese di assicurazione nel dare compiuta attuazione, anche quando era vigente la legge n. 675/1996, ai diversi adempimenti derivanti dalla disciplina di protezione dei dati personali.

L'Ania ha richiamato in particolare l'attenzione sulle peculiarità dell'attività assicurativa, nella misura in cui essa:

- si può articolare in una pluralità di "fasi" (dalla c.d. fase assuntiva a quella liquidativa) che possono interessare, all'interno di un complesso tessuto di rapporti contrattuali, numerosi soggetti (persone fisiche e giuridiche, operanti in Italia e all'estero) con i quali le imprese di assicurazione cooperano nel gestire un medesimo rischio assicurativo, dando luogo al fenomeno della *cd.* "catena assicurativa";
- può coinvolgere, a seconda delle diverse tipologie assunte dai contratti di assicurazione, una pluralità di soggetti in veste di "interessati" (contraente, assicurato, beneficiario e, a certe condizioni, terzo danneggiato), taluni dei quali possono non entrare direttamente in contatto con l'assicurazione in sede di conclusione del contratto.

1.2. Ad avviso dell'Ania, il Codice entrato in vigore il 1° gennaio 2004 non avrebbe dissolto tutte le criticità che scaturirebbero dalle predette peculiarità; pertanto, con nota del 9 maggio 2006, ha rinnovato a questa Autorità, nell'interesse delle imprese associate, un'istanza volta, tra l'altro, ad ottenere, anche ai sensi dell'art. 13, comma 5, lett. *c*), del Codice, l'autorizzazione a rendere l'informativa alla clientela mediante un "modello unita-

(*) [doc. *web* n. 1410057]

rio". Tale informativa potrebbe essere resa *una tantum* da parte dell'impresa di assicurazione (titolare del trattamento) in sede di conclusione del contratto di assicurazione anche nell'interesse dei diversi soggetti che, in qualità di autonomi "titolari del trattamento", effettuano trattamenti relativi al medesimo rischio assicurato.

In questa stessa sede, sempre ad avviso dell'Ania, potrebbe essere raccolto, anche per conto dei medesimi soggetti, l'eventuale consenso al trattamento dei dati personali degli interessati. Ciò, in quanto i soggetti che intervengono nella *cd.* catena assicurativa (in particolare, i coassicuratori e i riassicuratori) pongono in essere operazioni di trattamento preordinate all'unica finalità di gestione del rischio assicurato a seguito della stipula di un contratto da parte dell'impresa di assicurazione.

L'informativa fornita singolarmente da parte di ciascun titolare del trattamento operante all'interno della c.d. catena assicurativa comporterebbe invece, secondo l'Ania, modalità complesse di realizzazione dell'adempimento, oltre che costi ed impegni amministrativi ritenuti sproporzionati rispetto al diritto tutelato. Ciò, *"in quanto, il più delle volte,* [detti soggetti] *non hanno alcun contatto diretto con l'interessato stesso, giacché ricevono i dati personali dall'assicuratore dell'interessato o da altri soggetti"* (cfr. nota Ania, cit.).

2. I profili soggettivi

2.1. Il settore assicurativo è caratterizzato da una frequente molteplicità di soggetti che, secondo i casi, vengono coinvolti nella prestazione dei servizi assicurativi relativi alla copertura di un medesimo rischio, ed effettuano (in taluni casi in qualità di "titolari", in altri come "responsabili del trattamento") operazioni di trattamento di dati personali (talvolta di natura sensibile) necessari per adempiere ad obblighi (di legge o connessi all'esecuzione del contratto) assunti nell'ambito dello svolgimento di tale peculiare attività d'impresa.

In questa cornice è necessario che le imprese di assicurazione valutino con la massima attenzione il ruolo effettivamente svolto dai soggetti che vengono chiamati a cooperare all'interno della c.d. catena assicurativa nell'esecuzione della prestazione dovuta alla clientela in base al rapporto assicurativo. Ciò, verificando se sussiste un reale ed autonomo potere decisionale in ordine alle finalità del trattamento (la cui effettiva esistenza consenta di ritenere che tali soggetti operino quali autentici "titolari del trattamento" ai sensi degli artt. 4, comma 1, lett. *f*) e 28 del Codice), o se essi devono invece conformare il proprio operato (che può comunque caratterizzarsi per ampi spazi di discrezionalità tecnica) alle istruzioni formulate dalle compagnie assicurative, sì da doversi correttamente qualificare quali "responsabili del trattamento" ai sensi degli artt. 4, comma 1, lett. *g*) e 29 del Codice.

In quest'ultima evenienza la designazione come responsabile del trattamento, che non è di per sé obbligatoria, *"diviene una soluzione in qualche modo obbligata quando una parte, sia pure strumentale, dei trattamenti necessari per perseguire le finalità del titolare del trattamento è curata, con una certa autonomia, da un soggetto esterno"* (Provv. 19 dicembre 1998, Boll. n. 6/1998, p. 117 e in *www.garanteprivacy.it*, doc. web n. 41941).

2.2. Nel settore assicurativo, la corretta qualificazione del ruolo svolto dai distinti soggetti che trattano dati personali assume quindi un valore particolarmente significativo, proprio in relazione alla pluralità dei soggetti partecipanti alla *cd.* catena assicurativa. Detta qualificazione, se aderente alla realtà, può infatti determinare per sé sola, con specifico riguardo alla figura dei "responsabili del trattamento", notevoli semplificazioni in relazione all'adempimento degli obblighi derivanti dalla disciplina di protezione dei dati personali (e, specificamente, quelli richiamati dall'Ania e relativi all'informativa, nonché all'eventuale raccolta del consenso dell'interessato) che gravano sulla sola compagnia assicurativa "titolare del trattamento".

3. L'informativa da rendere in caso di dati raccolti presso l'interessato

Gli effetti di semplificazione possono derivare non solo da una corretta qualificazione della funzione assolta dai partecipanti alla c.d. catena assicurativa. Specie nei rapporti destinati a svilupparsi lungo un ampio arco temporale (quali quelli connessi all'attivazione di

contratti assicurativi) può risultare infatti agevole rendere, (al più tardi) in sede di conclusione del contratto, un'informativa (anche in relazione ai dati raccolti presso terzi: art. 13, comma 4, del Codice), per tutte le operazioni necessarie a dare corretta esecuzione al rapporto contrattuale al quale si riferisce l'informativa medesima e per altri trattamenti che (talora anche in base ad esplicite previsioni di legge) possono essere effettuati lecitamente (in tal senso v. già *Provv.* 28 maggio 1997 , doc. web n. 40425).

L'informativa, pur dovendo illustrare la (talora inevitabile) intensità dei flussi comunicativi, deve consentire all'interessato di rendersi conto con chiarezza dei medesimi; a tal fine essa deve indicare con precisione (evitando formulazioni generiche o dal significato oscuro, tenuto conto del destinatario della comunicazione) le finalità in concreto perseguite dalla compagnia di assicurazione, indicando altresì i soggetti o le tipologie di soggetti ai quali i dati possono essere comunicati (in qualità di autonomi titolari del trattamento) o che, considerando anche quanto sopra indicato al punto 2.2., possono venirne a conoscenza in qualità di "responsabili del trattamento".

Ulteriori elementi informativi possono essere forniti all'instaurarsi di nuovi rapporti (anziché in presenza di meri rinnovi di quelli in essere), qualora cambino le finalità o le modalità dell'originario trattamento (o altri elementi previsti dall'art. 13 del Codice).

Informazioni più dettagliate possono essere ottenute dall'interessato in sede di esercizio del diritto d'accesso di cui all'art. 7 del Codice; in particolare, l'assicurazione può essere chiamata ad indicare, su richiesta dell'interessato, i soggetti ai quali i dati sono stati comunicati o che ne hanno avuto conoscenza, ad esempio, in qualità di "responsabili del trattamento".

Un elenco aggiornato di tali soggetti deve essere comunque reso disponibile, anche online sul sito *web* delle compagnie di assicurazione, per agevolare l'esercizio del diritto d'accesso da parte dell'interessato (art. 13, comma 1, lett. *f*) del Codice).

4. Semplificazione ed esonero dal rendere l'informativa in caso di dati raccolti presso terzi da parte di altri titolari del trattamento, con particolare riferimento a coassicuratori e riassicuratori

In considerazione del principio di semplificazione degli adempimenti richiesti dalla disciplina in materia di protezione dei dati personali in capo ai titolari del trattamento, pur dovendosi assicurare un livello elevato di tutela dei diritti e delle libertà fondamentali dell'interessato nell'ambito di operazioni di trattamento (*cfr.* art. 2, comma 2, del Codice; considerando n. 49 direttiva 95/46/Ce), risulta necessario individuare soluzioni operative che evitino la superflua reiterazione degli stessi adempimenti (talora percepita anche dagli interessati come meramente formalistica), a vantaggio di soluzioni che, sul piano dell'informativa, siano idonee a rendere meglio edotto il contraente della circolazione delle informazioni relative alla gestione del rischio assicurato.

Tale soluzione è stata, peraltro, seguita già nel modello unico di informativa, approvato dal Garante, allegato al *"codice di deontologia e di buona condotta per i sistemi informativi gestiti da soggetti privati in tema di crediti al consumo, affidabilità e puntualità nei pagamenti"* (pubblicato in *G.U.* 23 dicembre 2004, n. 300).

Analogamente a quanto in passato deciso da questa Autorità (*cfr. Provv.* 26 novembre 1998, doc. *web* n. 39624), va rilevato che l'adempimento all'obbligo di rendere l'informativa di cui all'art. 13 del Codice da parte degli autonomi "titolari" operanti nell'ambito della *cd.* "catena assicurativa", può comportare, attese le "complesse modalità di realizzazione dell'adempimento" derivanti dalla descrizione sopra fornita della *cd.* "catena assicurativa", un impiego di mezzi sproporzionato rispetto al diritto tutelato dalla medesima disposizione.

Con il presente provvedimento, ai sensi dell'art. 13, commi 3 e 5, lett. *c*) del Codice, il Garante individua modalità semplificate affinché l'assicurazione stipulante titolare dell'originario trattamento di dati possa rendere un'idonea informativa anche nell'interesse degli altri titolari del trattamento (con particolare riferimento ai coassicuratori e ai riassicuratori) che, in relazione ad un medesimo rischio assicurato, trattino nell'ambito della *cd.* catena

assicurativa informazioni riferite al contraente raccogliendole presso l'assicurazione che con il medesimo ha concluso il contratto. Tali ulteriori titolari del trattamento, ai sensi del predetto art. 13, comma 5, lett. *c*), non sono di conseguenza tenuti a rendere un'ulteriore informativa sul trattamento già reso noto all'interessato, a condizione che:

- i medesimi titolari del trattamento siano già individuati univocamente nell'informativa resa anche nel loro interesse dall'impresa assicuratrice stipulante o siano comunque individuabili presso quest'ultima;
- l'informativa sia formulata in modo da esplicitare univocamente anche le eventuali finalità ulteriori rispetto alla sola gestione del rischio assicurato perseguite da detti titolari del trattamento.

L'informativa fornita secondo le descritte modalità deve comunque contenere gli elementi indicati nell'art. 13 del Codice.

5. Consenso

In riferimento ad una larga parte dei trattamenti effettuati nell'ambito della c.d. catena assicurativa, il consenso dell'interessato non è richiesto dal momento che i dati sono necessari (per instaurare o) per dare esecuzione a un contratto di assicurazione (art. 24, comma 1, lett. *b*), del Codice), oppure in quanto gli stessi sono trattati sulla base di uno dei presupposti equipollenti di cui all'art. 24 del Codice (e, ovviamente, in tutti i casi in cui il "titolare del trattamento" si avvalga in conformità al Codice di un "responsabile" cui trasmetta i dati personali).

Qualora il consenso dell'interessato sia necessario (talora in forma scritta, come accade per il trattamento dei dati sensibili), l'operatività della formula di consenso può essere limitata ai soli trattamenti effettuati dall'assicurazione stipulante (compresa la comunicazione ai terzi indicati nell'informativa), oppure estendersi, in relazione al medesimo rischio assicurato, anche ai trattamenti ulteriori effettuati da altri "titolari" appartenenti alla c.d. catena assicurativa.

In quest'ultima evenienza, dal momento che il consenso deve essere prestato in forma specifica, esso deve riferirsi agli specifici trattamenti effettuati dal distinto titolare del trattamento, chiaramente individuabile nell'informativa resa (in tal senso *cfr. Provv.* 28 maggio 1997, *cit.*).

La formulazione utilizzata, tenendo conto del principio di finalità di cui all'art. 11 del Codice, deve comunque essere specifica, evitando indicazioni generiche che non permettano all'interessato di rendersi conto della reale ampiezza della sua dichiarazione, in particolare quando ciò appaia riferibile ad attività diverse da quelle relative alla gestione del rischio assicurato (come, ad esempio, nel caso di trattamento dei dati personali per finalità di *marketing*).

6. Riassicuratore e bilanciamento di interessi

Con riferimento all'eventuale comunicazione di dati (diversi da quelli indicati all'art. 4, comma 1, lett. *d*), del Codice) a vantaggio dei riassicuratori, per i quali può risultare necessaria la conoscenza dei dati personali dell'interessato per dare esecuzione alla prestazione dovuta, la medesima può avvenire, per effetto del presente provvedimento, in base all'ipotesi prevista dall'art. 24, comma 1, lett. *g*), del Codice, atteso che, in base all'art. 1929 del codice civile, la figura contrattuale della riassicurazione può perfezionarsi in virtù del solo accordo tra assicuratore e riassicuratore, indipendentemente, quindi, dalla partecipazione dei soggetti coinvolti nel contratto di assicurazione (oggetto della riassicurazione). Ciò, in quanto il Garante ravvisa con la presente decisione i presupposti per applicare l'istituto del bilanciamento degli interessi in relazione al legittimo interesse dei titolari del trattamento coinvolti.

TUTTO CIÒ PREMESSO, IL GARANTE

a) individua, ai sensi dell'art. 13, commi 3 e 5, lett. *c*), del Codice, modalità semplificate per rendere l'informativa da parte dell'assicurazione stipulante titolare del trattamento e degli altri titolari del trattamento diversi da quello che stipula il

contratto di assicurazione (con particolare riferimento ai coassicuratori e ai riassicuratori) che, in relazione ad un medesimo rischio assicurato, trattino nell'ambito della *cd.* "catena assicurativa" informazioni riferite al contraente raccogliendole presso l'assicurazione che con il medesimo ha concluso il contratto (punto 4). Ciò, a condizione che:

- detti titolari del trattamento siano già individuati univocamente nell'informativa resa anche nel loro interesse dall'impresa assicuratrice stipulante o siano comunque individuabili presso quest'ultima;
- l'informativa sia formulata in modo da esplicitare univocamente anche le eventuali finalità ulteriori rispetto alla sola gestione del rischio assicurato perseguite da detti titolari del trattamento;

b) individua, ai sensi dell'art. 24, comma 1, lett. *g*), del Codice, nei termini di cui in motivazione (punto 6), i casi nei quali il trattamento dei dati personali di natura non sensibile possono essere effettuati per perseguire un legittimo interesse dei riassicuratori anche senza il consenso degli interessati.

Roma, 26 aprile 2007

IL PRESIDENTE
Pizzetti

IL RELATORE
Chiaravalloti

IL SEGRETARIO GENERALE
Buttarelli

47 Pubblicità dei dati di debitori nelle esecuzioni immobiliari (*)
7 febbraio 2008

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Nella riunione odierna, in presenza del prof. Francesco Pizzetti, presidente, del dott. Giuseppe Chiaravalloti, vice presidente, del dott. Mauro Paissan e del dott. Giuseppe Fortunato, componenti, e del dott. Giovanni Buttarelli, segretario generale;

Esaminate le numerose segnalazioni pervenute riguardo al trattamento di dati personali effettuato nell'ambito di procedimenti di espropriazione forzata;

Visto il Codice in materia di protezione dei dati personali (d.lg. 30 giugno 2003, n. 196), con particolare riferimento agli artt. 11, 47 e 174;

Vista la documentazione in atti;

Viste le osservazioni dell'Ufficio, formulate dal segretario generale ai sensi dell'art. 15 del regolamento del Garante n. 1/2000;

Relatore il dott. Giuseppe Chiaravalloti;

PREMESSO

Sono pervenute al Garante numerose segnalazioni in merito al regime di pubblicità nell'ambito dei procedimenti di espropriazione forzata. Le questioni sollevate riguardano l'applicazione delle modifiche apportate all'art. 490 c.p.c. (previste dalla riforma del processo esecutivo entrata in vigore il 1° marzo 2006), in relazione ai contenuti e alle modalità di pubblicazione degli atti attraverso cui viene data notizia delle vendite giudiziarie.

In particolare, la prevista pubblicazione in appositi siti Internet di copia dell'ordinanza del giudice che dispone sulla vendita forzata, nonché della relazione di stima dei beni da espropriare, in assenza di opportuni accorgimenti volti a tutelare la riservatezza degli interessati, avrebbe comportato, ad avviso dei segnalanti, un'ingiustificata diffusione dei nominativi dei debitori sottoposti alle procedure esecutive, nonché di eventuali terzi (ad esempio, dei proprietari di porzioni immobiliari confinanti con l'immobile dell'esecutato).

Sulla base degli approfondimenti svolti, il Garante ravvisa l'esigenza di indicare agli uffici giudiziari e ai professionisti delegati alle operazioni di vendita la necessità di adottare nell'espletamento delle procedure in esame modalità che, nel rispetto del pertinente dettato normativo, permettano di favorire ampia pubblicità agli atti del processo esecutivo rispettando, al contempo, i diritti degli interessati.

OSSERVA

1. Pubblicità degli atti e diritti degli interessati

Già con un provvedimento del 22 ottobre 1998, il Garante si è espresso sulla necessità di rispettare la dignità delle persone coinvolte nel processo esecutivo, auspicando un intervento del legislatore volto a evitare l'affissione di manifesti con i nominativi dei debitori e invitando gli uffici giudiziari ad adottare prassi più attente e rispettose dei diritti degli interessati (*Provv.* 22 ottobre 1998, disponibile sul sito Internet dell'Autorità *www.garanteprivacy.it*, doc. *web* n. 1104097).

Il Codice in materia di protezione dei dati personali ha poi modificato in tal senso il codice di procedura civile prevedendo, da un lato, che sia omessa l'indicazione del debitore

(*) *G.U.* 25 febbraio 2008, n. 47
[doc. *web* n. 1490838]

negli avvisi relativi agli atti esecutivi pubblicati sui quotidiani e nelle forme della pubblicità commerciale (art. 174, comma 9, del Codice; art. 490, comma 3, c.p.c.), e, dall'altro, che gli avvisi di vendita debbano indicare che *"maggiori informazioni anche relative alle generalità del debitore possono essere fornite dalla cancelleria del tribunale a chiunque vi abbia interesse"* (art. 174, comma 10, del Codice; art. 570 c.p.c.).

Recenti interventi normativi (art. 2, comma 3, lett. e), d.l. 14 marzo 2005, n. 35, convertito, con modificazioni, dalla l. 14 maggio 2005, n. 80) hanno riformulato integralmente l'art. 490, comma 2, c.p.c. disponendo, in particolare, che gli avvisi, *"in caso di espropriazione di beni mobili registrati, per un valore superiore a 25.000 euro, e di beni immobili"*, *"unitamente a copia dell'ordinanza del giudice e della relazione di stima del bene"* debbano essere *"inseriti in appositi siti Internet almeno quarantacinque giorni prima del termine per la presentazione delle offerte o della data dell'incanto"*. Con decreto del Ministro della giustizia del 31 ottobre 2006 (pubblicato in *G.U.* della Repubblica italiana n. 297 del 22 dicembre 2006) sono stati individuati i siti Internet destinati all'inserimento dei predetti avvisi.

Il descritto quadro normativo rivela, quindi, la particolare attenzione posta dal legislatore nel bilanciare le esigenze di pubblicità degli atti e i diritti degli interessati nell'ambito del processo esecutivo. Da un lato, l'omissione del nominativo del debitore nell'avviso di vendita (art. 490, terzo comma, c.p.c.) risponde alla necessità di tutelare il diritto degli interessati a non subire un'ingiustificata divulgazione dei dati personali che li riguardano. Dall'altro, la possibilità di conoscere le generalità del debitore, e ogni altra ulteriore utile informazione, attraverso le strutture degli uffici giudiziari (art. 570 c.p.c.) consente a chi sia realmente interessato all'acquisto un'informata valutazione circa l'effettiva situazione giuridica del bene da espropriare.

2. Pubblicazione *on-line* dell'ordinanza e della relazione di stima

La menzionata riforma del processo esecutivo ha assicurato una più ampia pubblicità alle vendite giudiziarie prevedendo, come accennato, l'inserimento in appositi siti *web*, oltre che dell'avviso di vendita, anche di copia dell'ordinanza del giudice che dispone sulla vendita e della relazione di stima.

Come è emerso nei casi segnalati al Garante, talvolta le copie dell'ordinanza e della relazione di stima pubblicate contengono le generalità del debitore e di eventuali altri soggetti, quali i proprietari di porzioni immobiliari confinanti con il bene dell'esecutato, non direttamente interessati dalla procedura esecutiva.

Al riguardo, deve essere rilevato che la prevista consultabilità *on-line* di atti del procedimento esecutivo senza l'omissione delle generalità del debitore vanifica la tutela chiaramente garantita in altra parte della stessa disposizione, nella parte in cui (art. 490, terzo comma, c.p.c.), anche in relazione ad altre forme di pubblicità meno invasive, è precisamente disposto che nell'avviso in questione *"è omessa l'indicazione del debitore"*.

Pertanto, al fine di mantenere effettiva la tutela dei soggetti sottoposti a esecuzione forzata, come garantita dal Codice in materia di protezione dei dati personali e dallo stesso art. 490, occorre che gli uffici giudiziari e i professionisti delegati alle operazioni di vendita ai sensi dell'art. 591-*bis* c.p.c. omettano l'indicazione del debitore e di ogni altro dato personale idoneo a rivelarne l'identità, oltre che nell'avviso di vendita, anche nelle copie dell'ordinanza del giudice e della relazione di stima.

D'altra parte, occorre che nelle copie pubblicate di tali atti non siano riportati i dati personali di soggetti estranei alla procedura esecutiva ove ciò non sia previsto da una specifica norma di legge, trattandosi di informazioni eccedenti e non pertinenti rispetto alle finalità cui è preordinato il procedimento espropriativo. Ciò, al fine di assicurare il rispetto del principio di proporzionalità nel trattamento dei dati posto dall'art. 11, comma 1, lett. *d*) del Codice, disposizione che trova applicazione anche in relazione ai trattamenti effettuati *"per ragioni di giustizia"* (art. 47 del Codice).

Resta fermo che le generalità del debitore e ogni altra ulteriore informazione potranno essere richieste e ottenute presso la cancelleria del tribunale da chiunque vi abbia interesse (art. 570 c.p.c.).

Copia del presente provvedimento viene inviata al Ministero della giustizia e al Consiglio superiore della magistratura, per opportuna conoscenza in relazione alle rispettive attribuzioni, anche al fine di assicurare l'adozione di ogni idonea iniziativa volta a favorirne la diffusione presso gli uffici giudiziari interessati.

Tenuto conto dell'alto numero di questi ultimi, va infine disposta, ai sensi dell'art. 143, comma 2, del Codice, la pubblicazione del provvedimento sulla *Gazzetta Ufficiale* della Repubblica italiana.

TUTTO CIÒ PREMESSO, IL GARANTE

a) ai sensi dell'art. 154, comma 1, lett. *c*), del Codice in materia di protezione dei dati personali, indica agli uffici giudiziari e ai professionisti delegati alle operazioni di vendita la necessità di non riportare, oltre che nell'avviso di vendita, nelle copie pubblicate delle ordinanze e delle relazioni di stima l'indicazione delle generalità del debitore e di ogni altro dato personale idoneo a rivelare l'identità di quest'ultimo e di eventuali soggetti terzi non previsto dalla legge e comunque eccedente e non pertinente rispetto alle procedure di vendita in corso;
b) dispone che copia del presente provvedimento venga inviata al Ministero della giustizia e al Consiglio superiore della magistratura, per opportuna conoscenza in relazione alle rispettive attribuzioni, anche al fine di assicurare l'adozione di ogni idonea iniziativa volta a favorirne la diffusione presso gli uffici giudiziari interessati;
c) ai sensi dell'art. 143, comma 2, del Codice, dispone la pubblicazione del medesimo provvedimento sulla *Gazzetta Ufficiale* della Repubblica italiana.

Roma, 7 febbraio 2008

IL PRESIDENTE
Pizzetti

IL RELATORE
Chiaravalloti

IL SEGRETARIO GENERALE
Buttarelli

Altri provvedimenti

48 Provvedimenti di particolare rilievo (*)

Misure in materia di propaganda politica ed elettorale
3 maggio 2007 [doc. *web* n. 1409206]

Esonero dall'informativa per partiti e movimenti politici sino al 31 luglio 2008
28 febbraio 2008 [doc. *web* n. 1493909]

Garanzie a tutela degli invalidi civili
21 marzo 2007 [doc. *web* n. 1395821]

Internet - Caso Peppermint: illecito "spiare" gli utenti che scambiano *file* musicali e giochi
28 febbraio 2008 [doc. *web* n. 1495246]

Trattamento dati sensibili per l'accesso di medici in zone a traffico limitato
14 giugno 2007 [doc. *web* n. 1424100]

Modalità di partecipazione dei comuni all'accertamento fiscale
25 luglio 2007 [doc. *web* n. 1428047]

Servizi *on-line* e uso dei dati a fini di *marketing*
22 febbraio 2007 [doc. *web* n 1388590]

Diffusione di dati reddituali ordine commercialisti Bologna
18 ottobre 2007 [doc. *web* n. 1454901]

(*) Reperibili sul sito
www.garanteprivacy.it

Diffusione di dati personali concernenti una attività di indagine in corso presso gli uffici giudiziari di Potenza
15 marzo 2007 [doc. *web* n. 1390923]

Pubblicazione di fotografie riprese all'interno di dimora privata
8 maggio 2007 [doc. *web* n. 1409488]

Invio di posta elettronica per finalità commerciali senza consenso
14 giugno 2007 [doc. *web* n. 1424068]

Videosorveglianza comunale e riprese all'interno di abitazioni private
4 ottobre 2007 [doc. *web* n. 1457505]

***Media* e sport: regole per chi telefona in trasmissione**
11 ottobre 2007 [doc. *web* n. 1449505]

49 Ulteriori provvedimenti citati (*)

Comunicazione all'anagrafe tributaria delle somme erogate da operatori del settore assicurativo
11 gennaio 2007 [doc. *web* n. 1381575]

Comunicazioni all'anagrafe tributaria da parte degli operatori finanziari
11 gennaio 2007 [doc. *web* n. 1381941]

Istituzione di registri e cartelle sanitarie di lavoratori esposti ad agenti nocivi
11 gennaio 2007 [doc. *web* n. 1378712]

Trattamento di dati sensibili nell'attività di intermediazione immobiliare
11 gennaio 2007 [doc. *web* n. 1381620]

Cessione in blocco e cartolarizzazione dei crediti
18 gennaio 2007 [doc. *web* n. 1392461]

Regole in tema di casellario giudiziale, anagrafe di alcune sanzioni amministrative e relativi carichi pendenti
18 gennaio 2007 [doc. *web* n. 1381963]

Trasmissione di dati relativi a crediti d'imposta per la ricerca scientifica e tecnologica
25 gennaio 2007 [doc. *web* n. 1381925]

Verifica sulle misure di sicurezza adottate presso un tribunale
1 febbraio 2007 [doc. *web* n. 1385301]

Verifica sulle modalità di inserimento delle segnalazioni (art. 99 convenzione di applicazione dell'Accordo di Schengen)
8 febbraio 2007 [doc. *web* n. 1388902]

(*) Reperibili sul sito
www.garanteprivacy.it

Diffusione di telefonata registrata per finalità di servizio
8 febbraio 2007 [doc. *web* n. 1388922]

Comunicazioni per finalità di controllo alle frontiere
13 febbraio 2007 [doc. *web* n. 1388444]

Trattamenti dei dati sensibili e giudiziari del Ministero del lavoro e della previdenza sociale
28 febbraio 2007 [doc. *web* n. 1409015]

Accessi abusivi alla centrale rischi
8 marzo 2007 [doc. *web* n. 1390872]

Combinazione di elementi identificativi e personalità dei dati
8 marzo 2007 [doc. *web* n. 1396630]

Diritti dell'interessato e dati contenuti in sistemi di informazioni creditizie
8 marzo 2007 [doc. *web* n. 1396584]

Videosorveglianza negli spogliatoi di una piscina
8 marzo 2007 [doc. *web* n. 1391803]

Archivi informatici delle tasse automobilistiche
16 marzo 2007 [doc. *web* n. 1397123]

Prove di ammissione a corsi di laurea per l'anno accademico 2007-2008
4 aprile 2007 [doc. *web* n. 1401716]

Organizzazione e funzionamento della Commissione per le adozioni internazionali
12 aprile 2007 [doc. *web* n. 1401738]

Trasmissione telematica dei corrispettivi giornalieri da parte di soggetti che effettuano attività di commercio al minuto
12 aprile 2007 [doc. *web* n. 1402655]

Trattamento dei dati sensibili e giudiziari presso l'Agenzia italiana del farmaco
12 aprile 2007 [doc. *web* n. 1403241]

Trasmissione telematica dell'elenco dei soggetti nei cui confronti sono state emesse fatture
26 aprile 2007 [doc. *web* n. 1402616]

Trattamenti dei dati sensibili e giudiziari presso l'Istituto per lo sviluppo della formazione professionale dei lavoratori
26 aprile 2007 [doc. *web* n. 1407772]

Invio di *fax* pubblicitari e consenso dell'interessato
4 aprile 2007 [doc. *web* n. 1402646]
3 maggio 2007 [doc. *web* n. 1410276]
24 maggio 2007 [doc. *web* n. 1418805]
28 giugno 2007 [doc. *web* n. 1433896]
11 luglio 2007 [doc. *web* n. 1433939]

Essenzialità della notizia e completezza delle circostanze
3 maggio 2007 [doc. *web* n. 1408971]

Limiti al diritto di cronaca nei confronti di un candidato alle elezioni politiche
8 maggio 2007 [doc. *web* n. 1410586]

Acquisto di crediti derivanti da assegni e trattamento di dati dei debitori
17 maggio 2007 [doc. *web* n. 1409251]

Diffusione di corrispondenza privata
24 maggio 2007 [doc. *web* n. 1419749]

Chiamate promozionali e servizi telefonici non richiesti
30 maggio 2007 [doc. *web* n. 1412557]
30 maggio 2007 [doc. *web* n. 1412586]
30 maggio 2007 [doc. *web* n. 1412598]
30 maggio 2007 [doc. *web* n. 1412610]

Chiamate promozionali indesiderate
30 maggio 2007 [doc. *web* n. 1412626]

Conversazioni al ristorante e *scoop* giornalistico
7 giugno 2007 [doc. *web* n. 1419429]

Essenzialità dell'informazione e lesione della dignità personale
7 giugno 2007 [doc. *web* n. 1421351]

Campione biologico e dato personale genetico
21 giugno 2007 [doc. *web* n. 1433975]

Artifici nello svolgimento dell'attività di giornalista
5 luglio 2007 [doc. *web* n. 1435035]
5 luglio 2007 [doc. *web* n. 1436163]

Immagini televisive idonee a identificare bambini
19 luglio 2007 [doc. *web* n. 1425235]

Disposizioni in materia di pagamenti da parte delle pubbliche amministrazioni
25 luglio 2007 [doc. *web* n. 1434395]

Liberalizzazione mercato energia e gas: utilizzazione dei dati della clientela
25 luglio 2007 [doc. *web* n. 1428567]

Osservatorio per il contrasto della pedofilia e della pornografia minorile
25 luglio 2007 [doc. *web* n. 1436237]

Regione Toscana: programma statistico regionale 2006-2008
25 luglio 2007 [doc. *web* n. 1428057]

Rilascio certificati casellario giudiziale
25 luglio 2007 [doc. *web* n. 1431017]

Regole tecniche e di sicurezza relative alla carta d'identità e al documento d'identità elettronici
1 agosto 2007 [doc. *web* n. 1436216]

Trasparenza nel trattamento di dati personali per un sondaggio politico
13 settembre 2007 [doc. *web* n. 1523633]

Informazioni idonee a identificare minori
19 settembre 2007 [doc. *web* n. 1445858]

Trattamento dei dati sensibili e giudiziari presso il Comitato olimpico nazionale italiano (Coni)
19 settembre 2007 [doc. *web* n. 1443411]

Agenzia delle entrate: trattamento di dati comunicati dai gestori di servizi di smaltimento dei rifiuti urbani
4 ottobre 2007 [doc. *web* n. 1457706]
6 dicembre 2007 [doc. *web* n. 1470750]

Completezza nella comunicazione all'interessato dei dati trattati
4 ottobre 2007 [doc. *web* n. 1449401]

Inoltro senza consenso di comunicazioni commerciali a mezzo *telefax*
4 ottobre 2007 [doc. *web* n. 1457973]

Banca dati Dna
15 ottobre 2007 [doc. *web* n. 1448799]

Diffusione indifferenziata di risultanze audio di intercettazioni
25 ottobre 2007 [doc. *web* n. 1458851]

Apposizione della dicitura "pignoramento" su un cedolino di pensione
31 ottobre 2007 [doc. *web* n. 1459297]

Informazioni su un fallimento risalente di oltre vent'anni
31 ottobre 2007 [doc. *web* n. 1458863]

Rilevazioni biometriche per l'accesso alla sala operativa di una soprintendenza archeologica
8 novembre 2007 [doc. *web* n. 1461908]

Programma statistico nazionale 2008-2010
15 novembre 2007 [doc. *web* n. 1464806]

Trattamento di dati personali e fidelizzazione della clientela
15 novembre 2007 [doc. *web* n. 1466930]
15 novembre 2007 [doc. *web* n. 1466898]
15 novembre 2007 [doc. *web* n. 1466971]
15 novembre 2007 [doc. *web* n. 1466985]
15 novembre 2007 [doc. *web* n. 1466956]

Opposizione al trattamento di dati personali raccolti per una trasmissione televisiva
22 novembre 2007 [doc. *web* n. 1470697]

Diffusione di dati d'interesse clinico e dignità della persona
29 novembre 2007 [doc. *web* n. 1478083]

Utilizzo dei telefoni cellulari o di altri dispositivi elettronici nelle comunità scolastiche
29 novembre 2007 [doc. *web* n. 1466996]

Dignità della persona e diffusione di dati d'interesse clinico
6 dicembre 2007 [doc. *web* n. 1478059]

Differimento dell'accesso a dati utilizzabili in giudizio
10 dicembre 2007 [doc. *web* n. 1497600]

Diritti dell'interessato con riferimento a dati contenuti in una relazione investigativa
21 dicembre 2007 [doc. *web* n. 1490154]

Dati relativi a procedimento penale ed essenzialità dell'informazione
10 gennaio 2008 [doc. *web* n. 1489978]

Dichiarazione di appartenenza o aggregazione al gruppo linguistico in provincia di Bolzano
10 gennaio 2008 [doc. *web* n. 1484669]

Prescrizioni sulla conservazione dei dati di traffico
10 gennaio 2008 [doc. *web* n. 1524263]
10 gennaio 2008 [doc. *web* n. 1484695]
10 gennaio 2008 [doc. *web* n. 1484726]
10 gennaio 2008 [doc. *web* n. 1484758]

Trattamento dei dati sensibili e giudiziari presso la Provincia autonoma di Trento
10 gennaio 2008 [doc. *web* n. 1482234]

Informazioni commerciali e diritti dell'interessato
23 gennaio 2008 [doc. *web* n. 1490183]

Messaggi promozionali e consenso dell'interessato
23 gennaio 2008 [doc. *web* n. 1487925]

Rilevazioni biometriche per verificare la presenza a corsi di formazione
23 gennaio 2008 [doc. *web* n. 1487903]

Trattamento di dati biometrici in banca
23 gennaio 2008 [doc. *web* n. 1490382]
23 gennaio 2008 [doc. *web* n. 1490463]
23 gennaio 2008 [doc. *web* n. 1490477]
23 gennaio 2008 [doc. *web* n. 1490533]

Diritto di cronaca ed informazioni sull'età e la residenza di una persona
31 gennaio 2008 [doc. *web* n. 1491621]

Divieto di invio di fax promozionali senza consenso
31 gennaio 2008 [doc. *web* n. 1488781]
31 gennaio 2008 [doc. *web* n. 1489843]

Privacy in albergo: vietato "spiare" i gusti dei clienti
31 gennaio 2008 [doc. *web* n. 1490553]

Trattamento dei dati sensibili e giudiziari presso la Scuola superiore della pubblica amministrazione locale
7 febbraio 2008 [doc. *web* n. 1491594]

Limiti alla conservazione di dati relativi a comportamento debitorio
21 febbraio 2008 [doc. *web* n. 1501246]

Richiesta di cancellazione di dati inseriti in sistemi di informazioni creditizie
28 febbraio 2008 [doc. *web* n. 1500676]

Canone Rai: correttezza nei solleciti agli utenti
5 marzo 2008 [doc. *web* n. 1501024]

Coincidenza di dati identificativi e cancellazione da un sistema di informazioni creditizie
5 marzo 2008 [doc. *web* n. 1501621]

Conservazione di dati relativi al traffico e all'ubicazione delle persone, nonché dei dati connessi necessari per identificare l'abbonato o l'utente
5 marzo 2008 [doc. *web* n. 1523089]

Interruzione volontaria di gravidanza - Divieto di diffondere le generalità della donna
5 marzo 2008 [doc. *web* n. 1523741]

Limiti alla funzione informativa della pubblicazione di intercettazioni in formato audio
5 marzo 2008 [doc. *web* n. 1517832]

Preavviso sulla registrazione di dati in sistemi di informazioni creditizie
13 marzo 2008 [doc. *web* n. 1502131]

Trattamento di dati genetici a fini di disconoscimento di paternità
25 marzo 2008 [doc. *web* n. 1519557]

Tutela della salute e sicurezza nei luoghi di lavoro
31 marzo 2008 [doc. *web* n. 1504941]

Notizie sulle conseguenze di un incidente ed essenzialità dell'informazione
2 aprile 2008 [doc. *web* n. 1519908]

Dignità della persona e dettagli sulle condizioni di ritrovamento di un cadavere
24 aprile 2008 [doc. *web* n. 1519915]

Principali attività internazionali

50 Unione europea (*)

Accordo Pnr tra Usa e Ue del 2007
Accordo tra l'Unione europea e gli Stati uniti d'America sul trattamento e sul trasferimento dei dati del codice di prenotazione (Passenger name record, Pnr) da parte dei vettori aerei al Dipartimento per la sicurezza interna degli Stati uniti (Dhs) (Accordo Pnr del 2007)
23 - 27 luglio 2007 [doc. *web* n. 1531335]

Decisione del Consiglio Ue in merito all'Accordo Pnr tra Usa e Ue del 2007
Decisione del Consiglio 2007/551/Pesc/Gai relativa alla firma, a nome dell'Unione europea, dell'accordo tra l'Unione europea e gli Stati uniti d'America sul trattamento e sul trasferimento dei dati del codice di prenotazione (Passenger name record, Pnr) da parte dei vettori aerei al Dipartimento per la sicurezza interna degli Stati uniti (Dhs) (Accordo Pnr del 2007)
23 luglio 2007 [doc. *web* n. 1531383]

Decisione del Consiglio Ue sull'istituzione, l'esercizio e l'uso del Sis II
Decisione 2007/533/Gai del Consiglio sull'istituzione, l'esercizio e l'uso del sistema d'informazione Schengen di seconda generazione (Sis II)
12 giugno 2007 [doc. *web* n. 1531387]

Proposta di decisione-quadro sull'uso dei dati Pnr per finalità di contrasto
Proposta di decisione-quadro del Consiglio sull'uso dei dati del codice di prenotazione (Passenger name record, Pnr) nelle attività di contrasto (presentata dalla Commissione)
6 novembre 2007 [doc. *web* n. 1531454]

Iniziativa tedesca per l'adozione di una Decisione del Consiglio sull'attuazione della Decisione sul potenziamento della cooperazione transfrontaliera
Iniziativa della Repubblica federale di Germania in vista dell'adozione della decisione 2007/.../Gai del Consiglio del ... relativa all'attuazione della decisione 2007/.../Gai sul rafforzamento della cooperazione transfrontaliera, soprattutto nella lotta al terrorismo ed alla criminalità transfrontaliera (2007/C 267/06)
9 novembre 2007 [doc. *web* n. 1531421]

(*) Reperibili sul sito *www.garanteprivacy.it*

Comunicazione della Commissione in materia di Rfid
Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni - L'identificazione a radiofrequenza (Rfid) in Europa: verso un quadro politico
15 marzo 2007 [doc. *web* n. 1531371]

Comunicazione della Commissione in materia di Privacy Enhancing Technologies
Comunicazione della Commissione al Parlamento europeo e al Consiglio sulla promozione della protezione dei dati mediante tecnologie di rafforzamento della tutela della vita privata (Pet)
2 maggio 2007 [doc. *web* n. 1531367]

Comunicazione della Commissione sulla revisione del quadro normativo in materia di comunicazioni elettroniche
Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni - Relazione sull'esito del riesame del quadro normativo comunitario per le reti ed i servizi di comunicazione elettronica a norma della direttiva 2002/21/Ce e Sintesi delle proposte di riforma del 2007
13 novembre 2007 [doc. *web* n. 1531471]

Proposta di direttiva che modifica la direttiva 2002/58/Ce
Proposta di Direttiva del Parlamento europeo e del Consiglio recante modifica della direttiva 2002/22/Ce relativa al servizio universale e ai diritti degli utenti in materia di reti e di servizi di comunicazione elettronica, della direttiva 2002/58/Ce relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche e del regolamento (Ce) n. 2006/2004 sulla cooperazione per la tutela dei consumatori (presentata dalla Commissione)
13 novembre 2007 [doc. *web* n. 1531925]

Comunicazioni della Commissione in materia di "border management"
Communication from the Commission to the European Parliament, the Council, the European economic and social committee and the Committee of the Regions - Preparing the next steps in border management in the European Union
13 febbraio 2008 [doc. *web* n. 1531510]

Communication from the Commission to the European Parliament, the Council, the European economic and social committee and the Committee of the Regions - Examining the creation of a European Border Surveillance System (Eurosur)
13 febbraio 2008 [doc. *web* n. 1531359]

Communication from the Commission to the European Parliament, the Council, the European economic and social committee and the Committee of the Regions - Report on the evaluation and future development of the Frontex Agency
13 febbraio 2008 [doc. *web* n. 1531363]

Protezione dei dati e tutela del copyright
Sentenza della Corte di Giustizia (Grande Sezione) - C 275/06
Productores de Musica de España (Promusicae) e Telefónica de España
29 gennaio 2008 [doc. *web* n. 1531462]

---

51 Gruppo art. 29 (*)

Concetto di "dati personali"
Wp 136 - Parere 4/2007 sul concetto di dati personali
20 giugno 2007 [doc. *web* n. 1531857]

Prima azione comune di enforcement
Wp 137 - Report 1/2007 on the first joint enforcement action: evaluation and future steps
20 giugno 2007 [doc. *web* n. 1531897]

Nuovo accordo Pnr tra Usa e Ue
Wp 138 - Parere 5/2007 relativo al nuovo accordo tra l'Unione europea e gli Stati uniti d'America sul trattamento e sul trasferimento dei dati del codice di prenotazione (Passenger name record, Pnr) da parte dei vettori aerei al Dipartimento per la Sicurezza interna degli Stati uniti concluso nel luglio 2007
17 agosto 2007 [doc. *web* n. 1531861]

Sistema di cooperazione per la tutela dei consumatori
Wp 139 - Parere 6/2007 su temi riguardanti la protezione dei dati connessi con il Sistema di cooperazione per la tutela dei consumatori (Cpcs)
21 settembre 2007 [doc. *web* n. 1531865]

Sistema informativo del mercato interno
Wp 140 - Parere 7/2007 sugli aspetti relativi alla protezione dei dati con riferimento al Sistema di informazione del mercato interno (Imi)
21 settembre 2007 [doc. *web* n. 1531869]

Adeguatezza protezione dati a Jersey
Wp 141 - Parere 8/2007 sul livello di protezione dei dati personali a Jersey
9 ottobre 2007 [doc. *web* n. 1531901]

Adeguatezza protezione dati nelle Isole Faer Øer
Wp 142 - Parere 9/2007 sul livello di protezione dei dati personali nelle Isole Faer Øer
9 ottobre 2007 [doc. *web* n. 1531952]

(*) Reperibili sul sito
www.garanteprivacy.it

Ottava direttiva sulle revisioni legali dei conti
Wp 143 - Parere 10/2007 - Ottava direttiva sulle revisioni legali dei conti
23 novembre 2007 [doc. *web* n. 1531877]

Parere congiunto WP29/WPPJ sulla proposta di decisione-quadro sull'uso del Pnr per le attività di contrasto
Wp 145 - Parere comune relativo alla proposta di decisione-quadro del Consiglio sull'uso dei dati del codice di prenotazione (Passenger name record, Pnr) nelle attività di contrasto, presentata dalla Commissione il 6 novembre 2007
5 e 18 dicembre 2007 [doc. *web* n. 1531958]

Programma di lavoro
Wp 146 - Programma di lavoro 2008-2009
18 febbraio 2008 [doc. *web* n. 1531885]

Protezione dati e minori
Wp 147 - Working Document 1/2008 on the protection of children's personal data (General guidelines and the special case of schools)
18 febbraio 2008 [doc. *web* n. 1531889]

Motori di ricerca
Wp 148 - Opinion on data protection issues related to search engines
4 aprile 2008 [doc. *web* n. 1531893]

(*) Reperibili sul sito *www.garanteprivacy.it*

52 Autorità di controllo Europol (*)

Terza relazione di attività dell'Autorità di controllo comune dell'Europol
Novembre 2004 - Ottobre 2006 [doc. *web* n. 1531416]

(*) Reperibili sul sito
www.garanteprivacy.it

53 Unità di controllo Eurodac (*)

Rapporto di attività Eurodac 2007
Coordinated Supervision of Eurodac - Activity Report 2005-2007
21 Aprile 2008 [doc. *web* n. 1531906]

(*) Reperibili sul sito
www.garanteprivacy.it

54 Gruppo di lavoro in materia di attività giudiziarie e di polizia - *Working Party on Police and Justice* (*)

Cooperazione transfrontaliera
Posizione delle autorità europee per la protezione dei dati rispetto alla proposta di decisione del Consiglio sul potenziamento della cooperazione transfrontaliera, con particolare riguardo alla lotta contro il terrorismo, la criminalità transnazionale e l'immigrazione illegale
maggio 2007 [doc. *web* n. 1531379]

Decisione-quadro Terzo pilastro
Commenti del Working Party on Police and Justice rispetto alla proposta di decisione del Consiglio sulla protezione dei dati personali trattati nell'ambito della cooperazione giudiziaria e di polizia in materia penale
ottobre 2007 [doc. *web* n. 1531355]

Decisione-quadro Terzo pilastro
Lettera al Consiglio Ue relativa agli *standard* di protezione dati fissati nel progetto di decisione-quadro Terzo pilastro
31 ottobre 2007 [doc. *web* n. 1531425]

Accesso a Eurodac
Lettera su accesso a Eurodac da parte forze di polizia
13 dicembre 2007 [doc. *web* n. 1531331]

Valutazioni del WPPJ sulle disposizioni contenute nell'Allegato tecnico alla decisione attuativa della decisione del Consiglio sull'attuazione del Trattato di Prüm
Position Paper of the European Data Protection Authorities – the Working Party on Police and Justice – WPPJ- on the Draft Council Decision on the Implementation of Decision 2007/.../Jha on the stepping up of cross-border cooperation and the technical annex of 18 October 2007 concerning the implementation
aprile 2008 [doc. *web* n. 1531847]

Lettera di trasmissione delle valutazioni del WPPJ concernenti in particolare l'allegato tecnico alla decisione attuativa della decisione del Consiglio sull'attuazione del Trattato di Prüm
7 aprile 2008 [doc. *web* n. 1531430]

(*) Reperibili sul sito *www.garanteprivacy.it*

Commenti congiunti WP29/WPPJ sul "pacchetto Frattini" in materia di gestione delle frontiere esterne
Joint Comments of the Article 29 Working Party and the Working Party on Police and Justice on the Communications from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of Regions, namely: "Preparing the next steps in border management in the European Union", Com (2008) 69 final,"Examining the creation of a European Border Surveillance System (Eurosur)" Com (2008) 68 final, and "Report on the evaluation and future development of the Frontex Agency" Com (2008) 67 final
29 aprile 2008 [doc. *web* n. 1531347]

Lettera congiunta WP29/WPPJ al *Commissioner for Justice Freedom and Security sul "pacchetto Frattini"*
29 aprile 2008 [doc. *web* n. 1531434]

55 Corte europea dei diritti dell'uomo (*)

Privacy *sul luogo di lavoro*
European Court of Human Rights, Case of Copland *v.* the United Kingdom
(Application no. 62617/00)
3 aprile 2007 [doc. *web* n. 1531450]

(*) Reperibili sul sito
www.garanteprivacy.it

56 29ma Conferenza internazionale dei Garanti *privacy* (*)

Risoluzione sugli standard *globali per garantire i dati dei passeggeri*
"Resolution on the urgent need for global standards for safeguarding passenger data to be used by governments for law enforcement and border security purposes"
28 settembre 2007 [doc. *web* n. 1531481]

Risoluzione sullo sviluppo di standard *internazionali*
"Resolution on Development of International Standards"
28 settembre 2007 [doc. *web* n. 1531485]

Risoluzione sulla cooperazione internazionale
"Resolution on International Co-operation"
28 settembre 2007 [doc. *web* n. 1531910]

(*) Reperibili sul sito *www.garanteprivacy.it*

57 Conferenza di primavera 2007 (*)

Dichiarazione sul principio di disponibilità
Dichiarazione adottata in occasione della Conferenza delle autorità europee per la protezione dei dati tenutasi a Cipro dal 10 all'11 maggio 2007
11 maggio 2007 [doc. *web* n. 1531408]

Dichiarazione sulla decisione-quadro "Terzo pilastro"
Dichiarazione adottata in occasione della Conferenza delle autorità europee per la protezione dei dati tenutasi a Cipro dal 10 all'11 maggio 2007
11 maggio 2007 [doc. *web* n. 1531412]

Decisione sul futuro del Police Working Party
Decisione adottata in occasione della Conferenza delle autorità europee per la protezione dei dati tenutasi a Cipro dal 10 all'11 maggio 2007
11 maggio 2007 [doc. *web* n. 1531392]

(*) Reperibili sul sito
www.garanteprivacy.it

58 Conferenza di primavera 2008 (*)

Dichiarazione sul controllo dei viaggiatori

Dichiarazione adottata in occasione della Conferenza delle autorità europee per la protezione dei dati tenutasi a Roma dal 17 al 18 aprile 2008

18 aprile 2008 [doc. *web* n. 1531404]

(*) Reperibili sul sito *www.garanteprivacy.it*

59 Ocse (*)

Raccomandazione sull'attuazione transfrontaliera della normativa in materia di privacy
Oecd Recommendation on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy
12 giugno 2007 [doc. *web* n. 1531438]

Raccomandazione sull'autenticazione elettronica
Oecd Recommendation on Electronic Authentication and Oecd Guidance for Electronic Authentication
12 giugno 2007 [doc. *web* n. 1531442]

(*) Reperibili sul sito *www.garanteprivacy.it*

60 Gruppo internazionale sulla *privacy* nelle telecomunicazioni (*)

Telemarketing *transfrontaliero*
Working Paper on Cross-Border Telemarketing
4 settembre 2007 [doc. *web* n. 1531495]

Digital media *e Tv digitale*
Working Paper - Privacy Issues in the Distribution of Digital Media Content and Digital Television
4 - 5 September 2007 [doc. *web* n. 1531499]

Biglietto elettronico nel trasporto pubblico
Working Paper - E-Ticketing in Public Transport
4 - 5 September 2007 [doc. *web* n. 1531343]

Servizi di social network
Rapporto e Linee-Guida in materia di *privacy* nei servizi di *social network* - "Memorandum di Roma"
4 Marzo 2008 [doc. *web* n. 1531466]

Applicazione della Convenzione sul cybercrime
Recommendation on the Implementation and Application of the Council of Europe Convention No. 185 on Cybercrime (a.k.a. "Budapest Convention")
4 Marzo 2008 [doc. *web* n. 1531339]

(*) Reperibili sul sito *www.garanteprivacy.it*

61 Consiglio d'Europa – Comitato T-Pd (*)

Studio sull'applicazione della Convenzione 108 alla profilazione
Application of Convention 108 to the profiling mechanism. Some ideas for the future work of the consultative committee (T-Pd)
11 gennaio 2008 [doc. *web* n. 1531489]

(*) Reperibili sul sito
www.garanteprivacy.it