GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

Relazione2008

Protezione dei dati e nuove tecnologie nel mondo in trasformazione

www.garanteprivacy.it

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

Piazza di Monte Citorio, 121
00186 Roma
tel. 06 696771 - fax 06 69677785
www.garanteprivacy.it
www.dataprotection.org

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

Relazione2008

Protezione dei dati e nuove tecnologie nel mondo in trasformazione

www.garanteprivacy.it

INDICE

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

II. L'ATTIVITÀ SVOLTA DAL GARANTE

INDICE

INDICE

INDICE

IV. DOCUMENTAZIONE

Provvedimenti del Garante

Principali attività internazionali

INDICE

Elenco delle abbreviazioni

La presente Relazione è riferita al 2008 e contiene talune notizie già anticipate nella precedente Relazione, nonché alcune ulteriori informazioni, aggiornate al 29 aprile 2009, relative a sviluppi che si è ritenuto opportuno menzionare.

ad es.	*ad esempio*
art.	*articolo*
c.c.	*codice civile*
c.p.c.	*codice di procedura civile*
c.p.p.	*codice di procedura penale*
cd.	*cosiddetto/a*
cfr.	*confronta*
Codice	*Codice in materia di protezione dei dati personali (d.lg. 30 giugno 2003, n. 196)*
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 2008

1.1. Provvedimenti più significativi

1.1.1. Trattamenti collegati allo svolgimento di funzioni di giustizia e di sicurezza pubblica

I trattamenti di dati effettuati per lo svolgimento di funzioni di giustizia e sicurezza pubblica hanno un considerevole impatto sulle persone interessate, come risulta dagli atti adottati nel 2008 dal Garante per assicurare il rispetto dei princìpi sulla protezione dati in questi delicati settori.

Con le *"Linee-guida in materia di trattamento di dati personali da parte dei consulenti tecnici e dei periti ausiliari del giudice e del pubblico ministero"* (*Provv.* 26 giugno 2008 [doc. *web* n. 1534086]) è stato individuato un quadro unitario di misure e di accorgimenti relativi ai trattamenti di consulenti tecnici e periti dell'Autorità giudiziaria. Tali trattamenti devono svolgersi nel rispetto dei princìpi di liceità e qualità dei dati (art. 11 del Codice), e devono essere adottate le necessarie misure di sicurezza (artt. 31 e ss. e disciplinare tecnico Allegato B. al Codice).

Il 27 ottobre 2008 è stato sottoscritto da parte delle associazioni rappresentative dell'avvocatura e degli investigatori privati il *"Codice di deontologia e di buona condotta per il trattamento di dati personali effettuato per svolgere le investigazioni difensive o per far valere o difendere un diritto in sede giudiziaria"* (adottato con *Provv.* 6 novembre 2008, in *G.U.* 24 novembre 2008, n. 275 in vigore dal 1° gennaio 2009 [doc. *web* n. 1565171]).

Il codice per le indagini difensive, il cui rispetto costituisce condizione essenziale per la liceità e la correttezza dei trattamenti di dati personali (art. 12, comma 3, del Codice), disciplina in particolare i tempi di conservazione delle informazioni, i rapporti con i terzi

e la stampa e le modalità di trattamento dei dati personali, specie per quanto attiene all'essenzialità ed alla pertinenza dei dati trattati.

Con il *provvedimento* del 13 marzo 2008 sono state confermate le prescrizioni impartite l'8 maggio 2007 al Dipartimento di Pubblica sicurezza del Ministero dell'Interno sul trattamento dei dati da parte del Ced, con riferimento, in particolare, alla pertinenza e all'aggiornamento e ai tempi di conservazione dei dati, alle informazioni acquisite da soggetti pubblici, alla connessione con altre banche dati e all'esercizio dei diritti da parte degli interessati (*v. Relazione* 2007, *p.* 69).

Anche le prescrizioni impartite il 15 novembre 2007 al Tribunale ordinario di Roma, ai sensi dell'art. 160 del Codice, volte a rafforzare il livello di protezione dei dati personali trattati ai sensi dell'art. 47, comma 2, del Codice sono rimaste in gran parte inattuate (*v. Relazione* 2007, *p.* 127).

L'attuazione di tali prescrizioni dipende, in misura preponderante, da misure strutturali – oltre che dalla disponibilità delle indispensabili risorse finanziarie – di competenza del Ministero della giustizia, in relazione alle sue attribuzioni in tema di organizzazione e funzionamento dei servizi relativi alla giustizia.

Con *provvedimento* del 13 ottobre 2008 è stata rappresentata, pertanto, al Ministero della giustizia la necessità di fornire al Tribunale ordinario di Roma le risorse necessarie ad attuare le prescrizioni impartite con il citato *provvedimento* del 2007, che sono state confermate, invitando altresì il Ministero ad un tempestivo riscontro circa le determinazioni da adottare.

Di rilievo anche il *provvedimento* del 29 maggio 2008 [doc. *web* n. 1537606], relativo al trattamento dei dati nel sistema Eurodac per l'esame delle domande di asilo presentate ad uno Stato membro e in applicazione della Convenzione di Dublino (regolamento Ce n. 2725/2000). In particolare, il citato *provvedimento* ha ad oggetto il confronto delle impronte digitali dei richiedenti l'asilo registrate già presso l'unità centrale al fine di concorrere alla determinazione dello Stato membro competente.

Le prescrizioni impartite sono relative, tra l'altro, all'individuazione del titolare e degli eventuali responsabili del trattamento, all'informativa da fornire agli interessati, anche per

consentire loro l'esercizio del diritto di accesso e degli altri diritti collegati, alle misure per garantire la sicurezza del trattamento nelle diverse operazioni compiute.

1.1.2. Trattamento dei dati di traffico telefonico e telematico

Con *provvedimento* del 24 luglio 2008 (*G.U.* 13 agosto 2008, n. 189 [doc. *web* n. 1538224]) è stato individuato il termine del 30 aprile 2009 entro il quale i gestori telefonici devono mettersi in regola con le prescrizioni che l'Autorità aveva già individuato nel *provvedimento* 17 gennaio 2008 (*G.U.* 5 febbraio 2008, n. 30 [doc. *web* n. 1482111]) per garantire elevati *standard* tecnologici ed organizzativi a protezione dei dati di milioni di utenti. Il *provvedimento* del 24 luglio reca in allegato il testo aggiornato del *provvedimento* del 17 gennaio 2008 (*v. Relazione* 2007, *p.* 122 ss.).

Il nuovo *provvedimento* si è reso necessario anche per le novità introdotte dalla Convenzione del Consiglio d'Europa sul *cybercrime* (ratificata dall'Italia con la l. n. 48/2008) e, soprattutto, dalla direttiva 2006/24/Ce, *cd. "direttiva Frattini"* (recepita con il d.lg. n. 109/2008), che ha ridotto i tempi di conservazione dei dati di traffico telefonico: due anni per il traffico telefonico e un anno per quello telematico. Nel gennaio 2008, all'epoca del primo *provvedimento* del Garante, i dati di traffico telefonico potevano invece essere conservati, per essere utilizzati solo in caso di indagini penali, fino ad otto anni, mentre quelli di traffico telematico fino a circa quattro anni.

Con il *provvedimento* del 29 aprile 2009 (in corso di pubblicazione nella *Gazzetta Ufficiale* [doc. *web* n. 1612508]), l'Autorità ha fissato al 15 dicembre 2009, limitatamente alle misure specificamente indicate, il nuovo termine per adempiere, prevedendo altresì che, entro la medesima data, tutti i titolari del trattamento interessati debbano dare conferma al Garante delle misure e degli accorgimenti adottati, attestandone l'integrale adempimento.

Il termine tiene conto anche delle istanze pervenute da Asstel e da Assoprovider, associazioni che rappresentano le società che forniscono servizi di telecomunicazioni, che hanno chiesto ampi margini di tempo per completare l'adozione delle complesse misure di sicurezza indicate nel *provvedimento* del luglio 2008.

1.1.3. Sicurezza e trasparenza dei dati relativi all'attività tributaria

Anagrafe tributaria: sicurezza e accessi

L'attività tributaria presenta, da un lato, esigenze di trasparenza da ricollegare all'obbligo sancito dalla Costituzione di contribuire alle spese pubbliche in ragione della capacità contributiva, dall'altro, esigenze di sicurezza per la delicatezza e la rilevanza dei dati trattati, e in primo luogo per prevenire accessi impropri ai dati medesimi.

Nel 2008 entrambi i profili sono stati oggetto di provvedimenti del Garante.

Più in particolare, al termine della prima fase dell'attività ispettiva del Garante sull'Anagrafe tributaria (*v. Relazione* 2007, *p.* 49) sono stati riscontrati molti punti di criticità: mancata conoscenza del numero complessivo degli utenti che accedono al sistema informativo e della loro effettiva identità; scarsa capacità di monitoraggio su eventuali accessi anomali o utilizzi impropri di *password* e credenziali; inadeguate misure tecnologiche a protezione dei dati contenuti nel *database*.

Per porre rimedio alle carenze riscontrate e rendere il trattamento dei dati conforme alle norme sulla protezione dei dati l'Autorità ha imposto all'Agenzia delle entrate, con *provvedimento* del 18 settembre 2008 [doc. *web* n. 1549548] un'articolata serie di misure, tecnologiche ed organizzative, in particolare per innalzare i livelli di sicurezza degli accessi all'Anagrafe tributaria da parte degli enti esterni. Le misure dovranno essere adottate dall'Agenzia delle entrate entro un periodo che va da tre mesi ad un anno, a seconda della complessità degli adempimenti.

L'iniziativa va inquadrata in un più ampio programma di controllo sul sistema informativo della fiscalità, volto anche ad anticipare l'enorme lavoro di messa in sicurezza della gestione delle banche dati, tributarie e fiscali, che la realizzazione del federalismo fiscale renderà sempre più complessa e strategica.

Pubblicazione *on-line* dei dati dei contribuenti da parte dell'Agenzia delle entrate

L'Autorità era in precedenza intervenuta in via d'urgenza (*Provv.* 30 aprile 2008 [doc. *web* n. 1510761]) sulla pubblicazione, nel sito Internet dell'Agenzia delle entrate, dei dati relativi ai contribuenti per l'anno d'imposta 2005, decisa, senza acquisire il parere del Garante, dal Direttore dell'Agenzia delle entrate.

La forma di diffusione adottata poneva, infatti, evidenti problemi di conformità con il quadro normativo in materia. L'Autorità, il 30 aprile, ha chiesto ulteriori delucidazioni

all'Agenzia, invitandola a sospendere la diffusione dei dati su Internet.

Con *provvedimento* del 6 maggio 2008 [doc. *web* n. 1512255] poi, a conclusione dell'istruttoria, ha stabilito che la modalità utilizzata dall'Agenzia è stata illegittima, poiché contrastava con la disposizione secondo cui all'Agenzia spetta solo il compito di fissare annualmente le modalità di formazione degli elenchi delle dichiarazioni dei redditi, non le modalità della loro pubblicazione, che rimangono prerogativa del legislatore.

In seguito, la modifica dell'art. 69 del d.P.R. 29 settembre 1973, n. 600 (*cfr.* art. 42, d.l. 25 giugno 2008, n. 112, convertito, con modificazioni, in l. 6 agosto 2008, n. 133), ha ammesso la visione e l'estrazione di copia degli elenchi nei modi e con i limiti stabiliti dalla disciplina in materia di accesso ai documenti amministrativi, nonché da specifiche disposizioni di legge, durante l'anno di deposito degli elenchi presso i comuni e gli uffici dell'Agenzia.

1.1.4. Giornalismo - Dati di vittime di abusi. Accessibilità on-line *di archivi storici dei quotidiani*

Il delicato bilanciamento tra libertà d'informazione e diritto alla riservatezza ha impegnato il Garante nel 2008 in relazione a diversi aspetti dell'attività giornalistica.

In particolare con riferimento a tre episodi di violenza sessuale, l'Autorità è intervenuta (*Provv.* 10 luglio 2008 [doc. *web* n. 1536583], 2 ottobre 2008 [doc. *web* n. 1557470], 16 febbraio 2009 [doc. *web* n. 1590076]), come in precedenti occasioni (*v. Relazione* 2007, *p.* 73-74), nei confronti di testate giornalistiche che hanno violato le specifiche garanzie poste a tutela delle vittime. In particolare, oggetto dei citati interventi è stata la pubblicazione di numerosi dettagli (tra i quali iniziali di nome e cognome delle vittime, quartiere di residenza, professione dei genitori e di parenti, luoghi di villeggiatura frequentati, *ecc.*) la cui compresenza nel servizio giornalistico (diversamente articolata nei tre casi esaminati) era idonea a rendere identificabili le vittime stesse. Nei riguardi delle testate è stato disposto un divieto del trattamento per la violazione del principio di *"essenzialità dell'informazione"* (art. 137, comma 3, del Codice) e delle specifiche disposizioni a tutela dei minori (*v.* in particolare, art. 114, comma 6, c.p.p.; art. 7 del codice di deon-

tologia relativo al trattamento dei dati personali nell'esercizio dell'attività giornalistica; Carta di Treviso).

Presentano, invece, caratteri di novità le questioni connesse alla libera disponibilità degli archivi storici *on-line* dei principali quotidiani.

Tale disponibilità ha comportato che, anche attraverso i motori di ricerca, notizie risalenti nel tempo (spesso legate alla cronaca giudiziaria) divengano facilmente rintracciabili, proiettando un'immagine negativa dei protagonisti, anche quando il tempo trascorso ha invece portato ad un loro naturale oblio.

Del contrasto fra le esigenze conoscitive e quelle, contrapposte, di tutela della riservatezza è significativo esempio la decisione adottata su ricorso l'11 dicembre 2008 [doc. *web* n. 1583162].

Accogliendo, seppur in parte, la domanda dell'interessato, a suo tempo coinvolto in un'inchiesta penale, l'Autorità ha voluto evitare gli effetti pregiudizievoli derivanti dalla rappresentazione istantanea e cumulativa, ottenuta con l'utilizzo di motori di ricerca, di fatti ormai risalenti. A tal fine si è ordinato all'editore di adottare ogni misura tecnicamente idonea ad evitare che le generalità del ricorrente contenute nell'articolo di un quotidiano continuino ad essere rinvenibili direttamente attraverso l'utilizzo dei motori di ricerca generalisti, ferma rimanendo la possibilità di consultare la versione integrale dell'articolo medesimo accedendo direttamente al sito *web* dell'editore.

La soluzione mira al contemperamento fra due interessi confliggenti e la sua tenuta potrà essere verificata in progresso di tempo in relazione alla molteplicità delle fattispecie concrete (in materia *v.* anche le decisioni adottate l'11 dicembre 2008 [doc. *web* n. 1582866] ed il 19 dicembre 2008 [doc. *web* n. 1583152]).

1.1.5. Iniziativa economica: profilazioni personalizzate e marketing *telefonico*

L'utilizzo a fini commerciali di dati personali può risultare in contrasto con la normativa in materia, sia per ragioni inerenti alla qualità dei dati trattati, sia per quanto riguarda i presupposti stessi del trattamento e, in particolare, il consenso dell'interessato. Di entrambi i profili, talora connessi, si è occupato il Garante nel 2008.

L'improprio trattamento dei dati relativi ad informazioni commerciali è stato oggetto di diversi provvedimenti del Garante, tra i quali uno – relativo al maggiore operatore del settore (*Provv.* 30 ottobre 2008 [doc. *web* n. 1570327]) ed adottato in esito ad un'approfondita istruttoria in relazione a numerosi reclami e segnalazioni degli interessati – utile a fornire indicazioni di carattere generale sull'applicazione, anche in tale materia, del principio di pertinenza dei dati (art. 11 del Codice).

Le informazioni commerciali esprimono, seppure in forma sintetica, apprezzamenti sull'affidabilità degli operatori economici e, se non pienamente soddisfacenti, sostanziano in modo particolarmente rilevante il pregiudizio per gli interessati.

In sintesi, dall'attività svolta è risultato che in diversi casi il *"dossier persona"* relativo ad un individuo, conteneva informazioni riferibili a terzi (*v.* anche, *infra par.* 17.2.4, decisione su ricorso del 12 giugno 2008 [doc *web* n. 1537684] sull'arbitrario accostamento fra l'interessato ed il fallimento di una società di cui lo stesso era stato socio accomandante).

Anche gli elementi utilizzati per le valutazioni sintetiche sull'affidabilità commerciale degli interessati sono risultati talora riconducibili a soggetti diversi dall'interessato (*ad es.*, riferiti anche a eventi – talora negativi – riconducibili a *"imprese connesse"*) e perciò in contrasto con i princìpi di correttezza, pertinenza e non eccedenza, oltre che in violazione del diritto all'identità personale (artt. 2 e 11 del Codice).

Inoltre, è emerso che la società ha utilizzato congiuntamente (e indifferentemente), per classificare l'affidabilità degli operatori, un indice costituito da due aggettivi – nullo/basso – e che la modalità di utilizzo di tali aggettivi, che non sono sinonimi, non forniva un quadro chiaro dell'affidabilità commerciale del soggetto censito.

L'associazione impropria degli elementi è stata ritenuta non pertinente, anche per la possibile alterazione della proiezione sociale e professionale che può derivarne al soggetto censito e la lesione del diritto all'identità personale (art. 2 del Codice).

I *dossier* contenenti indici sull'affidabilità commerciale dei soggetti censiti sono risultati essere non – come prospettato dalla società – mere sintesi di informazioni tratte da pubblici registri, bensì autonome valutazioni, sulla base di un peso ponderato attribuito alle diverse informazioni e, come tali, dati personali autonomi, distinti dalle informazioni

originarie ricavate dalle fonti pubbliche, il cui trattamento – a differenza di quello relativo a dati pubblicamente disponibili – necessita del consenso degli interessati (art. 23 del Codice) o di altro presupposto equipollente previsto dall'art. 24 del Codice.

Nel corso degli accertamenti è emerso, inoltre, che la società non solo trattava informazioni eccessive e non pertinenti, ma raccoglieva anche dati personali da fonti dalle quali non poteva attingere, come le liste elettorali, o addirittura le dichiarazioni dei redditi del 2005, acquisite in occasione della loro messa *on-line* da parte dell'Agenzia delle entrate (diffusione dichiarata dall'Autorità illegittima *v. supra* n. 1.1.3).

È stata perciò prescritta alla società l'adozione di ogni misura necessaria e idonea ad evitare l'associazione a un soggetto di informazioni al medesimo non direttamente riconducibili.

Il Garante ha altresì prescritto alla società di tenere distinti i casi in cui l'indice sia *"basso"* da quelli in cui sia *"nullo"* e ha inoltre vietato alla medesima, in particolare: l'utilizzo di informazioni non pertinenti agli interessati per l'elaborazione degli indici sintetici; il trattamento per le finalità dichiarate dalla società dei dati provenienti dalle liste elettorali; il trattamento dei dati relativi alle dichiarazioni dei redditi pubblicati dall'Agenzia delle entrate, con prescrizione di cancellarli.

Divieto di utilizzo di banche dati a fini di *marketing* telefonico

L'altro profilo, riguardante il consenso degli interessati, è emerso con particolare rilievo nei provvedimenti relativi all'utilizzo di banche dati a fini di *marketing* telefonico, dapprima vietato dal Garante per l'assenza di consenso dell'interessato, poi consentito sino al 31 dicembre 2009 da una modifica normativa e, di conseguenza, oggetto di nuovo *provvedimento* dell'Autorità.

I provvedimenti inibitori del 26 giugno 2008 [doc. *web* nn. 1544315, 1544326, 1544338] sono stati emanati dopo verifiche svolte, su segnalazioni di numerosi abbonati, presso le società che hanno fornito i *database*. Dagli accertamenti è emerso che i dati degli utenti erano stati raccolti e ceduti a terzi senza informare gli interessati, o informandoli in maniera inadeguata, e senza un loro preventivo specifico consenso. Una delle società offriva sul proprio sito i dati di oltre quindici milioni di famiglie italiane suddivise per redditi e stili di vita, senza che gli interessati fossero stati informati o avessero dato il loro assenso alla comunicazione dei dati a terzi.

Da parte loro le aziende e le compagnie telefoniche che hanno acquistato i dati, utilizzandoli a fini di *marketing* telefonico, non si erano preoccupate di accertare, come prevede invece la disciplina sulla protezione dei dati, che gli abbonati avessero acconsentito alla comunicazione dei propri dati e al loro uso a fini commerciali.

Successivamente, l'art. 44, comma 1-*bis* del d.l. 30 dicembre 2008, n. 207, convertito, con modificazioni, in l. 27 febbraio 2009, n. 14 (*G.U.* 28 febbraio 2009, n. 28), ha stabilito che i dati personali presenti nelle banche dati costituite sulla base dei vecchi elenchi telefonici sono utilizzabili per fini promozionali fino al 31 dicembre 2009 da coloro che hanno creato tali banche dati precedentemente al 1° agosto 2005. Il *provvedimento* del 12 marzo 2009 (*G.U.* 20 marzo 2009, n. 66 [doc. *web* n. 1598808]) precisa i limiti entro i quali le società che effettuano attività promozionale, anche tramite *call center*, possono avvalersi della deroga.

Il mancato rispetto delle prescrizioni del *provvedimento* comporta una sanzione amministrativa che va da trentamila a centottantamila euro e che, nei casi più gravi, può raggiungere anche i trecentomila euro. In sintesi, le società devono documentare in modo adeguato che la banca dati, costituita con i numeri telefonici e gli indirizzi degli abbonati, sia stata effettivamente creata prima del 1° agosto 2005. Esse devono usare questi dati direttamente e non possono cederli a nessun titolo ad altre aziende.

L'eventuale contrarietà dell'abbonato ad essere nuovamente contattato deve essere registrata immediatamente dall'operatore, tenuto, se richiesto, a comunicare all'abbonato stesso il suo identificativo. I dati non possono in alcun modo essere usati per acquisire nuove informazioni o il consenso degli abbonati ad effettuare chiamate dopo la data del 31 dicembre 2009, poiché in tal modo gli effetti della temporanea deroga verrebbero a protrarsi oltre il termine previsto dal legislatore.

Le società che svolgono attività di *marketing* devono comunicare al Garante, entro quindici giorni dalla pubblicazione in *Gazzetta Ufficiale* del *provvedimento*, di essere in possesso di banche dati costituite anteriormente al 1° agosto 2005 e di volerle utilizzare per attività promozionali, chiarendo se il trattamento di dati venga effettuato anche per conto terzi.

1.1.6. Protezione dei dati dei lavoratori dipendenti e dei collaboratori

In questo settore gli interventi del Garante sono stati relativi principalmente alla trasparenza del trattamento, per evitare utilizzi dei dati non oggetto di informativa agli interessati, al rispetto delle forme di legge per il controllo a distanza dei lavoratori (art. 4 della l. n. 300/1970), alla qualità dei dati, perlopiù per evitare il trattamento di dati non pertinenti.

In termini generali, esprimendo il parere previsto dall'art. 154 del Codice (*Provv.* 31 marzo 2008 [doc. *web* n. 1504941]) sullo 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, è stata evidenziata l'esigenza di verificare l'indispensabilità e la necessità dei dati da trattare, di adottare le misure di sicurezza necessarie e di salvaguardare il segreto professionale.

Accogliendo il reclamo di un'organizzazione sindacale (*Provv.* 2 aprile 2008 [doc. *web.* n. 1519695]) è stato bloccato – nelle more dell'espletamento delle procedure di legge – l'ulteriore trattamento dei dati dei dipendenti di una compagnia aerea, limitatamente alle informazioni connesse all'utilizzo per finalità formative di *computer* portatili. È, infatti, emerso che le funzioni di tracciamento e registrazione degli accessi al corso di formazione, utili al monitoraggio dell'andamento del processo formativo, erano idonee al controllo a distanza dell'attività lavorativa dei dipendenti, ciò senza l'osservanza delle procedure a tal fine richieste dall'art. 4 della l. n. 300/1970, oltre che in assenza dell'informativa agli interessati e del loro consenso.

Sistemi di localizzazione, *event data recorder* e servizi di trasporto pubblico

Per garantire la sicurezza dei passeggeri e l'efficienza del servizio è stato consentito ad una società di trasporto pubblico, in sede di verifica preliminare (*Provv.* 5 giugno 2008 [doc. *web* n. 1531604]), l'utilizzo di sistemi di localizzazione e di registrazione di *"eventi di guida"*, previo rispetto delle procedure previste dallo Statuto dei lavoratori.

Il sistema prevede il riconoscimento attraverso un codice identificativo cifrato del conducente del veicolo, al quale – direttamente o anche in un secondo tempo – possono essere associati tutti i dati ricavati dal sistema. Le garanzie procedurali previste dall'art. 4 della l. n. 300/1970 (accordo sindacale o autorizzazione della Direzione provinciale del

lavoro) dovranno essere rispettate poiché il sistema può determinare un controllo a distanza dei lavoratori, ancorché giustificato da esigenze organizzative e produttive della società.

I dati raccolti dovrebbero confluire in un *database* gestito dal fornitore del servizio e fruibile dall'azienda grazie ad un portale (compreso anch'esso nel progetto) al quale si accederà solamente attraverso l'utilizzo di un sistema identificativo comprensivo di *userId* e *password*.

Il Garante ha stabilito, inoltre, che siano fornite agli interessati informazioni dettagliate sulla natura dei dati trattati e sulle caratteristiche del sistema e che l'accesso ai dati dovrà essere consentito ai soli incaricati della società. L'Autorità ha sottolineato, infine, che le informazioni ricavate da tale sistema di localizzazione potranno essere utilizzate a fini di sicurezza e miglioramento del servizio e conservate per il tempo necessario a perseguire le finalità indicate nel provvedimento.

Comunicazione a terzi di dati relativi a procedimenti penali pendenti

Decidendo su un reclamo, l'Autorità ha vietato a due società l'ulteriore comunicazione a terzi di dati personali relativi, tra l'altro, ad un procedimento penale a carico di una ex collaboratrice (*Provv.* 2 aprile 2008 [doc. *web* n. 1519711]), essendo stata la comunicazione effettuata in violazione dei princìpi di necessità e finalità (artt. 3 e 11, comma 1, lett. *b*), del Codice), oltre che in assenza della prescritta informativa. Il Garante ha rilevato che non era necessario dare notizia ai terzi del procedimento penale, essendo sufficiente comunicare l'interruzione del rapporto di collaborazione.

Trattamento di dati personali raccolti in occasione di programmi di fidelizzazione e loro utilizzo per fini disciplinari nell'ambito del rapporto di lavoro

Due divieti (*Provv.* 2 aprile 2008 [doc. *web* n. 1519679] e 6 novembre 2008 [doc. *web* n. 1573780]) sono stati emessi su istanze degli interessati, in relazione all'utilizzo per procedimenti disciplinari, sfociati in licenziamenti, di dati dei dipendenti raccolti per finalità di *marketing* e fidelizzazione (gli interessati, dipendenti di esercizi commerciali, "caricavano" sulla propria carta di fidelizzazione gli acquisti effettuati dalla clientela).

I dati acquisiti sono stati utilizzati anche per controllare l'esecuzione della prestazione lavorativa e l'osservanza dell'obbligo di fedeltà dei dipendenti anziché essere trattati, come sarebbe dovuto accadere in base all'informativa fornita agli interessati, nel solo ambito del programma di fidelizzazione.

Il Garante ha vietato pertanto alle due società di effettuare, nel contesto del rapporto di lavoro, ulteriori trattamenti dei dati connessi all'utilizzo della carta di fidelizzazione in violazione dei princìpi di liceità e finalità (artt. 11, comma 1, lett. *a*) e *b*), del Codice).

1.1.7. Adempimenti semplificati per finalità amministrative e in materia di sicurezza dei dati

L'esigenza di snellire gli adempimenti formali previsti dalla normativa, per dare maggior rilievo agli aspetti sostanziali che incidono sull'effettiva protezione dei dati degli interessati, ha portato all'adozione nel 2008 di importanti misure di semplificazione.

Semplificazione di taluni adempimenti rispetto a trattamenti per finalità amministrative e contabili

Con *provvedimento* del 19 giugno 2008 [doc. *web* n. 1526724] sono state individuate soluzioni per agevolare il trattamento dei dati nell'ordinaria attività di gestione amministrativa e contabile – in particolare nei casi in cui non sono trattati dati di carattere sensibile o giudiziario – enunciando nuove linee-guida interpretative della normativa ed individuando alcune modalità innovative per semplificare taluni adempimenti, in modo particolare per l'informativa agli interessati e il consenso.

In sostanza, l'Autorità ha fornito indicazioni per la redazione di un'informativa unica per il complesso dei trattamenti di dati personali a fini esclusivamente amministrativi e contabili; gli operatori potranno redigere una prima informativa breve che può rinviare a un testo più articolato, disponibile su siti Internet, reti Intranet, in bacheca o presso gli sportelli. Le associazioni di categoria sono state invitate a predisporre informative-tipo per determinati settori o categorie di trattamenti.

Per quanto riguarda il consenso sono stati indicati i casi in cui esso non è richiesto, ad esempio quando i trattamenti sono svolti per adempiere ad obblighi contrattuali o normativi o quando i dati provengono da registri o elenchi pubblici, o sono relativi allo svolgimento di attività economiche.

Semplificazione delle misure di sicurezza

Con *provvedimento* del 27 novembre 2008 (*G.U.* 9 dicembre 2008, n. 287 [doc. *web* n. 1571218]) sono state dettate modalità più snelle per l'applicazione delle misure di sicurezza alle attività di corrente gestione amministrativa e contabile, svolte specie presso piccole e medie imprese, liberi professionisti e artigiani, senza ridurre le garanzie per i cittadini.

In particolare, il *provvedimento* riguarda sia amministrazioni pubbliche e società private che utilizzano dati personali non sensibili o che trattano come unici dati sensibili dei dipendenti quelli relativi allo stato di salute o all'adesione a organizzazioni sindacali, sia piccole e medie imprese, liberi professionisti o artigiani che trattano dati solo per fini amministrativi e contabili.

In base al citato *provvedimento*, il Garante ha stabilito, tra l'altro, che le istruzioni in materia di misure minime possono essere impartite agli incaricati anche oralmente; per l'accesso ai sistemi informatici è possibile utilizzare qualsiasi sistema di autenticazione basato su un *username* e una *password*; l'*username* deve essere disattivato quando vengono meno le condizioni per il legittimo accesso ai dati. Con riguardo alle misure di sicurezza, i programmi volti a prevenire la vulnerabilità di strumenti elettronici (*ad es.*, gli antivirus) devono essere aggiornati almeno annualmente e i dati possono essere salvaguardati anche attraverso il loro salvataggio almeno mensile. Sono state anche fornite alcune indicazioni per la redazione del documento programmatico per la sicurezza semplificato ed indicate procedure più snelle per chi tratta dati senza l'impiego di sistemi informatici.

Semplificazione delle notificazioni

Il 22 ottobre 2008 il Garante ha adottato un *provvedimento* (*G.U.* 9 dicembre 2008, n. 287 [doc. *web* n. 1571196]) che semplifica il modello utilizzato per effettuare le notificazioni (*cfr.* art. 38 del Codice, come modificato dalla l. 6 agosto 2008, di conversione, con modificazioni, del d.l. 25 giugno 2008, n. 112), ossia le dichiarazioni da fare all'Autorità quando si intende avviare un trattamento di particolari tipi di dati (genetici, biometrici, procreazione assistita, *ecc.*). Il *provvedimento* sulla notificazione non comporta l'obbligo di notificare di nuovo o modificare le notificazioni a carico di chi lo abbia già fatto.

1.1.8. Prescrizioni in materia di gestione di sistemi complessi e di rottamazione di apparecchiature elettroniche

Amministratori di sistema

Con *provvedimento* del 27 novembre 2008 (*G.U.* 24 dicembre 2008, n. 300 [doc. *web* n. 1577499]) il Garante, in considerazione della particolare delicatezza delle funzioni di amministratore di sistema in una banca dati, ha fissato le regole per l'adozione, da parte

di enti, amministrazioni pubbliche e società private, delle misure tecniche e organizzative che riguardano tali peculiari figure, chiamate a svolgere delicate funzioni di gestione e manutenzione di un impianto di elaborazione, che comportano spesso la concreta possibilità di accedere a tutti i dati trattati informaticamente nelle banche dati.

Tali misure sono dirette a migliorare i criteri di individuazione degli amministratori di sistema, e ad agevolare la verifica sull'attività degli amministratori da parte di chi ha la titolarità delle banche dati e dei sistemi informatici, e non riguardano i trattamenti di dati effettuati a fini amministrativo-contabili, che pongono solitamente minori rischi per gli interessati.

In particolare, è prevista la registrazione degli accessi logici degli amministratori ai sistemi di elaborazione e agli archivi elettronici, da conservare per un periodo non inferiore a sei mesi. L'operato degli amministratori di sistema deve essere verificato almeno annualmente da parte dei titolari del trattamento, analogamente a quanto richiesto dal Codice relativamente ai responsabili. Gli estremi identificativi degli amministratori di sistema e l'elenco delle funzioni loro attribuite devono essere indicati in un documento disponibile in caso di accertamenti da parte del Garante.

L'Autorità, in ragione della complessità degli interventi necessari per l'adeguamento dei sistemi, su richiesta dalle associazioni degli operatori interessati ha prorogato i termini per gli adempimenti.

In particolare, dopo l'unificazione dei vari termini e il differimento al termine unico del 30 giugno 2009 (*Provv.* 12 febbraio 2009, in *G.U.* 24 febbraio 2009, n. 45 [doc. *web* n. 1591970]), ha avviato, con *provvedimento* del 21 aprile 2009 (in corso di pubblicazione in *Gazzetta Ufficiale* [doc. *web* n. 1611986]), una consultazione pubblica per *"acquisire osservazioni e commenti da parte dei titolari del trattamento ai quali il provvedimento si rivolge con esclusivo riferimento a quanto prescritto al punto 2 del dispositivo del provvedimento del 27 novembre 2008"*.

Sicurezza dei dati personali nella rottamazione di apparecchiature elettroniche

Con *provvedimento* del 13 ottobre 2008 [doc. *web* n. 1571514] sono state indicate le misure organizzative e tecniche da adottare per garantire l'effettiva cancellazione (o la trasformazione in forma non intelligibile) dei dati personali contenuti in apparati elettrici ed

elettronici, quali i *personal computer*, in occasione della loro dismissione (artt. 31 e ss. del Codice).

Al riguardo, è previsto che si possano incaricare soggetti tecnicamente qualificati, qualora il titolare non sia in grado di cancellare effettivamente i dati o di renderli anonimi. L'Autorità ha anche indicato ai titolari dei trattamenti alcune procedure (suscettibili di aggiornamento alla luce dell'evoluzione tecnologica) ritenute idonee a garantire che, in sede di reimpiego, riciclaggio, ovvero di smaltimento di apparecchiature elettriche ed elettroniche, siano stati effettivamente cancellati o resi anonimi i dati personali ivi memorizzati.

1.1.9. Dati genetici e sanitari, verifiche anti-doping *e sperimentazioni di medicinali*

Dati genetici

Con *provvedimento* del 27 novembre 2008 [doc. *web* n. 1581365] l'Autorità ha vietato l'ulteriore trattamento di dati genetici, raccolti in segreto da un genitore e dal suo legale, per verificare l'effettiva consanguineità del figlio, senza informare l'interessato e senza il suo consenso.

In particolare, l'Autorità ha ritenuto violati i diritti del figlio, rilevando che la raccolta e il trattamento dei dati genetici possono avvenire esclusivamente con il consenso informato dell'interessato, *"manifestato previamente e per iscritto"*. Si può derogare all'obbligo del previo consenso per far valere o difendere un proprio diritto in sede giudiziaria, solo se l'accertamento sia assolutamente *"indispensabile"* e venga svolto nel rispetto delle regole fissate dal Garante. Nel caso di specie, sulla base delle dichiarazioni dello stesso legale, l'accertamento non è risultato indispensabile per tutelare in sede giudiziaria un diritto del genitore, sicché sarebbe stato necessario acquisire il consenso del figlio.

Linee-guida in tema di fascicolo sanitario elettronico e di *dossier* sanitario

Sulle *"Linee-guida in tema di fascicolo sanitario elettronico"*, messe a punto dal Garante con *deliberazione* del 5 marzo 2009 (*G.U.* 26 marzo 2009, n. 71 [doc. *web* n. 1598313]), è stata avviata una consultazione pubblica per acquisire, entro il 31 maggio 2009, osservazioni e suggerimenti da parte di cittadini, operatori del settore, associazioni di malati.

Il *"Fascicolo sanitario elettronico"* (*Fse*), già in via di sperimentazione in alcune regioni, raccoglie i dati sanitari di ogni paziente – patologie, interventi chirurgici, esami clinici, farmaci – in un documento elettronico consultabile dall'interessato e aggiornabile *on-line*

da medici ed enti ospedalieri. In sintesi, il fascicolo sanitario elettronico dovrà essere costituito esclusivamente per finalità di prevenzione, diagnosi, cura e riabilitazione. Sarà consultabile dall'interessato e dal personale sanitario, strettamente autorizzato, solo per finalità sanitarie.

Al paziente deve essere consentito di scegliere se far costituire o meno un fascicolo sanitario elettronico, con tutte o solo alcune informazioni sanitarie che lo riguardano. Deve essere prevista la possibilità di "oscurare" la visibilità di alcuni eventi clinici e devono essere assicurate le prestazioni del servizio sanitario nazionale anche ai pazienti che non aderiscono al Fse. L'informativa deve indicare con semplicità, in particolare, chi ha accesso ai dati, quali operazioni può compiere, e se il conferimento dei dati è obbligatorio o meno. La delicatezza dei dati trattati impone l'adozione di specifiche misure per limitare il più possibile i rischi di accesso abusivo, furto, smarrimento.

Controlli *anti-doping* e dati personali dei ciclisti

Su segnalazione presentata dall'Accpi (Associazione corridori ciclisti professionisti italiani) il Garante, con *provvedimento* del 13 ottobre 2008 [doc. *web* n. 1563970], ha stabilito che i controlli previsti dal nuovo protocollo *anti-doping* (basato sugli *standard* stabiliti dalla Agenzia mondiale *anti-doping* (*Wada*) sono leciti, ma l'informativa del Coni sui controlli effettuati al di fuori delle competizioni deve essere modificata.

Per evitare di raccogliere dati che possono comportare indebite interferenze sulla vita privata o rivelare dati sensibili o giudiziari degli atleti o di soggetti terzi, vanno infatti specificate le informazioni personali sulla localizzazione e reperibilità giornaliera che gli atleti devono conferire. Deve, inoltre, essere chiarito se sia o meno obbligatorio fornire i dati, indicando sia le conseguenze del loro mancato conferimento, sia i destinatari, sia la circostanza che i dati stessi vengono trasmessi all'estero.

Riguardo ai luoghi di esecuzione dei controlli, il Garante ha preso atto degli impegni del Coni di introdurre nuove istruzioni operative per gli ispettori, perché sia prestata la massima attenzione al rispetto della riservatezza dell'atleta e dei terzi eventualmente presenti nel domicilio al momento del *test*.

Sperimentazione farmaci

Con *provvedimento* del 24 luglio 2008 (*G.U.* 14 agosto 2008, n. 190 [doc. *web* n. 1533155]) sono state adottate, anche tenendo conto delle osservazioni pervenute nel

corso di una consultazione pubblica, *le "Linee-guida per i trattamenti dei dati personali nelle sperimentazioni cliniche di medicinali"*. Le linee-guida sono volte a fornire maggiori tutele ai pazienti interessati, ridurre i tempi di conservazione dei dati e dei campioni biologici ed assicurare l'adozione di misure di sicurezza corrispondenti alla delicatezza dei dati trattati.

Con l'introduzione di regole *ad hoc* l'Italia si pone all'avanguardia in Europa nella protezione della *privacy* in questo settore.

L'Autorità ha messo a punto un modello per informare i pazienti sul trattamento dei dati che li riguardano. Devono essere specificati la natura dei dati trattati, la circostanza che essi vengano trasmessi all'estero, l'effettivo ruolo svolto dalla casa farmaceutica *sponsor* e promotrice della ricerca, i soggetti ai quali i dati possono essere comunicati, l'esercizio del diritto di accesso e gli altri diritti (rettifica, aggiornamento) riconosciuti al paziente.

È stata inoltre individuata una formula per l'acquisizione del consenso dei pazienti unitamente al modello d'informativa, relativa anche ad eventuali trattamenti effettuati presso altri soggetti che, non solo in Italia, collaborano alla ricerca.

Senza tale assenso il trattamento dei dati personali è illecito.

In considerazione, infine, del fatto che le case farmaceutiche sono nella gran parte società multinazionali che hanno necessità di trasferire i dati in diversi Paesi, è stata prescritta l'adozione di elevati *standard* di sicurezza, soprattutto per i trasferimenti in via telematica. Obbligatorie, quindi, procedure di autenticazione per l'accesso ai dati, sistemi per la memorizzazione e l'archiviazione che prevedono, ad esempio, la cifratura e protocolli di comunicazione sicuri per la trasmissione dei dati tra i centri di sperimentazione, il *database* della società farmaceutica e i soggetti incaricati del monitoraggio.

Il *provvedimento* è stato inviato al Ministero della salute, all'Istituto superiore di sanità, all'Agenzia italiana del farmaco e alla Conferenza Stato-Regioni.

Con *provvedimento* del 24 luglio 2008 [doc. *web* n. 1544575] è stato vietato ad una multinazionale farmaceutica il trattamento illecito dei dati, erroneamente ritenuti anonimi, delle persone sottoposte ai *test* sui farmaci.

Alla società è stato prescritto, inoltre, di conformarsi, entro un termine piuttosto breve, alle linee-guida sopra descritte.

Sono emerse criticità anche in relazione ai trattamenti di dati effettuati dagli informatori scientifici nel corso delle visite periodiche ai medici. È stato, pertanto, vietato l'ulteriore utilizzo dei dati raccolti dalla casa farmaceutica nel corso di questa attività promozionale e prescritto alla stessa di conformarsi alla normativa in materia.

1.1.10. Videosorveglianza

Con *deliberazione* del 13 maggio 2008 [doc. *web* n. 1523997] il Garante ha segnalato al Parlamento e al Governo l'opportunità di disciplinare alcuni aspetti del trattamento di dati personali derivante dall'installazione di impianti di videosorveglianza nei condomìni.

Da segnalazioni e quesiti pervenuti relativi al caso in cui non i singoli condomini, ma l'intero condominio intende installare tali impianti in aree comuni (quali portoni d'ingresso, androni o cortili) è emersa la contrapposizione tra l'esigenza di sicurezza delle persone e la libertà di muoversi, senza essere controllati, nel proprio domicilio e all'interno delle aree comuni.

La questione non trova regolamentazione nel codice civile del 1942, né in base ai princìpi generali appare chiaro quale sia la maggioranza necessaria per deliberare l'installazione di sistemi di videosorveglianza (se sia cioè sufficiente la sola volontà dei proprietari o se si debba tener conto anche del consenso, in particolare, dei conduttori). Al riguardo, è stato altresì rappresentato che il divieto di procurarsi indebitamente immagini relative alla vita privata che si svolge nel domicilio (art. 615-*bis* del c.p.) – nozione che secondo alcune decisioni giurisprudenziali può giungere fino a ricomprendere le aree comuni – potrebbe rendere necessario acquisire il consenso di un numero assai ampio di soggetti, non sempre di agevole identificazione.

Con *provvedimento* del 4 dicembre 2008 [doc. *web* n. 1576125] adottato in seguito a ispezioni disposte su segnalazione, il Garante ha ordinato ad un centro dietetico di rimuovere l'impianto di videosorveglianza (le telecamere erano collocate all'ingresso esterno, negli spogliatoi e nell'ambulatorio dove si effettuano le visite mediche) e cancellare le immagini registrate. Nel *provvedimento* l'Autorità ha ritenuto che la collocazione di telecamere operanti in modo continuo negli spogliatoi, benché segnalata da appositi avvisi e

giustificata dalla struttura medica con riferimento a svariati furti verificatisi in passato, risultasse lesiva della riservatezza e dignità delle persone interessate.

Con *deliberazione* del 2 ottobre 2008 [doc. *web* n. 1581352] è stato vietato il trattamento dei dati relativi alla voce degli interessati connesso all'utilizzo di un sistema di videosorveglianza presente all'interno di un esercizio commerciale.

Da accertamenti svolti in seguito a segnalazioni, oltre alla non visibilità dei cartelli apposti per informare della presenza delle telecamere, è risultato altresì che una delle tre telecamere interne, collocata vicino al registratore di cassa, risultava dotata di registratore audio. L'Autorità ha ritenuto illecita la registrazione delle voci perché non conforme al principio di finalità, secondo cui il trattamento deve essere effettuato per finalità determinate, esplicite e legittime, che non risultano ricorrere nel caso esaminato. Il Garante, inoltre, ha imposto al titolare del negozio di designare quale responsabile del trattamento il soggetto che ha la manutenzione dell'impianto, disponendo fino ad allora il blocco della comunicazione delle immagini dello stesso.

1.1.11. Utilizzo del cellulare per localizzare persone disperse

Con *provvedimento* del 19 dicembre 2008 [doc. *web* n. 1580543] il Garante ha chiarito che il Codice, nel caso vi sia la necessità di salvaguardare la vita o l'incolumità di una persona, consente alla società telefonica di comunicare senza indugio all'organismo di soccorso, anche senza il consenso dell'interessato, dati quali quelli concernenti i ponti e le celle attivate o "agganciate" dal telefono mobile della persona dispersa. La decisione ha, infatti, ad oggetto solo i dati relativi all'ubicazione diversi dai dati relativi al traffico, ossia i dati che possono essere reperiti sulla rete di comunicazione elettronica a prescindere da una comunicazione tra soggetti.

Il *provvedimento* riguarda il soccorso alpino, ma afferma princìpi applicabili, con le dovute cautele, anche in altri casi di soccorso. L'Autorità ha inoltre chiarito che i dati acquisiti dagli organismi di soccorso dovranno essere utilizzati solo per ricercare e soccorrere la persona dispersa.

L'Autorità ha altresì ricordato che i servizi abilitati a ricevere le chiamate di emergenza,

possono comunque trattare i dati relativi all'ubicazione dei telefoni relativi a chi chiama, anche quando l'utente o l'abbonato abbiano già rifiutato o omesso di prestare il consenso (*cfr.* considerando 36 e art. 10, comma 1, lett. *b*), della direttiva 2002/58/Ce e art. 127, comma 4, del Codice).

1.2. RAPPORTI CON IL PARLAMENTO E ALTRE ISTITUZIONI

1.2.1. Le audizioni del Garante in Parlamento

In questo primo scorcio della XVI legislatura 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 30 gennaio 2009, presso il Comitato parlamentare per la sicurezza della Repubblica, un'audizione sulla nota vicenda della raccolta di dati effettuata nell'ambito di una inchiesta giudiziaria della procura di Catanzaro (*cd. "caso Genchi"*);
- il 10 dicembre 2008, presso la Commissione giustizia della Camera, un'audizione sul disegno di legge del Governo e sulle proposte abbinate concernenti la riforma della disciplina delle intercettazioni di comunicazioni. Il Garante si è soffermato, in particolare, sul trattamento dei dati effettuato nell'ambito degli uffici giudiziari e sulle connesse misure di sicurezza, sulle disposizioni concernenti la videosorveglianza e l'acquisizione dei tabulati di traffico telefonico, nonché sulle disposizioni in materia di pubblicazione degli atti di indagine e sul rapporto fra diritto di cronaca e tutela dei dati personali degli interessati;
- il 22 ottobre 2008, presso la Commissione finanze della Camera, un'audizione informale sulle problematiche del settore assicurativo. In tale occasione il Garante ha condiviso l'esigenza di migliorare la perseguibilità delle frodi nel settore delle assicurazioni auto, ritenendo però non necessario istituire una nuova banca dati, ma semmai migliorare quella già esistente presso l'Isvap, utilizzando l'esperienza e l'at-

tività fin qui svolta da tale istituto nel settore e assicurando, al tempo stesso, maggiori garanzie per gli interessati anche attraverso il potenziamento della sicurezza dei dati registrati nell'archivio;

- il 23 settembre 2008, presso la Commissione bicamerale di vigilanza sull'anagrafe tributaria, un'audizione sulle problematiche concernenti i trattamenti di dati e gli accessi a tale banca dati. Il Garante, dopo aver illustrato le problematiche derivanti in tale settore dalla riforma in materia di federalismo fiscale, si è soffermato sulle iniziative assunte dall'Autorità in relazione al trattamento dei dati registrati nell'Anagrafe tributaria. In tal senso, ha dato conto della complessa attività ispettiva svolta sul funzionamento della banca dati, all'esito della quale, con *provvedimento* del 18 settembre 2008 [doc. *web* n. 1549548], sono state imposte all'Agenzia delle entrate misure, sia tecnologiche che organizzative, per innalzare i livelli di sicurezza degli accessi all'Anagrafe da parte degli enti esterni e rendere il trattamento conforme alle norme sulla protezione dei dati;
- il 31 luglio 2008, presso la Commissione finanze e tesoro del Senato, un'audizione informale in merito ai disegni di legge relativi all'istituzione di un sistema di prevenzione delle frodi nel settore del credito al consumo. L'Autorità ha richiamato l'attenzione sull'importanza della scelta di configurare il sistema come uno *"snodo tecnico"* attraverso il quale il soggetto pubblico preposto provvede a riscontrare le richieste di verifica provenienti dai soggetti aderenti al sistema su dati e informazioni registrati in altre, distinte banche dati, senza inutili duplicazioni di banche dati. Il Garante ha, peraltro, evidenziato alcune criticità e, in particolare, l'esigenza: a) di individuare nella legge le specifiche finalità perseguite e i dati oggetto di verifica, circoscrivendo l'ambito applicativo dei decreti di attuazione alle modalità tecniche e alla sicurezza dei dati; b) di limitare la platea dei soggetti aderenti al sistema, in chiave di proporzionalità rispetto alle finalità del sistema antifrode; c) di affrontare il problema delle frodi nel settore assicurativo con una riflessione legislativa a parte, più completa.

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

Nel 2008 l'Autorità ha fornito la consueta collaborazione al Governo in riferimento ad atti di sindacato ispettivo e ad attività di indirizzo e di controllo del Parlamento riguardanti aspetti di specifico interesse in materia di protezione dei dati personali.

In particolare, sono stati forniti elementi di valutazione al Ministero dell'interno in relazione ad un'informativa urgente su un articolo di stampa riguardante il Ministro per la pubblica amministrazione e l'innovazione.

La vicenda riguardava un trattamento di dati personali effettuato in ambito giornalistico, la cui liceità e correttezza è stata valutata alla stregua della disciplina, anche comunitaria, in materia di protezione dei dati personali per l'attività giornalistica. In base a tale disciplina, ogni trattamento effettuato per tale finalità deve comunque rispettare i limiti del diritto di cronaca e, in particolare, l'essenzialità dell'informazione riguardo a fatti di interesse pubblico.

Chi esercita l'attività giornalistica, purché rispetti i predetti limiti, può effettuare un trattamento di dati personali anche senza il consenso dell'interessato e può riportare dati e informazioni relativi a circostanze o fatti resi noti direttamente dagli interessati o attraverso loro comportamenti in pubblico (art. 137 del Codice).

Il giornalista deve rispettare anche il codice di deontologia relativo al trattamento dei dati personali nell'esercizio dell'attività giornalistica, in base al quale la divulgazione di notizie è lecita *"quando l'informazione, anche dettagliata, sia indispensabile in ragione dell'originalità del fatto o della relativa descrizione dei modi particolari in cui è avvenuto, nonché della qualificazione dei protagonisti"* (art. 6, comma 1, codice deontologico). Inoltre, *"la sfera privata delle persone note o che esercitano funzioni pubbliche deve essere rispettata se le notizie o i dati non hanno alcun rilievo sul loro ruolo o sulla loro vita pubblica"* (art. 6, comma 2, codice deontologico).

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

Nel quadro dell'attività consultiva relativa 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 2008 diversi pareri i quali hanno riguardato, in particolare:

- uno schema di decreto predisposto dal Ministero dell'interno recante l'individuazione dei trattamenti effettuati da forze di polizia e altri soggetti pubblici per finalità di prevenzione e repressione di reati o di tutela dell'ordine e della pubblica sicurezza e dei rispettivi titolari, ai sensi dell'art. 53 del Codice (*Parere* 19 dicembre 2008 [doc. *web* n. 1584251]);
- uno schema di *provvedimento* dell'Agenzia delle entrate concernente la segnalazione di omessa comunicazione sull'imposta patrimoniale (*Parere* 19 dicembre 2008 [doc. *web* n. 1584260]);
- lo schema di *"Linee-guida"* sul censimento dei campi nomadi adottate dal Ministero dell'interno (*Parere* 17 luglio 2008 [doc. *web* n. 1537659]);
- uno schema di decreto predisposto dal Ministero dell'economia e delle finanze per la gestione e il rilascio della *cd. "carta acquisti"* a persone in condizioni di particolare disagio economico e sociale (*Parere* 18 settembre 2008 [doc. *web* n. 1553367]);
- uno schema di decreto predisposto dal Dipartimento per l'innovazione e le tecnologie della Presidenza del Consiglio dei ministri in materia di certificatori di autenticazione della Carta nazionale dei servizi (*Parere* 24 luglio 2008 [doc. *web* n. 1545983]);
- uno schema di decreto redatto dal Ministero della giustizia sul processo civile telematico (*Parere* 19 maggio 2008 [doc. *web* n. 1521729]);
- uno schema di decreto del Ministero della giustizia sui registri informatizzati delle cancellerie e di altri uffici giudiziari (*Parere* 19 maggio 2008 [doc. *web* n. 1521788]);
- uno schema di decreto predisposto dal Ministero dello sviluppo economico concernente la disciplina del diritto di accesso dei contraenti e dei danneggiati agli atti delle imprese di assicurazione di veicoli a motore e natanti, ai sensi dell'art. 146 del codice delle assicurazioni (*Parere* 30 aprile 2008 [doc. *web* n. 1514729]);
- uno schema di regolamento predisposto dal Ministero della difesa recante modifi-

che al d.m. 28 dicembre 1991 n. 96, in materia di iscrizione al registro nazionale delle imprese operanti su materiali d'armamento (*Parere* 24 aprile 2008 [doc. *web* n. 1514260]);

- uno schema di d.P.C.M. in materia di firme digitali (*Parere* 15 aprile 2008 [doc. *web* n. 1519647]);
- uno schema di decreto predisposto dal Ministero dell'università e della ricerca riguardante le modalità delle prove di ammissione a corsi di laurea per l'anno accademico 2008/2009 (*Parere* 10 aprile 2008 [doc. *web* n. 1519655]);
- uno schema di d.P.R. predisposto dal Ministero della difesa in materia di documenti caratteristici di alcune categorie di personale militare (*Parere* 2 aprile 2008 [doc. *web* n. 1519667]);
- uno schema di regolamento predisposto dal Ministero dell'economia e delle finanze in materia di bilancio delle fondazioni bancarie (*Parere* 20 marzo 2008 [doc. *web* n. 1502866]);
- uno schema di decreto predisposto dalla Presidenza del Consiglio dei ministri recante regole tecniche per il formato elettronico degli atti da presentare al registro delle imprese (*Parere* 20 marzo 2008 [doc. *web* n. 1519563]);
- uno schema di d.P.C.M. predisposto dal Ministero della solidarietà sociale sulla determinazione delle modalità di inserimento negli elenchi dei beneficiari del 5 per mille per il 2008 (*Parere* 13 marzo 2008 [doc. *web* n. 1500816]);
- uno schema di d.P.C.M. sull'accesso degli Organismi di informazione per la sicurezza agli archivi informatici della pubbliche amministrazioni, ai sensi dell'art. 13 della legge di riforma del sistema di informazione per la sicurezza della Repubblica 3 agosto 2007 n. 124 (*Parere* 13 marzo 2008);
- uno schema di decreto predisposto dalla Presidenza del Consiglio dei ministri attuativo dell'articolo 9 del decreto-legge 21 gennaio 2007 n. 7, convertito in legge n. 40/2007, sull'individuazione delle regole tecniche per le modalità di presentazione della comunicazione unica per la nascita dell'impresa (*Parere* 13 marzo 2008 [doc. *web* n. 1500799]);

- uno schema di d.P.C.M. riguardante lo sportello unico doganale (*Parere* 28 febbraio 2008 [doc. *web* n. 1523079]);
- uno schema di d.P.C.M. predisposto dal Ministero della solidarietà sociale sulla determinazione delle modalità di inserimento negli elenchi dei beneficiari del 5 per mille delle associazioni sportive dilettantistiche in possesso del riconoscimento ai fini sportivi rilasciato dal Coni (*Parere* 21 febbraio 2008 [doc. *web* n. 1497596]);
- uno schema di decreto predisposto dal Ministero dell'Università e della ricerca riguardante le pre-iscrizioni universitarie per l'anno accademico 2008/2009 (*Parere* 31 gennaio 2008 [doc. *web* n. 1489926]);
- uno schema di decreto di modifica del d.P.R. 13 febbraio 1967, n. 429 recante il regolamento in materia di documenti caratteristici degli ufficiali, dei sottufficiali e dei militari di truppa della Guardia di finanza (*Parere* 10 gennaio 2008 [doc. *web* n. 1484662]).

A fronte dei diversi pareri sopra menzionati, continuano tuttavia a registrarsi casi di mancata consultazione dell'Autorità, fra i quali in particolare:

- il decreto del Ministero dell'economia e delle finanze 22 settembre 2008 (*G.U.* 3 novembre 2008, n. 257), recante l'abrogazione della deliberazione 3 maggio 1999, concernente l'istituzione di un separato archivio accentrato per la rilevazione dei rischi di importo contenuto ed il suo affidamento in gestione alla società interbancaria per l'automazione;
- il provvedimento della Conferenza permanente per i rapporti fra lo Stato, le Regioni e le Province autonome di Trento e Bolzano 18 settembre 2008 (*G.U.* 8 ottobre 2008, n. 236), contenente Accordo fra Stato, Regioni e Province autonome sul documento recante procedure per gli accertamenti sanitari di assenza di tossicodipendenza o di assunzione di sostanze stupefacenti o psicotrope in lavoratori addetti a mansioni che comportano particolari rischi per la sicurezza, l'incolumità e la salute di terzi;
- il decreto del Ministero del lavoro, della salute e delle politiche sociali 9 luglio 2008 (*G.U.* 18 agosto 2008, n. 192), recante le modalità di tenuta e conservazione del libro unico del lavoro e disciplina del relativo regime transitorio;

- il provvedimento dell'Agenzia del territorio 16 aprile 2008 (*G.U.* 23 aprile 2008, n. 96), recante determinazione delle modalità dirette a garantire ai comuni, anche in forma associata o attraverso la comunità montane e le unioni di comuni, l'accessibilità e l'interoperabilità applicativa per la gestione della banca dati catastale;
- il decreto del Ministero dell'economia e delle finanze 4 aprile 2008 (*G.U.* 22 aprile 2008, n. 101), recante modifica del decreto ministeriale 24 giugno 2004, attuativo del comma 4 dell'art. 50 della legge n. 326 del 2003 (progetto tessera sanitaria), concernente i parametri tecnici per la trasmissione telematica dell'associazione medico-ricettario da parte delle ASL/AO;
- il d.P.C.M. 1° aprile 2008 (*G.U.* 21 giugno 2008, n. 144), recante regole tecniche e di sicurezza per il funzionamento del sistema pubblico di connettività previste dall'art. 71, comma 1-*bis*, del codice dell'amministrazione digitale (d.lg. 7 marzo 2005, n. 82);
- il decreto del Ministro della salute 31 marzo 2008 (*G.U.* 28 luglio 2008, n. 175) recante istituzione del sistema di sorveglianza delle nuove diagnosi di infezioni da Hiv;
- il d.P.C.M. 26 marzo 2008 (*G.U.* 28 maggio 2008, n. 124), in materia di regole tecniche e trasmissione dati di natura sanitaria, nell'ambito del sistema pubblico di connettività (art. 1, comma 810, lett. *c*), l. 27 dicembre 2006, n. 296);
- il decreto del Ministero dell'economia e delle finanze 18 marzo 2008 (*G.U.* 11 aprile 2008, n. 86 S.O. n. 89), recante revisione del decreto ministeriale 27 luglio 2005, attuativo del comma 5 dell'art. 50 della legge n. 326 del 2003 (progetto tessera sanitaria), concernente i parametri tecnici per la trasmissione telematica delle ricette;
- il decreto del Ministro dell'economia e delle finanze 17 marzo 2008 (*G.U.* 11 aprile 2008, n. 86 S.O. n. 89), recante revisione del decreto ministeriale 18 maggio 2004, attuativo del comma 2 dell'art. 50 della legge n. 326 del 2003 (progetto tessera sanitaria), concernente il modello di ricettario medico a carico del Servizio sanitario nazionale;
- il decreto del Ministro della salute 11 marzo 2008 (*G.U.* 4 aprile 2008, n. 80),

recante integrazione del decreto 8 aprile 2000 sulla ricezione delle dichiarazioni di volontà dei cittadini circa la donazione di organi a scopo di trapianto;

- il provvedimento dell'Agenzia delle Entrate n. 2008/31934 del 29 febbraio 2008 (pubblicato sul sito Internet dell'Agenzia dell'Entrate il 5 marzo 2008), recante disposizioni integrative del provvedimento del 19 gennaio 2007 in materia di comunicazione dell'esistenza di operazioni di natura finanziaria al di fuori di un rapporto continuativo (art. 7, comma 6, del d.P.R. 29 settembre 1973, n. 605, come modificato dall'art. 63, comma 1, del d. lg. 21 novembre 2007, n. 231);
- il decreto del Ministro delle comunicazioni 22 gennaio 2008 (*G.U.* 10 marzo 2008, n. 59 S.O. n. 55), concernente il numero unico di emergenza europeo 112;
- il decreto del Ministro dell'economia e delle finanze 7 gennaio 2008 (*G.U.* 31 gennaio 2008, n. 26), recante autorizzazione alla Banca d'Italia a chiedere ad operatori residenti, ad amministrazioni, enti e organismi pubblici l'invio anche periodico di informazioni e dati concernenti la bilancia dei pagamenti.

1.2.4. Altri pareri

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

- uno schema di decreto legislativo in materia di ricongiungimenti familiari e prelievo del Dna (*Parere* 5 giugno 2008 [doc. *web* n. 1526943]);
- 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 [doc. *web* n. 1504941]);
- 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 [doc. *web* n. 1523089]);
- 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]).

2. Quadro normativo in materia di protezione dei dati personali

2.1. Le garanzie previste nel Codice e alcuni recenti interventi modificativi

Le Relazioni del Garante degli scorsi anni hanno ampiamente evidenziato come il Codice abbia consolidato il quadro delle garanzie per i diritti fondamentali della persona rispetto al trattamento dei dati personali.

Mentre nel 2006 e nel 2007 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 e in questo primo scorcio della XVI si sono registrati ulteriori interventi modificativi del Codice in alcuni settori, dei quali si fornisce di seguito una sintesi.

Gli interventi hanno riguardato nuovamente la materia del trattamento dei dati di traffico al fine di dare piena attuazione alla normativa comunitaria, misure di semplificazione di taluni adempimenti previsti dalla legge e una razionalizzazione dell'apparato sanzionatorio; da ultimo, un'ulteriore modifica del Codice ha trovato spazio in un più generale intervento del Governo in materia di trasparenza dell'attività della pubblica amministrazione.

2.1.1. Le modifiche in materia di trattamento di dati di traffico

Le modifiche in materia di trattamento di dati di traffico (*v.* al riguardo anche *par.* 14.1) sono state apportate all'articolo 132 del Codice dal decreto legislativo 30 maggio 2008, n. 109, nonché, prima ancora, dalla legge 18 marzo 2008, n. 48, con la quale è stata data esecuzione alla Convenzione del Consiglio d'Europa sulla criminalità informatica, stipulata a Budapest il 23 novembre 2001.

I nuovi termini di conservazione dei dati di traffico e gli adempimenti a carico dei fornitori di servizi di comunicazione

Con il citato decreto legislativo n. 109/2008 il Governo ha dato piena attuazione alla direttiva 2006/24/Ce (*cd. "Frattini"*) riguardante la conservazione dei dati di traffico telefonico e telematico, la quale contiene specifiche indicazioni sia sui tempi di conservazione dei dati di traffico (da un minimo di sei mesi a un massimo di due anni), sia sulla uni-

forme individuazione delle categorie di dati da conservare, in relazione ad alcuni specifici servizi offerti dai fornitori (telefonia di rete fissa e telefonia mobile, accesso a Internet, posta elettronica in Internet e telefonia via Internet).

L'articolo 132 del Codice, già più volte modificato, aveva individuato differenti tempi di conservazione dei dati di traffico telefonico e telematico per finalità di accertamento e repressione dei reati, in base alla gravità del reato e alle specifiche finalità d'indagine, prevedendo per i fornitori di servizi di comunicazione elettronica l'obbligo di conservare i dati di traffico telefonico per due periodi di ventiquattro mesi ciascuno e quelli di traffico telematico, esclusi i contenuti, per due periodi di sei mesi ciascuno.

Il decreto legislativo – sul cui schema l'Autorità ha reso un parere (*v. supra*) – ha individuato termini di conservazione di tali dati più proporzionati e rispondenti alla normativa comunitaria, individuando un periodo unico di conservazione per ciascuna categoria di dati, senza ulteriori distinzioni in base al tipo di reato, pari a ventiquattro mesi per i dati di traffico telefonico e a dodici mesi per i dati di traffico telematico (art. 132, comma 1, del Codice). Lo stesso decreto ha, inoltre, stabilito in trenta giorni il periodo di conservazione dei dati relativi alle *"chiamate senza risposta"* (art. 132, comma 1-*bis*, del Codice).

Tale assetto normativo, previsto *"a regime"*, non ha trovato ancora piena esplicazione, anche perché ha continuato ad avere efficacia la generale previsione di conservazione dei dati di traffico contenuta nell'articolo 6 del d.l. n. 144/2005, convertito in l. n. 155/2005, in materia di lotta al terrorismo internazionale, *cd. "Pisanu"*. Tale disposizione, a seguito di una recente, ulteriore proroga (d.l. 2 ottobre 2008, n. 151, convertito in l. n. 186/2008), ha previsto per i fornitori l'obbligo di conservare indistintamente i dati di traffico telefonico e telematico fino al 31 marzo 2009.

Il d.lg. n. 109/2008, con autonome disposizioni, ha inoltre individuato le categorie di dati di traffico telefonico e telematico oggetto di specifica conservazione e disciplinato, anche con norme transitorie, l'obbligo per i fornitori di servizi di comunicazione elettronica di conservare i dati relativi alle chiamate senza risposta e al *cd. "indirizzo Ip"* univocamente assegnato, indispensabile per individuare i soggetti che accedono a Internet.

Il già citato decreto-legge n. 151/2008 ha prorogato, sempre al 31 marzo 2009, anche il termine previsto a carico dei fornitori per portare ad esecuzione tali adempimenti. Per quanto concerne i dati di traffico telefonici relativi alle chiamate senza risposta il termine è stato ulteriormente prorogato al 31 dicembre 2009 nel caso di chiamate originate da rete mobile e al 31 dicembre 2010 nel caso di chiamate originate da rete fissa (art. 12-*ter* d.l. 23 febbraio 2009, n. 11, convertito, con modificazioni, in l. 23 aprile 2009, n. 38).

Al riguardo, è importante ricordare che, nel corso dei lavori di conversione del d.l. n. 151/2008, il Governo ha accettato un ordine del giorno della Camera con il quale si è impegnato a favorire ogni iniziativa diretta ad assicurare l'univocità degli indirizzi IP, sollecitando i fornitori di servizi di comunicazione elettronica che offrono servizi di accesso ad Internet (*Internet access provider*) ad adoperarsi al più presto per garantire detta prestazione nell'interesse della giustizia (o.d.g. 9/1857/7). Tale ordine del giorno è il frutto anche della collaborazione prestata dall'Autorità ad un apposito tavolo di lavoro organizzato presso il Ministero dell'interno.

Infine, il d.lg. n. 109/2008, in attuazione di specifiche previsioni della direttiva, ha:

- completato il quadro delle garanzie per il trattamento dei dati di traffico in relazione al previsto *provvedimento* del Garante in materia di conservazione di tali dati, in particolare per quanto riguarda *"la qualità, sicurezza e protezione dei dati in rete"* (art. 132, comma 5, del Codice);
- precisato che il Garante esercita il controllo sul rispetto della disciplina in materia di protezione dei dati personali anche *"con riferimento alla conservazione dei dati di traffico"* (art. 154, comma 1, lett. *a*), del Codice);
- introdotto specifiche fattispecie sanzionatorie in materia di conservazione di dati di traffico (art. 162-*bis* del Codice; art. 5, comma 2, d.lg. n. 109/2008).

Il *cd.* "congelamento" dei dati di traffico telematico

Nella *Relazione* 2007 (*p.* 21 e ss.), si è riferito dell'attuazione nel nostro ordinamento (legge 18 marzo 2008, n. 48) della Convenzione del Consiglio d'Europa in materia di criminalità informatica. Si sono evidenziati, al riguardo, i profili problematici riguardanti le disposizioni che consentono in determinate circostanze la conservazione temporanea, ma prorogabile, di specifici dati informatici, già in possesso dei fornitori di servizi di comu-

nicazione elettronica o comunque sotto il loro controllo (*cd. "congelamento"*) (artt. 16 e 17 Conv.). In particolare, la legge attribuisce a specifici organi di polizia il potere di 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.

Si conferma in proposito che tali disposizioni – considerando anche che la libertà di ogni forma di comunicazione può essere limitata solo per atto motivato dell'autorità giudiziaria (art. 15 Cost.) – dovranno essere 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.

2.1.2. La semplificazione di taluni adempimenti per alcune realtà professionali e produttive e il trasferimento di dati all'estero

Il secondo *"blocco"* di modifiche normative concerne significative semplificazioni a taluni adempimenti in materia di protezione dei dati personali, compatibili con le direttive comunitarie, volti a ridurre l'onere che grava su talune attività professionali e produttive, specie se riferite a realtà di piccole dimensioni (liberi professionisti, artigiani, piccole e medie imprese).

Le modifiche al Codice sono state apportate dall'articolo 29 (Trattamento dei dati personali) del d.l. 25 giugno 2008, n. 112, convertito, con modificazioni, in l. 6 agosto 2008, n. 133, recante misure urgenti per lo sviluppo economico, la semplificazione e la competitività, nell'ambito di una più generale iniziativa di semplificazione adottata dal Governo e, in particolare, dal Ministro per la semplificazione normativa.

In tale quadro, il Garante – al termine di un'approfondita riflessione svolta a margine degli interventi di semplificazione deliberati rispetto ai trattamenti di dati svolti per finalità amministrative e contabili (*Provv.* 19 giugno 2008 [doc. *web* n. 1526724]) – ha rap-

presentato al Ministro l'opportunità di adeguare la disciplina delle misure minime di sicurezza e del documento programmatico alle caratteristiche che le attività di corrente gestione amministrativa e contabile presentano, specie presso piccole realtà professionali e produttive (*Nota* 19 giugno 2008).

L'iniziale proposta e quelle successive del Garante (*Nota* 3 luglio 2008), frutto di collaborazione fra i rispettivi uffici, sono state, poi, tenute nella dovuta considerazione dal Governo nella definitiva stesura dell'articolo 29 i cui contenuti si possono così sintetizzare:

- è stato semplificato l'onere della redazione del documento programmatico sulla sicurezza e di altri adempimenti concernenti le misure minime di sicurezza. In particolare, è stato soppresso l'obbligo di tenere un documento programmatico sulla sicurezza in tutti i casi in cui siano trattati solo dati personali non sensibili e i cui unici eventuali dati sensibili (al cui trattamento corrisponde l'obbligo di redigere il documento programmatico sulla sicurezza) siano costituiti dallo stato di salute o dalla malattia dei dipendenti senza indicazione della diagnosi, nonché dall'adesione a organizzazioni a carattere sindacale. In queste ipotesi, i soggetti interessati sono ora tenuti a rendere un'autocertificazione dalla quale emerga che sono trattati solo tali dati sensibili e che il relativo trattamento è eseguito nel rispetto delle altre misure di sicurezza prescritte (artt. 31-35 e disciplinare tecnico di cui all'Allegato B. del Codice). È previsto, infine, che in relazione a tali trattamenti, nonché a trattamenti effettuati per correnti finalità amministrative e contabili il Garante, sentito il Ministro per la semplificazione normativa, individui modalità semplificate di applicazione del predetto disciplinare in relazione a tutte le misure minime previste (art. 34, comma 1-*bis,* del Codice). Tali modalità sono state individuate dal Garante con *provvedimento* del 27 novembre 2008 [doc. *web* n. 1571218] (sul quale si veda *amplius* al *par.* 10);
- si è ulteriormente semplificata la notifica al Garante dei trattamenti di dati personali (nei casi in cui tale adempimento è già previsto dalla legge, come, ad esempio, per i trattamenti concernenti dati genetici o idonei a rivelare lo stato di salute), individuando le sole informazioni che, conformemente alla direttiva comunitaria,

devono essere contenute nella notifica e prevedendo che il Garante, entro due mesi dall'entrata in vigore della legge di conversione del decreto-legge, adegui il modello che i soggetti interessati sono tenuti ad utilizzare per tale adempimento (art. 38 del Codice). Il Garante ha provveduto ad individuare tali ulteriori semplificazioni con il *provvedimento* del 22 ottobre 2008 [doc. *web* n. 1571196] (sul quale si veda *amplius* al *par.* 10);

- è stato ampliato l'ambito del trasferimento lecito di dati verso Paesi non appartenenti all'Unione europea (art. 44 del Codice), con riferimento a ulteriori garanzie per i diritti dell'interessato individuate dal Garante (*cd. "regole vincolanti di gruppo"* nell'ambito di società appartenenti ad un medesimo gruppo).

2.1.3. Le modifiche in materia di sanzioni

Il decreto-legge 30 dicembre 2008, n. 207, (*cd. "milleproroghe"*), convertito in legge 27 febbraio 2009, n. 41, ha apportato significative modifiche all'apparato sanzionatorio del Codice. Le modifiche si sono concentrate, in massima parte, sulle sanzioni amministrative, mentre è rimasto sostanzialmente inalterato l'impianto sanzionatorio penale.

L'intervento normativo è il frutto di un'iniziativa dell'Autorità che ha segnalato informalmente al Governo la necessità di tali modifiche, in particolare per fronteggiare in maniera efficace i gravi fatti criminosi di acquisizione e diffusione illecite di dati personali provenienti, per lo più, da banche dati di grandi dimensioni e di particolare rilevanza.

In linea generale, le modifiche hanno comportato: un aumento delle pene pecuniarie previste per ciascuna violazione; la previsione di nuove ipotesi sanzionatorie; la creazione di meccanismi per consentire una maggiore modulabilità della sanzione in rapporto al caso concreto in ragione della minore o maggiore gravità, della circostanza che le violazioni siano state commesse in relazione a banche di dati di particolare rilevanza o dimensioni, del coinvolgimento di un maggior numero di interessati e delle condizioni economiche del contravventore.

Fra le nuove fattispecie sanzionatorie amministrative sono state previste, all'art. 162, comma 2-*bis*, le ipotesi di trattamento illecito e di omissioni nell'adozione delle misure

minime di sicurezza (già sanzionate penalmente dagli articoli 167 e 169 del Codice, articoli tuttora vigenti).

La sanzione amministrativa (da ventimila euro a centoventimila euro) potrà essere contestata in tutti i casi di violazione delle disposizioni richiamate dall'art. 167, nonché nei casi di violazione delle misure minime di sicurezza previste dal Codice e, per quanto riguarda queste ultime, senza la possibilità di avvalersi dell'estinzione del procedimento sanzionatorio con il pagamento in misura ridotta.

È stata inoltre introdotta all'art. 162, comma 2-*ter*, una specifica sanzione amministrativa (da trentamila euro a centottantamila euro) nei casi di inottemperanza ai provvedimenti del Garante che prescrivono, anche d'ufficio, ai titolari del trattamento le misure necessarie o opportune al fine di rendere il trattamento conforme alle disposizioni vigenti o che prevedono il blocco o il divieto del trattamento.

La norma rafforza la cogenza delle determinazioni dell'Autorità, fino ad oggi garantita, limitatamente alla violazione dei provvedimenti di blocco e di divieto del trattamento nonché di quelli relativi alla decisione dei ricorsi, dalla sanzione penale prevista dall'art. 170 del Codice.

Per quanto riguarda i meccanismi introdotti al fine di modulare le sanzioni amministrative, va evidenziato, in primo luogo, che l'art. 164-*bis*, comma 1, prevede la possibilità di contestare le sanzioni accertate applicando una riduzione a due quinti dei limiti minimo e massimo previsto per ciascuna violazione, nei casi di minore gravità della violazione stessa o in relazione alla natura economica e sociale dell'attività svolta dal contravventore.

Di contro, i commi 2 e 3 del medesimo articolo prevedono delle particolari *"aggravanti"* che determinano un sensibile aumento delle sanzioni:

- in caso di più violazioni di un'unica o di più disposizioni commesse, anche in tempi diversi, in relazione a banche di dati di particolare rilevanza o dimensioni (sanzione da cinquantamila euro a trecentomila euro senza la possibilità di avvalersi dell'estinzione del procedimento sanzionatorio con il pagamento in misura ridotta);
- in altri casi di maggiore gravità e, in particolare, di maggiore rilevanza del pregiudizio per uno o più interessati, ovvero quando la violazione coinvolge numerosi

interessati, con aumento dei limiti minimo e massimo delle sanzioni previste per ciascuna violazione in misura pari al doppio.

Tutte le sanzioni possono essere, inoltre, ai sensi dell'art. 164-*bis*, comma 4, aumentate fino al quadruplo quando possono risultare inefficaci in ragione delle condizioni economiche del contravventore.

2.1.4. La trasparenza nella pubblica amministrazione

La legge 4 marzo 2009, n. 15 recante delega al Governo per l'ottimizzazione della produttività del lavoro pubblico, nel quadro di un più ampio intervento in materia di trasparenza dell'attività delle pubbliche amministrazioni e in virtù dell'approvazione di un emendamento d'iniziativa parlamentare, ha introdotto una modifica all'art. 1, comma 1, del Codice, tesa a sancire la conoscibilità delle notizie inerenti lo svolgimento delle prestazioni lavorative in ambito pubblico e la relativa valutazione. La norma prevede, infatti, che *"le notizie concernenti lo svolgimento delle prestazioni di chiunque sia addetto ad una funzione pubblica e la relativa valutazione non sono oggetto di protezione della riservatezza personale"*.

Al riguardo, si sottolinea come il Garante abbia informalmente segnalato al Governo l'opportunità di assicurare la corretta collocazione sistematica della norma – di cui si è rilevata la dubbia legittimità costituzionale e comunitaria, in quanto sottrae talune categorie di informazioni e i relativi soggetti interessati alle garanzie in materia di protezione dei dati personali – nel capo del Codice riguardante i trattamenti effettuati dai soggetti pubblici e di apportarvi alcuni correttivi, demandando, tra l'altro, a un successivo decreto l'individuazione delle notizie relative alle prestazioni lavorative oggetto della disposizione.

Tale richiesta è stata recepita dal Governo e trasfusa in un emendamento, presentato dal Relatore, al disegno di legge collegato alla manovra finanziaria sulla disciplina del rapporto di lavoro (AS 1167), teso a sopprimere la modifica apportata all'articolo 1, comma 1, del Codice, e a demandare a un regolamento, emanato previa acquisizione del parere del Garante, l'individuazione delle notizie concernenti lo svolgimento delle prestazioni di chiunque sia addetto ad una funzione pubblica di cui è ammessa la comunicazione.

Sul punto va peraltro rilevato come, in sede di votazione del disegno di legge-delega in terza lettura al Senato, è stato approvato un ordine del giorno con cui si è impegnato il Governo ad applicare, in sede di esercizio della delega legislativa, il principio della trasparenza totale "*in modo tale che sia consentita e resa effettiva l'accessibilità diretta, anche mediante i siti Internet delle pubbliche amministrazioni, secondo i criteri e le modalità individuate dal Garante per la protezione dei dati personali, a norma dell'articolo 20, comma 3, del decreto legislativo 30 giugno 2003 n. 196, delle informazioni relative a retribuzioni individuali, provvedimenti disciplinari, dati aggregati per ufficio relativi ai tassi di assenze dal lavoro per qualsiasi motivo, dati e parametri posti alla base delle valutazioni, contenuto delle valutazioni stesse, formulato in modo tale da garantire la confrontabilità tra strutture omologhe*".

2.2. NOVITÀ NORMATIVE CON RIFLESSI IN MATERIA DI PROTEZIONE DEI DATI PERSONALI

Nei primi mesi della XVI legislatura sono stati approvati alcuni provvedimenti normativi che hanno riguardato il trattamento dei dati personali e l'attività del Garante.

Vanno ricordati, in particolare:

Videosorveglianza e chiamate senza risposta

- il decreto-legge 23 febbraio 2009, n. 11, convertito in legge n. 23 aprile 2009, n. 28, recante misure urgenti in materia di sicurezza pubblica e di contrasto alla violenza sessuale, in base al quale i comuni possono utilizzare sistemi di videosorveglianza in luoghi pubblici o aperti al pubblico *"per la tutela della sicurezza urbana"* e possono conservare i dati e le immagini raccolti al massimo per sette giorni, fatte salve speciali esigenze di conservazione (art. 6, commi 7 e 8). Inoltre, l'articolo 12-*ter* del decreto-legge, inserito dalla legge di conversione, ha ulteriormente differito (sino al 31 dicembre 2009 nel caso di chiamate originate da rete mobile e sino al 31 dicembre 2010 nel caso di chiamate originate da rete fissa) il termine a partire dal quale i gestori telefonici devono rendere disponibili, alla polizia e all'autorità giudiziaria, i dati di traffico telefonico relativi alle chiamate senza risposta. Tale disposizione deriva dall'approvazione, in prima lettura, alla Camera dei deputati, di un emendamento d'iniziativa parlamentare;

- il già citato decreto-legge 30 dicembre 2008, n. 207, convertito in legge 27 febbraio 2009, n. 14, che contiene un'importante disposizione in materia di attività promozionali effettuate mediante l'utilizzo di elenchi telefonici. Il comma 1-*bis* dell'articolo 44 del provvedimento d'urgenza, introdotto dalla legge di conversione, prevede che i dati personali presenti nelle banche dati costituite sulla base di elenchi telefonici pubblici formati prima del 1° agosto 2005 siano lecitamente utilizzabili per fini promozionali sino al 31 dicembre 2009, anche in deroga agli articoli 13 e 23 del Codice, dai soli titolari del trattamento che hanno provveduto a costituire dette banche dati prima del 1° agosto 2005.

Durante i lavori parlamentari di conversione del decreto-legge, il Garante ha manifestato la propria contrarietà a tale disposizione – frutto di un emendamento parlamentare – segnalando al Parlamento e al Governo la delicatezza della questione e l'impatto della proposta emendativa su una vasta platea di cittadini (Note del 2 febbraio 2009).

L'attuale disciplina in materia di elenchi telefonici (Direttiva 2002/58/Ce; art. 129 del Codice) stabilisce che i dati personali degli abbonati inseriti negli elenchi telefonici possono essere utilizzati per finalità di ricerca dell'abbonato per comunicazioni interpersonali.

Per contemperare le esigenze di riservatezza dei cittadini con la possibilità per gli operatori economici di svolgere attività di carattere promozionale, il Garante è intervenuto con diversi provvedimenti chiarendo, fra l'altro, che possono essere utilizzati per finalità di *marketing* anche i dati personali presenti in banche dati costituite utilizzando dati estratti da elenchi formati secondo la previgente disciplina, purché il titolare del trattamento dimostri di aver fornito, a suo tempo, l'informativa agli interessati (art. 13 del Codice).

La norma approvata opera, invece, in sostanza, una *"sanatoria"* per tutte le banche dati costituite illecitamente sulla base di *"vecchi"* elenchi telefonici, in violazione di norme che già dal 1997 prevedevano specifici obblighi per tutti i titolari in materia di informativa e consenso al trattamento dei dati (*cfr.* artt. 10 e 11 legge 31 dicembre 1996, n. 675, ed ora artt. 13 e 23 del Codice).

Nell'occasione l'Autorità ha richiamato l'attenzione del Parlamento e del Governo sul

fatto che la nuova disposizione normativa è destinata ad acuire il noto fenomeno delle chiamate indesiderate, continuamente al centro di numerose segnalazioni al Garante, rendendo vani i provvedimenti di carattere inibitorio e sanzionatorio adottati in materia dall'Autorità.

Indirizzi di posta elettronica

- il decreto-legge 29 novembre 2008, n 185, convertito in legge 28 gennaio 2009, n. 2 che contiene le seguenti disposizioni di interesse: 1) riduzione dei costi amministrativi a carico delle imprese: l'articolo 16, nella parte in cui prevede la pubblicazione in elenchi riservati, di dati identificativi ed indirizzi di posta elettronica certificata dei professionisti iscritti ad ordini o collegi professionali. Tali elenchi sono consultabili per via telematica esclusivamente dalla pubblica amministrazione. L'articolo prevede altresì che per i singoli indirizzi di posta elettronica la consultazione è ammessa liberamente e senza oneri, mentre l'estrazione di elenchi dei medesimi indirizzi è consentita esclusivamente alle pubbliche amministrazioni per le comunicazioni relative ad adempimenti amministrativi di loro competenza; 2) misure di semplificazione per le famiglie e per le imprese: l'articolo 16-*bis*, ai sensi del quale, per favorire la massima diffusione delle tecnologie telematiche, ai cittadini che ne fanno richiesta è attribuita una casella di posta elettronica certificata (pec). Per i medesimi fini, ogni pubblica amministrazione utilizza unicamente la posta elettronica certificata con effetto equivalente, ove necessario, alla notificazione per mezzo posta, per le comunicazioni e le notificazioni aventi come destinatari dipendenti della stessa o di altra pubblica amministrazione; 3) riscossione: l'articolo 32 prevede che, allo scadere dei 60 giorni dalla notifica della cartella esattoriale, gli agenti della riscossione possano accedere ai dati relativi ai rapporti finanziari del contribuente, compresi quelli che fanno riferimento a depositi bancari o postali (art. 35, comma 25, del d.l. 4 luglio 2006, n. 223; art. 7, comma 6, del d.P.R. 29 novembre 1973, n. 605).

Impronte digitali: dati dei contribuenti

- il già citato decreto-legge 25 giugno 2008, n. 112, che contiene anche le seguenti ulteriori disposizioni di interesse: 1) durata e rinnovo della carta d'identità: l'articolo 31 che prolunga da cinque a dieci anni il periodo di validità della carta d'identità – fis-

sato dall'articolo 3 del testo unico delle leggi di pubblica sicurezza, di cui al r.d. 18 giugno 1931, n. 773 – e prevede che a partire dal 1° gennaio 2010 essa dovrà essere munita anche delle impronte digitali dell'interessato; 2) accesso agli elenchi dei contribuenti: l'articolo 42 che al fine di attuare il principio di trasparenza nei rapporti fiscali modifica il d.P.R. n. 600 del 1973, prevedendo che gli elenchi dei contribuenti siano depositati per un anno sia presso l'ufficio delle imposte, sia presso i comuni interessati e che, in tale periodo, ne sia consentita l'estrazione di copia in conformità alla disciplina sul diritto di accesso. Viene previsto, inoltre, che fuori dei casi disciplinati la diffusione degli elenchi, al di là delle ipotesi in cui costituisca reato, è punita con una sanzione amministrativa; 3) carta acquisti: l'articolo 81, comma 32, che prevede il rilascio di una *"carta acquisti"* alle persone che versano in condizione di maggior disagio economico da disciplinare con apposito decreto (sul cui schema il Garante ha poi reso parere – *v. supra*); 4) efficienza dell'amministrazione finanziaria: l'articolo 83 in base al quale: a) per garantire maggiore efficacia ai controlli fiscali, l'Inps e l'Agenzia delle entrate predispongono piani di controllo anche sulla base dello scambio di dati e informazioni anche in via telematica (comma 1); b) si incrementa lo strumento di accertamento che si fonda sul *cd. "redditometro"* (comma 8); c) si prevede l'accesso dei comuni e delle società di riscossione ai dati disponibili presso il sistema informativo dell'Agenzia delle entrate, ivi compresi quelli di cui alla *cd. "anagrafe dei conti correnti"*, fino ad ora non attuata in assenza del decreto ministeriale previsto dall'art. 1, comma 225, della legge n. 244/2007 (comma 28-*sexies*);

- il decreto-legge 23 maggio 2008, n. 92, convertito in legge 24 luglio 2008, n. 125, recante misure urgenti in materia di sicurezza pubblica, con specifico riferimento ai seguenti articoli: 1) l'articolo 6 che ha apportato diverse modifiche sostanziali all'articolo 54 del testo unico degli enti locali – che disciplina le attribuzioni del sindaco nelle funzioni di competenza statale – al fine di potenziare il ruolo dell'amministrazione locale. In particolare, il novellato comma 4 dell'art. 54 amplia il potere del sindaco di emanare ordinanze contingibili e urgenti, prevedendo, quale situazione legittimante il provvedimento *extra ordinem*, anche il grave pericolo per la *"sicurezza urbana"* (che si

Attribuzioni del sindaco e della polizia municipale

affianca così al grave pericolo per l'incolumità dei cittadini, già previsto). Tali provvedimenti d'urgenza vanno comunicati al prefetto in quanto la situazione che li legittima attiene alla sicurezza, tematica che vede comunque un ruolo centrale e "strategico" dell'autorità locale di Governo, cui competono in via generale gli interventi attuativi dell'ordinanza sindacale; 2) l'articolo 8 che amplia le possibilità di accesso della polizia municipale ai dati presenti nel Ced interforze del Ministero dell'interno-Dipartimento della pubblica sicurezza. Prima dell'entrata in vigore del provvedimento in esame, gli agenti di polizia municipale – se addetti ai servizi di polizia stradale e in possesso della qualifica di agente di pubblica sicurezza – potevano accedere, presso il Ced, allo schedario dei veicoli rubati. Ora, a seguito delle modifiche introdotte, essi possono accedere anche allo schedario dei documenti d'identità rubati o smarriti, nonché alle informazioni concernenti i permessi di soggiorno. Ciò, in relazione alle aggiornate competenze del sindaco in tale materia (*cfr.* art. 6 *cit.*). Inoltre, la norma in esame permette al personale della polizia municipale, previa apposita abilitazione, di inserire nella banca dati i predetti dati relativi ai veicoli e ai documenti autonomamente acquisiti; 3) attribuzioni del personale del Corpo delle capitanerie di porto: a seguito delle integrazioni apportate in sede di conversione, l'articolo 8-*bis* estende l'accesso al Ced e la relativa immissione di alcuni dati anche al personale del Corpo delle capitanerie di porto, nei limiti delle funzioni esercitate. Appositi decreti dovranno stabilire le modalità dei collegamenti fra le predette forze dell'ordine e il Ced ai fini dell'accesso ai dati e, per quanto riguarda il personale del Corpo delle capitanerie di porto, anche le tipologie di dati consultabili. In entrambi i casi il Garante dovrà esprimere il parere di competenza sugli schemi di decreto;

Criminalità informatica

- la già citata legge 18 marzo 2008, n. 48 (*v. supra*) recante ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica, della quale si è riferito nella *Relazione* 2007 (*p.* 21 e *ss.*);

Durata in carica dei membri delle autorità indipendenti

- il decreto-legge 31 dicembre 2007, n. 248, convertito in legge 28 febbraio 2008, n. 31 (*cd. "decreto milleproroghe"* per il 2008), 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.

Infine, il Governo ha adottato alcuni decreti legislativi di interesse in materia di protezione dei dati personali, sui cui schemi l'Autorità ha, peraltro, reso parere (*v. supra*) fra i quali, in particolare: 1) (movimenti transfrontalieri di denaro) il decreto legislativo 19 novembre 2008, n. 195, recante modifiche alla normativa in materia valutaria in attuazione del regolamento (Ce) n. 1889/2005, volto a contrastare l'introduzione di proventi di attività illecite nel sistema economico e finanziario e ad istituire un adeguato sistema di sorveglianza sui movimenti transfrontalieri di denaro contante; 2) ricongiungimenti familiari e prelievo del Dna: il decreto legislativo 3 ottobre 2008, n. 160, recante attuazione della direttiva 2003/86/Ce, in materia di ricongiungimenti familiari, di particolare delicatezza in quanto prevede il trattamento di dati genetici. In base al decreto, infatti, le rappresentanze diplomatiche o i consolati possono rilasciare certificazioni *"sulla base del Dna"* quando lo *status* di figlio o di coniuge, ai fini del ricongiungimento, non possa essere documentato in modo certo mediante certificati o attestazioni rilasciati da competenti autorità straniere, a causa della mancanza di un'autorità riconosciuta o quando sussistano fondati dubbi sull'autenticità della documentazione prodotta; 3) sicurezza nei luoghi di lavoro: il decreto legislativo 9 aprile 2008, n. 81, volto a dare attuazione alla legge 3 agosto 2007, n. 123, in materia di salute e sicurezza nei luoghi di lavoro, che riguarda trattamenti di dati personali concernenti informazioni idonee a rivelare lo stato di salute del lavoratori, in particolare dipendenti da infortuni sul lavoro o da malattie professionali, effettuati anche nell'ambito del Sistema informativo nazionale per la prevenzione nei luoghi di lavoro; 4) il decreto legislativo 30 maggio 2008, n. 109, di attuazione della direttiva 2006/24/Ce riguardante la conservazione di dati di traffico trattati nell'ambito della fornitura di servizi di comunicazione elettronica, ampiamente illustrato in altra parte della *Relazione* (*v. par.* 14).

L’attività svolta dal Garante

II. L'attività svolta dal Garante

3. Il Garante e le pubbliche amministrazioni

3.1. I regolamenti sui trattamenti di dati sensibili e giudiziari

3.1.1. I regolamenti delle amministrazioni centrali e regionali

La Scuola superiore della pubblica amministrazione locale ha presentato nel 2009 un nuovo schema di regolamento recependo le condizioni alle quali l'Autorità aveva subordinato il proprio parere favorevole sul precedente schema (*Provv.* 7 febbraio 2008 [doc. *web* n. 1491594]).

In particolare, il nuovo testo documenta adeguatamente l'indispensabilità dei dati sullo stato di salute delle persone coinvolte trattati per l'esclusiva finalità di *"elaborare studi e ricerche rilevanti in materia di servizi sociali d'interesse per gli enti locali"* (art. 1, comma 2, lett. *e*), del d.P.R. 28 gennaio 2008, n. 27) e delimita rigorosamente le operazioni di interconnessione e di raffronto eseguibili con altre banche dati (art. 22, commi 9 e 11, del Codice) (*Provv.* 12 febbraio 2009 [doc. *web* n. 1597595]).

Per quanto concerne gli enti regionali, va invece segnalata la richiesta della Conferenza dei presidenti delle assemblee legislative delle regioni e delle province autonome su alcune modifiche e integrazioni apportate allo schema tipo di regolamento, già sottoposto all'esame dell'Autorità, riguardante i trattamenti dei dati sensibili e giudiziari effettuati dalle assemblee legislative presso le regioni e le province autonome (*cfr. Provv.* 29 dicembre 2005 [doc. *web* n. 1210939]).

In linea generale, con riferimento alla possibilità di rilevare accidentalmente informazioni concernenti, in particolare, l'origine razziale o etnica degli interessati, menzionata in calce alle descrizioni di tutti i trattamenti presi in considerazione nelle schede, l'Autorità ha sottolineato l'inutilità del riferimento, atteso che la disciplina sulla protezione dei dati personali preclude l'utilizzo delle informazioni che risultano eccedenti, non pertinenti o non indispensabili, eventualmente acquisite in modo occasionale o fornite spontaneamente dall'interessato o desumibili indirettamente da altre informazioni trattate legitti-

mamente, salvo che per l'eventuale conservazione, a norma di legge, dell'atto o del documento che li contiene (art. 22, comma 5, del Codice).

Con riferimento, poi, ad alcuni organismi di garanzia, per quanto attiene al Garante del contribuente, previa verifica dell'effettiva riconducibilità dei trattamenti effettuati presso tale organismo agli enti regionali, piuttosto che all'amministrazione finanziaria (art. 13, legge 27 luglio 2000, n. 212), si è evidenziata la necessità di delimitare le operazioni di comunicazione alle sole pubbliche amministrazioni, gestori o concessionari di pubblico servizio *"coinvolti nell'attività istruttoria"*.

Riguardo ai trattamenti effettuati presso il Garante per l'infanzia e l'adolescenza, è stato, invece, suggerito di integrare le fonti normative con il riferimento alla legge nazionale di ratifica della Convenzione dell'Organizzazione delle Nazioni unite contro la tortura ed altre pene o trattamenti crudeli, disumani o degradanti firmata a New York il 10 dicembre 1984 (l. 3 novembre 1988, n. 498), con cui lo Stato italiano si è impegnato a configurare una serie di garanzie e di mezzi per assicurare alle persone in stato di privazione o di limitazione della libertà personale il rispetto dei propri diritti.

Il parere favorevole dell'Autorità sulle modifiche proposte è stato subordinato al rispetto delle indicazioni formulate (*Provv.* 12 giugno 2008 [doc. *web* n. 1537639]).

Il Garante ha, inoltre, espresso parere favorevole sullo schema di decreto volto a modificare il regolamento d.P.C.M. concernente i trattamenti dei dati sensibili e giudiziari effettuati dalla Presidenza del Consiglio dei Ministri (30 novembre 2006, n. 312, *cfr. Parere* del 18 maggio 2006 [doc. *web* n. 1298799) al fine di aggiungere un allegato relativo al trattamento di dati giudiziari per la gestione delle attività connesse al flusso delle comunicazioni delle irregolarità e delle frodi in materia di fondi strutturali (*Parere* del 19 dicembre 2008 [doc. *web* n. 1584241]).

3.1.2. I regolamenti degli enti locali

Nell'anno di riferimento sono notevolmente diminuiti i casi sottoposti dagli enti locali al Garante per la formulazione di un parere specifico relativamente a trattamenti di dati sensibili o 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'Upi-Unione delle province d'Italia [doc. *web* n. 1174562] e dall'Uncem-Unione nazionale comuni comunità enti montani [doc. *web* n. 1182195], *Relazione* 2006, *p.* 19), 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 (*v. Relazione* 2006, *pp.* 34 e 35 [doc. *web* nn. 1213424, 1298732, 1314392, 1370369, 1377640, 1434995]).

Con riferimento ad una richiesta di parere sull'utilizzo di determinati dati sensibili per attività ricreative o di promozione della cultura dello sport, ovvero per l'uso di beni immobili o per l'occupazione di suolo pubblico (art. 73, comma 2, lett. *c*), del Codice), è stato evidenziato che non risultava comprovata l'indispensabilità né del trattamento di dati idonei a rivelare lo stato di salute, né della loro diffusione. Al comune richiedente è stato, pertanto, fatto presente che, nell'ambito delle predette attività, si ritiene lecito unicamente l'utilizzo dei dati personali comuni, nonché l'espletamento delle operazioni individuate nel citato *Parere* del 29 dicembre 2005 [doc. *web* n. 1213424] (*Nota* 3 giugno 2008).

Ad un altro comune è stato evidenziato che non risultava comprovata l'indispensabilità della pubblicazione delle delibere ai sensi del d.P.R. 7 aprile 2000, n. 118 da esso individuata nelle schede riguardanti, rispettivamente, il trattamento di dati sensibili finalizzato all'iscrizione in albi comunali di associazioni ed organizzazioni di volontariato o per riconoscere titoli abilitativi previsti dalla legge (art. 68, comma 2, lett. *g*), del Codice), all'espletamento di attività ricreative o di promozione della cultura dello sport, ovvero per l'uso di beni immobili o per l'occupazione di suolo pubblico (art. 73, comma 2, lett. *c*), del Codice), nonché all'effettuazione della attività in materia di protezione civile (art. 73, comma 2, lett. *h*), del Codice). È stato quindi sottolineato che tale operazione, essendo comunque ricompresa nella scheda n. 20 dello schema tipo Anci [*cfr.* doc. *web* n. 1174532], riguardante il trattamento di dati sensibili effettuato per la concessione, liquidazione, modifica e revoca di benefici economici, agevolazioni, elargizioni, altri emolumenti ed abilitazioni (art. 68 del Codice), doveva essere espunta dalle schede in questione (*Nota* 30 maggio 2008).

Un comune ha chiesto un parere sull'introduzione di previsioni statutarie e/o regolamentari per rendere obbligatorio il conferimento, da parte dei consiglieri comunali, dei propri certificati del casellario giudiziale e dei carichi pendenti, nonché per diffondere i predetti dati. Al riguardo, è stato rappresentato che nel caso in cui il comune intenda trattare dati giudiziari, ovvero effettuare ulteriori operazioni, non ricomprese né nello schema tipo Anci (dove peraltro sono state previste specifiche limitazioni in ordine alla diffusione dei dati personali dei consiglieri comunali), né nei pareri positivi successivamente espressi dall'Autorità, deve adeguatamente documentarne la indispensabilità, individuando la specifica finalità perseguita, per sottoporre al Garante eventuali integrazioni allo schema tipo di regolamento, ai sensi dell'art. 20, comma 2, del Codice. Ciò, fermo restando che la diffusione di dati giudiziari è ammessa solo se prevista da espressa disposizione di legge, in quanto rientra tra le operazioni che possono spiegare effetti maggiormente significativi per gli interessati (*cfr.* art. 22, comma 11, del Codice) (*Nota* 30 maggio 2008).

L'Ufficio è stato chiamato a pronunciarsi in materia anche da parte di talune province.

Su una richiesta di trattare dati idonei a rivelare l'origine razziale od etnica; le convinzioni religiose, filosofiche, politiche, sindacali o di altro genere; le patologie pregresse, le terapie in corso e l'anamnesi familiare, al fine di garantire le pari opportunità da parte della consigliera o consigliere di parità (art. 112, comma 2, lett. *b*), del Codice), è stato osservato che dalla descrizione del trattamento non risultava comprovata l'indispensabilità del loro utilizzo. Nell'ambito di tale attività si è, quindi, continuato a ritenere lecito unicamente il trattamento dei dati personali, nonché l'espletamento delle operazioni individuate nello schema di regolamento per il trattamento dei dati sensibili e giudiziari predisposto dal Ministero del lavoro e della previdenza sociale in relazione alle attività della consigliera o consigliere di parità, sul quale il Garante ha espresso *Parere* favorevole il 28 febbraio 2007 ([doc. *web* n. 1409015] *v. Relazione* 2007, *p.* 38) (*Nota* 17 luglio 2008).

Il Garante, si è invece, espresso favorevolmente su una richiesta di parere della Provincia di Roma, concernente il trattamento di determinati dati sensibili, con specifico riferimento ad interventi di sostegno psico-sociale e di formazione in favore di giovani o di soggetti disagiati (art. 73, comma 1, lett. *a*), del Codice). Ciò, in attuazione sia del

sistema integrato di interventi e servizi sociali in favore di persone bisognose e in stato di disagio individuale e familiare, derivanti da inadeguatezza di reddito, difficoltà sociali e condizioni di non autonomia (l. 8 novembre 2000, n. 328), sia dei compiti attribuiti alla Provincia dalla Regione Lazio per l'istituzione di centri antiviolenza o case rifugio per donne maltrattate (*cfr.* l.r. 15 novembre 1993, n. 64) (*Parere* 10 aprile 2008 [doc. *web* n. 1507195]).

Sono stati inoltre resi chiarimenti al Dipartimento della protezione civile-Presidenza del Consiglio dei Ministri sulle modalità da osservare per permettere ai comuni di acquisire dalle aziende sanitarie i dati personali dei soggetti costretti all'immobilità, ai fini della predisposizione dei piani di emergenza in materia di protezione civile. In proposito è stato evidenziato che il predetto flusso di dati è stato espressamente individuato 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 e dalle province autonome (*cfr.* scheda n. 6 dell'allegato B), sul quale il Garante ha espresso *Parere* positivo il 13 aprile 2006 ([doc. *web* n. 1272225] *v. Relazione* 2005, *p.* 21). In tale quadro, le aziende sanitarie locali possono, altresì, comunicare ai comuni, oltre al nominativo e all'ubicazione delle persone costrette all'immobilità, informazioni attinenti alla patologia sofferta, indispensabili per approntare un idoneo piano di assistenza (*Nota* 31 ottobre 2008).

3.2. LA TRASPARENZA DELL'ATTIVITÀ AMMINISTRATIVA E L'ACCESSO AI DOCUMENTI AMMINISTRATIVI

Sul contemperamento tra trasparenza dell'attività amministrativa e protezione dei dati personali l'Ufficio si è espresso con notevole frequenza.

In un caso l'intervento del Garante è stato chiesto per inibire in via d'urgenza l'esercizio del diritto di accesso ad un parere formulato dall'Autorità per la vigilanza sui contratti pubblici di lavori, servizi e forniture (*Nota* 23 giugno 2008). In tale circostanza, come già in passato, si è evidenziata l'incompetenza del Garante in materia: le norme vigenti in materia di accesso ai documenti amministrativi non sono state abrogate (artt. 22 e *ss.* della l. 7

agosto 1990, n. 241, come modificata dalla l. 11 febbraio 2005, n. 15; art. 2 del d.P.R. 12 aprile 2006, n. 184) e spetta, pertanto, esclusivamente all'amministrazione destinataria della richiesta di accesso verificare, caso per caso, l'interesse e i motivi sottesi alla richiesta di accesso ai documenti amministrativi, nonché valutare la sussistenza di una delle ragioni per le quali il documento può essere sottratto alla conoscibilità del richiedente, essendo la stessa in possesso di tutti i necessari elementi di ponderazione della istanza in questione (art. 24, commi 6, lett. *d*), e 7 della l. n. 241/1990 *cit.*; art. 9 del d.P.R. n. 184/2006 *cit.*). Analoghe considerazioni sono state formulate ad un soggetto che lamentava un diniego, opposto dall'Istituto nazionale di previdenza per i dipendenti dell'amministrazione pubblica (Inpdap), di rendere ostensibili taluni documenti amministrativi richiesti ai sensi della l. n. 241/1990 (*Nota* 25 luglio 2008), nonché ad un altro soggetto che aveva chiesto l'intervento del Garante al fine di vedere soddisfatta una sua richiesta di accesso a taluni documenti detenuti da Sviluppo Italia S.p.A. (*Nota* 11 dicembre 2008).

In un altro caso è stata lamentata la comunicazione ai controinteresssati di una richiesta di accesso a documenti amministrativi, recante il nominativo e il recapito del richiedente medesimo. Considerato che la normativa di settore impone alle pubbliche amministrazioni, destinatarie di una richiesta di accesso di comunicare l'avvio del procedimento ai soggetti nei confronti dei quali il provvedimento finale è destinato a produrre effetti diretti ed a quelli che per legge debbono intervenirvi (art. 7 della l. n. 241/1990 *cit.*), è stato osservato che la conoscibilità delle predette informazioni in questione, resa possibile nei confronti del controinteressato, non configurava un illecito trattamento dei dati personali (*Nota* 12 novembre 2008).

Ad una società che lamentava, invece, di non essere stata interpellata in ordine all'avvenuta ostensione di taluni documenti amministrativi contenenti informazioni che la riguardavano da parte di una pubblica amministrazione ad un soggetto che ne aveva fatto richiesta ai sensi della l. n. 241/1990, è stato evidenziato che la valutazione sul rispetto, da parte dell'amministrazione interpellata, delle disposizioni di legge applicabili (art. 7 della l. n. 241/1990 *cit.*) non rientra nella competenza del Garante (art. 25 della l. n. 241/1990 *cit.*) (*Nota* 19 febbraio 2009).

Sotto un diverso profilo, le problematiche legate al difficile bilanciamento tra l'esigenza di pubblicità dell'attività amministrativa e il diritto degli interessati di non subire una divulgazione ingiustificata dei propri dati personali ha costituito oggetto di diversi interventi da parte dell'Ufficio.

Nel caso di un progetto, finalizzato alla catalogazione informatizzata di un archivio fotografico (contenente ventimila fotografie, risalenti prevalentemente agli anni settanta e ottanta, relative anche a persone portatrici di patologie psichiche, in cura presso presidi sanitari o in strutture per soggetti diversamente abili o socio assistenziali, nonché relative anche a minori in occasione di cerimonie religiose della fine dell'ottocento), l'Ufficio ha stato fatto presente che nel disciplinare per regolamento la conoscibilità delle informazioni in suo possesso (art. 10 d.lg. 18 agosto 2000, n. 267), l'ente locale può contemplarne la diretta divulgabilità tramite pubblicazioni anche telematiche, qualora lo ritenga opportuno per svolgere le proprie funzioni istituzionali, nel rispetto di quanto previsto dagli artt. 19, comma 3, 20 e 22 del Codice. È stato altresì sottolineato che in tali ipotesi la provincia si può avvalere legittimamente della disciplina del Codice riguardante le attività finalizzate alla pubblicazione o diffusione occasionale di articoli, saggi o altre manifestazioni del pensiero (art. 136, comma 1, lett. *c*)), potendo adempiere in modo semplificato agli obblighi di informativa di cui all'art. 13 del Codice (*v.* codice di deontologia per l'attività giornalistica, in *G.U.* del 3 agosto 1998, n. 179). Rimane fermo, in ogni caso, il divieto di pubblicare dati idonei a rivelare lo stato di salute delle persone (art. 22, comma 8, del Codice) (*Nota* 9 gennaio 2009).

Sono stati numerosi i casi esaminati anche alla luce delle *"Linee-guida in materia di trattamento di dati personali per finalità di pubblicazione e diffusione di atti e documenti di enti locali"* (*Provv.* 19 aprile 2007, in *G.U.* 25 maggio 2007, n. 120 [doc. *web* n. 1407101] *v. Relazione* 2007, *p.* 40), con specifico riferimento alla diffusione di dati personali effettuata da soggetti pubblici per dare pubblicità alla propria attività istituzionale, specie tramite l'impiego di tecniche informatiche e telematiche.

Una segnalazione ha riguardato una provincia che nel proprio sito *web* aveva reso consultabile l'elenco nominativo dei partecipanti, in qualità di portatori di *handicap*, ad un

bando per l'attribuzione di assegni di studio. In base ad un accertamento preliminare è stata verificata la visualizzabilità del suddetto elenco tramite l'inserimento del nominativo dei beneficiari o dei richiedenti anche nei più diffusi motori di ricerca esterni al sito *web* della provincia. Quest'ultima ha eliminato prontamente dal sito *web* la graduatoria dei soggetti disabili che avevano beneficiato degli assegni di studio, che permaneva, tuttavia, nella versione Html delle pagine *web* dei più noti motori di ricerca esterni; inoltre, l'abstract dell'esito della ricerca riportava le generalità dei beneficiari disabili, nonché dei richiedenti il beneficio ed il relativo punteggio. In seguito all'ulteriore intervento del Garante, l'amministrazione provinciale si è attivata per fare eliminare definitivamente i contenuti *web* dagli indici e dalle *cd. "cache"* dei motori di ricerca. Sulla base delle successive verifiche effettuate e delle idonee rassicurazioni da parte della provincia in ordine al rispetto, anche futuro, delle disposizioni del Codice, non sono state intraprese ulteriori iniziative in relazione a quanto segnalato (*v.* artt. 11, comma 1, punto 4, e 13, comma 4, del regolamento n. 1/2007) (*Nota* 2 settembre 2008).

In un'altra segnalazione, una cittadina aveva lamentato la consultabilità sul sito *web* comunale di una deliberazione di giunta riguardante un contenzioso in corso con la segnalante e contenente dati personali della medesima. Il Garante ha constatato che la predetta deliberazione era liberamente visualizzabile da chiunque, senza la previsione di forme di accesso in rete selezionato (*ad es.*, *username* e *password*; numero di protocollo o altri estremi identificativi di una pratica forniti dall'ente all'avente diritto): al comune è stato pertanto rappresentato che i dati delle pubbliche amministrazioni vanno resi accessibili con l'uso delle tecnologie dell'informazione alle condizioni fissate dall'ordinamento. In assenza di norme che impongano specificamente la messa a disposizione su Internet di dati personali per puntuali periodi, l'ente è tenuto – 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 – ad 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 (*v. par.* 5, 6 e 9 delle linee-guida *cit.*).

Avendo ricevuto idonee rassicurazioni da parte del comune in ordine al rispetto dei predetti princìpi, non sono state intraprese iniziative per l'adozione di specifici provvedimenti da parte del Garante (*v.* artt. 11, comma 1, punto 4, e 13, comma 4, del regolamento n. 1/2007) (*Nota* 15 luglio 2008).

Considerazioni di analogo tenore sono state comunicate, a seguito di una segnalazione, ad un comune che aveva pubblicato sul suo sito *web* istituzionale una graduatoria nominativa per un soggiorno estivo di soggetti anziani, recante il punteggio assegnato e le generalità dei beneficiari in rapporto all'Isee dichiarato. Ricevute rassicurazioni dal Comune e verificato sul sito il rispetto delle norme, non sono state avviate ulteriori iniziative (artt. 11, comma 1, punto 4, e 13, comma 4, del regolamento n. 1/2007) (*Nota* 23 gennaio 2009).

Un'azienda sanitaria locale aveva interpellato l'Ufficio sull'eventuale pubblicazione, anche sul suo sito *web*, di talune deliberazioni e determinazioni in conformità alle vigenti leggi regionali. Al riguardo, è stato rappresentato che una legge regionale deve ritenersi fonte idonea a disciplinare il trattamento dei dati personali, fermo restando il rispetto dei presupposti e dei limiti stabiliti dal Codice, nonché dalla legge e dai regolamenti (artt. 18, commi 2 e 3, del Codice). I soggetti pubblici possono trattare dati sensibili o giudiziari, invece, nei limiti in cui ciò risulti indispensabile ad assicurare il rispetto del principio di pubblicità dell'attività istituzionale degli enti, fermo restando il divieto di diffondere dati idonei a rivelare lo stato di salute (artt. 22, comma 8, 65, comma 5, e 68, comma 3, del Codice) e quanto previsto dallo schema tipo di regolamento per i trattamenti dei dati sensibili e giudiziari di competenza delle regioni e delle province autonome, nonché delle aziende sanitarie (*v. Relazione* 2005, *p.* 21; *v.* in particolare allegato B dello schema tipo citato [doc. *web* n. 1272225]) (*Nota* 3 giugno 2008).

Il divieto assoluto di diffondere dati idonei a rivelare lo stato di salute degli interessati, richiamando anche le indicazioni fornite dal Garante il 19 aprile 2007, con le già citate linee-guida, è stato sottolineato anche nel definire una segnalazione sulla presunta pubblicazione integrale sull'albo pretorio di una deliberazione su una riduzione di retribuzione dovuta ad una prolungata assenza dal servizio per malattia. I responsabili dei servizi comunali hanno invece rappresentato – con dichiarazione la cui non veridicità è penal-

mente sanzionata (art. 168 del Codice) – che la determinazione in questione non era stata pubblicata sull'albo pretorio. Non essendo stati ravvisati gli estremi di una violazione, è stata conclusa l'istruttoria preliminare senza iniziative in relazione a quanto segnalato (*v.* artt. 11, comma 1, punto 2, e 13, comma 4, del regolamento n. 1/2007) (*Nota* 12 novembre 2008).

Con un reclamo è stata prospettata l'avvenuta diffusione, da parte di un gruppo politico, di un manifesto indicante il beneficio che sarebbe stato apportato al bilancio comunale dalla riduzione della prestazione lavorativa giornaliera del segretario comunale. Sul punto è stato osservato che le informazioni attinenti ai profili retributivi dei segretari comunali e provinciali sono assoggettati ad un particolare regime di pubblicità (*v.* Ccnl dei segretari comunali e provinciali), che li rendono conoscibili da chiunque; pertanto, in relazione al quadro normativo di settore vigente, non si è proceduto ad ulteriori iniziative in merito (*v.* art. 11, comma 1, punto 2, del regolamento n. 1/2007) (*Nota* 17 luglio 2008).

Sulla base delle citate linee-guida è stato evidenziato ad un comune, che aveva chiesto delucidazioni in proposito, come non sia lecito diffondere indifferenziatamente tutti i presupposti oggettivi e soggettivi che hanno determinato l'assegnazione degli alloggi di edilizia agevolata, 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 o a situazioni di grave disagio abitativo sofferte). La 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 dati personali contrastanti con i princìpi di pertinenza e non eccedenza (art. 11, comma 1, lett. *d*), del Codice), fermo restando il divieto di pubblicare dati idonei a rivelare lo stato di salute (*cfr.* art. 22, comma 8, del Codice, *par.* 10.2.3 delle linee-guida *cit.*) (*Nota* 5 febbraio 2009).

È stato oggetto d'esame anche il diritto dei consiglieri comunali e provinciali di accedere a notizie e informazioni in possesso dell'amministrazione contenenti dati personali di terzi.

Un comune aveva chiesto chiarimenti sulla possibilità di rendere ostensibili ad un soggetto, rivestente la duplice qualifica di assessore e consigliere, taluni documenti contenenti anche dati sensibili.

Nel fornire riscontro, la questione è stata necessariamente esaminata su due piani diversi. È stato precisato, da un lato, che la legge riconosce ai consiglieri il diritto di ottenere dal comune tutte le notizie e le informazioni in suo possesso, utili all'espletamento del proprio mandato (art. 43, comma 2, del d.lg. 18 agosto 2000, n. 267). L'esercizio di tale diritto nei confronti di documenti contenenti dati sensibili è consentito se strettamente necessario allo svolgimento della funzione di controllo, di indirizzo politico, di sindacato ispettivo e di altre forme di accesso a documenti riconosciute dalla legge e dai regolamenti degli organi interessati per l'espletamento di un mandato elettivo (art. 65, comma 4, lett. *b*), del Codice; *v.* scheda n. 33 dello schema tipo Anci *cit.*). Dall'altro lato, è stato evidenziato che, per quanto riguarda gli assessori comunali, la normativa di settore stabilisce unicamente che questi ultimi, per gli specifici settori ad essi delegati, sovrintendano al funzionamento degli uffici e dei servizi non con atti di diretta gestione, bensì con direttive generali cui pure i dirigenti degli uffici sono tenuti a conformarsi (artt. 50 e 109, d.lg. n. 267/2000 *cit.*).

Il testo unico delle leggi sull'ordinamento degli enti locali (art. 88 del d.lg. n. 267/2000) dispone, poi, che gli statuti e i regolamenti di tali enti siano informati ai princìpi sanciti nel d.lg. 30 marzo 2001, n. 165), tra i quali la distinzione tra funzioni di indirizzo e controllo politico-amministrativo, che spettano agli organi di governo, e funzioni di attuazione e gestione amministrativa, che spettano ai funzionari di livello dirigenziale, i quali godono, tra l'altro, di autonomi poteri di organizzazione e controllo delle risorse umane.

Pertanto, nel solo caso in cui la richiesta di dati personali, anche di natura sensibile, sia indispensabile all'assessore per espletare la funzione di controllo politico-amministrativo sull'andamento dell'ufficio e, più in particolare, per esercitare una verifica dell'osservanza delle direttive impartite al dirigente responsabile del servizio, l'acquisizione di tali dati potrebbe non apparire contraria alle disposizioni in materia di protezione dei dati personali (art. 67, comma 1, lett. *a*) e *b*), del Codice; *v.* scheda n. 33 dello schema tipo Anci già *cit.* e il *Parere* del 7 dicembre 2006 *cit.*) (*Nota* 27 giugno 2008).

Sulla base dei predetti princìpi, è stato chiarito ad un comune che spetta all'amministrazione destinataria della richiesta accertare il fondamento della pretesa all'informazione

ratione officii del consigliere comunale, con valutazione eventualmente sindacabile dal giudice amministrativo. Resta ferma la necessità che i dati personali così acquisiti dagli aventi diritto siano utilizzati effettivamente per le sole finalità realmente pertinenti al mandato, rispettando il dovere di segreto nei casi specificamente determinati dalla legge, nonché i divieti di divulgazione dei dati personali (*v.* art. 22, comma 8, del Codice, che vieta la diffusione dei dati idonei a rivelare lo stato di salute) (*Nota* 12 gennaio 2009).

Sulla possibilità per un consigliere comunale di ottenere la *cd.* "*mailing-list*" dei cittadini in possesso dell'ente di riferimento, al fine di inviare talune comunicazioni da parte della minoranza consiliare, è stato formulato un duplice ordine di considerazioni. Quanto all'invio di comunicazioni istituzionali, nel quadro di ordinarie relazioni amministrative con gli interessati, il soggetto pubblico può trovarsi a raccogliere i recapiti direttamente dall'interessato, che intende essere informato in uno specifico contesto (*ad es.*, ai fini dell'accesso a documenti amministrativi), o ricevere sistematicamente determinati messaggi inviati da uffici per le relazioni con il pubblico, nell'ambito dei servizi usufruibili anche tramite reti civiche o richiesti tramite siti *web* istituzionali. In tali casi il soggetto pubblico può procedere a comunicazioni istituzionali per le sole finalità connesse ad una specifica richiesta o indicazione dell'interessato (*Provv.* 12 marzo 2003 [doc. *web* n. 29844]; *v. Relazione* 2003, *p.* 87) (*Nota* 22 dicembre 2008).

Sotto un diverso profilo, alla luce del *provvedimento* del 28 febbraio 2008 (*G.U.* 8 marzo 2008, n. 58 [doc. *web* n. 1493909]; *v. Relazione* 2007, *p.* 85), alcune particolari modalità di comunicazione politica o propaganda elettorale, in particolare attraverso messaggi di posta elettronica, richiedono il consenso specifico di abbonati a servizi di comunicazione elettronica. Il consenso, che può essere acquisito *una tantum*, deve precedere il messaggio ed essere raccolto sulla base di formule chiare che specifichino espressamente la finalità di comunicazione politica o propaganda elettorale. Non è possibile ricorrere a modalità di silenzio-assenso.

L'Ufficio ha avuto occasione di pronunciarsi in ordine all'utilizzo di apparecchiature videofotografiche durante le seduta del consiglio comunale, evidenziando che il testo unico delle leggi sull'ordinamento degli enti locali garantisce espressamente la pubblicità

degli atti e delle sedute del consiglio comunale, rinviando ad uno specifico regolamento l'introduzione di eventuali limiti a detto regime di pubblicità. Per verificare, quindi, l'esistenza di particolari restrizioni occorre fare riferimento a tale regolamento, laddove esistente (artt. 10 e 38 d.lg. n. 267/2000 *cit.*). Nell'ipotesi in cui sia prevista la possibilità di effettuare le riprese delle sedute del consiglio comunale, l'Amministrazione deve rendere l'informativa prevista dall'art. 13 del Codice (*Nota* 21 gennaio 2009).

Con una segnalazione, era stata lamentata la diffusione da parte di un consigliere comunale, tramite il proprio sito, di documentazione inerente la sua attività di consigliere, tra cui deliberazioni della giunta e del consiglio comunale, nonché numerose denunce ed esposti nei confronti di amministratori e dipendenti comunali dal medesimo presentate alla competenti autorità.

L'Ufficio ha osservato che le deliberazioni comunali sono documenti pubblici conoscibili da chiunque (art. 124 del d.lg. n. 267/2000 *cit.*) e che la pubblicazione sul sito Internet dell'ente degli atti affissi all'albo pretorio è ritenuta non automaticamente lecita, ma comunque possibile, sia pure sulla base di una valutazione attenta e responsabile dei princìpi e dei limiti in materia di protezione dei dati personali (*par.* 5 e 6 delle linee-guida *cit.*). Tali princìpi, pur non essendo rivolti direttamente ai trattamenti posti in essere nei siti *web* privati, devono comunque essere tenuti presenti da questi ultimi quando si intenda in essi ripubblicare o diffondere i suddetti dati.

Inoltre, specifiche disposizioni estendono l'ambito applicativo delle norme concernenti il trattamento dei dati personali in ambito giornalistico ad altre attività di manifestazione del pensiero che implicano un trattamento di dati personali, effettuato da soggetti che non esercitano professionalmente l'attività giornalistica (art. 136, comma 1, lett. *c*), del Codice). Possono quindi essere diffusi dati personali, anche senza il consenso dell'interessato, nei limiti dell'essenzialità dell'informazione riguardo a fatti di interesse pubblico (art. 137, comma 3, del Codice; art. 6 del codice di deontologia relativo al trattamento dei dati personali nell'esercizi o dell'attività giornalistica, Allegato A.1. del Codice). Nel caso di specie, pertanto, pur non ravvisando una violazione della disciplina sulla protezione dei dati personali (artt. 11, comma 1, punto 2, e 13, comma 4, del rego-

lamento n. 1/2007 *cit.*), è stato evidenziato che la persona interessata, se ritiene lesa la propria reputazione in conseguenza della diffusione di dati che la riguardano, può agire qualora ne ricorrano i presupposti, presso le competenti sedi giudiziarie (*Nota* 10 febbraio 2009).

Sono stati forniti chiarimenti al Ministero dell'interno-Dipartimento per gli affari interni e territoriali sull'accesso, da parte di un consigliere comunale, ai tabulati telefonici del cellulare di servizio in dotazione al sindaco di un comune.

Sul punto è stata fatta presente l'esigenza di coordinare il diritto di accesso riconosciuto ai consiglieri comunali dall'art. 43 del d.lg. n. 267/2000 citato con altre norme vigenti che tutelano, in particolare, la segretezza della corrispondenza e delle conversazioni, in considerazione della natura particolarmente delicata dei dati di traffico telefonico, la cui utilizzazione impropria può avere ripercussioni sulla sfera personale di più soggetti interessati (il chiamante, l'abbonato e il chiamato). Al riguardo, la giurisprudenza costituzionale, in più occasioni, ha evidenziato la stretta attinenza della libertà e della segretezza della comunicazione al nucleo essenziale dei valori della personalità tale da ricomprendere *"non soltanto la segretezza del contenuto della comunicazione, ma anche quella relativa ai dati esterni ad essa, ovvero all'identità dei soggetti e ai riferimenti di tempo e di luogo della comunicazione stessa"*. L'art. 15 della Costituzione, *"in mancanza delle garanzie ivi previste, preclude la divulgazione o, comunque, la conoscibilità da parte di terzi delle informazioni e delle notizie idonee a identificare i dati esteriori della conversazione telefonica (autori della comunicazione, tempo e luogo della stessa), dal momento che, facendone oggetto di uno specifico diritto costituzionale alla tutela della sfera privata attinente alla libertà e alla segretezza della comunicazione, ne affida la diffusione, in via di principio, all'esclusiva disponibilità dei soggetti interessati"* (Corte costituzionale, sentenze 26 febbraio - 11 marzo 1993, n. 81; 11-23 luglio 1991, n. 366; 7-17 luglio 1998, n. 281) (*Nota* 15 gennaio 2009).

3.3. LA DOCUMENTAZIONE ANAGRAFICA E LA MATERIA ELETTORALE

Il trattamento dei dati personali contenuti sia nell'anagrafe della popolazione residente, sia nelle liste elettorali, è stato oggetto di particolare attenzione da parte del Garante.

In riscontro ad un quesito riguardante la possibilità di rendere accessibile, tramite Internet, l'anagrafe della popolazione residente ai Comandi dell'Arma dei Carabinieri, è stato osservato che la relativa disciplina consente alle forze dell'ordine di accedere e consultare direttamente gli atti anagrafici. All'ufficiale di anagrafe devono essere comunicati gli estremi del personale abilitato alla consultazione, il quale opererà secondo modalità tecniche adottate d'intesa tra gli uffici anagrafici comunali e gli organi interessati (art. 19, comma 2, del Codice, e art. 37, commi 1 e 4, d.P.R. 30 maggio 1989, n. 223) (*Nota* 26 settembre 2008).

Al Consiglio dell'Ordine degli Avvocati di Roma, che prospettava la possibilità di un collegamento telematico dei singoli studi professionali alla banca dati dell'anagrafe della popolazione residente del Comune di Roma, è stato rappresentato che le relative disposizioni non sono state modificate dal Codice; pertanto, occorre rispettare le specifiche norme di settore che subordinano la consultazione al rispetto di determinati limiti e modalità (*v.* art. 19, comma 3, del Codice e artt. 33, 34 e 37 del d.P.R. n. 223/1989 *cit.*). In tale quadro, con il *provvedimento* del 6 ottobre 2005 (*G.U.* 2 ottobre 2005, n. 248 [doc. *web* n. 1179484], *v. Relazione* 2005, *p.* 30) il Garante ha opportunamente evidenziato come le richieste di certificazione o attestazione, oppure di rilascio di elenchi ad amministrazioni pubbliche motivato da accertate ragioni di pubblica utilità, possano essere inoltrate e riscontrate anche automaticamente, per via telematica, escludendo però la consultazione diretta, anche *on-line*, degli atti di provenienza anagrafica da parte di soggetti interni ed esterni diversi da quelli preposti all'ufficio anagrafe (*Nota* 13 novembre 2008).

L'Ufficio è stato interpellato dalla Prefettura di Belluno-Utg, sulla richiesta avanzata dal Consolato onorario di Serbia in Italia di ottenere dati riguardanti i soggetti di nazionalità serba, serbo-croata e serbo-bosniaca contenuti nell'anagrafe della popolazione residente sul territorio. In linea generale, la disciplina sugli atti anagrafici consente all'ufficiale dell'anagrafe di rilasciare (anche periodicamente) 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 *cit.*). È però compito dell'Amministrazione interpellata accertare i predetti requisiti ai fini del

rilascio (art. 19, comma 2 del Codice) (*Nota* 23 gennaio 2009). In proposito il Ministero dell'interno-Dipartimento per gli affari interni e territoriali, interpellato per un parere sulla questione, ha affermato di ritenere che il Consolato onorario di Serbia non possa rientrare nel concetto di pubblica amministrazione.

È pervenuto al Garante un quesito concernente l'iniziativa di un comune volta ad invitare i cittadini ad una manifestazione riguardante le istituzioni scolastiche locali: il Dipartimento competente ha fatto presente che il trattamento dei dati contenuti nell'anagrafe della popolazione residente può essere legittimamente effettuato per esclusivo uso di pubblica utilità anche in caso di applicazione della disciplina in materia di comunicazione istituzionale da parte dei soggetti pubblici, i quali sono tenuti a rispettare la vigente normativa a tutela della riservatezza dei dati personali (art. 177, comma 1, del Codice; art. 34, comma 1, d.P.R. n. 223/1989 *cit.*; art. 1, comma 4, l. 7 giugno 2000, n. 150). In ogni caso gli interessati possono ottenere, rivolgendosi direttamente al titolare del trattamento, l'indicazione dell'origine dei dati trattati, delle finalità e modalità del trattamento (art. 7 del Codice) (*Nota* 10 febbraio 2009).

Un legale, a fronte del diniego opposto da un comune, ha chiesto l'autorizzazione ad acquisire i dati anagrafici dei genitori di un suo assistito, al fine di ricostruire la sua identità biologica. Al riguardo è stato evidenziato che le scelte dell'amministrazione, in caso di diniego, espresso o tacito, dell'accesso a documenti amministrativi contenenti dati personali non sono sindacabili dall'Autorità, bensì innanzi alle competenti autorità in conformità alle specifiche disposizioni di settore. In proposito si applicano le norme in materia di stato civile, adozione e affidamento, non abrogate dal Codice, che prevedono specifiche cautele a tutela delle generalità della madre che abbia eventualmente scelto alla nascita di conservare l'anonimato (art. 9 r.d.l. 8 maggio 1927, n. 798; art. 28 l. l4 maggio 1983, n. 184; art. 70 r.d. 9 luglio 1939, confluito nell'art. 30 d.P.R. 3 novembre 2000, n. 396; artt. 92, 93, comma 2, e 177, comma 2, del Codice) (*Nota* 23 febbraio 2009).

Il Ministero dell'interno-Direzione centrale per i servizi demografici si è rivolto al Garante prospettando l'intenzione di ampliare le funzionalità dell'Indice nazionale delle anagrafi (I.n.a.) mediante l'introduzione di nuovi dati personali oltre quelli già previsti

dalle norme di settore (d.m. 13 ottobre 2005, n. 240; l. 24 dicembre 1954, n. 1228; d.l. 27 dicembre 2000, n. 392 convertito, con modificazioni, dall'art. 1 della l. 28 febbraio 2001, n. 26). Al riguardo, per la rilevante incidenza di quest'ultima progettata innovazione sull'ordinamento anagrafico, il Garante ha invitato la predetta Direzione a valutare l'opportunità di promuovere tale ampliamento attraverso un'eventuale modificazione delle disposizioni attualmente in vigore (*Nota* 28 gennaio 2009).

In materia elettorale, una segnalante ha ipotizzato la violazione del Codice da parte di un candidato al Senato italiano, il quale aveva utilizzato i dati tratti dall'anagrafe dei cittadini italiani residenti all'estero – Aire (d.P.R. 2 aprile 2003, n. 104) – per sostenere una candidatura in relazione alle consultazioni elettorali del Canton Ticino. In proposito, è stato interpellato il Dipartimento per gli affari interni e territoriali-Direzione centrale dei servizi elettorali del Ministero dell'interno, secondo il quale a rappresentanti dei partiti o forze politiche che ne facciano espressa e motivata richiesta viene fornito, per le sole finalità inerenti all'esercizio dell'elettorato attivo e passivo, l'elenco degli elettori residenti all'estero compilato ai sensi dell'art. 5 della l. del 27 dicembre 2001, n. 459 e dell'art. 5 del d.P.R. 2 aprile 2003, n. 104. Alla luce di tali considerazioni, non sono stati ravvisati i presupposti per adottare specifici provvedimenti da parte dell'Autorità (*v.* artt. 11, comma 1, punto 2, e 13, comma 4, del regolamento n. 1/2007 del 14 dicembre 2007) (*Nota* 13 novembre 2008).

È stata poi denunciata al Garante una violazione del divieto previsto, dalla data di convocazione dei comizi elettorali e fino alla chiusura delle operazioni di voto, per tutte le amministrazioni pubbliche di svolgere attività di comunicazione politica (*v.* art. 9 l. 22 febbraio 2000, n. 28). In proposito, il Codice non ha attribuito all'Autorità alcuna competenza sanzionatoria in merito alle violazioni delle disposizioni previste dalla l. n. 28/2000 *cit.* (*Nota* 22 dicembre 2008).

In un caso si è rivolto al Garante un comune, chiedendo delucidazioni sulla legittimità della richiesta avanzata da un'associazione di ottenere rilascio di copia delle liste elettorali, con l'intento di informare i cittadini sulle attività socio-assistenziali svolte. L'Ufficio ha risposto facendo presente che le predette liste possono essere rilasciate in

copia solo *"per finalità di applicazione della disciplina in materia di elettorato attivo e passivo, di studio, di ricerca statistica, scientifica o storica, o carattere socio-assistenziale o per il perseguimento di un interesse collettivo o diffuso"* (art. 177, comma 5, del Codice) (*Nota* 23 giugno 2008). Solo l'amministrazione destinataria dell'istanza può valutare se la specifica finalità dichiarata dal richiedente sia conforme all'attività svolta e se rientri effettivamente tra le ipotesi di cui all'art. 177 *cit.*, tenendo presente che le finalità che legittimano il rilascio delle liste elettorali devono risultare – oltre che motivate ai sensi dell'art. 51 d.P.R. 30 marzo 1967, n. 223 – proprie del richiedente e, "[...] *ove si tratti di un ente o di un'associazione, devono essere coerenti con l'oggetto dell'attività di tale organismo* [...] " (*v. Relazione* 2006, *par.* 3.6).

I predetti princìpi sono stati rappresentati anche ad un comune, nei cui confronti l'Ufficio si è attivato in base a talune notizie di stampa, secondo le quali l'amministrazione in questione forniva copia delle liste elettorali senza effettuare alcuna verifica in ordine ai presupposti di legittimità per il relativo rilascio. È stata evidenziata, in particolare, l'esigenza di effettuare gli opportuni controlli in ordine alla veridicità delle dichiarazioni contenute nelle richieste presentate secondo il quadro normativo di riferimento (d.P.R. 28 dicembre 2000, n. 445, in particolare art. 71 relativamente ai controlli) (*Nota* 8 gennaio 2009). Al riguardo le procedure adottate dal Comune per il rilascio di copia delle liste elettorali sono risultate rispettose della disciplina di settore e, pertanto, non sono stati avviati ulteriori accertamenti.

Un'ipotesi diversa ha riguardato, ai sensi dell'art. 75, comma 4, del d.P.R. 16 maggio 1960, n. 570, l'istanza di un cittadino elettore volta ad ottenere copia dei verbali delle operazioni espletate presso i seggi elettorali, considerato che i predetti verbali contengono anche indicazioni sull'eventuale esercizio del diritto di voto assistito. Il Garante ha osservato che l'accesso a documenti amministrativi concernenti dati idonei a rivelare lo stato di salute dell'interessato – come nel caso delle indicazioni sull'eventuale esercizio del diritto di voto assistito – è consentito se la situazione che si intende tutelare con la richiesta di accesso ai documenti amministrativi è di rango almeno pari ai diritti dell'interessato, ovvero consiste in un diritto della personalità o in un altro diritto o libertà fonda-

mentale e inviolabile (artt. 59 e 60 del Codice). La disposizione contenuta nell'art. 75, comma 4, del d.P.R. n. 570/1960 citato, in base alla quale *"ogni elettore della circoscrizione ha diritto"* di prender conoscenza dei verbali delle operazioni elettorali, va ritenuta idonea fonte normativa per la comunicazione di dati personali a soggetti diversi dall'interessato (*v.* Consiglio di Stato, sez. V, sentenze 9 maggio 2006, n. 2531; 19 giugno 2006, n. 3593; 6 febbraio 2007, n. 476; Corte costituzionale, ordinanza 12-27 luglio 2000, n. 386). L'amministrazione destinataria della richiesta dovrà valutare, caso per caso, la sussistenza di tutte le condizioni previste dalla normativa di riferimento per accedere ai predetti verbali, tenendo conto dei parametri sopra richiamati, nonché dei princìpi di pertinenza, non eccedenza e indispensabilità con riguardo al trattamento di dati sensibili (art. 22, commi 5 e 9, del Codice) (*Nota* 5 febbraio 2009).

Ad un quesito della Presidenza del Consiglio dei Ministri-Dipartimento per il coordinamento amministrativo sul rilascio di copia degli atti contenenti le sottoscrizioni degli elettori per la presentazione delle liste elettorali, nonché le accettazioni delle candidature per il rinnovo della carica di sindaco e di consigliere comunale, è stato risposto che tali documenti contengono informazioni idonee a rivelare opinioni politiche. I soggetti pubblici possono comunicare dati sensibili qualora tale operazione risulti indispensabile al perseguimento di determinate finalità di rilevante interesse pubblico, tra le quali sono ricomprese quelle relative all'applicazione della normativa sull'accesso ai documenti amministrativi (art. 59 citato del Codice). È stato evidenziato, altresì, che il trattamento dei dati idonei a rivelare le opinioni politiche effettuato da parte della commissione elettorale circondariale finalizzato all'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 2006 ([doc. *web* n. 1289890] *v. Relazione* 2007, *p.* 39) (*Nota* 12 gennaio 2009).

3.4. L'ISTRUZIONE

3.4.1. La scuola

Anche nel 2008 il Garante è intervenuto più volte sul trattamento dei dati degli studenti.

In particolare, nella trattazione di due ricorsi, è emerso che nel sito Internet di due uffici scolastici provinciali era consultabile l' *"elenco dei riservisti (Gruppo 2-disabili art. 1, l. n. 68/99) delle graduatorie permanenti provinciali redatte ai sensi della l. n. 124/1999"*. La pubblicazione in Internet di tali dati configura una diffusione di dati personali, idonei, per la dicitura *"elenco dei riservisti" "Gruppo 2-disabili art. 1, l. n. 68/99"* a rivelare lo stato di salute degli interessati, in contrasto con le norme del Codice (art. 4, comma 1, lett. *d*) e art. 22, comma 8).

La separata graduatoria dei soggetti appartenenti alle categorie protette di cui all'art. 1 della legge n. 68 del 23 marzo 1999 non è risultata espressamente prevista dalla normativa vigente, ed il divieto di pubblicazione dei dati sensibili in tali graduatorie è stato ribadito dal Ministero della pubblica istruzione-Dipartimento per l'istruzione con nota del 7 marzo 2008.

Gli uffici scolastici interessati, su espressa richiesta del Garante, si sono impegnati a rimuovere dal sito il citato elenco (*Nota* 22 aprile 2008)

Sulla base di alcune notizie di stampa, poi, l'Ufficio ha avviato accertamenti sulla distribuzione in alcuni asili nido comunali di un questionario sul temperamento dei bambini, predisposto da una psicologa universitaria. Sono stati richiesti elementi utili alla valutazione del caso, con particolare riferimento all'eventuale possibilità di identificare, anche indirettamente, i minori, il cui comportamento veniva analizzato attraverso il questionario ed è stata richiamata l'attenzione sulla particolare delicatezza del trattamento dei dati ipotizzato (*Nota* 11 aprile 2008). A seguito di tale richiesta il Comune ha deciso di astenersi dalla somministrazione del menzionato questionario.

L'Ufficio ha avuto altresì occasione di fornire chiarimenti ad un ufficio scolastico provinciale in merito all'utilizzo di fotografie in ambito scolastico.

In proposito è stata richiamata la direttiva emanata il 30 novembre 2007 dal Ministero

della pubblica istruzione, con parere favorevole del Garante che, nel disciplinare l'uso dei dispositivi elettronici per la ripresa di immagini e filmati in ambito scolastico, chiarisce i casi in cui trova applicazione il Codice.

In particolare, se i filmati, le immagini o i suoni, relativi ad altre persone, siano acquisiti per "*fini esclusivamente personali*", non operano gli obblighi di informativa e di acquisizione del consenso, purché le informazioni così raccolte "*non siano destinate ad una comunicazione sistematica o alla diffusione*" (*cfr.* punto 3.1, citata direttiva; art. 5, comma 3, del Codice) (*Nota* 3 marzo 2008).

Analoghe considerazioni sono state espresse sul quesito di una direzione didattica riguardante le immagini raccolte attraverso videocamere o macchine fotografiche per documentare eventi scolastici e conservare ricordi dei propri figli (*Nota* 25 febbraio 2008; *v.* anche comunicati stampa del 17 dicembre 2003 e 6 giugno 2007, *Newsletter* n. 195, 8-21 dicembre 2003).

Una scuola professionale aveva chiesto al Garante l'autorizzazione a fornire ad enti pubblici non economici operanti nella provincia di riferimento gli elenchi di dati anagrafici al *"fine di promuovere le attività legate alla formazione professionale e alla formazione continua sul lavoro"*. L'Autorità ha rappresentato che specifiche disposizioni legislative consentono ai soggetti pubblici, ivi compresi gli istituti scolastici, su richiesta degli interessati, di fornire, anche a privati e per via telematica, dati relativi agli esiti scolastici degli studenti e altri dati personali non sensibili o giudiziari, pertinenti "*al fine di agevolare l'orientamento, la formazione e l'inserimento professionale*" (art. 96 del Codice) (*Nota* 12 settembre 2008).

È stato, inoltre, comunicato a questa Autorità, ai sensi dell'art. 39, comma 1, lett. *a*), del Codice, che un Ufficio scolastico aveva richiesto al dirigente scolastico di una scuola l'elenco degli alunni che conseguono il diploma di licenza media.

Al riguardo, è stato chiarito che tale comunicazione, se necessaria all'esplicazione delle funzioni istituzionali (art. 19, commi 2 e 3), deve rispettare il principio di pertinenza e non eccedenza, senza determinare presso l'amministrazione ricevente un afflusso di dati esuberante rispetto alle finalità perseguite (art. 11 del Codice).

Ferme restando le specifiche disposizioni normative relative all'anagrafe nazionale degli studenti (art. 3, d.lg. 15 aprile 2005, n. 76), spetta all'amministrazione richiedente individuare i presupposti normativi, relativi all'esercizio delle funzioni istituzionali, e legittimanti l'acquisizione dei dati richiesti, verificando altresì se le finalità che si intende porre in essere siano realizzabili anche senza la preventiva costituzione di una banca dati degli studenti che hanno conseguito il diploma di licenza media (*Nota* 17 aprile 2008).

3.4.2. L'università

Nel settore universitario, l'Autorità è stata interpellata soprattutto in relazione a specifiche richieste di trasmissione di dati relativi a studenti.

In particolare, un'università ha formulato un quesito in merito alla possibilità di comunicare ad un giornalista l'elenco dei laureati che, negli ultimi due anni, abbiano avuto il riconoscimento di sessanta crediti.

Al riguardo, in assenza di disposizioni statali sul punto, ciascuna università, nel quadro della propria autonomia regolamentare, può disciplinare il regime di conoscibilità dei dati riguardanti i laureati, con apposite disposizioni. Comunque, il Codice (artt. 59 e 60) non ha abrogato le norme vigenti in materia di accesso ai documenti amministrativi (artt. 22 e *ss.* legge 7 agosto 1990, n. 241, così come modificata dalla legge 11 febbraio 2005, n. 15). Spetta quindi all'amministrazione destinataria della richiesta accertare la sussistenza dei presupposti previsti dalla citata disciplina, anche alla luce dell'orientamento giurisprudenziale che riconosce ad una testata giornalistica l'interesse a conoscere documentazione amministrativa determinata al chiaro e univoco fine di esercitare la libertà di stampa su singole questioni (*cfr.* Consiglio di Stato, sez. IV, 6 maggio 1996, n. 570) (*Nota* 21 gennaio 2009).

In un'altra occasione, un'università ha comunicato all'Ufficio del Garante di aver sottoscritto un protocollo di intesa con un comune, che prevedeva la trasmissione di taluni dati (codice fiscale, domicilio e residenza) degli studenti immatricolati nell'anno accademico 2008/2009, con specifici requisiti di residenza. Tale iniziativa, proposta dalla Guardia di finanza, aveva la finalità di aumentare il grado di conoscenza sugli alloggi nel

Comune e di fornire agli studenti fuori sede tutte le informazioni sulla locazione di immobili, sulle diverse forme di contratto e sui vantaggi della registrazione, nell'ambito della lotta all'evasione fiscale connessa alla locazione non dichiarata.

L'Ufficio non ha rinvenuto una norma che preveda la comunicazione di tali dati da parte delle università ai comuni per le finalità sopra descritte.

È stato tuttavia verificato che l'amministrazione finanziaria può "*inviare ai contribuenti questionari relativi a dati e notizie di carattere specifico rilevanti ai fini dell'accertamento nei loro confronti nonché nei confronti di altri contribuenti con i quali abbiano intrattenuto rapporti, con invito a restituirli compilati e firmati*" (*v.* art. 32, comma 1, n. 8-*bis*, d.P.R. 29 settembre 1973, n. 600; art. 11 d.lg. 18 dicembre 1997, n. 471).

In tale quadro i dati relativi agli studenti immatricolati nell'anno accademico 2008/2009 possono essere acquisiti, in conformità alla normativa di settore, direttamente dai Comandi provinciali della Guardia di finanza, per lo svolgimento delle funzioni istituzionali legittimamente perseguite.

La finalità dell'iniziativa, rientrando tra i compiti istituzionali del Comune, può essere utilmente raggiunta con altre modalità (*ad es.*, mediante la distribuzione di specifico materiale informativo presso le facoltà universitarie) nel rispetto dei princìpi di necessità e di pertinenza e non eccedenza dei dati raccolti rispetto alle finalità perseguite (artt. 3 e 11 del Codice) (*Nota* 5 dicembre 2008).

Infine, un'università ha comunicato a questo Ufficio l'intenzione di rilasciare all'Istituto per lo sviluppo della formazione professionale dei lavoratori (Isfol) taluni dati personali relativi a soggetti laureati nei corsi di laurea triennali nell'anno solare 2007 (nome e cognome, residenza, recapiti telefonici, indirizzi *e-mail*, sesso, eventuale iscrizione a laurea specialistica o *master*), al fine di contattare direttamente i laureati e verificare la loro disponibilità a svolgere un'intervista telefonica con una società accreditata nell'albo Isfol; in relazione a tale richiesta, è stato precisato che l'attività di ricerca statistica è regolata da una specifica disciplina di settore (d.lg. 6 settembre 1989, n. 322, recante norme sul Sistema statistico nazionale; codice di deontologia e di buona condotta per i trattamenti di dati personali a scopi statistici e di ricerca scientifica effettuati

nell'ambito del Sistema statistico nazionale-Allegato A.3. del Codice) che consente di realizzare progetti di ricerca anche raccogliendo dati personali originariamente trattati presso altre amministrazioni per fini diversi da quelli statistici (*ad es.*, per finalità amministrative).

In tale quadro, pur facendo parte l'Isfol del Sistema statistico nazionale (art. 2, comma 1, del d.P.C.M. 19 marzo 2003), la ricerca Isfol *"Impatto occupazionale lauree triennali"* non è risultata ricompresa nel Programma statistico nazionale.

In conformità alla disciplina di settore citata, pertanto, l'iniziativa in esame, ove non risulti effettivamente inserita nel Programma statistico nazionale, potrebbe essere utilmente realizzata dall'Isfol senza acquisire dati personali dall'università, *ad es.*, mediante la somministrazione del questionario oggetto dell'intervista ai laureati, con la facoltà per gli stessi, di fornire le informazioni richieste direttamente all'Isfol (*Nota* 16 gennaio 2009).

3.5. ATTIVITÀ FISCALE, TRIBUTARIA E DOGANALE

Sistemi informativi della fiscalità

Anche nel 2008 il trattamento di dati personali effettuato nell'ambito dell'attività fiscale e tributaria è stato oggetto di particolare attenzione da parte dell'Autorità.

Prima fase di accertamenti

Sulla base di un'analisi preliminare del sistema informativo della fiscalità, alla fine del 2007 il Garante aveva deliberato l'avvio di accertamenti volti a verificare, in più fasi, i trattamenti di dati personali effettuati presso l'anagrafe tributaria, rilevando che elementi di maggior criticità e urgenza erano da ravvisarsi nelle misure di sicurezza adottate per gli accessi da parte di enti esterni, pubblici e privati, all'amministrazione finanziaria.

Nel settembre 2008 si è conclusa la prima fase dell'attività ispettiva del Garante sull'anagrafe tributaria.

Sono stati numerosi i punti di criticità riscontrati con il *provvedimento* adottato il 18 settembre 2008 (doc. *web* n. 1549548): mancata conoscenza del numero complessivo degli utenti che accedono al sistema informativo, della loro effettiva identità e delle finalità dei loro accessi; accessi anomali o utilizzi impropri di *password* e credenziali; misure tecnologiche e capacità di monitoraggio da rafforzare al fine di proteggere i dati contenuti nel *database*.

L'anagrafe tributaria è un delicato e complesso sistema informativo al quale ha accesso – attraverso diversi strumenti telematici (applicativi Siatel, Puntofisco, Entratel, servizi *web*, *ecc.*) – un numero considerevolmente elevato di soggetti, tra i quali comuni, regioni, province, università, asl, tribunali, camere di commercio, enti previdenziali, gestori telefonici, forze di polizia, con migliaia di punti di accesso. Il solo sistema di collegamento *web* Siatel viene utilizzato da novemilaquattrocento enti convenzionati e sessantamila utenze, mentre Puntofisco da circa centottanta enti e diciottomila utenze.

Per porre rimedio alle criticità riscontrate, l'Autorità ha imposto all'Agenzia delle entrate un'articolata serie di misure, tecnologiche e organizzative, in particolare per innalzare i livelli di sicurezza degli accessi all'anagrafe tributaria e rendere il trattamento dei dati effettuato conforme alle norme sulla protezione dei dati, che dovranno essere adottate dall'Agenzia delle entrate secondo una precisa tempistica (da tre mesi ad un anno, a seconda della complessità degli adempimenti).

In particolare è stato previsto che l'Agenzia effettui una ricognizione periodica degli enti che accedono all'anagrafe tributaria e una verifica delle effettiva necessità di mantenere attivi gli accessi concessi, anche riguardo al numero delle utenze, bloccando degli accessi non conformi alle norme di legge o a quanto previsto dalle convenzioni stipulate con gli enti.

È stato disposto, inoltre, che l'Agenzia effettui un censimento aggiornato di tutti i flussi di trasferimento dei dati da e verso l'anagrafe tributaria e di tutti gli accessi di tipo interattivo, specificando per ciascun flusso o accesso l'identità dei soggetti legittimati a farlo, la base normativa, la finalità istituzionale, la natura e la qualità dei dati trasferiti o a cui si è avuto accesso, la frequenza ed il volume dei trasferimenti o degli accessi, il numero di soggetti che utilizzano la procedura. Dovranno, inoltre, essere predefinite soglie relative al numero di utenti che possono essere abilitati da ciascun ente ad accedere all'anagrafe tributaria e gli enti che accedono devono garantire una tempestiva disabilitazione all'accesso del personale adibito ad altre mansioni o non più in servizio e l'adeguamento costante dei profili di autorizzazione.

Oltre ad alcuni specifici accorgimenti relativi agli applicativi utilizzati dall'Agenzia, il

Garante ha disposto che i dati visualizzabili dovranno essere compartimentati: ciascun utente legittimato potrà accedere ai soli dati necessari a svolgere i compiti di cui è incaricato con l'indicazione obbligatoria del numero della pratica per la quale si consulta l'anagrafe. L'Agenzia dovrà adottare sistemi di allarme per eventuali comportamenti anomali o a rischio, ed effettuare controlli periodici sugli accessi degli enti esterni e sull'attività svolta da Sogei Spa.

I sistemi di autenticazione dovranno essere rafforzati attraverso il censimento delle postazioni dei terminali dai quali si ha accesso ai dati, in modo differenziato a seconda degli incaricati o dei profili di autorizzazione assegnati. Dovrà essere implementato un sistema di certificazione digitale per gestire l'identità elettronica dei sistemi informatici e degli utenti della banca dati e gli accessi contemporanei con le medesime credenziali potranno avvenire solo in casi eccezionali. Inoltre, gli utenti che accedono via *web* dovranno essere tracciati e deve essere assicurato un livello minimo di accesso ai dati con limitazioni quantitative e qualitative delle interrogazioni, anche al fine di evitare duplicazioni improprie di banche dati da parte di soggetti esterni.

Particolare attenzione è stata posta, infine, ai vincoli che l'Agenzia, attraverso le convenzioni, deve imporre agli enti che accedono all'anagrafe tributaria e che devono fornire adeguate istruzioni agli *"amministratori locali"* (soggetti preposti all'abilitazione delle utenze all'interno dei vari enti convenzionati) e regolare compiutamente le condizioni del collegamento, inibendo gli accessi realizzati in modo non conforme alle stesse.

Riscossione

Il Garante ha, inoltre, avviato una seconda fase di accertamenti volta a verificare i collegamenti della società Equitalia e degli agenti della riscossione all'anagrafe tributaria, nonché, più in generale, i trattamenti di dati personali effettuati a scopo di riscossione.

Ulteriori accertamenti

L'Autorità ha, altresì, già programmato per i prossimi mesi un'ulteriore attività di controllo sul sistema informativo della fiscalità, con particolare riguardo alla struttura degli archivi, alla tipologia delle informazioni raccolte, alle modalità con le quali i dati confluiscono nel *database* e alle modalità con le quali vengono trattati all'interno dell'amministrazione finanziaria.

Con questa iniziativa, così articolata e ampia, il Garante intende anche anticipare

l'enorme lavoro di messa in sicurezza della gestione delle banche dati tributarie e fiscali che la realizzazione del federalismo fiscale renderà sempre più complessa e strategica.

Audizione del Presidente

Le risultanze dell'attività ispettiva sono state anche illustrate dal presidente dell'Autorità in occasione delle audizioni presso la Commissione parlamentare di vigilanza sull'anagrafe tributaria.

Diffusione dei dati reddituali dei contribuenti

Ancora una volta il Garante è intervenuto sulla pubblicità degli elenchi dei contribuenti. Infatti, il provvedimento del Direttore dell'Agenzia delle entrate del 5 marzo 2008 volto ad individuare le modalità e i termini di formazione degli elenchi relativi all'anno di imposta 2005, adottato senza il parere del Garante, ha disposto la pubblicazione di tali elenchi in un'apposita sezione del sito Internet *http://www.agenziaentrate.gov*. Tali elenchi, suddivisi in relazione agli uffici dell'Agenzia delle entrate territorialmente competenti, sono stati resi liberamente consultabili anche con la possibilità di salvarne una copia con funzioni di trasferimento *file*.

Al riguardo, è stato rilevato che la disciplina di settore vigente prevedeva, ai fini della consultazione dei predetti elenchi, il loro deposito, per la durata di un anno, sia presso l'ufficio dell'amministrazione finanziaria, sia presso i comuni interessati (art. 69 del d.P.R. 29 settembre 1973, n. 600 - ora in parte modificato dall'art. 42 d.l. 25 giugno 2008, n. 112, convertito con la l. 6 agosto 2008, n. 133).

Tale disciplina, come già rilevato più volte da questa Autorità, costituisce, la base giuridica per pubblicare gli elenchi dei contribuenti, per favorire la trasparenza dei dati raccolti dalla pubblica amministrazione attraverso le dichiarazioni fiscali (*Provv.* 17 gennaio 2001 [doc. *web* n. 41031], *Provv.* 2 luglio 2003 [doc. *web* n. 1081728], nonché *Provv.* 18 ottobre 2007 [doc. *web* n. 1454901]). Tuttavia, il legislatore ha demandato all'Amministrazione finanziaria esclusivamente il compito di formare annualmente gli elenchi dei contribuenti avendo già individuato lo specifico regime di pubblicità di tali elenchi (art. 69, comma 6, *cit.*).

L'Autorità, pertanto, è intervenuta in via d'urgenza, anche richiamando le sue diverse pronunce in materia, poiché la forma di diffusione adottata poneva evidenti e rilevanti problemi di conformità con il quadro normativo in materia. Il Garante ha quindi chiesto

ulteriori delucidazioni all'Agenzia e l'ha invitata a sospendere nel frattempo la diffusione dei dati in Internet (*cfr. Provv.* 30 aprile 2008 [doc. *web* n. 1510761].

In seguito, con il *provvedimento* del 6 maggio 2008 [doc. *web* n. 1512255], il Garante ha concluso l'istruttoria e, nel ribadire quanto già sostenuto nel *provvedimento* con il quale aveva immediatamente invitato a sospendere la pubblicazione *on-line*, ha stabilito che la modalità utilizzata dall'Agenzia è stata illegittima, poiché contrastava con la normativa in materia secondo cui all'Agenzia delle entrate spetta solo il compito di fissare annualmente le modalità di formazione degli elenchi delle dichiarazioni dei redditi, non le modalità della loro pubblicazione, che rimangono prerogativa del legislatore.

L'inserimento dei dati in Internet, inoltre, appare di per sé non proporzionato rispetto alla finalità della conoscibilità di questi dati. Infatti, l'uso di uno strumento come Internet rende indispensabili rigorose garanzie a tutela dei cittadini. L'immissione in rete generalizzata e non protetta dei dati di tutti i contribuenti italiani (non sono stati previsti *"filtri"* per la consultazione *on-line*) da parte dell'Agenzia delle entrate ha comportato una serie di conseguenze: la centralizzazione della consultazione a livello nazionale ha consentito, in poche ore, a numerosissimi utenti, non solo in Italia ma in ogni parte del mondo, di accedere a innumerevoli dati, di estrarne copia, di formare archivi, di modificare ed elaborare i dati stessi, di creare liste di profilazione e di immettere ulteriormente dati in circolazione, ponendo a rischio la loro stessa esattezza. Tale modalità ha, inoltre, dilatato senza limiti il periodo di conoscibilità di dati che la legge stabilisce invece in un anno.

L'Autorità ha poi rilevato che non è stato chiesto al Garante il parere preventivo prescritto per legge.

Con il medesimo *provvedimento*, l'Autorità ha altresì specificato che va ritenuta illecita anche l'eventuale ulteriore diffusione dei dati dei contribuenti da parte di chiunque li abbia acquisiti, anche indirettamente, dal sito Internet dell'Agenzia. Tale ulteriore diffusione può esporre a conseguenze di carattere civile e penale. Il Garante ha tuttavia ribadito che resta fermo il diritto-dovere dei mezzi di informazione di rendere noti i dati delle posizioni di persone che, per il ruolo svolto, sono o possono essere di sicuro interesse pubblico, purché

tali dati vengano estratti secondo le modalità attualmente previste dalla legge.

Il Garante ha, inoltre, contestato all'Agenzia, con separato *provvedimento*, l'assenza di un'idonea informativa ai contribuenti riguardo alla forma adottata per la diffusione dei loro dati, anche al fine di determinare la relativa sanzione amministrativa.

Ai sensi della recente modifica dell'art. 69 del d.P.R. 29 settembre 1973, n. 600 (*cfr.* art. 42, d.l. 25 giugno 2008, n. 112, convertito con la l. 6 agosto 2008, n. 133), durante l'anno di deposito degli elenchi presso i comuni e gli uffici dell'Agenzia, è ora ammessa la visione e l'estrazione di copia degli elenchi nei modi e con i limiti stabiliti dalla disciplina in materia di accesso ai documenti amministrativi, nonché da specifiche disposizioni di legge. Al di fuori di tali casi, la comunicazione o diffusione, totale o parziale, con qualsiasi mezzo, degli elenchi o dei dati personali ivi contenuti, ove il fatto non costituisca reato, è punita con una sanzione amministrativa.

In risposta alle segnalazioni pervenute sull'argomento l'Ufficio ha richiamato i contenuti del suddetto *provvedimento* del 6 maggio 2008, e la successiva evoluzione normativa.

Il Garante, da ultimo, ha chiesto all'Agenzia di far conoscere se, in seguito alle suddette modifiche normative in materia, siano state fornite indicazioni agli uffici e ai comuni in ordine alle modalità di visione e di estrazione di copia degli elenchi (*Nota* del 20 febbraio 2009).

Società di gestione del risparmio

Su richiesta dell'Agenzia delle entrate il Garante ha espresso parere favorevole in ordine ad uno schema di provvedimento che individua le modalità e i termini per la segnalazione dell'omessa comunicazione alle società di gestione del risparmio da parte dei partecipanti a fondi immobiliari delle informazioni necessarie ai fini dell'applicazione della prevista imposta patrimoniale (*Parere* del 19 dicembre 2008 [doc. *web* n. 1584260]).

"Scontrino fiscale parlante"

Nel corso del 2008 il Garante ha esaminato le numerose segnalazioni relative dal trattamento dei dati personali connessi al *cd. "scontrino fiscale parlante"* che comporta il trattamento di dati personali del contribuente idonei a rivelarne le specifiche patologie. È previsto, infatti, che sullo scontrino per beneficiare delle agevolazioni fiscali siano indicati, oltre al codice fiscale del destinatario anche l'espressa menzione della denominazione commerciale del farmaco. In particolare, il Garante ha coinvolto nell'istruttoria

l'Agenzia delle entrate e Federfarma al fine di individuare, nel rispetto della normativa, una diversa tipologia di informazioni – rilevabili dal farmacista mediante la lettura ottica del codice a barre del farmaco acquistato – che potrebbero essere utilmente riportate sullo stesso scontrino fiscale quale univoca individuazione del bene acquistato. È in corso l'istruttoria.

Sanzioni in materia valutaria

L'Unità di informazione finanziaria della Banca d'Italia ha comunicato all'Autorità, ai sensi degli artt. 19, comma 2, e 39 del Codice, l'intenzione di trasmettere alla Guardia di finanza, all'Agenzia delle dogane ed al Ministero dell'economia e delle finanze i dati riguardanti l'estinzione in via breve dei procedimenti sanzionatori disposti tra il 1° gennaio ed il 31 dicembre 2008 per violazione dell'obbligo di dichiarazione, previsto in capo a chiunque effettui movimenti di denaro contante, titoli o valori mobiliari di importo superiore a diecimila euro in entrata o in uscita dal territorio nazionale. Pur in assenza di una espressa previsione di legge o di regolamento tale comunicazione è stata ritenuta necessaria a garantire il coordinamento dell'attività sanzionatoria per la violazione degli obblighi dichiarativi stabiliti dal quadro normativo di riferimento. Per quanto riguarda, invece, la realizzazione di un sistema informatico sui movimenti transfrontalieri di denaro, è stato ribadito che lo scambio di dati personali tra le autorità competenti deve in ogni caso avvenire nel rispetto del Codice (*Nota* del 14 gennaio 2009).

3.6. TRATTAMENTI EFFETTUATI PRESSO REGIONI ED ENTI LOCALI

Le questioni riguardanti il trattamento dei dati personali presso gli enti locali hanno evidenziato problematiche eterogenee.

Da una segnalazione, è emerso che un comune, nell'informare i cittadini di determinate fasce di età sull'attivazione di un servizio relativo a differenti problematiche legate al benessere psico-fisico, aveva inserito un opuscolo intitolato "*La salute delle donne: benessere in menopausa*" in un involucro trasparente, recante un'etichetta con le generalità e l'indirizzo dei destinatari. L'amministrazione comunale è stata interessata per evitare che, in eventuali analoghe circostanze future, le missive recassero segni o indicazioni dai quali potesse desumersi il contenuto dell'atto, al fine di rispettare il principio di per-

tinenza, non eccedenza ed indispensabilità (artt. 11 e 22, comma 3, del Codice) (*Nota* 29 luglio 2008).

Secondo talune testate giornalistiche, clienti di prostitute sarebbero stati ripresi dal sindaco di un comune mediante apparecchiature video fotografiche, a fini di deterrenza e controllo. Dall'istruttoria preliminare non sono emerse violazioni del Codice in quanto il sindaco, interpellato, ha dichiarato che non erano state fotografate persone e che non risultavano leggibili le targhe delle poche auto transitate durante lo scatto di alcune istantanee, inviando documentazione fotografica a conferma di quanto dichiarato (*Nota* 22 dicembre 2008).

Un segnalante ha lamentato la comunicazione da parte di un comune, a volontari del servizio civile operanti nell'ambito di un progetto in favore di soggetti disabili, di dati anche sensibili riguardanti il segnalante stesso ed il figlio, minore di età e diversamente abile. Il comune ha fornito idonee assicurazioni sul rispetto della disciplina, in particolare, dichiarando di aver designato con atto scritto, quali incaricati del trattamento, i privati dei quali si era avvalso per lo svolgimento di attività istituzionali, che restano nella titolarità dell'amministrazione (art. 30 del Codice) (*Nota* 11 luglio 2008).

Da una segnalazione riguardante la raccolta da parte di un comune dei dati personali riguardanti dei richiedenti l'iscrizione al servizio di refezione scolastica, è emerso che i dati venivano trattati per finalità diverse (invio di comunicazioni commerciali) rispetto all'erogazione del predetto servizio, con richiesta del consenso dell'interessato. Al comune è stato fatto presente che i soggetti pubblici possono trattare dati personali solo per lo svolgimento delle funzioni istituzionali (art. 18, comma 2, del Codice), tra le quali non rientra la predetta finalità; che essi non devono richiedere il consenso degli interessati (art. 18, comma 4), ma rendere comunque un'informativa completa (art. 13 del Codice) (*Nota* 22 dicembre 2008).

Tra i casi più rilevanti, una segnalazione ha paventato l'accesso di taluni consiglieri comunali ad informazioni detenute dal Comune di Bolzano riguardanti i minori frequentanti le scuole materne comunali tedesche, idonei a rivelarne l'appartenenza etnico-linguistica sulla base dei cognomi, al fine stabilire se negli asili di lingua tedesca fossero iscritti troppi minori

di lingua italiana ed introdurre eventuali limitazioni in base alla predetta appartenenza.

Nell'istruttoria preliminare è emerso che la trasmissione delle informazioni da parte del comune a gruppi consiliari era avvenuta in base all'art. 13 d.P.Reg. 1 febbraio 2005, n. 3/L (che disciplina il diritto di accesso dei consiglieri comunali a tutte le notizie e le informazioni in possesso del comune di appartenenza). I gruppi consiliari, da parte loro, hanno dichiarato di aver chiesto i dati (nome cognome, indirizzo e data di nascita dei bambini) solo per espletare i compiti connessi al mandato elettivo, in particolare per verificare il rispetto dei criteri di ripartizione dei minori tra le scuole sulla base della residenza, ma non al fine di individuarne l'appartenenza etnico-linguistica.

In proposito è stata evidenziata, ad ogni buon conto, l'esigenza di rispettare la normativa sulla raccolta delle dichiarazioni di appartenenza etnico-linguistica che devono essere rilasciate esclusivamente dai cittadini di età superiore agli anni diciotto, qualora intendano beneficiare, nei casi previsti, degli effetti giuridici derivanti dall'appartenenza o dall'aggregazione al gruppo medesimo (*v.* art. 20-*ter* del d.P.R. 26 luglio 1976, n. 752). Nel precisare che i dati richiesti dai consiglieri non possono essere utilizzati al fine di individuare l'appartenenza linguistica dei minori, in considerazione delle dichiarazioni pervenute in ordine al loro utilizzo da parte dei consiglieri comunali, non sono stati adottati specifici provvedimenti dell'Autorità, in quanto non sono stati ravvisati gli estremi di una violazione della disciplina rilevante in materia di protezione dei dati personali (*v.* art. 11, comma 1, punti 2 e 4, e art. 13, comma 4, del regolamento del Garante 1/2007 del 14 dicembre 2007) (*Nota* 12 gennaio 2009).

Una provincia autonoma ai fini dell'applicazione del Codice, aveva chiesto se una società da essa istituita e preposta al servizio pubblico di edilizia abitativa, doveva considerarsi quale soggetto pubblico o privato. In proposito è stato chiarito che la qualificazione giuridica della predetta società esula dall'ambito di competenza del Garante. In ogni caso, è stato ricordato che, ai fini dell'applicazione delle disposizioni in materia di tributi, Equitalia S.p.A. e le società dalla stessa partecipate sono state equiparate ai soggetti pubblici ai sensi del Codice dall'art. 3, comma 29, d.l. 30 settembre 2005, n. 203, come modificato dalla legge di conversione 2 dicembre 2005, n. 248 (*Nota* 2 ottobre 2008).

Un interessato lamentava che dati personali riguardanti i destinatari di verbali di contravvenzione per infrazioni al codice della strada fossero trattati da un soggetto – esterno al comune competente – incaricato della rilevazione delle predette infrazioni, nonché dell'elaborazione e trasmissione dei verbali di contestazione. Al riguardo sono state richiamate le regole in base alle quali, nello svolgimento dei compiti istituzionali, ciascun soggetto pubblico può avvalersi di privati, affidando ad essi attività che restano nella titolarità dell'amministrazione. In tale ipotesi il soggetto privato è vincolato ad utilizzare i dati per le sole finalità perseguite dall'amministrazione in base al particolare regime previsto per quest'ultima e deve essere designato per iscritto quale responsabile del trattamento (art. 29 del Codice). In mancanza di tale designazione, la trasmissione di dati personali al soggetto esterno si configura come una comunicazione, in quanto tale assoggettata alle norme più stringenti previste per tale operazione (art. 19, comma 3, del Codice). Il cittadino è stato quindi invitato ad esercitare i diritti di cui all'art. 7 del Codice nei confronti del comune, per ottenere l'indicazione dei soggetti o delle categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di responsabili o incaricati (*Nota* 16 giugno 2008).

Con riferimento alla lamentata comunicazione di dati personali non pertinenti ed eccedenti da parte di un segretario comunale ad un difensore civico regionale nell'ambito della definizione di un ricorso pendente presso l'autorità giudiziaria è stata riscontrata una condotta non conforme alla disciplina applicabile. Tuttavia, in considerazione delle assicurazioni rese dal sindaco, per quanto riguarda il rispetto, per il futuro, del Codice, non è stata promossa l'adozione di specifici provvedimenti da parte del Garante relativamente al caso di specie (*v.* artt. 11, comma 1, punto 4, e 13, comma 4, del regolamento n. 1/2007) (*Nota* 22 dicembre 2008).

Un comune ha prospettato all'Ufficio l'intenzione di istituire un servizio di ricezione delle prescrizioni farmaceutiche ripetibili dei singoli cittadini, per recapitarle ai rispettivi medici di medicina generale per la nuova prescrizione, da distribuire poi agli interessati a cura degli uffici comunali, in buste chiuse e singole. In proposito, in particolare, è stata ricordata la necessità di fornire agli utenti interessati una idonea informativa, che illustri

in particolare la volontarietà dell'adesione al servizio (art. 13 del Codice). È stato poi sottolineato che i medici di medicina generale coinvolti nel progetto possono consegnare le prescrizioni farmaceutiche a persone diverse dal diretto interessato solo in busta chiusa sulla base di una delega scritta di quest'ultimo (*v. Provv.* 9 novembre 2005 [doc. *web* n. 1191411] *v. Relazione* 2005, *p.* 44). In caso di mancato ritiro da parte dell'utente, le singole buste chiuse devono essere riconsegnate al medico entro un congruo termine, in quanto il comune non deve trattenere alcuna informazione, neanche tramite la compilazione di un apposito registro, riguardante il flusso di dati oggetto del predetto servizio. I menzionati documenti devono poi essere custoditi e controllati, in modo da ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati stessi, ovvero non autorizzato accesso ad essi o di trattamento non consentito (artt. 31 e *ss.* del Codice) (*Nota* 18 febbraio 2009).

In diversi casi soggetti pubblici hanno comunicato al Garante l'intenzione di attivare flussi di dati personali, diversi da quelli sensibili e giudiziari, verso altri soggetti pubblici per lo svolgimento di funzioni istituzionali, in assenza di una norma di legge o di regolamento (artt. 19, comma 2, e 39, comma 1, lett. *a*), del Codice).

In particolare, un comune aveva dichiarato di voler trasmettere ad un'altra amministrazione comunale i dati personali contenuti nella graduatoria per l'assunzione a tempo determinato di educatori nel servizio comunale di asilo nido, affinché l'amministrazione destinataria potesse reperire personale supplente anche per il proprio servizio. La comunicazione, – in quanto necessaria per consentire all'amministrazione ricevente di svolgere le sue funzioni di gestione dei servizi sociali e di instaurazione e gestione di rapporti di lavoro (l. 6 dicembre 1971, n. 1044; artt. 88 e *ss.* d.lg. 18 febbraio 2000, n. 267; d.lg. 30 marzo 2001, n. 165) – è stata ammessa a condizione che il comune medesimo rendesse un'idonea informativa agli interessati evidenziando, in particolare, il diritto di opporsi per motivi legittimi al trattamento (artt. 13 e 7, comma 4, lett. *a*), del Codice) (*Nota* 30 ottobre 2008).

Ad una società che aveva manifestato l'intenzione di trasmettere i dati degli utenti dei servizi di somministrazione di gas e/o acqua ad un'altra società che svolge, per conto di taluni comuni, attività di controllo e accertamento tributario, è stato evidenziato che la

comunicazione di dati personali ai sensi degli artt. 19, comma 2, e 39, è ammissibile solo quando il flusso di dati venga effettuato fra soggetti pubblici. Comunque, nel provvedimento del Direttore dell'Agenzia delle entrate concernente le modalità di partecipazione dei comuni all'accertamento fiscale (adottato il 3 dicembre 2007, in *G.U.* 17 dicembre 2007 n. 292, previo *Parere* favorevole del Garante [doc. *web* n. 1428047] *v. Relazione* 2007, *p.* 50) è previsto che, entro tre mesi dalla data della pubblicazione, l'Agenzia delle entrate renda disponibili ai comuni che ne facciano richiesta i flussi informativi relativi contratti di somministrazione di energia elettrica, gas e acqua disponibili in anagrafe tributaria (*Nota* 22 settembre 2008).

Un sindacato ha reclamato il trattamento, da parte del Consiglio della Provincia autonoma di Bolzano, di dati personali relativi all'origine etnica di lavoratori iscritti ai sindacati, con riferimento alla procedura di riconoscimento della maggiore rappresentatività ai sensi dell'art. 9 del d.P.R. 6 gennaio 1978, n. 58. In tale ambito è emerso che il Consiglio ha effettuato il menzionato accertamento della maggior rappresentatività sindacale per la prima e unica volta, nel 1978; che nessun dato sensibile dei lavoratori aderenti a sindacati era stato a suo tempo acquisito d'ufficio dal Consiglio provinciale e che, infine, l'amministrazione consiliare, allo stato, non tratta dati personali connessi alla procedura di cui in oggetto.

Sentite le parti e non essendo emersi nuovi elementi, non sono state intraprese iniziative per l'adozione di specifici provvedimenti da parte dell'Autorità, non essendo stati ravvisati gli estremi di una violazione nella procedura posta in essere dal Consiglio della Provincia autonoma di Bolzano. Con l'occasione si è ritenuto opportuno precisare che eventuali nuovi trattamenti di dati sensibili nell'ambito della suddetta procedura dovranno avvenire nel rispetto delle garanzie di cui agli artt. 20 e 22 del Codice, previo conforme parere del Garante.

Diffusione di dati personali contenuti in documenti pubblici tramite Internet

Una segnalazione inviata da un Comune lamentava l'avvenuta pubblicazione, su sito *web* non direttamente riconducibile al comune medesimo, di dati personali concernenti contributi erogati dall'Amministrazione per l'acquisto di libri di testo per l'anno scolastico 2005/2006, e, in particolare, l'ammontare del contributo nonché, in taluni casi, le coordinate del relativo conto corrente bancario.

Le risultanze istruttorie hanno evidenziato che la lista dei destinatari dei contributi era stata divulgata via Internet dal capogruppo consiliare di minoranza (cui una copia era stata precedentemente consegnata in ragione di asserite motivazioni concernenti l'esercizio del proprio mandato politico) e che tale divulgazione consentiva l'immediata accessibilità a chiunque alle citate informazioni tramite mera ricerca nominativa dei beneficiari, anche con l'ausilio di eventuali motori di ricerca.

In proposito, si è rilevato che i consiglieri comunali che abbiano avuto accesso ad atti dell'amministrazione comunale per ragioni connesse all'espletamento del loro mandato devono rispettare il diritto alla riservatezza degli interessati. Poiché il trattamento dei menzionati dati è risultato, allo stato degli atti, in violazione dei princìpi di liceità, finalità e pertinenza e non eccedenza (art. 11, comma 1, lett. *a*), *b*) e *d*), del Codice), è stato disposto il blocco del relativo trattamento nelle more della definizione di ulteriori accertamenti da parte dell'Autorità (*Provv.* 28 febbraio 2008 [doc. *web* n. 1501081]).

3.7. L'ATTIVITÀ GIUDIZIARIA

Pubblicità dei dati nei procedimenti di espropriazione forzata

Anche nel 2008 sono pervenute al Garante numerose segnalazioni relative al regime di pubblicità nell'ambito dei procedimenti di espropriazione forzata introdotto dalla riforma del processo esecutivo (decreto-legge 14 marzo 2005, n. 35, convertito, con modificazioni, dalla legge 1 maggio 2005, n. 80), che prevede la pubblicazione in appositi siti Internet di copia dell'ordinanza del giudice che dispone sulla vendita forzata e della relazione di stima dei beni da espropriare. Gli interessati hanno in particolare lamentato la diffusione dei nominativi dei debitori sottoposti alle procedure esecutive e talvolta di terzi (*ad es.*, dei proprietari di porzioni immobiliari confinanti con l'immobile dell'esecutato).

Nel fornire riscontro a tali segnalazioni il Garante ha richiamato il *provvedimento* del 7 febbraio 2008 ([doc. *web* n. 1490838], *v. Relazione* 2007, *p.* 55) sull'esigenza di omettere nelle copie pubblicate sia dell'avviso di vendita, sia delle ordinanze e delle relazioni di stima, l'indicazione delle generalità e di ogni altro dato personale idoneo a rivelare l'identità del debitore e di eventuali soggetti terzi non previsto dalla legge e comunque non pertinente rispetto alla procedura in corso.

Mezzi di prova

Continuano a pervenire all'Autorità numerose segnalazioni in ordine all'ammissibilità delle prove dedotte nell'ambito di procedimenti giudiziari.

Al riguardo, è stato ribadito che non spetta al Garante, ma al giudice, secondo le pertinenti disposizioni processuali, valutare la validità, l'efficacia e l'utilizzabilità di atti, documenti e provvedimenti nel procedimento giudiziario anche se basati su un trattamento di dati personali non conforme a disposizioni di legge o di regolamento (art. 160, comma 6, del Codice).

Consulenti e periti dell'autorità giudiziaria

Con le *"Linee-guida in materia di trattamento di dati personali da parte dei consulenti tecnici e dei periti ausiliari del giudice e del pubblico ministero"* (*Provv.* 26 giugno 2008 [doc. *web* n. 1534086]) il Garante ha individuato un quadro unitario di misure e di accorgimenti relativi ai trattamenti di consulenti tecnici e periti dall'Autorità giudiziaria. Tali trattamenti – che, in quanto direttamente correlati alla trattazione dei processi, sono svolti "*per ragioni di giustizia*" (art. 47, comma 2, del Codice) – devono svolgersi nel rispetto dei princìpi di cui all'art. 11 del Codice, e adottando le necessarie misure di sicurezza (artt. 31 e *ss.* e disciplinare tecnico Allegato B. al Codice).

Il consulente e il perito possono raccogliere e trattare lecitamente i dati personali nei limiti di quanto strettamente necessario all'adempimento dell'incarico ricevuto. Le relazioni e le informative fornite al magistrato ed, eventualmente, alle parti, non devono riportare dati, in particolare se di natura sensibile o di carattere giudiziario, non pertinenti all'oggetto della perizia, né contenere informazioni personali di soggetti estranei al procedimento. Le informazioni acquisite nel corso dell'accertamento possono essere comunicate alle parti con le modalità e nel rispetto dei limiti fissati dalle norme sulla segretezza e riservatezza degli atti processuali. Eventuali comunicazioni di dati a terzi, se ritenute indispensabili per le finalità dell'indagine, devono rispettare quanto stabilito per legge o essere preventivamente autorizzate dal magistrato.

L'eventuale utilizzo incrociato dei dati è consentito se chiaramente collegato alle indagini che sono state delegate e se autorizzato dalle singole Autorità giudiziarie interessate.

Per quanto concerne la conservazione dei dati, una volta espletato l'incarico l'ausiliario deve depositare non solo la propria relazione, ma anche la documentazione fornitagli dal

magistrato e quella ulteriore acquisita nel corso dell'attività svolta. Al di fuori delle ipotesi stabilite dalla legge o da specifiche autorizzazioni del magistrato, il consulente e il perito non possono conservare, in originale o in copia, in formato elettronico o su carta, le informazioni personali raccolte nel corso dell'incarico.

Infine, fino al momento della consegna al giudice o al pubblico ministero delle risultanze dell'attività svolta, consulenti e periti sono obbligati ad adottare misure tecniche ed organizzative volte ad evitare un'indebita divulgazione delle informazioni o la loro perdita o distruzione.

Notificazioni di atti e comunicazioni

Anche nel 2008, l'Autorità, in risposta alle numerose segnalazioni che hanno lamentato modalità di notificazione di atti giudiziari, verbali di contravvenzione e avvisi fiscali non conformi alle prescrizioni del Codice, ha in particolare richiamato l'attenzione degli uffici interessati (U.n.e.p.) al rispetto scrupoloso della vigente normativa posta a tutela della riservatezza dei destinatari degli atti e all'adozione di misure idonee ad evitare il ripetersi di episodi di conoscenza dei dati da parte di terzi non autorizzati. L'art. 174 del Codice prevede infatti che, qualora la notificazione non possa essere eseguita nelle mani del destinatario, la copia dell'atto debba essere consegnata in busta sigillata e su questa non debbano essere apposte indicazioni da cui possa desumersi il contenuto dell'atto.

4. La sanità

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

4.1.1. I trattamenti per fini amministrativi

Nel corso del 2008 l'Autorità è più volte intervenuta in merito al trattamento dei dati sanitari effettuato da soggetti pubblici e privati per finalità di prevenzione, diagnosi, cura e riabilitazione dell'interessato.

Per quanto concerne la manifestazione del consenso dell'interessato, è stato ribadito che questo è indispensabile per procedere al trattamento dei dati sanitari per finalità di cura e che deve essere richiesto all'interessato prima dell'erogazione della prestazione sanitaria, fatti salvi i casi di prestazioni d'urgenza o di richieste dell'Autorità giudiziaria (*Nota* 4 dicembre 2008).

Con riferimento al trattamento dei dati personali effettuato da un centro trasfusionale del nord Italia, l'Ufficio ha ricordato che la comunicazione alle associazioni di volontariato dei dati anagrafici e del giudizio di idoneità/non idoneità alla trasfusione relativi al volontario donatore iscritto deve essere limitata solo a tali informazioni (e non anche ai risultati delle analisi ematologiche effettuate) e può avvenire solo previo consenso dell'interessato, che deve essere manifestato, di volta in volta e in forma specifica (*Nota* 26 maggio 2008).

L'Ufficio è stato inoltre interessato in merito alla possibilità che i farmacisti possano chiedere alla donna che intenda acquistare un medicinale ad uso sistemico contenente isotretinoina di esibire il *test* di gravidanza. Al riguardo, è stato osservato che, anche in relazione a quanto indicato nel "*Programma di prevenzione del rischio teratogeno*" approvato dall'Aifa – pubblicato in *G.U.* 9.11.2005, n. 261 – non risulta sussistere a carico del farmacista alcun onere di controllare l'assenza di uno stato di gravidanza della donna che intenda acquistare tali medicinali, permanendo, invece, il compito di dispensare detti medicinali solo dietro presentazione di ricetta medica nei tempi di validità della ricetta stessa e limitatamente al fabbisogno mensile ivi riportato (*Nota* 27 aprile 2008).

In una prospettiva di modernizzazione del sistema sanitario pubblico e privato si col-

loca l'istituzione di un Fascicolo sanitario elettronico (Fse) del cittadino, idoneo ad attuare tra professionisti e organismi sanitari che intervengono nella storia clinica dell'individuo una condivisione informatica dei documenti sanitari che lo riguardano e che, nel corso del tempo, vengono formati e aggiornati. In considerazione della peculiarità della condivisione tra soggetti diversi e della natura delle informazioni trattate, l'Autorità ha predisposto delle linee-guida, al fine di delineare precise forme di tutela per i trattamenti dei dati personali ed, in particolare, di quelli idonei a rivelare lo stato di salute effettuati tramite il Fse. Attesa la particolare complessità e delicatezza dei trattamenti in parola, il citato documento è stato, dapprima, sottoposto alla consultazione del gruppo di lavoro all'uopo costituito presso il Ministero del lavoro, della salute e delle politiche sociali al fine di acquisire opportune osservazioni in ordine agli accorgimenti e alle misure previste e alle relative modalità attuative (22 gennaio 2009). Al termine di tale attività consultiva il documento, aggiornato alla luce delle osservazioni emerse e prima della definitiva adozione, è stato sottoposto a consultazione pubblica in data 5 marzo 2009 [doc. *web* n. 1598313].

Il documento contenente le linee-guida in tema di fascicolo sanitario elettronico e *dossier* sanitario che avrà origine all'esito della consultazione pubblica dovrebbe costituire, da un lato, uno strumento di riferimento per i soggetti pubblici e privati che si accingono a porre in essere iniziative in materia di Fse e, dall'altro, una rete di garanzie per i cittadini che acconsentiranno alla costituzione di un fascicolo sanitario relativo alla propria storia clinica. Il Fse, infatti, costituito esclusivamente per il perseguimento di finalità di prevenzione, diagnosi, cura e riabilitazione dell'interessato, dovrà essere uniformato al principio di autodeterminazione (artt. 75 e *ss.* del Codice); all'interessato dovrà essere consentito di scegliere in piena libertà se far confluire o meno le informazioni cliniche che lo riguardano in un fascicolo elettronico, garantendo anche la possibilità che i suoi dati sanitari restino disponibili solo per il professionista o l'organismo sanitario che li ha redatti, senza la loro necessaria inclusione in un fascicolo sanitario condiviso.

La centralità del consenso dell'interessato è stata ribadita dall'Ufficio anche nei confronti di una regione del nord Italia, che ha così provveduto a semplificare ulteriormente

il linguaggio dell'informativa allo scopo di evidenziare la facoltatività della costituzione del fascicolo elettronico (*Nota* 11 giugno 2008).

Sulla tematica del Fse l'Autorità ha preso parte a diversi tavoli di lavoro aperti, come anzidetto, con il Ministero del lavoro, della salute e delle politiche sociali, con alcune regioni e con la Presidenza del Consiglio dei Ministri (*Note* del 2 ottobre 2008, del 18 luglio 2008 e del 10 luglio 2008).

Con riferimento alla notizia riportata sulla stampa nazionale relativa alla pubblicazione sul *social network Facebook* di fotografie che ritraggono pazienti e operatori del pronto soccorso, sono stati avviati accertamenti ispettivi presso un'Azienda ospedaliera di Torino. All'esito dell'esame preliminare delle risultanze ispettive, l'Ufficio non ha riscontrato violazioni della disciplina sulla protezione dei dati personali da parte dell'Azienda. L'Autorità ha comunque deciso di invitare l'Azienda a intensificare l'attività formativa dei dipendenti in materia di protezione dei dati personali, in conformità alla pianificazione prevista sul tema, anche con iniziative di *e-learning*, in considerazione della complessità organizzativa della struttura.

All'esito del completamento dell'istruttoria, il Garante si è riservato di valutare il rispetto delle prescrizioni contenute nelle "*Linee-guida del Garante per posta elettronica e Internet*" del 1° marzo 2007 [doc. *web* n. 1387522] e della disciplina sui controlli a distanza dei lavoratori (artt. 113, 114 e 184, comma 3, del Codice; artt. 4 e 8, l. 20 maggio 1970, n. 300), con riferimento all'accertato periodo di conservazione dei dati personali relativi agli accessi al traffico telematico da parte dei lavoratori dell'ospedale (*Note* 27 e 30 gennaio 2009).

Muovendo da un interpello presentato al Garante da una cooperativa farmaceutica, l'Ufficio ha deciso di avviare specifici approfondimenti, anche ispettivi, sul tema più generale dei trattamenti di dati finalizzati alla fidelizzazione della clientela delle farmacie aderenti. Tale progetto si basa su l'istituzione di una banca dati contenente dati personali relativi alla salute e alla vita sessuale dei clienti, con riferimento dettagliato ai prodotti acquistati.

L'Ufficio ha sollecitato la cooperativa a valutare ulteriormente profili quali l'effettiva

natura "*anonima*" dei dati di carattere socio-demografico, la vendita di prodotti associata ai codici delle tessere fedeltà, la congruità delle ipotizzate finalità di facilitazione del sistema delle agevolazioni fiscali per l'acquisto di farmaci rispetto a quanto previsto dalle recenti modifiche normative in materia (art. 39, comma 3, d.l. 1° ottobre 2007, n. 159 convertito in l. 29 novembre 2007, n. 222), l'idoneità dei modelli di informativa e consenso predisposti, nonché l'adeguatezza degli accorgimenti previsti per impedire che i dati riferiti al dettaglio dei prodotti acquistati dagli interessati fossero utilizzati a fini di profilazione o di *marketing* diretto in violazione delle indicazioni fornite dal Garante sulle carte fedeltà (*Provv.* 24 febbraio 2005 [doc. *web* n. 1103045], punti 2 e 4, delle autorizzazioni generali n. 2 e 5/2008, nonché art. 5, c. 2 e 3, d.l. 4 luglio 2006, n. 223 convertito in l. 4 agosto 2006, n. 248) (*Nota* del 23 gennaio 2009).

L'Autorità sta valutando l'adozione di un provvedimento che regolamenti la materia in modo specifico.

I trattamenti per fini amministrativi correlati all'attività di cura

Nel corso del 2008 il Garante ha continuato ad esaminare i trattamenti di dati sensibili e, in particolare, di quelli idonei a rivelare lo stato di salute, effettuati da parte di strutture sanitarie pubbliche per finalità amministrative correlate a quelle di prevenzione, diagnosi, cura e riabilitazione dei soggetti assistiti dal Servizio sanitario nazionale (art. 85, comma 1, lett. *a*), del Codice).

In particolare, è stato più volte ricordato che le strutture sanitarie pubbliche devono richiedere il consenso dell'interessato solo per il trattamento di dati personali effettuato per finalità di cura, mentre questo non è richiesto per le correlate finalità amministrative. In questo caso vanno tuttavia rispettati i limiti e le garanzie individuate nei regolamenti regionali adottati in conformità allo schema-tipo di regolamento per i trattamenti dei dati sensibili e giudiziari da effettuarsi presso le regioni e le province autonome, le aziende sanitarie, gli enti regionali/provinciali, gli enti vigilati e controllati dalle regioni e dalle province autonome, su cui il Garante ha espresso parere favorevole (*Provv.* 13 aprile 2006 [doc. *web* n. 1272225]).

A seguito dell'intervento dell'Ufficio un'azienda sanitaria del nord Italia ha modificato i modelli di informativa e di consenso utilizzati nei rapporti con i pazienti, al fine di

meglio descrivere le finalità perseguite, distinguendo in particolare tra quelle di cura della salute e quelle amministrative ad esse correlate (*Nota* 4 dicembre 2008).

Con riferimento alla possibilità che le aziende termali comunichino alle aziende sanitarie territorialmente competenti dati sensibili dei soggetti che hanno usufruito delle terapie, al fine di ottenere la corresponsione delle competenze spettanti, l'Ufficio ha ricordato che tale flusso di dati deve avvenire nel rispetto del principio di indispensabilità e, come previsto nel suddetto schema-tipo di regolamento, nel rispetto dell'intesa Regioni-Federterme, i cui contenuti sono regolamentati con atti formali delle singole Regioni (*Nota* 11 febbraio 2009).

L'Autorità è stata poi chiamata a fornire alcune indicazioni in merito alla richiesta di una questura lombarda di ricevere da parte dei sindaci l'elenco nominativo dei soggetti sottoposti a trattamento sanitario obbligatorio (Tso), al fine di procedere con le verifiche di legge nei confronti di coloro tra questi che fossero in possesso di una licenza di porto d'armi.

Al riguardo è stato chiarito che, allo stato degli elementi acquisiti dall'Ufficio e forniti dalla stessa questura, tale comunicazione di dati sensibili non risulterebbe autorizzata da alcuna disposizione di legge. L'Ufficio ha poi osservato che anche nello schema-tipo di regolamento per il trattamento dei dati sensibili e giudiziari dei comuni promosso dall'Anci, le questure non sono indicate tra i soggetti nei cui confronti è prevista una comunicazione di dati sensibili relativi a soggetti sottoposti a Tso (*Nota* 11 febbraio 2009).

Con riferimento al settore sanitario privato l'Ufficio, nel ribadire che il Codice prevede espressamente la possibilità di fornire in ambito sanitario un'unica informativa e di acquisire un solo consenso in merito ad una pluralità di trattamenti effettuati (*cfr.* artt. 77-81 del Codice), ha più volte ricordato che le strutture sanitarie private, a differenza delle pubbliche, devono richiedere il consenso dell'interessato sia per finalità di cura, sia per finalità amministrative ad esse correlate, eccezion fatta per i trattamenti effettuati in ottemperanza ad un obbligo di legge. Al riguardo è stata rappresentata ad un laboratorio di analisi lombardo la necessità di indicare in modo più analitico le finalità perseguite, distinguendo tra quelle amministrative e quelle di cura della salute e di richiedere uno specifico

consenso dell'interessato qualora intenda trattare i dati personali dei pazienti anche per inviare loro informazioni di carattere commerciale (*Nota* 25 febbraio 2008).

Comunicazioni ex art. 39 del Codice

Alcune comunicazioni pervenute ai sensi dell'art. 39 del Codice hanno riguardato il trattamento di dati sanitari per fini amministrativi correlati ai compiti del Servizio sanitario nazionale e degli altri organismi sanitari pubblici. Tra i casi più rilevanti va menzionato quello di un'azienda sanitaria che intendeva realizzare un'interconnessione tra dati personali detenuti da servizi sociali sanitari e da enti locali per istituire un sistema informativo del lavoro sociale (progetto Sils).

Al riguardo, l'Ufficio ha evidenziato che a tale operazione di trattamento non è applicabile la speciale disciplina prevista dall'art. 39 del Codice in quanto essa riguarda esclusivamente le comunicazioni tra soggetti pubblici aventi ad oggetto dati personali diversi da quelli sensibili, ovvero i trattamenti di dati sensibili per scopi di ricerca scientifica (artt. 19, comma 2, e 110, comma 1). Con specifico riferimento alla prospettata interconnessione, è stato precisato che occorreva fare riferimento al quadro di garanzie previsto dal Codice per i trattamenti di dati sensibili da parte dei soggetti pubblici, in conformità al quale è consentito effettuare le sole operazioni di trattamento previste da disposizioni legislative o regolamentari per perseguire finalità di rilevante interesse pubblico individuate da norme di rango primario (artt. 18, 20, 22 e 85, comma 2, del Codice).

Sul punto sono stati pertanto richiamati i limiti e le garanzie previsti dal già ricordato regolamento sul trattamento dei dati sensibili e giudiziari da effettuarsi presso le regioni, le province autonome e le aziende sanitarie (*Provv.* 13 aprile 2006 [doc. *web* n. 1272225]) invitando l'azienda, nel caso in cui valuti positivamente l'indispensabilità dell'iniziativa, a promuovere presso l'amministrazione regionale di riferimento un'eventuale integrazione al regolamento da sottoporre all'Autorità per un nuovo parere (*Nota* 16 ottobre 2008).

Anti-doping

Il Garante ha esaminato alcuni dei rilievi segnalati dall'Accpi (Associazione corridori ciclisti professionisti italiani) riguardo alla nuova normativa *anti-doping* adottata dal Coni sulla base di quanto previsto dalla Wada, l'Agenzia mondiale *anti-doping*.

In particolare, l'Accpi ha chiesto al Garante una valutazione sulle modalità individuate per la reperibilità degli atleti e sull'assenza di limiti di orario e di luogo per l'espletamento

dei controlli fuori competizione. In base alla nuova disciplina, infatti, gli atleti professionisti devono fornire alle autorità *anti-doping* alcune informazioni personali compilando un apposito modulo (*cd.* "*whereabouts*") che contiene indicazioni dettagliate relative ai propri spostamenti e alla residenza per ogni giorno dell'anno, al fine di consentire l'esecuzione di controlli a sorpresa. Tali informazioni potrebbero confluire nel previsto sistema *Adams*, progettato dalla Wada per il controllo tramite Internet delle informazioni *anti-doping* relative agli atleti.

Inoltre, secondo quanto riferisce l'Associazione, la raccolta dei dati personali viene svolta dal Coni sulla base di un'informativa inadeguata: non viene specificato se sia facoltativo o obbligatorio fornire i dati, quali potrebbero essere le conseguenze derivanti dal loro mancato rilascio, a chi questi dati possano essere comunicati.

Un ulteriore aspetto della disciplina criticato dall'Accpi riguarda i luoghi di esecuzione dei controlli: essi possono infatti svolgersi in qualsiasi luogo e in qualsiasi momento senza preavviso, anche presso il domicilio dell'atleta, consentendo così all'ispettore di acquisire informazioni potenzialmente sensibili sulla vita privata di chiunque eventualmente presente al momento del *test.*

Il Garante (*Provv.* 13 ottobre 2008 [doc. *web* n. 1563970]) ha ritenuto inidonea l'informativa utilizzata dal Coni e ne ha chiesto la riformulazione. Il Coni dovrà specificare le informazioni personali sulla localizzazione e reperibilità giornaliera che gli atleti devono conferire, in modo tale da evitare la raccolta di informazioni che possono comportare indebite interferenze nella vita privata o rivelare dati sensibili o giudiziari degli atleti o di soggetti terzi, come i familiari. Dovranno inoltre essere indicate la natura obbligatoria o facoltativa dei dati, le conseguenze derivanti dal loro mancato conferimento ed il loro ambito di comunicazione (in particolare i destinatari e la circostanza che vengano trasmessi all'estero).

Per quanto riguarda invece l'utilizzo dell'applicazione Adams, il Coni si è impegnato formalmente a non trattare i dati personali attinenti l'attività *anti-doping* attraverso tale sistema fino al momento in cui non siano state introdotte le garanzie necessarie per il compiuto rispetto della disciplina in materia di protezione dei dati personali, con particolare riferimento al loro trasferimento all'estero.

Riguardo ai luoghi di esecuzione dei controlli, il Garante ha invece preso atto degli impegni che il Coni si è assunto, di introdurre nuove istruzioni operative per gli ispettori, affinché venga prestata la massima attenzione al rispetto della riservatezza dell'atleta e dei terzi eventualmente presenti nel domicilio al momento del *test*.

La legittimità dei trattamenti di dati personali effettuati per finalità *anti-doping* anche attraverso Adams è stata peraltro oggetto del parere da parte del Gruppo art. 29 della Direttiva 95/46/Ce (*v. par.* 20.1) che ha sollevato dubbi sulla compatibilità della disciplina internazionale in materia con la normativa comunitaria sulla protezione dei dati.

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

L'Autorità è più volte intervenuta in merito alle garanzie da adottare nel trattamento di dati personali in occasione dell'accertamento dell'infezione da Hiv. Più volte sono state ricordate le specifiche previsioni della legge 5 giugno 1990, n. 135, in base alle quali la comunicazione dei referti relativi al *test* per l'Hiv, risultati degli accertamenti diagnostici diretti o indiretti, può essere data esclusivamente alla persona cui tali accertamenti si riferiscono. Tale disposizione, del 1990, poiché stabilisce rispetto alla disciplina generale divieti o limiti più restrittivi in materia di trattamento di taluni dati personali, non è stata abrogata dall'entrata in vigore del Codice.

In merito alla comunicazione ai familiari dello stato di sieropositività del paziente, è stato inoltre evidenziato che non si può prescindere dal consenso di quest'ultimo.

Al riguardo – in ottemperanza alle indicazioni del Garante intervenuto a seguito di segnalazione – un'azienda ospedaliero-universitaria di Palermo ha posto in essere le misure necessarie a dare piena attuazione alle suddette garanzie di legge (*Nota* 2 ottobre 2008).

In altra occasione è stato precisato dall'Autorità, che la normativa in materia di prevenzione e lotta contro l'Aids non prevede – in via generale – l'anonimato del *test* per accertare l'infezione da Hiv imponendo, altresì, precise cautele in relazione al trattamento del dato successivamente all'accertamento dell'infezione.

In caso di rilevazione statistica dell'infezione da Hiv vanno adottate modalità che non consentano l'identificazione della persona; analogamente gli accertamenti di infezione da

Hiv nell'ambito di programmi epidemiologici sono consentiti soltanto su campioni di sangue resi anonimi con assoluta impossibilità di pervenire all'identificazione delle persone interessate (art. 5 l. n. 135/1990).

Con riferimento alle modalità di consegna agli interessati dei risultati relativi agli accertamenti dell'infezione da Hiv, è pervenuta all'Ufficio una segnalazione con la quale si lamentava che un'azienda ospedaliera subordinava il rilascio del risultato del *test* per l'Hiv alla sottoscrizione di un registro nominativo, senza specifici accorgimenti a tutela dei diritti, delle libertà fondamentali nonché della dignità degli interessati che si erano sottoposti al *test* (art. 5 l. n. 135/1990; artt. 83, comma 2, lett. *d*) e *e*), e 178, comma 2, del Codice).

A seguito dell'intervento del Garante, l'azienda ha provveduto alla sostituzione del registro nominativo con una scheda individuale ad uso del singolo paziente, per attestare l'avvenuto ritiro dei referti relativi al *test* per l'Hiv (*Nota* 19 marzo 2008).

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

Nel periodo in esame più volte è stata segnalata all'Autorità la violazione delle misure previste dal Codice a tutela della dignità delle persone in ambito sanitario (art. 83). Già con il *provvedimento* generale del 9 novembre 2005 [doc. *web* n. 1191411] il Garante aveva richiamato gli organismi sanitari pubblici e privati al rispetto di una serie di misure volte ad assicurare il rispetto della dignità della persona e il massimo livello di tutela dei diritti del malato.

L'Autorità ha avviato un'istruttoria preliminare in relazione alle procedure adottate da organismi sanitari pubblici e privati, richiamandoli al rispetto delle norme previste dal Codice a tutela del diritto del malato. Le strutture sanitarie hanno risposto modificando le prassi in uso e adottando specifiche soluzioni più rispettose della riservatezza dei pazienti (*cfr. Newsletter* n. 317, del 19 dicembre 2008 [doc. *web* n. 1575495]).

In particolare, a seguito dell'intervento dell'Ufficio un'azienda sanitaria veneta ha migliorato la modulistica utilizzata per fini amministrativi non correlati a quelli di cura (*ad es.*, per giustificare un'assenza dal lavoro o l'impossibilità di presentarsi ad una procedura concorsuale) eliminando il riferimento al reparto che redige il certificato. Tale cau-

tela consente di evitare che soggetti estranei siano in grado di evincere l'esistenza di uno stato di salute del paziente attraverso la correlazione tra la sua identità e l'indicazione della struttura o del reparto presso cui si è recato (*Nota* 3 settembre 2008).

Per quanto riguarda la distribuzione dei referti, un ospedale universitario emiliano ha perfezionato il funzionamento e l'organizzazione delle procedure distributive. Al riguardo è stato previsto che la cartella ambulatoriale sia "*incapsulata*" in un apposito plico-contenitore munito di apposita finestrella trasparente che renda visibili all'esterno i soli dati indispensabili al ritiro del referto (*Nota* 3 settembre 2008).

Analogamente, due strutture sanitarie milanesi hanno rivisto le procedure interne affinché tutti gli esami e i referti siano correttamente imbustati e consegnati in busta chiusa al diretto interessato, ovvero a persona da lui delegata (*Note* 4 dicembre 2008 e 17 settembre 2008).

A seguito dell'intervento preliminare dell'Ufficio, una ditta fornitrice di materiale per incontinenza per conto del Servizio sanitario nazionale ha assicurato che non saranno più poste all'esterno del plico di spedizione informazioni circa il contenuto dello stesso, dalle quali si possa evincere lo stato di salute del destinatario (*Nota* 24 aprile 2008).

Al fine di prevenire l'indebita conoscenza da parte di terzi di informazioni idonee a rivelare lo stato di salute dei pazienti un ospedale milanese, su sollecitazione dell'Ufficio, ha provveduto ad effettuare corsi di formazione sulle procedure da adottare per evitare l'indebita conoscenza dei dati e per garantire che le prestazioni sanitarie non avvengano in situazioni di promiscuità (*Nota* 26 febbraio 2008).

Un policlinico universitario siciliano ha invece modificato la collocazione delle stanze adibite alle visite mediche per evitare che le informazioni sulla salute possano essere conosciute da terzi e ha introdotto, in luogo della chiamata nominativa dei pazienti, l'applicazione di un codice alfanumerico (*Nota* 7 ottobre 2008).

Interessata dall'Autorità un'azienda sanitaria pugliese ha modificato la causale degli assegni per la borsa lavoro destinati ai ragazzi con problemi e disagi psicologici, eliminando l'espressione "*liquidazione pagamento malati di mente*" e sostituendola con una formula generica (*Nota* 17 settembre 2008).

Specifiche indicazioni sono state, infine, rivolte nei confronti di alcuni medici di medicina generale per ricordare la necessità di adottare idonee cautele in occasione dei colloqui con i pazienti, affinché le informazioni sulla salute dell'interessato non possano essere conosciute da terzi presenti in sala di attesa (*Nota* 30 aprile 2008). È stato anche ribadito che le prescrizioni mediche, nell'attesa che vengano consegnate all'interessato, devono essere custodite con modalità tali da impedire che altri pazienti presenti nello studio possano averne accesso e devono essere consegnate solo al paziente o ritirate anche da persone diverse da questo, purché sulla base di una delega scritta e mediante la consegna delle stesse in busta chiusa (*Nota* 22 ottobre 2008).

5. I DATI GENETICI

Per quanto attiene al piano normativo, si è riferito nel *par.* 2.2. del decreto legislativo 3 ottobre 2008, n. 160, che consente il trattamento di dati genetici per accertare lo *status* di figlio o di coniuge ai fini del ricongiungimento con familiari, e nel paragrafo 20.2 del disegno di legge di ratifica del *cd.* "Trattato di Prüm" (d.l. n. 586) che prevede tra l'altro l'istituzione della banca dati Dna.

Per quanto riguarda l'attività propria del Garante, ad oltre un anno di applicazione dell'autorizzazione generale al trattamento di dati genetici rilasciata il 22 febbraio 2007 (*G.U.* 19 marzo 2007, n. 65 [doc. *web* n. 1389918]), non sono state rilevate sostanziali problematiche applicative tali da giustificare la revisione delle disposizioni dell'autorizzazione.

Considerata la scadenza al 31 dicembre 2008 dell'autorizzazione in parola, l'Autorità ne ha prorogato l'efficacia di dodici mesi (*G.U.* 20 gennaio 2009, n. 15 [doc. *web* n. 1582871]).

Questo anche per tener conto, nel rilascio di una nuova autorizzazione, di eventuali indicazioni e suggerimenti provenienti dal settore direttamente interessato. Al riguardo la Società di genetica umana (Sigu), all'esito del XI Congresso Nazionale, ha anticipato che intende sottoporre all'attenzione del Garante alcune proposte di modifica riguardanti, in particolare, la definizione di *"dato genetico"* tenendo conto dello sviluppo della conoscenza scientifica in materia.

È stato istituito un tavolo di lavoro con l'Ufficio del Garante e la Società di genetica umana per definire alcuni profili applicativi dell'autorizzazione generale; il Garante ha dichiarato la propria disponibilità a collaborare nell'individuazione della soluzione per assicurare un livello elevato di tutela dei diritti e delle libertà fondamentali degli interessati, conformando il trattamento dei dati genetici ai princìpi di semplificazione, armonizzazione ed efficacia (*Nota* 25 giugno 2008).

In questo ambito è stato messo a punto un modello di informativa ad uso dei laboratori di genetica al fine di informare l'interessato che si sottopone a *test* genetici circa il trattamento di dati che lo riguardano.

Per la casistica, sul *provvedimento* del 27 novembre 2008 [doc. *web* n. 1581365] rela-

tivo al trattamento di dati genetici da parte di un genitore per verificare la consanguineità del figlio, *v. par.* 12. Nel *par.* 7.2, infine, si dà conto della realizzazione, da parte dell'Arma dei Carabinieri-Reparto investigazioni scientifiche di Parma (Ris) delle misure di sicurezza volte a rafforzare, tra l'altro, il livello di protezione dei profili genetici conservati presso il Reparto (*v. Relazione* 2007, *p.* 70).

6. LA RICERCA STATISTICA E STORICA

Istat

L'Istituto nazionale di statistica ha chiesto al Garante un parere sull'aggiornamento 2009-2010 del Programma statistico nazionale (di seguito Psn) 2008-2010, già oggetto di *Parere* del Garante (*Provv.* 15 novembre 2007 [doc. *web* n. 1464806]). L'aggiornamento esaminato riguarda unicamente i prospetti identificativi dei progetti presentati per la prima volta e quelli modificati rispetto a quelli contenuti nel Programma.

Il codice deontologico di settore prevede che, qualora la raccolta di dati personali non avvenga presso l'interessato e fornire a quest'ultimo l'informativa richiede uno sforzo sproporzionato rispetto al diritto tutelato, l'informativa si considera resa se il trattamento è inserito nel Psn (art. 6, comma 2, del codice di deontologia e di buona condotta per i trattamenti di dati personali a scopi statistici e di ricerca scientifica effettuati nell'ambito del Sistan, Allegato A.3. al Codice). Nel parere il Garante ha evidenziato che tale modalità semplificata di conferimento dell'informativa deve comunque consentire all'interessato di conoscere tutti gli elementi indicati dal Codice all'art. 13 che devono essere indicati, anche cumulativamente, nei prospetti identificativi dei progetti. Per i trattamenti non inseriti formalmente nel Psn (o nei relativi aggiornamenti) l'informativa deve essere resa con altre idonee modalità.

I trattamenti di dati sensibili e giudiziari trattati nell'ambito del Psn, se non puntualmente individuati da norme di legge o di regolamento, possono essere effettuati solo previa acquisizione del parere del Garante sul Psn e se conformi a quanto riportato nei prospetti identificativi dei progetti.

A fronte delle difficoltà rappresentate negli anni passati per la corretta interpretazione del concetto di *"dato personale"* da parte dei ricercatori, il Garante ha poi invitato l'Istituto a prestare particolare attenzione alla valutazione preliminare dei progetti da inserire nel Psn, al fine di individuare correttamente il trattamento di dati personali di persone fisiche o giuridiche attraverso una puntuale disamina delle variabili rilevate o elaborate.

Il Garante ha ribadito inoltre che l'obbligo di fornire tutti i dati richiesti per le rilevazioni previste dal Psn non può riguardare i dati sensibili e giudiziari anche in caso di raccolta presso terzi; occorre in tal caso individuare modalità in concreto idonee ad assicu-

rare il rispetto dell'eventuale volontà dell'interessato di non aderire alla ricerca. In assenza di specifiche disposizioni normative che, in ipotesi, andrebbero accuratamente indicate nell'informativa agli interessati, deve essere infatti salvaguardata la volontarietà dell'adesione al trattamento dei dati personali per finalità statistiche.

Analogamente a quanto evidenziato nei pareri espressi sui precedenti programmi statistici nazionali, il Garante ha evidenziato che anche alcuni dei nuovi progetti continuano a prevedere deroghe agli obblighi di anonimizzazione dei dati dopo la raccolta e alla conservazione dei dati identificativi. L'Autorità ha pertanto invitato l'Istat ha motivare analiticamente le comprovate esigenze in relazione alle quali è necessario disporre di dati identificativi anche dopo la raccolta in casi attentamente selezionati.

Il Garante ha inoltre precisato le specifiche garanzie richieste per la comunicazione di dati sensibili e giudiziari tra i soggetti facenti parte del Sistan, che deve essere indicata nelle schede informative inserite nel Psn o in altra idonea disposizione legislativa o regolamentare (*Parere* del 22 ottobre 2008 [doc. *web* n. 1565063]).

Ricerca statistica privata

Per la ricerca statistica effettuata, al di fuori del Sistema statistico nazionale, secondo il codice di deontologia di settore (Allegato A.4. al Codice), è necessario che, oltre alle modalità di diffusione alternative prescelte, la comunicazione preventiva al Garante contenga il testo dell'informativa da pubblicare. Devono, altresì, essere indicate le ragioni che giustificano il ricorso alle forme alternative di pubblicità individuate dal codice di deontologia in rapporto alla natura dei dati raccolti o delle modalità del trattamento, ovvero degli oneri che esse comportano rispetto al tipo di ricerca svolta (art. 6, comma 5, codice di deontologia).

La valutazione del Garante avviene, peraltro, mediante l'analisi di elementi specifici del progetto di ricerca, anche in relazione alla natura e alla tipologia dei dati raccolti, ai soggetti cui gli stessi si riferiscono, all'ambito, anche territoriale, di riferimento del trattamento statistico, alle modalità di trattamento e alle garanzie adottate (*Nota* del 26 gennaio 2009).

Ricerca storica

Il Garante si è espresso positivamente su un'Intesa stipulata dalla Provincia autonoma di Trento con l'Arcidiocesi di Trento sui termini e le modalità di consultazione dell'Indice

dei nati in Trentino dal 1815 al 1923 (anno fino al quale nella predetta Regione le funzioni di stato civile erano svolte dai parroci). Tale Indice è stato elaborato attraverso la consultazione dell'Archivio diocesano Tridentino, dove sono conservati i microfilm dei registri dei nati, dei morti e dei matrimoni presenti negli archivi delle parrocchie del Trentino, inizialmente con lo scopo di agevolare la ricerca genealogica ai fini dell'evasione delle richieste certificatorie inoltrate alle parrocchie dai discendenti degli emigrati trentini per il riconoscimento della cittadinanza italiana ai sensi della l. 14 dicembre 2000, n. 379.

In particolare la previsione relativa alla comunicazione di taluni dati personali contenuti nell'Indice a soggetti previamente registrati e identificati, esclusivamente per finalità di ricerca storica, non è risultata contrastante con le norme di settore. L'Intesa non ha infatti consentito la consultazione di notizie quali separazioni, divorzi, regime patrimoniale dei coniugi, provvedimenti di inabilitazione e interdizione e cambio del nome. Inoltre, con riferimento alla madre che abbia dichiarato di non voler essere nominata, la fruibilità dei campi relativi alle generalità dei genitori può avvenire solo decorsi centotre anni dalla data di nascita delle singole persone elencate nell'Indice. Il Garante ha comunque rilevato, da un lato, che la consultazione dell'Indice deve conformarsi alle specifiche disposizioni di settore che vietano di comunicare particolari tipologie di dati personali (*cfr.*, per il rapporto di adozione, l'art. 28 della legge 4 maggio 1983, n. 184 e, per la rettificazione del sesso, l'art. 5 della legge 14 aprile 1982, n. 164); dall'altro, che l'utente deve essere reso edotto del fatto che sono consultabili esclusivamente (con le predette limitazioni normative) i dati contenuti negli atti di stato civile decorsi settanta anni dalla loro annotazione (*Provv.* 19 dicembre 2008 [doc. *web* n. 1584224]).

Sono stati altresì forniti i chiarimenti richiesti dalla Direzione centrale per i servizi demografici del Ministero dell'interno sull'accesso e la consultazione degli atti di stato civile da parte di soggetti privati che intendono effettuare ricerche storiche. La specifica disciplina di tali atti permette di accedere a notizie e informazioni anche in relazione agli atti di corrente uso, ma esclude la libera consultazione non *"filtrata"* dall'intervento dell'ufficiale dello stato civile, che pure è legittimato a fornire alcune notizie ai sensi dell'art. 450 c.c.. Se per un verso l'art. 122 del codice dei beni culturali e del paesaggio

(d.lg. 22 gennaio 2004, n. 42) si applica agli archivi storici di enti pubblici territoriali e di ogni altro ente ed istituto pubblico, alcune disposizioni sulla consultabilità dei documenti già previste per gli archivi di Stato (*cfr.* l'art. 63 del Codice), risulta alquanto problematico includere gli atti dello stato civile nella categoria degli *"affari esauriti"* (cioè, dei *"documenti"* che costituiscono gli archivi storici degli enti pubblici territoriali: art. 30 Codice beni culturali *cit.*). È apparso parimenti difficile, allo stato della vigente disciplina, stabilire quando un atto dello stato civile possa considerarsi appieno *"affare esaurito"*. Questa difficoltà deriva anche dalla circostanza secondo cui gli atti dello stato civile – anche ultrasettantennali – sono interessati nel tempo da varie annotazioni più recenti che devono figurare in essi per legge. Pertanto, l'Ufficio ha invitato il predetto Dicastero, titolare della competenza in materia, a valutare l'opportunità di promuovere un più dirimente chiarimento, anche di eventuale natura normativa (*Nota* 22 settembre 2008).

7. Attività di polizia

7.1. Il controllo sul Ced del Dipartimento di pubblica sicurezza

Si è riferito nella *Relazione* 2007 (*p.* 69) del *provvedimento* dell'8 maggio 2007, con il quale l'Autorità ha prescritto le modificazioni da apportare ai trattamenti di dati personali svolti presso il Centro elaborazione dati (Ced), 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.

Con *provvedimento* del 13 marzo 2008 sono state confermate le prescrizioni già impartite, non tutte attuate.

A seguito di segnalazioni ricevute, l'Autorità ha inoltre assicurato il riscontro da parte del Dipartimento della pubblica sicurezza e degli uffici periferici della polizia di Stato a 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 ad ulteriori attività di forze di polizia

Conservazione ed utilizzazione di dati genetici a fini di indagine giudiziaria

Il Garante ha preso positivamente atto che l'Arma dei Carabinieri-Reparto investigazioni scientifiche di Parma (Ris) ha realizzato, entro il termine stabilito, le misure di sicurezza indicate nel *provvedimento* del 19 luglio 2007, (*v. Relazione* 2007, *p.* 70), volte a rafforzare il livello di protezione dei profili genetici e dei campioni biologici acquisiti nel corso di attività di polizia giudiziaria e conservati presso il Reparto.

7.3. Il controllo sul sistema di informazione Schengen

Accertamenti disposti dal Garante

Si sono conclusi nei primi mesi del 2008 gli accertamenti (di cui si è fatto cenno nella *Relazione* 2007, *p.* 71, deliberati dal Garante con *Provv.* 8 febbraio 2007 [doc. *web* n. 1388902]) volti 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, nonché la liceità e correttezza dei trattamenti di dati personali comunque effettuati per l'attuazione della Convenzione.

Con *provvedimento* del 10 luglio 2008 il Garante, ai sensi degli artt. 154 e 160 del Codice, ha prescritto al Ministero dell'interno-Dipartimento della pubblica sicurezza alcune modificazioni da apportare ai trattamenti, con particolare riferimento alle procedure volte a garantire la liceità degli inserimenti delle segnalazioni nel sistema, l'esattezza e l'aggiornamento dei relativi dati, a individuare le figure responsabili nei vari uffici per il loro inserimento, a determinare le condizioni per la conservazione e la distruzione dei dati. Il Dipartimento deve inoltre comunicare all'Autorità l'elenco dei soggetti abilitati ad accedere al sistema e l'indicazione dei dati consultabili da ciascun soggetto.

Il Dipartimento ha fornito il richiesto riscontro, che è all'esame dell'Autorità.

Accesso diretto

Il Codice ha introdotto nuove modalità di esercizio dei diritti relativamente ai dati registrati nell'N-Sis, in virtù delle quali l'interessato 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"*). Il numero ed il contenuto delle richieste degli interessati che ancora pervengono direttamente al Garante non hanno subito sostanziali variazioni rispetto all'anno precedente (*v. Relazione* 2007 *p.* 71).

8. Attività giornalistica e tecnologie della comunicazione

8.1. Minori

Vittime di abusi

L'Autorità è intervenuta in diverse occasioni nei confronti di testate giornalistiche che, occupandosi di episodi di violenza sessuale su minori, hanno violato le specifiche garanzie poste a tutela di tali soggetti. In particolare, con riferimento a tre diversi casi di cronaca, il Garante ha riscontrato che alcuni giornali, pur omettendo nome e cognome delle vittime, avevano riportato numerosi dettagli riferibili alle vittime stesse (*ad es.*, iniziali del nome e cognome, sesso, età) e al contesto familiare e sociale di vita (*ad es.*, quartiere di residenza, tipologia di scuola frequentata, professione dei genitori e di parenti, presenza in famiglia di fratelli o sorelle e/o di animali domestici, luoghi di villeggiatura frequentati, *ecc.*) o, ancora, dati relativi all'autore della violenza (ad es., grado di parentela con la vittima, professione, stato civile *ecc.*), la cui compresenza nel servizio giornalistico (diversamente articolata nei tre casi esaminati), ad avviso dell'Autorità, era idonea a rendere identificabili le vittime stesse. Nei riguardi delle testate interessate il Garante ha, dunque, disposto un divieto del trattamento per la violazione del principio di "*essenzialità dell'informazione*" (art. 137, comma 3, del Codice) e delle specifiche disposizioni a tutela dei minori. Infatti – fermo restando il divieto di carattere generale previsto dall'art. 734-*bis* c.p., di divulgare le generalità e l'immagine della persona offesa da atti di violenza sessuale, nel caso in cui la persona offesa da un reato sia minore di età – l'ordinamento vieta la divulgazione di elementi che anche indirettamente possano portare alla sua identificazione (art.114, comma 6, c.p.p.; art. 7 del codice di deontologia relativo al trattamento dei dati personali nell'esercizio dell'attività giornalistica; Carta di Treviso) (*Provv.* 10 luglio 2008 [doc. *web* n. 1536583]; *Provv.* 2 ottobre 2008 [doc. *web* n. 1557470]; *Provv.* 16 febbraio 2009 [doc. *web* n. 1590076].

Al di fuori di episodi di cronaca così gravi, per altri tipi di notizie segnalate al Garante e coinvolgenti minori (episodi di bullismo nelle scuole, casi di risultati scolastici oggetto di vertenze giudiziarie,) l'Ufficio, pur non ravvisando i presupposti per promuovere l'adozione di un *provvedimento* di divieto, ha ritenuto comunque opportuno richiamare l'at-

tenzione delle testate interessate dalle segnalazioni sul principio, espressamente enunciato dal codice di deontologia, in base al quale il diritto del minore alla riservatezza deve sempre essere considerato come primario rispetto al diritto di critica e di cronaca (art. 7 *cit.*).

Al Garante è stato chiesto di esprimersi in merito alla diffusione di un servizio televisivo girato presso alcuni campi nomadi di Roma. L'Autorità ha osservato che, con riferimento alla scelta di riprendere scene collettive di minori, ancorché riconoscibili, la diffusione delle immagini poteva ritenersi giustificata dal principio di "*essenzialità dell'informazione riguardo a fatti di interesse pubblico*", anche alla luce della rilevante finalità di denuncia riguardo alle condizioni di disagio in cui tali minori si trovavano a crescere. Diversa, invece, è stata la valutazione per una specifica fase della trasmissione nella quale un minore riconoscibile è stato direttamente coinvolto in un'intervista su argomenti particolarmente delicati; ciò è apparso in contrasto con le indicazioni contenute al riguardo dalla Carta di Treviso richiamata espressamente dall'art. 7 del codice di deontologia.

8.2. CRONACHE GIUDIZIARIE

Anche nell'anno di riferimento sono stati esaminati numerosi casi relativi alle cronache giudiziarie.

In particolare, sono pervenute segnalazioni concernenti la pubblicazione di dati e immagini relativi alle vittime di reato, nelle quali l'Autorità ha chiarito che il limite dell'*"essenzialità dell'informazione"* va valutato con particolare rigore quando il trattamento riguardi dati personali di persone che sono state vittime di episodi criminosi. Tale rigore si giustifica anche alla luce di una specifica considerazione degli ulteriori rischi cui la diffusione di tali dati può esporre l'interessato, tanto più considerato il contesto sociale o familiare in cui egli è già inserito. In tale ambito sono stati adottati dal Collegio due provvedimenti di divieto di ulteriore diffusione nei confronti di quotidiani che avevano riportato dati eccedenti rispetto alla finalità di informazione sui reati in questione: il primo, perché aveva diffuso riferimenti idonei a identificare in modo diretto la persona offesa del reato di *"circonvenzione di incapace"*, unitamente a delicati riferimenti attinenti alle sue condizioni psichiche (*Provv.* 5 giugno 2008 [doc. *web* n. 1527037]); il secondo,

in quanto aveva diffuso riferimenti idonei a identificare una donna vittima di aggressione e di violenza sessuale da parte del coniuge (*Provv.* 13 ottobre 2008 [doc. *web* n. 1563958]).

L'Ufficio ha altresì esaminato e dato riscontro a segnalazioni e reclami riguardanti la pubblicazione di dati personali di persone sottoposte a misure cautelari, a indagini o a condanna. L'Autorità ribadendo princìpi ormai consolidati, ha chiarito che la pubblicazione dei dati relativi a procedimenti penali 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 in concreto, caso per caso, e nel rispetto delle disposizioni che tutelano il segreto delle indagini e degli atti processuali (artt. 114 e 329 c.p.p.). Si segnala, in questo ambito, il reclamo presentato da un noto personaggio, che lamentava la diffusione di dati relativi a un accertamento da parte dell'Agenzia delle entrate per evasione fiscale. Nella risposta dell'Ufficio sono stati richiamati i princìpi dell'esercizio del diritto/dovere di informazione e quello di trasparenza dell'attività giudiziaria, in base ai quali i dati relativi a persone oggetto di indagine, di regola, possono essere pubblicati, venendo in rilievo l'interesse pubblico a conoscere i fatti ivi descritti.

Tali princìpi sono stati nuovamente ricordati dal Garante in relazione altresì alla pubblicazione di intercettazioni di conversazioni telefoniche o di altro materiale di indagine, rappresentando a tutti i *media* la necessità di valutare con il massimo scrupolo e con senso di responsabilità la sussistenza dell'interesse pubblico alla eventuale diffusione delle informazioni e raccomandando il più rigoroso rispetto delle leggi in vigore, del codice deontologico e dei princìpi posti a tutela della persona (*Comunicato stampa* 2 luglio 2008). In più occasioni è stato lamentato il contenuto diffamatorio di alcune notizie pubblicate. In proposito 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.

8.3. TUTELA DELLA DIGNITÀ DELLA PERSONA E DIFFUSIONE DI INFORMAZIONI RELATIVE ALLE ABITUDINI SESSUALI

Il Garante si è occupato della cronaca relativa all'omicidio della studentessa inglese avvenuto a Perugia il 2 novembre 2007.

Già nel corso del 2008 l'Autorità era intervenuta nei confronti di un'emittente televisiva che aveva diffuso alcune immagini del corpo della giovane raccolte dalla Polizia scientifica durante uno dei sopralluoghi sul luogo dell'omicidio. Il Garante ha ritenuto che la diffusione delle predette immagini non fosse giustificata dal punto di vista dell'"*essenzialità dell'informazione riguardo a fatti di interesse pubblico*" e fosse gravemente lesiva della dignità della persona e ne ha, pertanto, vietata l'ulteriore diffusione.

Il Garante ha poi ricevuto un reclamo sulla pubblicazione di un volume e di alcuni articoli relativi alla complessa vicenda di cronaca. L'Ufficio ha rilevato che le pubblicazioni oggetto del reclamo erano in termini generali riconducibili al legittimo esercizio del diritto di cronaca su un fatto di interesse pubblico, ma ha altresì riscontrato che taluni passi indugiavano in una eccessiva esposizione dei dettagli relativi ai rapporti sessuali di taluni degli indagati e dei dettagli relativi alla sfera sessuale della stessa vittima. Pertanto, l'Ufficio ha raccomandato ai titolari del trattamento l'adozione di cautele a tutela dei diritti fondamentali della persona in caso di un'eventuale ristampa o riedizione del libro o di nuove trattazioni del caso in ragione degli sviluppi del procedimento penale in corso (*Nota* 18 febbraio 2009).

8.4. INFORMAZIONI RELATIVE A PERSONE E FATTI D'INTERESSE PUBBLICO

Dati relativi a personaggi pubblici e che esercitano funzioni pubbliche

Anche nel periodo di riferimento il Garante ha ricevuto segnalazioni, reclami e ricorsi riguardanti personaggi *"pubblici"*. Al riguardo, l'Autorità ha ribadito il principio in base al quale esiste un margine più ampio per la diffusione di informazioni che riguardano tali persone, nei limiti dell'interesse pubblico della notizia.

Tra i casi pervenuti si segnala un quesito in merito alla liceità della pubblicazione del dato relativo alla spesa sostenuta per l'uso di un cellulare di servizio da parte di un consi-

gliere comunale. L'Ufficio ha osservato che tale pubblicità può ragionevolmente giustificarsi sul piano dell'esercizio legittimo del diritto di cronaca per ragioni di trasparenza sull'uso delle risorse pubbliche. Tale dato, inoltre, può essere lecitamente conosciuto dai terzi, in base alle disposizioni di legge vigenti (art. 59 del Codice e art. 10 del Testo unico delle leggi sull'ordinamento degli enti locali – d.lg. 18 agosto 2000, n. 267; Capo V l. 7 agosto 1990 n. 241 e succ. modificazioni; *cfr.* anche *deliberazione* del Garante 19 aprile 2007 n. 17 *"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.* 25 maggio 2007, n. 120 [doc. *web* n. 1407101]). L'Ufficio ha però precisato che il dato, oltre ad essere acquisito lecitamente, deve essere trattato correttamente e, quindi, essere completo e aggiornato.

Il Garante ha poi ritenuto infondata la richiesta di opposizione al trattamento formulata dai dipendenti di un comune che avevano lamentato la pubblicazione, da parte di un quotidiano locale, dei loro nomi e dei compensi che avrebbero ricevuto a titolo di incentivo per la progettazione di un'opera la cui realizzazione era stata sospesa con una sentenza del giudice amministrativo. L'Autorità ha rilevato che le informazioni erano state diffuse senza travalicare i limiti del diritto di cronaca per illustrare un fatto di interesse pubblico nel contesto locale di maggiore diffusione della testata giornalistica. Inoltre, i dati erano contenuti in una determina del segretario comunale lecitamente conoscibile in base alle disposizioni che disciplinano il regime di pubblicità degli atti dell'amministrazione comunale e provinciale (*Provv.* 29 maggio 2008 [doc. *web* n. 1531687].

Sempre in applicazione dei princìpi sopra ricordati, il Garante ha rigettato una richiesta di opposizione al trattamento, formulata con ricorso da un personaggio noto nel mondo dello spettacolo e della cronaca rosa, in relazione a un'intervista pubblicata su un sito dedicato a un pubblico omosessuale e rilasciata da un giovane che dichiarava di aver avuto una relazione sentimentale con il ricorrente. Il Garante ha ritenuto che l'intervista andava inquadrata nell'ambito di una tematica più generale di interesse pubblico, soprattutto per il pubblico omosessuale (quella relativa al *cd.* "*outing*") e le informazioni relative alla sfera privata del ricorrente potevano giustificarsi in considerazione del rilievo che le stesse assumevano rispetto al ruolo e alla vita pubblica del ricorrente medesimo, così come

"costruita" da quest'ultimo attraverso il proprio sito *web*, dichiarazioni e interviste rese pubblicamente (dalle quali emergeva la figura di un attore continuamente agli onori della cronaca per vere e presunte relazioni sentimentali e sessuali con donne) (*Provv.* 2 ottobre 2008 [doc. *web* n. 1559207].

Informazioni idonee a rivelare opinioni politiche e adesione ad associazioni

Il Garante ha esaminato un ricorso con il quale alcuni dirigenti della Rai radiotelevisione italiana S.p.A. hanno lamentato la pubblicazione, da parte di un quotidiano, di un presunto organigramma della Rai medesima in cui compariva una loro asserita appartenenza a una determinata area politica. Il Garante – senza entrare nel merito della questione relativa alla veridicità dell'organigramma e delle informazioni in esso contenute (con i ritenuti, possibili effetti diffamatori), sulla quale si sarebbe potuta eventualmente pronunciare l'autorità giudiziaria – ha rilevato che la pubblicazione è stata effettuata nel quadro del diritto di cronaca e di critica rispetto ad un fatto (l'esistenza di tale organigramma) che costituisce l'elemento essenziale della notizia pubblicata e che si inserisce nell'ampio dibattito, di evidente interesse pubblico, sulla struttura e sull'organizzazione del servizio pubblico radiotelevisivo (*Provv.* 19 maggio 2008 [doc. *web* n.151719] e *Provv.* 30 ottobre 2008 [doc. *web* n.1523831]).

Da segnalare anche la risposta a un quesito in merito alla liceità della pubblicazione, da parte di taluni quotidiani, dei dati relativi agli iscritti a un'associazione massonica. L'Ufficio ha richiamato i princìpi generali dettati dal codice per i trattamenti effettuati per finalità giornalistiche osservando che i dati in questione possono essere diffusi, anche senza il consenso degli interessati, ma nel rispetto dei limiti posti dall'art. 137 del Codice e, in particolare, di quello dell' *"essenzialità dell'informazione rispetto a fatti di interesse pubblico"*. Ciò implica una valutazione caso per caso del tipo di dati diffusi e del contesto in cui si essi inseriscono, tenendo conto della *"qualificazione"* dei soggetti menzionati e delle diverse caratteristiche del fatto (*cfr.* artt. 5 e 6 del codice di deontologia). Deve quindi escludersi, in linea di principio, la liceità di una pubblicazione degli elenchi degli iscritti indiscriminata e carente dei presupposti suindicati.

8.5. INFORMAZIONE *ON-LINE*

Sempre più frequentemente pervengono al Garante segnalazioni per chiedere la cancellazione di dati e immagini personali diffusi e in vario modo reperibili su Internet (*Emule*, *Youtube*, *forum*, *blog*), reputati lesivi della sfera personale dei segnalanti.

L'Autorità non è potuta intervenire quando, da verifiche d'ufficio, è risultato che il titolare del trattamento del sito Internet in questione non risiede in Italia (*v.* art. 5 del Codice). In queste situazioni è stata fornita agli interessati l'indicazione del soggetto titolare, estratto dai registri *"Whois"*, cui il segnalante può direttamente richiedere la rimozione immediata dei contenuti ritenuti diffamatori. Ciò, in ottemperanza ad una prassi nota come *"notice and take down"*, riconosciuta sia negli Usa sia in ambito comunitario (*cfr.* Direttiva 2000/31/Ce, relativa a taluni aspetti giuridici dei servizi della società dell'informazione nel mercato interno, con particolare riferimento al commercio elettronico, recepita in Italia con il d.lg. n. 70/2003).

Sulle problematiche connesse alla pubblicazione *on-line* degli archivi storici delle principali testate giornalistiche, emerse in occasione di ricorsi presentati all'Autorità, *v. infra*, *par.* 17.2.5

Social network

Sempre con riferimento al tema Internet, nella 30ma Conferenza internazionale delle Autorità di protezione dei dati personali, tenutasi a Strasburgo nell'ottobre 2008, è stata approvata una *"risoluzione sulla tutela della privacy nei servizi di social network"* che evidenzia come i servizi di *social network*, pur offrendo una gamma del tutto nuova di opportunità comunicative, possono comportare anche rischi per la *privacy* sia degli utenti sia di terzi (*v. infra*, *par.* 20, con riferimento alle conferenze delle autorità su scala internazionale).

8.6. RETI DI COMUNICAZIONE

8.6.1. Invio di comunicazioni commerciali non sollecitate (spam)

Anche nel corso del 2008 il Garante ha ricevuto diverse richieste d'intervento relativamente ad attività di *spam*.

In diverse occasioni l'Autorità ha vietato l'ulteriore invio di comunicazioni promozio-

nali a terzi senza il consenso preventivo, specifico e informato degli interessati ai sensi dell'art. 130 del Codice, adottando appositi provvedimenti (*Provv.* 31 gennaio 2008 [doc. *web* n. 1489843] *Provv.* 13 maggio 2008 [doc. *web* n. 1521775] e *Provv.* 11 dicembre 2008 [doc. *web* n. 1584213]), talora preceduti da un'attività ispettiva mirata. In tali interventi, il Garante ha inoltre ricordato che un indirizzo *e-mail*, per il solo fatto di essere reperibile in rete, non può essere oggetto di un uso indiscriminato e che occorre ottenere il consenso preventivo del destinatario prima di utilizzare l'indirizzo di posta elettronica per fini di pubblicità e di *marketing*, in quanto la pubblicità di un dato non ne comporta la libera utilizzabilità. In tutti i casi di trattamento illecito per l'invio tramite posta elettronica di comunicazioni non richieste l'Autorità ha comminato le previste sanzioni amministrative.

Il Garante si è occupato del fenomeno dell'invio di *fax* pubblicitari a destinatari che non avevano mai prestato il loro consenso a ricevere tali comunicazioni con diversi provvedimenti di divieto, accompagnati dall'emanazione delle conseguenti sanzioni amministrative, in particolare con *provvedimenti* 31 gennaio 2008 [doc. *web* n. 1488781] e 13 maggio 2008 [doc. *web* nn. 1520217, 1520243 e 1520263]. In tali occasioni l'Autorità ha ribadito che la reperibilità dei dati sugli elenchi pubblici, quali ad esempio gli elenchi categorici, 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* in considerazione della specifica disciplina prevista all'art. 130 del Codice.

Il Garante in molti casi, a seguito di complesse istruttorie, ha verificato che l'invio di *fax* avviene da società localizzate all'estero (Francia, Regno Unito e Romania). Pertanto, in questi casi ha provveduto a richiedere la collaborazione delle Autorità competenti dei rispettivi Paesi al fine di far cessare detti invii indesiderati.

In tale contesto è da segnalare il *provvedimento* inibitorio del 19 dicembre 2008 [doc. *web* n. 1580492], con il quale l'Autorità ha disposto il divieto di proseguire il trattamento risultato illecito. In tale caso il Garante ha riscontrato che il consenso non può definirsi *"libero"*, quando sia riferito a un ulteriore trattamento dei dati personali che l'interessato

deve acconsentire per conseguire una prestazione richiesta. Gli interessati devono essere messi in condizione di esprimere consapevolmente e liberamente le proprie scelte in ordine al trattamento dei dati che li riguardano, manifestando il proprio consenso per ciascuna distinta finalità perseguita dal titolare. Inserendo tra le condizioni generali per la fruizione di un servizio le ulteriori finalità di contatto a fini pubblicitari, i dati personali raccolti lecitamente dal titolare (e conferiti dall'interessato) per l'esecuzione del rapporto contrattuale vengono di fatto piegati a un utilizzo diverso dallo scopo che ne ha giustificato la raccolta, con inevitabile lesione quindi del principio di finalità (art. 11, comma 1, lett. *b*), del Codice).

Il Garante ha ribadito in questa occasione che si deve in ogni caso garantire agli interessati il diritto di esprimere liberamente un valido consenso informato per i trattamenti per finalità di *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'Autorità ha partecipato ad una serie di eventi internazionali tra le autorità, e con il supporto dei soggetti privati, per arginare il dilagare del fenomeno dello *spam*. In particolare, il Garante ha preso parte a diverse iniziative del *Cnsa* (*The Eu Contact Network of Spam Authorities*) a Bruxelles e, in tale contesto, è stato presentato uno studio effettuato per la Commissione europea su tutti i Paesi dell'Unione relativamente alle attività avviate per affrontare fenomeni quali *spam*, programmi spia e *software* maligni. Dall'analisi delle iniziative intraprese dalle Autorità competenti e dai fornitori di servizi, nonché delle sanzioni comminate e del livello di cooperazione anche internazionale, il nostro Paese risulta tra i primi sia per impegno sia per risultati raggiunti.

8.6.2. Banche dati utilizzate per il telemarketing

A seguito delle numerose segnalazioni pervenute nel 2007 e nel 2008, relative a chiamate indesiderate con finalità promozionali effettuate principalmente da parte delle società telefoniche, il Garante è intervenuto nuovamente sulla materia del *telemarketing*, dopo i provvedimenti del 2007 indirizzati a diversi titolari del trattamento ([doc. *web* nn. 1412626, 1412610, 1412598, 1412557, 1412586] *v. Relazione* 2007, *p.* 83]).

I provvedimenti inibitori del 2008 [doc. *web* nn. 1544315, 1544326, 1544338, 1562780, 1562758] sono stati diretti non solo nei confronti di società che hanno effettuato tali attività direttamente, o tramite soggetti esterni nominati responsabili del trattamento, ma anche verso alcune tra le primarie società che hanno costituito e hanno venduto le banche dati contenenti le informazioni relative agli interessati da contattare telefonicamente per finalità promozionali.

Ai provvedimenti si è giunti dopo ripetuti richiami, istruttorie e ispezioni effettuate in alcuni casi anche con l'ausilio del Nucleo speciale *privacy*, avviate a seguito di reclami e segnalazioni ricevute dall'Autorità.

Dalla documentazione acquisita nel corso delle predette attività istruttorie, è emerso che le società che hanno fornito i *database* agli operatori telefonici avevano raccolto e ceduto a terzi i dati degli interessati senza informarli (o informandoli in maniera inadeguata) ed anche senza un loro preventivo specifico consenso. Una delle società offriva sul proprio sito i dati di oltre quindici milioni di famiglie italiane suddivise per reddito e stile di vita, senza che gli interessati fossero stati informati o avessero dato il loro assenso alla comunicazione dei dati a terzi.

Da parte loro le aziende e le compagnie telefoniche che hanno acquistato i dati e li hanno utilizzati a fini di *marketing* telefonico (il *cd.* "*teleselling*"), non si sono preoccupate di accertare, come prevede invece la disciplina sulla protezione dei dati, che gli abbonati avessero acconsentito alla comunicazione dei propri dati e al loro uso a fini commerciali.

Successivamente, con l'art. 44, comma 1-*bis* del decreto-legge 30 dicembre 2008, n. 207 (*cd. "decreto milleproroghe"*), convertito, con modificazioni, nella legge 27 febbraio 2009, n. 14 (*G.U.* 28 febbraio 2009 n. 49, S.O. 28), è stato stabilito che i dati personali presenti nelle banche dati costituite sulla base di elenchi telefonici pubblici formati prima del 1° agosto 2005 sono lecitamente utilizzabili per fini promozionali sino al 31 dicembre 2009, anche in deroga agli articoli 13 e 23 del Codice, dai soli titolari del trattamento che hanno provveduto a costituire dette banche dati prima del 1° agosto 2005.

Di seguito all'entrata in vigore di tale disposizione, che ha introdotto un regime derogatorio e transitorio in materia di *telemarketing*, il Garante ha ritenuto necessario interve-

nire al fine di chiarire rigorosamente i limiti entro i quali le società che operano nel settore possono avvalersi della deroga, precisando altresì le regole che le stesse dovranno seguire nell'uso dei dati degli abbonati.

Con il *provvedimento* del 12 marzo 2009 (*G.U.* 20 marzo 2009 n. 66 [doc. *web* n. 1598808]), l'Autorità ha così stabilito che le aziende e i *call center*, che intendano avvalersi della citata deroga e contattare gli utenti per fare promozioni e offerte commerciali utilizzando le predette banche dati, devono innanzitutto documentare in modo adeguato che la banca dati, costituita con i numeri telefonici e gli indirizzi degli abbonati, sia stata effettivamente creata prima del 1° agosto 2005, chiarendo altresì se il trattamento di dati venga effettuato anche per conto terzi. Le società e le aziende del settore, inoltre, sono tenute ad usare questi dati direttamente, senza possibilità di cederli a nessun titolo ad altre aziende.

Gli operatori che telefoneranno agli abbonati dovranno, poi, ad ogni contatto specificare per quale società chiamano e ricordare agli interessati i loro diritti, registrando immediatamente l'eventuale contrarietà dell'abbonato ad essere nuovamente contattato e comunicandogli l'identificativo dell'operatore.

I dati presenti nelle banche dati dovranno essere utilizzati solo a fini promozionali e non potranno in alcun modo essere usati per acquisire nuove informazioni o il consenso degli abbonati ad effettuare chiamate dopo la data del 31 dicembre 2009, poiché ciò determinerebbe di fatto la costituzione di nuove banche dati, andando al di là delle finalità stabilite dalla legge e prorogando, oltre il termine previsto, gli effetti della deroga temporanea.

Il Garante ha infine ricordato che il mancato rispetto del *provvedimento* comporta una sanzione amministrativa che va da 30.000 a 180.000 euro e che, nei casi più gravi, può raggiungere anche i 300.000 euro.

8.6.3. Telefonia

Rintracciabilità di persone disperse in montagna tramite localizzazione del cellulare

Anche nel 2008 diversi comuni hanno evidenziato che le ricerche di persone in pericolo, non in grado di comunicare la propria posizione, ad esempio perché in stato di incoscienza, potrebbero essere agevolate dalla possibilità di ottenere in tempo reale dal competente operatore telefonico la localizzazione del telefono cellulare delle persone stesse. I comuni

richiedenti hanno fatto riferimento all'attività svolta dal Corpo nazionale del soccorso alpino e speleologico (Cnsas), una delle strutture operative del Servizio nazionale della protezione civile (*cfr.* art. 11, comma 1, della l. n. 225/1992), che, infatti, ha spesso la concreta necessità di localizzare con urgenza persone disperse, in particolare in zone montane.

Pertanto, con il *provvedimento* del 19 dicembre 2008 [doc. *web* n. 1580543] il Garante ha chiarito che il Codice, nel caso vi sia la necessità di salvaguardare la vita o l'incolumità di una persona, consente alla società telefonica di comunicare senza indugio all'organismo di soccorso, anche senza il consenso dell'interessato, dati quali quelli concernenti i ponti e le celle attivate o *"agganciate"* dal telefono mobile della persona dispersa. La decisione ha, infatti, ad oggetto solo i dati relativi all'ubicazione diversi dai dati relativi al traffico, ossia i dati che possono essere reperiti sulla rete di comunicazione elettronica a prescindere da una comunicazione tra soggetti.

Pur riguardando il soccorso alpino, il *provvedimento* afferma princìpi suscettibili di essere applicati, con le dovute cautele, anche in altri casi in cui v'è esigenza di soccorso; l'Autorità ha chiarito, tuttavia, che i dati acquisiti dagli organismi di soccorso dovranno essere utilizzati solo per ricercare e soccorrere la persona dispersa.

L'Autorità ha inoltre ricordato che i servizi abilitati a ricevere le chiamate di emergenza possono comunque trattare i dati relativi all'ubicazione dei telefoni relativi a chi chiama, anche quando l'utente o l'abbonato abbia già rifiutato o omesso di prestare il consenso (*cfr.* considerando 36 e art. 10, comma 1, lett. *b*) della Direttiva 2002/58/Ce e art. 127, comma 4, del Codice).

9. Associazioni e partiti politici

Nel corso dell'anno l'Autorità ha avuto modo di approfondire la tematica del trattamento dei dati personali all'interno delle realtà associative, nelle quali si esplicano i diritti fondamentali della persona e più intensa può essere la circolazione di informazioni personali, talora assai delicate (in quanto riferite a scelte, opinioni o condizioni individuali spesso riconducibili al novero dei dati sensibili).

Affissione nella bacheca associativa di provvedimenti disciplinari

Una reclamante ha lamentato che dati personali contenuti in provvedimenti disciplinari emanati nei suoi confronti da una federazione sportiva erano stati affissi in spazi liberamente accessibili ai soci di un circolo sportivo (affiliata alla medesima federazione). La pubblicazione dei provvedimenti disciplinari non sarebbe risultata consentita dallo statuto del circolo, né doverosa in attuazione di specifiche norme federali.

Dagli elementi acquisiti si è ritenuto che l'affissione non trovasse giustificazione nelle norme statutarie vigenti e che l'interessata non avesse ricevuto idonea informativa in ordine a tale eventualità.

In termini generali, il Codice rimette alle determinazioni adottate da organismi senza scopo di lucro le modalità ed i limiti nella divulgazione di dati personali relativi agli iscritti; ciò per consentire agli stessi iscritti di valutare in concreto – al di là delle necessarie misure organizzative da predisporre a livello associativo – le possibili *"ricadute"* individuali legate ad una più ampia circolazione delle informazioni anche nei confronti di tutti gli altri associati (talvolta di numero assai elevato) oltre che la natura (più o meno sensibile) delle informazioni suscettibili di comunicazione.

Peraltro, tenuto conto che i provvedimenti disciplinari emanati erano stati rimossi dalla bacheca e che il trattamento dei dati ivi contenuti era comunque cessato prima ancora che l'associazione avesse notizia del reclamo, non si sono ravvisati i presupposti per l'adozione di provvedimenti da parte dell'Autorità (art. 11, comma 1, lett. *d*), Reg. Garante n. 1/2007), fermi restando gli eventuali danni derivati all'interessata dall'avvenuta divulgazione di dati personali a sé riferiti (*Note* 19 agosto 2008 - 9 ottobre 2008).

Comunicazione ad un socio di dati personali riferiti agli associati

L'iscritto ad una federazione ha posto un quesito in tema di accesso ai dati personali degli altri associati (in forma di elenco, comprensivo di nominativi ed indirizzi) per l'esercizio di prerogative legate all'appartenenza all'associazione.

Al riguardo l'associazione, in base all'art. 26, comma 4, lett. *a*), del Codice, può determinare *"il se e il come"* della conoscibilità, all'interno della realtà associativa, dei dati personali degli aderenti, anche in difetto del consenso dei singoli associati, a condizione che la comunicazione avvenga nel rispetto di *"idonee garanzie"* determinate dalla stessa associazione in relazione ai trattamenti effettuati e che l'associazione medesima abbia reso note agli interessati, all'atto dell'informativa rilasciata ai sensi dell'art. 13 del Codice, le determinazioni in merito adottate, prevedendo espressamente le modalità di utilizzo dei dati (che dovranno essere comunque pertinenti e non eccedenti rispetto alle finalità sottese alla richiesta: art. 11, comma 1, lett. *d*), del Codice).

Resta comunque salva la possibilità per ciascuna associazione di individuare modalità diverse per veicolare messaggi o comunicazioni di singoli associati all'interno della compagine associativa (facendo così da tramite dei singoli iscritti), nelle forme ritenute più opportune senza che ciò comporti la comunicazione di indirizzari di tutti gli iscritti a taluni di essi (*Nota* del 24 giugno 2008).

Movimenti politici

Alcuni segnalanti hanno lamentato di aver ricevuto una tessera di iscrizione ad un Movimento politico senza averla mai richiesta (né aver pagato la relativa quota) ed in assenza della prescritta informativa.

In riscontro a quanto al riguardo richiesto dall'Autorità, il Movimento ha dichiarato di aver cancellato immediatamente i dati personali dei segnalanti a seguito di alcune comunicazioni ricevute da parte degli stessi. In ogni caso, uno dei segnalanti sarebbe stato in continuo contatto con l'organizzazione, in qualità diverse, con costante frequentazione dei relativi uffici; in occasione del Congresso nazionale del Movimento, uno dei segnalanti avrebbe richiesto il rinnovo della tessera anche per l'altro; le tessere *"scadute"* non sarebbero state ricusate dagli interessati. Inoltre il consenso dei segnalanti alla consegna della tessera dell'organizzazione sarebbe stato acquisito (verbalmente) da due addette alla segreteria, senza compilazione del relativo modulo di adesione (data anche la conoscenza personale degli interessati).

A conclusione dell'attività istruttoria espletata, non risultando comprovata l'avvenuta ricezione, da parte dell'organizzazione, di una domanda corredata dai dati anagrafici degli interessati (come richiesto dallo statuto), né che tale formalità potesse rientrare tra le garanzie previste ai fini dell'esonero dall'acquisizione del consenso scritto degli interessati (art. 26, comma 4, lett. *a*), del Codice), l'Autorità ha prescritto al Movimento di accertare l'effettiva cancellazione dei dati dei segnalanti da parte delle strutture locali, nonché di prevedere idonee garanzie in caso di trattamenti effettuati prescindendo dal consenso scritto degli interessati. Non è risultata invece comprovata, diversamente da quanto lamentato dai segnalanti, la violazione della disciplina di protezione dei dati avente ad oggetto l'abusiva utilizzazione di informazioni per finalità di rilascio di una tessera di iscrizione al Movimento, tenuto conto delle dichiarazioni univocamente rese in proposito dalle addette alla segreteria dell'organizzazione (*Provv.* 15 febbraio 2008 [doc. *web* n. 1523069]).

Propaganda politica ed elettorale

Anche nel 2008, come in analoghe occasioni, il Garante – in vista delle consultazioni elettorali europee, amministrative e referendarie di giugno 2009 – ha adottato un *provvedimento* generale (*Provv.* 2 aprile 2009, in *G.U.* 11 aprile 2009, n. 85 [doc. *web* n. 1603863]) recante misure in materia di propaganda elettorale.

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

In particolare, è stato previsto che, decorsa la data del 30 settembre 2009, partiti, movimenti politici, comitati promotori, sostenitori e singoli candidati possono continuare a trattare temporaneamente (anche mediante mera conservazione) i dati personali lecitamente raccolti secondo le modalità indicate nel predetto *provvedimento* del 7 settembre 2005, informando gli interessati entro il 31 dicembre 2009, nei modi previsti dal Codice.

Dai predetti provvedimenti emergono ulteriori princìpi che devono essere osservati da partiti, movimenti politici, comitati promotori, sostenitori e singoli candidati che intraprendono iniziative di selezione di candidati alle elezioni, di comunicazione e di propaganda elettorale.

In particolare, senza il preventivo consenso degli interessati, possono essere utilizzati solo i dati contenuti nelle fonti documentali detenute da soggetti pubblici, liberamente accessibili a chiunque in base a una specifica norma (*ad es.*, 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; tuttavia, 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 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*, nonché 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 il 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 dal verificare, anche 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.

10. Le attività economiche e i rapporti di lavoro

10.1. Settore bancario

Anche nel 2008 sono pervenuti numerosi reclami e segnalazioni relativi all'attività bancaria, molti su aspetti già trattati nelle *"Linee-guida in materia di trattamento di dati personali della clientela in ambito bancario"* (*Provv.* 25 ottobre 2007, *G.U.* 23 novembre 2007 n. 273 [doc. *web* n. 1457247]).

Banche, videosorveglianza e registrazione delle impronte digitali

Si è riferito nella *Relazione* 2007 (*p.* 88) degli accertamenti eseguiti nel 2008 per verificare il rispetto delle prescrizioni impartite nel *provvedimento* del 27 ottobre 2005 [doc. *web* n. 1246675] sul trattamento di dati personali dei clienti (immagini del volto e delle impronte digitali) per accedere all'interno delle filiali.

Attività bancaria ed elenchi di sospetti terroristi

Il cliente di un istituto di credito ha segnalato che, recatosi presso la propria banca per negoziare un assegno, dopo essere stato identificato, gli veniva comunicato dall'operatore di sportello, e confermato anche dal direttore, che l'operazione non poteva essere eseguita, poiché il suo nome e cognome risultavano inseriti *"nell'elenco dei latitanti terroristi"*. All'esito dell'attività istruttoria, il Garante ha precisato che nel caso di specie la banca non aveva utilizzato tutte le informazioni pertinenti, complete e non eccedenti in concreto disponibili nel conseguimento della legittima finalità perseguita (come prescritto dall'art. 11, comma 1, lett. *d*), del Codice). Tali informazioni, contenute nella lista formata e aggiornata periodicamente anche a cura dell'Ufficio italiano dei cambi, non si limitano infatti al solo nome e cognome del sospetto terrorista, ma includono dati ulteriori, quali data, luogo di nascita e codice fiscale. Secondo le indicazioni dell'Uic (provvedimento Uic, 9 novembre 2001, in *http://uif.bancaditalia.it/UICFEWebroot/*) tra i dati identificativi sono comprese le cariche, le qualifiche e ogni altro dato riferito nelle liste ai soggetti venuti in rilievo. A quest'ultimo riguardo, la coincidenza non sussiste qualora l'intermediario, sulla base di informazioni certe e secondo valutazioni di ragionevolezza, possa escludere che tali cariche e qualifiche siano attribuibili al cliente in quanto incompatibili con il tenore di vita ed ogni sua altra caratteristica oggettiva e soggettiva (*cfr. cit.* provvedimento Uic punto 2.4).

Il Garante ha pertanto prescritto alla banca di adottare tutte le misure necessarie ad assicurare il rispetto dei princìpi di qualità dei dati e correttezza del trattamento (art. 11 del Codice), adattando i sistemi operativi in modo da trattare nella stessa unità di tempo tutte le informazioni pertinenti e non eccedenti, in concreto disponibili, nel conseguimento della legittima finalità perseguita (*Provv.* 7 febbraio 2008 [doc. *web* n. 1523046]).

Home banking

In una segnalazione, un correntista ha lamentato che la *password* per l'accesso *on-line* ai conti correnti, di cinque caratteri numerici, sarebbe in contrasto con la regola 5 del *"Disciplinare tecnico in materia di misure minime di sicurezza"* Allegato B. al Codice, che prevede come misura minima di sicurezza l'utilizzo di una *password* di otto caratteri.

Dagli accertamenti, effettuati anche *in loco*, è emerso che la clientela del servizio di *home banking* riceve una tessera (*Password card*) contenente quaranta codici numerici composti da sei cifre decimali, ciascuno dei quali può essere utilizzato una sola volta in occasione di ciascuna operazione dispositiva; una volta esauriti i codici a disposizione, viene inviata al cliente una nuova scheda. Le modalità adottate dall'istituto di credito non sono state comunque ritenute in contrasto con la disciplina di protezione dei dati personali anche in considerazione della circostanza che l'Allegato B. al Codice riguarda le modalità tecniche che devono essere adottate dal titolare del trattamento e, quindi, la menzionata regola 5 si riferisce alle credenziali di autenticazione assegnate agli incaricati del trattamento e non ad altri soggetti, quali la clientela della banca che accede *on-line* ai servizi bancari (*Nota* 27 febbraio 2008).

Fusioni bancarie

Nel 2008 due istituti di credito hanno chiesto di essere esonerati dall'obbligo di rendere l'informativa agli interessati (clienti, fornitori e dipendenti) in relazione ai trattamenti di dati personali conseguenti alle operazioni di ristrutturazione societaria.

Al riguardo, il Garante non ha ritenuto necessaria l'adozione di provvedimenti ai sensi dell'art. 13, comma 5 del Codice, ma con due *provvedimenti* (11 dicembre 2008 [doc. *web* n. 1584328] e 19 dicembre 2008 [doc. *web* n. 1584272]), ha prescritto alle banche interessate dalle operazioni societarie di fornire agli interessati – sia attraverso il sito *web* delle banche, sia con comunicazione individualizzata in occasione della prima circostanza utile di contatto – la nuova denominazione del titolare del trattamento e gli estremi identifica-

tivi dell'eventuale nuovo responsabile presso il quale esercitare il diritto di accesso ai dati personali.

Tale soluzione (peraltro coerente con l'orientamento della Cass. Sez. un., 8 febbraio 2006, n. 2637) deriva dalla considerazione che per effetto della fusione per incorporazione, la banca incorporante assume i diritti e gli obblighi della banca incorporata, e diviene (unico) titolare del trattamento senza che si configuri alcuna (nuova) raccolta di dati. La continuità nei rapporti in corrispondenza di tali operazioni societarie posti in essere dalle banche, risulta conforme anche alla disciplina di settore contenuta nell'art. 57, comma 4, del d.lg. 1° settembre 1993, n. 385 (Testo unico delle leggi in materia bancaria e creditizia).

Trattamenti di dati personali e valutazione di adeguatezza e appropriatezza delle operazioni o dei servizi di investimento

Nel 2008 alcune associazioni di consumatori e privati cittadini si sono rivolti all'Autorità in merito alla raccolta di dati personali dei clienti effettuata, attraverso questionari prestampati, da parte di operatori bancari e finanziari che, per dare esecuzione a servizi di consulenza, raccolgono presso la clientela informazioni volte a valutare l'adeguatezza e l'appropriatezza delle operazioni o dei servizi di investimento raccomandati agli stessi clienti. In tal modo, gli operatori danno attuazione alla normativa di settore, che ha recepito le direttive comunitarie (2004/39/Ce del 21 aprile 2004, relativa ai princìpi quadro e 2006/73/Ce del 10 agosto 2006, recante le modalità di esecuzione della precedente) attraverso il Regolamento Consob di cui alla delibera n. 16190 del 29 ottobre 2007 in conformità alla previsione contenuta nell'art. 6, comma 2, lett. *b*), punto 1, d.lg. n. 59/1998 (come modificato dall'art. 2, d.lg. 17 settembre 2007, n. 164).

Al riguardo, l'Autorità ha precisato che le imprese di investimento devono rispettare la disciplina di protezione dei dati personali, in particolare, i princìpi di pertinenza e non eccedenza rispetto alla finalità legittimamente perseguita, in linea anche con le direttive comunitarie e la stessa disciplina nazionale di recepimento (art. 35, parr. 3 e 4, Direttiva 2006/73/Ce; art. 39, commi 2, 3 e 4, Reg. Consob) ed i dati raccolti non possono essere utilizzati dalle imprese di investimento per finalità incompatibili rispetto a quelle che ne hanno determinato la raccolta (art. 11, comma 1, lett. *d*), del Codice). È pertanto necessaria un'approfondita previa valutazione in ordine alla pertinenza e non eccedenza dei dati

personali trattati nell'ambito del servizio di consulenza e di gestione del portafoglio, anzitutto da parte dell'impresa di investimento, tenuto conto delle circostanze concrete relative a ciascuna delle operazioni effettuate o dei servizi resi. Per la mera esecuzione di ordini impartiti dal cliente (*cd. "execution only"*) la normativa vigente non prevede, ricorrendo le indicate condizioni, la raccolta delle menzionate informazioni (art. 43 Reg. Consob; art. 19, *par.* 6, Direttiva 2004/39/Ce) (*Nota* 26 marzo 2009).

Comunicazione a terzi di dati riferiti alla clientela

Alcuni casi (taluni dei quali in corso di approfondimento) hanno riguardato l'asserita comunicazione a terzi da parte della banca di dati personali dei clienti, anche con riferimento al successivo utilizzo di tali informazioni nell'ambito di procedimenti giudiziari.

In particolare in un reclamo è stata lamentata la comunicazione da parte di una banca, attraverso la produzione documentale e gli atti depositati in un procedimento giudiziario promosso dal cliente contro la stessa banca, di dati personali relativi non solo all'attore (che comunque lamentava l'eccedenza e non pertinenza di dati allo stesso riferiti), ma anche a soggetti estranei al procedimento giudiziario, quali il figlio (cointestatario con il padre del conto corrente oggetto del giudizio) e la nuora.

In via preliminare, l'Autorità ha rilevato che il giudizio sulla rilevanza e ammissibilità delle prove in giudizio (ivi compresi i profili derivanti dall'applicazione della disciplina sulla protezione dei dati personali) spetta all'autorità giudiziaria (art. 160, comma 6 del Codice, in conformità, dal punto di vista sistematico, con l'art. 116, primo comma c.p.c.). Nel caso in esame, il trattamento dei dati effettuato dalla banca convenuta nei riguardi del proprio cliente risultava essere avvenuto per fare *"valere o difendere un diritto in sede giudiziaria"* e, pertanto, non richiedeva il consenso degli interessati (art. 24, comma 1, lett. *f*), del Codice). Infatti, le informazioni trattate erano funzionali a valutare l'esperienza in materia di investimenti in strumenti finanziari, la situazione finanziaria, gli obiettivi di investimento, nonché la propensione al rischio del cliente. Analoghe considerazioni sono stata fatte in relazione ai confronti dei dati del figlio dell'attore, che era, comunque, cointestatario del conto oggetto del procedimento. Una diversa valutazione ha riguardato, invece, il trattamento di dati personali relativi alla nuora dell'attore, che risulta in contrasto con il principio di pertinenza e non eccedenza (oltre che con quello di finalità) dal

momento che la stessa non è risultata ad alcun titolo parte del contratto di investimento, né destinataria degli effetti economici dell'operazione (*Nota* 23 ottobre 2008).

Produzione ed esibizione di documentazione contenente informazioni bancarie in giudizio

In una segnalazione il socio di maggioranza di una società in nome collettivo – divenuto erede anche della quota di minoranza – ha contestato le modalità con le quali una banca, in esecuzione di una pronuncia dell'autorità giudiziaria, aveva fornito al notaio procedente alla formazione dell'inventario di beni ereditari dati in suo possesso riferibili al *de cuius* e relativi a prelievi e versamenti a qualunque titolo effettuati entro determinati limiti temporali. In particolare, la segnalante ha lamentato la comunicazione da parte della banca di dati inerenti operazioni riferite ad un conto corrente non intestato personalmente al defunto.

Dagli atti, tuttavia, è emerso che, ancorché nel momento in cui la banca ha dato esecuzione all'ordine impartitole dal giudice, il conto fosse già intestato all'impresa individuale di cui era titolare la segnalante (subentrata nel relativo contratto di conto corrente per effetto dell'intervenuto scioglimento della società), i dati personali comunicati si riferivano solo alle operazioni effettuate sul conto corrente bancario finché era stato intestato alla società di cui era socio il *de cuius*, senza riguardare l'impresa individuale. Considerato, inoltre, che la banca era tenuta a fornire i dati relativi a movimenti bancari *"a qualunque titolo"* riferibili al defunto e tenuto altresì conto della peculiare ragione sociale adottata dalla società, della quale il *de cuius* era socio, l'Autorità ha escluso che nel caso di specie la comunicazione da parte della banca sia avvenuta in violazione del Codice (*cfr.* le *"Linee-guida in materia di trattamento dei dati personali della clientela in ambito bancario"* per il caso in cui la comunicazione avvenga, nelle forme previste dalla legge, nei confronti dell'autorità giudiziaria - punto 3.3. del *provvedimento*) (*Nota* 12 novembre 2008).

In un altro caso, la segnalante ha chiesto l'intervento del Garante in relazione all'inottemperanza da parte di due istituti di credito ad un ordine di esibizione emesso dal giudice ai sensi dell'art. 201 c.p.c.. L'Autorità, nel richiamarsi al punto 3.3. delle menzionate *"Linee-guida"* ha invitato la segnalante ad attivare, ogni rimedio riconosciuto dall'ordinamento giuridico nei confronti dell'inottemperanza del terzo al provvedimento esibitorio, non essendo riconosciuta al riguardo alcuna competenza al Garante (*Nota* 6 novembre 2008).

Un'ulteriore segnalazione ha riguardato la produzione da parte di una banca, nel corso di un procedimento giudiziario contro la banca medesima, delle movimentazioni del conto corrente intestato alla segnalante, contenente informazioni relative ad operazioni bancarie non inerenti il giudizio.

Al riguardo, l'Autorità ha richiamato i princìpi contenuti nelle *"Linee-guida"* in materia, con specifico riferimento al fatto che in giudizio possono essere prodotti solo i dati pertinenti all'esigenza di far valere o difendere un diritto dell'istituto di credito, evitando proprio 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 (punto 4, anche in relazione al contenuto dell'art. 160, comma 6, del Codice). Nel caso di specie si è quindi ritenuto che la banca avrebbe dovuto oscurare, in tutto o in parte, le informazioni bancarie non pertinenti rispetto alla controversia pendente, restando in ogni caso impregiudicato il potere del giudice di richiedere (specie in caso di contestazione) la produzione integrale della documentazione (*Nota* del 17 ottobre 2008).

Abbandono di documentazione bancaria e misure di sicurezza

In un reclamo è stata lamentata la diffusione di dati personali di due clienti di una banca conseguente all'abbandono, in occasione del rilascio dei locali ove operava uno sportello dell'istituto di credito, di alcuni documenti prodotti in occasione dell'istruzione di una richiesta di mutuo alla quale i reclamanti avevano successivamente rinunciato. Da una complessa attività istruttoria (anche con accertamenti ispettivi) è emerso che i menzionati documenti, contenenti dati personali non sensibili né giudiziari, erano stati rinvenuti dal responsabile della sicurezza dello *"store"* dove era ubicato lo sportello bancario in un armadio che la banca si era impegnata a cedere con altre suppellettili ad un istituto di credito subentrato nell'utilizzo dello sportello. Gli accertamenti espletati hanno consentito di appurare che la banca aveva adottato, all'epoca dell'episodio segnalato, misure di sicurezza organizzative *"minime"* a protezione dei dati dei clienti trattati senza l'ausilio di strumenti elettronici già conformi a quanto attualmente prescritto dall'art. 35 del Codice e dalla regola 27 dell'Allegato B. al Codice, impartendo istruzioni scritte ai lavoratori incaricati del trattamento. Poiché tali istruzioni non avevano formato oggetto di rivisitazione dopo il 2000, si è rappresentato alla banca la necessità di aggiornarle alla luce della

maggiore articolazione della disciplina in materia contenuta nel Codice e del punto 2.1. delle *"Linee-guida"*. La banca è stata poi invitata ad adottare, ai sensi dell'art. 31 del Codice, misure di sicurezza idonee per il trattamento di dati personali diversi da quelli sensibili e/o giudiziari effettuato senza l'ausilio di strumenti elettronici, con specifico riferimento alla predisposizione di specifiche procedure atte a garantire un'adeguata vigilanza da parte del titolare del trattamento sull'operato del personale incaricato del trattamento dei dati personali dei clienti, con particolare riguardo all'ipotesi di cessazione dell'attività bancaria presso sportelli periferici detenuti in locazione (*Note* del 18 dicembre 2008 e 2 marzo 2009).

Un'altra segnalazione ha riguardato la diffusione di dati personali riferiti a taluni correntisti, contenuti in documenti rinvenuti accidentalmente da un passante sulla via ove ha sede la banca. Dagli elementi acquisiti *in loco* è emerso che la banca aveva adottato misure di sicurezza conformi al Codice e che per un disguido la documentazione era stata inserita nei contenitori per la raccolta della spazzatura ordinaria anziché in quelli destinati al macero. La banca è stata invitata ad assicurare (tramite l'attenta vigilanza sull'operato degli incaricati e in occasione delle iniziative formative prescritte dalla regola 19.6 dell'Allegato B. al Codice) la scrupolosa attuazione delle istruzioni impartite (con specifico riguardo a quelle riguardanti la custodia, la conservazione, nonché la restituzione dei documenti contenenti dati personali al termine del relativo trattamento) da parte degli incaricati del trattamento (*Nota* 2 marzo 2009).

Coordinate bancarie in fatturazione e principio di pertinenza e non eccedenza

In una segnalazione si è contestata l'avvenuta inclusione, tra i dati contenuti nella fattura recapitata da una società per la fruizione del servizio di telefonia, del numero di conto corrente riferito alla segnalante, ritenuto eccedente rispetto alla finalità perseguita (ai fini della fatturazione del servizio, infatti, sarebbe stato sufficiente, a detta della medesima segnalante, la mera indicazione dell'istituto creditizio presso il quale effettuare il prelievo). Al riguardo, è stato precisato che l'indicazione di detto numero in sede di fatturazione del servizio appare eccedente, poiché il corretto addebito della somma fatturata può essere riscontrato già dall'estratto conto inviato al cliente dalla banca domiciliataria. A conferma di quanto evidenziato, tra gli elementi che per legge deve contenere la fattura non figura

il numero di conto corrente del beneficiario della prestazione (art. 21, comma 2, d.P.R. n. 633/1972 e successive modifiche e integrazioni) (*cfr. Nota* del 21 ottobre 2008).

Anche nel 2008 sono diminuiti i reclami e le segnalazioni in materia di trattamento dei dati da parte dei Sistemi di informazione creditizia. La tendenza è riconducibile all'adozione del codice di deontologia di settore (*G.U.* 23 dicembre 2004, n. 300 [doc. *web* n. 1556693]), che risulta sostanzialmente rispettato da parte dei titolari del trattamento.

Sono pervenuti, tuttavia, alcuni reclami e segnalazioni al trattamento, da parte di un sistema di informazione creditizia, di dati personali tratti da pubblici registri e riferiti a pignoramenti e ipoteche nei cui confronti è intervenuta, nelle forme di legge, la cancellazione o altra annotazione, che nei *report* della società che gestisce il sistema risultavano con la sola locuzione sintetica *"atto colpito da annotamento"*.

Il Garante, al riguardo, ha stabilito che la locuzione sintetica *"atto colpito da annotamento"*, non risulta conforme ai princìpi di esattezza e completezza dei dati personali (art. 11, comma 1, lett. *c*) e *d*), del Codice), per il suo contenuto generico e i riflessi negativi sull'interessato (derivanti dal termine *"colpito"*), frutto di elaborazione propria della società che non rappresenta fedelmente e immediatamente quanto contenuto nei registri pubblici. L'art. 10, comma 3, del Codice stabilisce, inoltre, che *"il riscontro all'interessato comprende tutti i dati personali che riguardano l'interessato comunque trattati dal titolare"* (*cfr.* anche *Provv.* 4 maggio 2006, punto 7 [doc. *web* n. 1302311]). Pertanto la società, disponendo di informazioni di dettaglio riguardanti le vicende relative all' *"atto colpito da annotamento"*, deve comunicarle nella loro completezza anche nei riscontri forniti agli interessati, in caso di esercizio del diritto di accesso ai sensi dell'art. 7 del Codice.

Per tali motivi è stato ordinato alla società di sostituire la dizione sintetica *"atto colpito da annotamento"* con informazioni il cui contenuto sia completo e aggiornato rispetto a quello desumibile dai pubblici registri (*Provv.* 5 giugno 2008 [doc. *web* n. 1535726]).

10.2. INFORMAZIONI COMMERCIALI

Trattamento di dati personali e informazioni commerciali

A seguito di numerose istanze, e delle conseguenti verifiche (con accertamenti anche *in loco*), l'Autorità ha prescritto ad una società che fornisce informazioni commerciali le misure necessarie per rendere il trattamento conforme ai princìpi della disciplina sulla protezione dei dati personali (con particolare riferimento a quelli di correttezza, pertinenza e non eccedenza), fermi restando gli eventuali adeguamenti in applicazione dei codici deontologici previsti dagli artt. 61, 118 e 119 del Codice.

La società gestisce alcune banche dati contenenti informazioni estratte da altri archivi (detenuti per lo più da formati da soggetti pubblici) per fornire alla propria clientela servizi aventi contenuto informativo nell'ambito della *cd.* "*business information*".

I servizi vengono commercializzati mediante *dossier* informativi individualizzati, riferiti sia a persone fisiche che a persone giuridiche, differenziati in base alla tipologia e al grado di approfondimento delle informazioni ivi contenute (*"dossier impresa"*; *"dossier persona"*; *"report"*; *"quick report"* e *"quick report plus"*; *"prospetto"*). In sostanza, si tratta di servizi a contenuto sia informativo che valutativo, realizzati mediante l'aggregazione di dati (generalmente disponibili al pubblico) riguardanti, tra l'altro, profili organizzativi, produttivi, patrimoniali, il corretto adempimento di obbligazioni e la loro elaborazione in forma di giudizi sintetici relativi all'affidabilità commerciale di un assai elevato numero di soggetti (circa cinque milioni di imprese e otto milioni di persone fisiche).

L'Autorità ha evidenziato che la società può effettuare lecitamente il trattamento dei dati personali contenuti nei *dossier* informativi (e nel caso di informazioni ricavate da pubblici registri senza il consenso degli interessati art. 24, comma 1, lett. *c*), del Codice, nel rispetto però dei princìpi di cui all'art. 11 del Codice)

Dagli accertamenti è, tuttavia, emerso che la società associa ad un individuo (persona fisica o giuridica), per stimarne l'affidabilità commerciale, informazioni riferibili a un soggetto diverso, come tali non "relative" ai soggetti cui il prodotto informativo si riferisce (al riguardo *infra*, *par.* 17.2.4, decisione su ricorso del 12 giugno 2008 [doc. *web* n. 1537684] relativa all'arbitrario accostamento fra l'interessato ed il fallimento di una

società di cui lo stesso era stato socio accomandante, artt. 2314 e 2320 c.c.).

In proposito, l'Autorità ha ritenuto la menzionata associazione suscettibile di mettere in cattiva luce il soggetto cui l'informazione viene a riferirsi, ascrivendogli eventi anche pregiudizievoli non direttamente a lui imputabili o, comunque, riferibili, e pregiudicandone così la relativa affidabilità commerciale (fatta salva l'eventuale sussistenza di elementi che consentano di addebitare l'evento al comportamento dei soggetti cui il *dossier* si riferisce). L'associazione degli elementi è stata perciò ritenuta non corretta, né pertinente, attesa anche la possibile alterazione della proiezione sociale e professionale che può derivarne al soggetto censito (avuto altresì riguardo alla lesione del diritto all'identità personale dell'interessato: art. 2 del Codice).

È stata perciò prescritta alla società l'adozione di ogni misura necessaria e idonea ad evitare l'associazione in un unico contesto a un soggetto di informazioni al medesimo non direttamente riconducibili (fatte comunque salve le eccezioni sopra richiamate).

Con specifico riferimento ai *dossier* contenenti indici sull'affidabilità commerciale dei soggetti censiti, le risultanze istruttorie hanno evidenziato trattarsi non – come prospettato dalla società – di mere sintesi delle informazioni provenienti da pubblici registri, bensì di autonome valutazioni, sulla base di un peso ponderato attribuito (secondo criteri di stima non disponibili pubblicamente) alle diverse informazioni. Come tali, essi devono considerarsi dati personali autonomi, distinti dalle informazioni originarie ricavate dalle fonti pubbliche, il cui trattamento – a differenza di quello relativo a dati pubblicamente disponibili – necessita del consenso degli interessati (art. 23 del Codice) o di altro presupposto equipollente previsto dall'art. 24 del Codice (circostanze, queste, non desumibili alla luce della documentazione acquisita agli atti).

Anche gli elementi utilizzati per le valutazioni sintetiche sull'affidabilità commerciale degli interessati sono risultati riconducibili anche a soggetti diversi (*ad es.*, riferiti anche a eventi – talora negativi – riconducibili a *"imprese connesse"*). Anche tali operazioni sono state ritenute in contrasto con i princìpi di correttezza, pertinenza e non eccedenza, oltre che in violazione del diritto all'identità personale (artt. 2 e 11 del Codice). Ciò, peraltro, in assenza di prove circa l'effettivo contributo fornito dal soggetto censito (persona fisica)

all'evento pregiudizievole riferito al soggetto diverso (persona giuridica), con una sorta di *"responsabilità di posizione"* in alcun modo riconosciuta dall'ordinamento.

Similmente nella formazione dei *"dossier impresa"*, sono stati tenuti in considerazione elementi riconducibili a terzi (quali esponenti in carica o soci – con considerazione anche di eventi di natura personale, in alcun modo ricollegabili alle attività esercitate presso l'impresa censita).

È stato perciò vietato alla società l'ulteriore utilizzo, per l'elaborazione dei menzionati indici sintetici, di informazioni non direttamente riconducibili agli interessati, in quanto relative ad accadimenti riferiti a soggetti diversi e tali da ledere il diritto all'identità personale dei soggetti censiti.

È stato inoltre prescritto alla società di distinguere i casi nei quali non fossero risultati elementi pregiudizievoli riferiti ai soggetti censiti (ipotesi in cui l'indice è *"nullo"*) rispetto a quelli nei quali gli indici ne avessero segnalato una misura stimata *"bassa"*. Ciò, perché la stessa società, con un'unica locuzione *"bassa/nulla"*, era solita attribuire un giudizio sintetico che, vagliato nell'ambito di un contesto unitario, è risultato inidoneo a fornire una chiara e univoca contezza del quadro degli eventi pubblici ritenuti rilevanti in ordine al soggetto censito.

Sotto altro profilo, è risultato che nei *dossier* venivano inseriti, limitatamente agli ultimi sei mesi rispetto alla loro consultazione da parte dei clienti, il numero delle interrogazioni effettuate e la tipologia dei soggetti che hanno richiesto le informazioni. Rispetto a tale tipologia di operazioni non è risultato comprovato che la società avesse acquisito il consenso degli interessati (non potendo trovare applicazione, nel caso di specie, le esimenti del consenso previste dall'art. 24, comma 1, lett. *c*) e *d*), del Codice, trattandosi di informazioni non di pubblico dominio, né concernenti in alcun modo l'attività economica dei soggetti censiti). In ogni caso, si trattava di informazioni per le quali non è risultata comprovata la pertinenza rispetto alla finalità perseguita dalla società, anche in quanto idonee a rendere note, sia pure indirettamente, strategie commerciali del soggetto censito o il ricorso dello stesso ai canali creditizi.

È stata perciò vietata l'ulteriore comunicazione alla clientela dei dati relativi al numero

delle richieste di *dossier* informativi relativi ai soggetti censiti. Ancora, è stato vietato alla società l'utilizzo delle liste elettorali per verificare la congruità delle informazioni detenute nei *database* mediante controlli incrociati di dati, risultato in violazione quindi del principio di liceità del trattamento (art. 11, comma 1, lett. *a*), del Codice) in quanto non consentito, per tale finalità, dalla normativa in materia, (art. 51, comma 5 del d.P.R. 20/03/1967, n. 223).

Infine, la società aveva avviato l'acquisizione dei dati relativi ai redditi degli italiani nel 2005, all'atto della loro pubblicazione sul sito Internet dell'Agenzia delle entrate, senza tuttavia portarla a compimento a seguito del *Provv.* 6 maggio 2008 [doc. *web* n. 1512255] (*cfr. par.* 3.7). Tenuto conto che l'Autorità, con il citato *provvedimento*, aveva prescritto ai soggetti che ne avessero avuto la disponibilità di non mettere ulteriormente in circolazione tali dati, ne è stato vietato l'ulteriore trattamento, prescrivendone altresì la cancellazione (*Provv.* 30 ottobre 2008 [doc. *web* n. 1570327]).

Tutela dell'interessato in caso di omonimia

In un caso particolare è stata lamentata l'erronea attribuzione, in tempi diversi, di alcuni protesti in *dossier* informativi relativi alla persona del segnalante o a società delle quali egli rivestiva le cariche di amministratore unico e di socio. In particolare è risultato che i protesti contestati riportavano codici fiscali parzialmente diversi rispetto a quello dell'istante; inoltre, ulteriori protesti riferiti ad omonimi del segnalante, privi di codici fiscali, indicavano indirizzi diversi da quello del medesimo segnalante.

È stata inoltre evidenziata l'attribuzione diretta al medesimo segnalante di protesti originariamente collocati tra i casi di possibile omonimia, anch'essi peraltro recanti indirizzi e codice fiscale diversi da quello a lui riferito.

La società ha affermato di aver *"oscurato"* tutti i prodotti riguardanti il segnalante, anche alla luce del contenzioso al riguardo in atto.

Da accertamenti effettuati *in loco* è stato invece verificato che i dati relativi al segnalante risultavano ancora essere censiti (fatta eccezione per il *"dossier persona"* – nel quale erano contenuti anche i protesti a lui addebitati – volontariamente oscurato dalla società). È altresì emerso che la società attribuisce a persone fisiche o giuridiche determinate informazioni (nel caso di specie relative ai protesti) anche quando i dati personali non sono

pienamente coincidenti con quelli del soggetto censito (*ad es.*, in caso di codici fiscali diversi o di diversi indirizzi).

La Camera di commercio chiamata a rendere informazioni sulla vicenda ha dichiarato che nessun protesto risulta essere in concreto riconducibile al segnalante.

Il Garante ha, pertanto, prescritto alla società di ripristinare la visibilità del *"dossier persona"* riferito al segnalante, vietandole l'attribuzione al medesimo di protesti levati nei confronti di omonimi (ferme restando eventuali determinazioni dell'autorità giudiziaria in ordine alla corretta attribuzione dei protesti medesimi). È così risultato violato il principio di qualità, secondo cui i dati trattati devono essere esatti, aggiornati e completi rispetto a quelli tratti dagli archivi camerali (art. 11, comma 1, lett. *c*) e *d*) del Codice).

Il Garante inoltre ha ritenuto contrario al principio di correttezza nel trattamento dei dati (art. 11, comma 1, lett. *a*) del Codice) l' *"oscuramento"*, unilateralmente disposto dalla società nelle more della decisione giudiziaria, di ogni informazione relativa al segnalante (anziché dei soli dati riferiti ai protesti per i quali è controversa l'attribuzione), reputando tale comportamento lesivo del diritto all'identità personale dell'interessato (in quanto insuscettibile di fornire ai potenziali fruitori del servizio un'informazione commerciale completa in ordine al medesimo segnalante) (*Provv.* 13 ottobre 2008 [doc. *web* n. 1571459]).

10.3. SETTORE ASSICURATIVO

Su richiesta dell'Isvap, e a seguito di proficua collaborazione tra le due Autorità, il Garante ha espresso il proprio parere su uno schema di regolamento volto a incrementare l'efficacia della banca dati sinistri (già disciplinata dal Provvedimento Isvap n. 2179 del 10 marzo 2003, Banca dati sinistri r.c. auto: modalità operative per l'accesso e prevista dall'articolo 135 del Codice delle assicurazioni private e dall'art. 120 del Codice), con particolare riferimento alle modalità di funzionamento e accesso alla stessa (*Nota* del Presidente del 12 febbraio 2009).

Le considerazioni svolte, in parte già formulate in occasione di recenti audizioni parlamentari, sono state finalizzate ad assecondare la ricerca di una maggiore funzionalità

dell'archivio esistente, per un più efficace contrasto della frode nel settore dell'assicurazione obbligatoria della r.c. auto, preservando tuttavia un livello elevato di garanzie per gli interessati.

Il Garante ha valutato con favore le modifiche e le innovazioni che si intendono inserire con lo schema trasmesso dall'Isvap (che non presenta innovazioni in relazione alla tipologia di dati trattati) nella parte in cui snelliscono le operazioni di consultazione della banca dati. Sono state comunque formulate indicazioni, centrate in particolare sui princìpi di finalità (art. 11 del Codice), di *cd. "economicità"* (art. 3 del Codice), di pertinenza e non eccedenza (art. 11), e di correttezza e trasparenza nelle operazioni di trattamento (art. 11-13 e *ss.* del Codice) – recepite dall'Isvap – per salvaguardare comunque i diritti degli interessati pur in presenza di un possibile significativo incremento della *"visibilità"* delle informazioni connesse ai sinistri memorizzati nell'archivio a vantaggio di una platea più ampia di soggetti (segnatamente di incaricati delle imprese assicuratrici operanti a livello periferico).

Nello spirito di collaborazione che ha caratterizzato l'operato delle due Autorità, il Garante si è riservato di formulare ulteriori indicazioni sul testo di regolamento che potrà essere trasmesso dall'Isvap, conclusa la consultazione pubblica aperta sullo schema relativo al funzionamento della banca dati sinistri.

Comunicazione a terzi di dati relativi a procedimenti penali pendenti

Con un reclamo è stato rappresentato un illecito trattamento di dati personali da parte di due società – una deputata alla stipula di polizze fideiussorie e di cauzioni (presso la quale la reclamante ha collaborato in qualità di agente) e l'altra addetta, per conto della prima, alla riscossione e al controllo delle polizze fideiussorie (comprese quelle stipulate dalla reclamante) – le quali avrebbero a più riprese comunicato ad alcuni collaboratori *"esterni"* di cui la reclamante era solita avvalersi nell'esercizio della propria attività lavorativa, dopo l'interruzione del rapporto di collaborazione, alcuni dati personali alla medesima riferiti (nel dettaglio, alcune denunce presentate a suo carico da parte delle predette società per appropriazione indebita e per emissione di fideiussioni false, nonché la conseguente pendenza di un procedimento penale nei suoi confronti); ciò, in assenza della prescritta informativa e in violazione dei princìpi di necessità e finalità (artt. 3 e 11, comma 1, lett. *b*), del Codice).

Dall'istruttoria è emerso il coinvolgimento di entrambe le società nei fatti contestati, risultando comprovati i profili di violazione della disciplina di protezione dei dati personali lamentati dalla reclamante. L'Autorità ha, dunque, provveduto a disporre il divieto dell'ulteriore comunicazione a terzi dei dati personali riferiti alla reclamante (limitatamente al procedimento penale pendente e alle denunce penali presentate a suo carico) (*Provv.* 2 aprile 2008 [doc. *web* n. 1519711]).

10.4. RAPPORTI DI LAVORO E PREVIDENZA

10.4.1. Rapporto di lavoro in ambito pubblico

Anche nel 2008 l'attività dedicata al trattamento di dati personali dei dipendenti da parte dei datori di lavoro pubblici è stata particolarmente intensa.

Il richiamo alle indicazioni e agli orientamenti espressi dall'Autorità con le *"Linee-guida in materia di trattamento di dati personali di lavoratori per finalità di gestione del rapporto di lavoro in ambito pubblico"* adottate l'anno precedente (*Provv.* 14 giugno 2007 [doc. *web* n. 1417809] ha innanzitutto consentito di dare risposta a molteplici istanze specifiche di amministrazioni pubbliche, dipendenti e organizzazioni sindacali.

Casistica individuale

In una segnalazione un appartenente al Corpo di polizia municipale lamentava che, durante un'intervista rilasciata ad un quotidiano locale concernente l'avvenuto decesso di un ambulante al termine di un'operazione di controllo contro il commercio abusivo, erano state indebitamente rese conoscibili le generalità del segnalante e dei colleghi intervenuti con lui nell'operazione. In risposta alla richiesta di elementi formulata dall'Ufficio, il Comune ha rappresentato che l'identità dell'interessato era stata diffusa durante un'intervista rilasciata, in conformità al regolamento comunale del Corpo, su autorizzazione del Comandante per fare chiarezza sull'accaduto e smentire le accuse sull'operato della polizia municipale sollevate dalla stampa e dalla comunità locale. Inoltre, al fine di chiarire l'estraneità dell'interessato all'accaduto, insieme all'informazione relativa alla sua partecipazione al controllo, era stato precisato che questi aveva svolto le mansioni di autista.

Attese le specifiche circostanze in cui erano avvenuti i fatti, la diffusione delle generalità dell'interessato non è stata ritenuta in contrasto con i princìpi della disciplina sulla

protezione dei dati personali, in considerazione del particolare risalto che la vicenda aveva assunto nella comunità locale, nonché delle precisazioni fornite circa la diversa posizione dell'interessato rispetto all'accaduto. Ciò, in relazione alle esigenze connesse alla tutela, nella vicenda, non solo del Corpo di polizia municipale, ma anche dei colleghi che avevano partecipato al controllo e delle persone nei cui confronti questo era diretto (artt. 11 e 19 del Codice; *v.* anche *Provv.* 16 febbraio 2000 [doc. *web* 42280] e *Provv.* 6 febbraio 2001 [doc. *web* n. 41067]) (*Nota* 2 febbraio 2009).

In un altro caso, l'Ufficio, pur non ravvisando i presupposti per l'adozione di un provvedimento collegiale, ha accertato l'inutilizzabilità delle informazioni sanitarie contenute in una perizia medico-legale e riguardanti le lesioni riportate da un vigile urbano in un sinistro stradale avvenuto al di fuori del servizio.

L'Ufficio non disponeva di elementi sufficienti a determinare se la perizia fosse stata acquisita lecitamente al protocollo del Comune. Tuttavia ha riscontrato profili di illiceità del trattamento effettuato dal datore di lavoro, in relazione alla rilevanza delle informazioni sanitarie riportate nella perizia, in quanto il documento anonimo, conteneva elementi da verificare nella loro veridicità e faceva riferimento a una vicenda risalente nel tempo a seguito della quale l'interessato aveva ripreso servizio essendo stato nel frattempo giudicato idoneo allo svolgimento delle proprie mansioni.

In proposito, la disciplina di settore prevede che il datore di lavoro pubblico, nel disporre gli accertamenti relativi all'idoneità al servizio dei dipendenti, sia tenuto a trasmettere all'organo verificatore una relazione contenente *"tutti gli elementi informativi disponibili"* (art. 15 d.P.R. 29 ottobre 2001, n. 461). Tuttavia trattandosi di dati personali relativi allo stato di salute, il loro trattamento per una finalità di per sé lecita avrebbe dovuto essere attentamente e specificatamente valutata alla luce del principio di indispensabilità, pertinenza e non eccedenza dei dati trattati (artt. 11, 22 e 112 del Codice) (*Nota* 9 luglio 2008).

Registrazioni di conversazioni telefoniche tra presenti

Nell'ambito dell'istruttoria preliminare su una segnalazione riguardante la produzione in giudizio di registrazioni di conversazioni telefoniche, l'Ufficio ha precisato che la registrazione di conversazioni tra persone presenti da parte di uno degli interlocutori rientra tra i trattamenti effettuati da persone fisiche per fini personali e pertanto non è soggetta

all'ambito di applicazione del Codice se i dati non sono destinati ad una comunicazione sistematica o alla diffusione (art. 5, comma 3). In termini più generali, si è poi rilevato che la giurisprudenza ritiene ammissibile la registrazione di conversazioni tra presenti, anche senza il consenso degli interessati e a loro insaputa, in quanto tale attività può costituire una legittima forma di memorizzazione di un fatto storico eventualmente utilizzabile anche in sede processuale per l'esercizio del diritto di difesa costituzionalmente riconosciuto (*v.* Cons. Stato 28 giugno 2007, n. 3796; C*ass.* pen., S.u., 28 maggio 2003, n. 36747) (*Nota* 24 luglio 2008).

Curricula degli operatori di imprese partecipanti a gare d'appalto

In relazione ad alcuni quesiti l'Ufficio ha ribadito che le amministrazioni appaltanti, come tutti i soggetti pubblici, possono legittimamente trattare dati personali, diversi da quelli sensibili, quando ciò sia necessario allo svolgimento dei loro compiti istituzionali in materia di appalti pubblici di lavori, servizi e forniture. Le amministrazioni appaltanti possono, in particolare, utilizzare i dati contenuti nella documentazione richiesta per comprovare il possesso dei requisiti necessari per la partecipazione alle gare, anche se riferiti a persone fisiche che operano presso le imprese partecipanti, senza richiedere il consenso degli interessati (art. 18 del Codice; artt. 42 e 197 d.lg. 12 aprile 2006, n. 163; *v.* anche *Provv.* 27 giugno 2001 e *Nota* 16 febbraio 1999 [doc. *web* nn. 40667 e 42320]).

Dal canto loro le imprese concorrenti possono comunicare tali dati alle amministrazioni appaltanti, anche in mancanza del consenso degli interessati, per eseguire gli obblighi previsti dalla normativa di settore o derivanti dal contratto di lavoro con gli operatori interessati, oppure, per adempiere prima della sua conclusione, a specifiche richieste dei medesimi interessati (artt. 23 e 24, comma 1, lett. *a*) e *b*), del Codice; *v.* anche *Provv.* 10 gennaio 2002 [doc. *web* n. 1064553]). Resta ferma, però, per le imprese la necessità di informare i propri operatori, sull'eventualità che alcuni dati siano forniti, su richiesta, ad amministrazioni appaltanti (*Nota* 19 dicembre 2008).

Pubblicazione *on-line* di dati riferiti al personale delle pubbliche amministrazioni

In corrispondenza dell'avvio dell'*"operazione trasparenza"* nella pubblica amministrazione da parte del Ministro per la pubblica amministrazione e l'innovazione, l'Autorità è stata investita di vari quesiti riguardanti la pubblicazione *on-line* di dati riferiti al personale e, in particolare, ai dirigenti pubblici, nonché riguardanti le collaborazioni

esterne e gli incarichi conferiti o autorizzati da amministrazioni pubbliche.

Nel fornire un preliminare riscontro alle amministrazioni interessate, in attesa di opportuni ulteriori approfondimenti in merito, considerate le modifiche normative attualmente all'esame del Parlamento (Atto Senato n. 1082 *"Disposizioni per lo sviluppo economico, la semplificazione, la competitività nonché in materia di processo civile"*), si è fatto in termini generali richiamo alle disposizioni del Codice che consentono di diffondere dati personali riferiti a singoli interessati in quanto ciò trovi fondamento in specifiche disposizioni legislative o regolamentari (art. 19, comma 3). Al riguardo, nel ricordare che la pubblicazione di taluni dati personali riguardanti il personale dirigenziale è già prevista in alcune disposizioni di legge (nominativi, incarichi conferiti, numero telefonico dell'ufficio, casella istituzionale di posta elettronica, *ecc.*; *v.* art. 2, comma 3, d.P.R. 23 aprile 2004, n. 108; art. 54 d.lg. 7 marzo 2005, n. 82), non sono stati ravvisati ostacoli in ordine alla pubblicazione sul sito Internet dell'amministrazione interessata di dati non riconducibili a persone identificate o identificabili (*ad es.*, dati quantitativi aggregati per uffici riguardanti le assenze o livelli retributivi ed accessori risultanti dai contratti collettivi o da atti interni di organizzazione), ovvero, a richiesta dell'interessato, ulteriori informazioni personali di ordine professionale pertinenti e non eccedenti (*tra le altre*, *Note* 20 maggio 2008, 5 novembre 2008 e 26 gennaio 2009).

Riguardo agli incarichi conferiti o autorizzati da amministrazioni pubbliche, uno specifico regime di pubblicità è previsto come obbligatorio per le singole amministrazioni limitatamente agli elenchi dei rispettivi collaboratori esterni e consulenti (art. 53, commi 12 e *ss.*, d.lg. 30 marzo 2001, n. 165; art. 1, comma 127, l. n. 662/1996). Infatti, la legge finanziaria 2008 ha individuato quale modalità di pubblicazione quella per via telematica sul sito istituzionale delle amministrazioni interessate (art. 3, comma 54, l. 24 dicembre 2007, n. 244).

In proposito, il Dipartimento della funzione pubblica ha informato l'Autorità di volere pubblicare sul proprio sito Internet alcuni tra i dati relativi agli incarichi di collaborazione e consulenza che le amministrazioni pubbliche sono tenute a comunicargli (amministrazione erogante, oggetto degli incarichi conferiti o autorizzati e ammontare dei relativi com-

pensi). L'Autorità, nel prendere atto dell'individuazione, da parte del Dipartimento, delle *"misure di pubblicità e trasparenza"* che la legge gli impone di adottare rispetto ai dati raccolti, ha sottolineato la necessità di individuare idonei accorgimenti volti a consentire forme proporzionate di consultabilità dei dati, prevedendo in particolare elenchi relativi a singole amministrazioni, consultabili distintamente (anche sulla base di eventuali *link* a siti *web* delle amministrazioni medesime), senza che per gli utenti sia possibile modificarli agevolmente o reperire direttamente dati mediante motori di ricerca (*Nota* 12 giugno 2008).

Con riferimento ad una segnalazione sull'avvenuta pubblicazione, su un periodico informativo di un comune, di alcuni dati personali riferiti ai singoli dipendenti dell'ente e riguardanti anche il loro stato di salute (trattamento economico, trattenute previdenziali, giorni di ferie, di malattia, permessi usufruiti ai sensi della legge n. 104/1992, assenze retribuite per maternità, congedo parentale e malattia figli, *ecc.*), l'Ufficio ha curato l'acquisizione di specifici elementi di valutazione, evidenziando che la disciplina sulla protezione dei dati personali impone il rispetto di particolari cautele per la divulgazione di tali informazioni e, segnatamente, vieta la diffusione dei dati idonei a rivelare lo stato di salute degli interessati (*Note* 5 novembre 2008 e 10 febbraio 2009).

Diffusione di dati sanitari tramite la pubblicazione *on-line* di una graduatoria di un concorso

L'Autorità è tempestivamente intervenuta in un caso segnalatole da un cittadino riguardante la diffusione su tre siti *web*, tra cui quello istituzionale del Comune di Roma, della graduatoria finale di un concorso di istruttore di polizia municipale che riportava, accanto ai nomi di alcuni idonei, diciture indicative dei titoli di preferenza previsti per legge (*ad es.*, *"invalido"* o *"figlio di invalido per servizio"*), in grado di rivelare lo stato di salute dei partecipanti o dei loro familiari.

Tali dati risultavano immediatamente accessibili a chiunque, attraverso una semplice ricerca nominativa effettuata in rete, anche tramite i motori di ricerca. In considerazione del divieto previsto per legge di diffondere dati idonei a rivelare lo stato di salute (art. 22, comma 8, del Codice), è stato disposto, in via d'urgenza, il *"blocco"* dei dati personali, imponendo al comune e alle due società che gestiscono i siti coinvolti di oscurare le informazioni riferite ai concorrenti, limitandosi alla sola conservazione delle medesime informazioni, in attesa di ulteriori accertamenti avviati anche per valutare la conformità al

Codice delle modalità di diffusione della graduatoria. Il Comune di Roma e le altre società coinvolte hanno immediatamente adempiuto al *provvedimento* inibitorio del Garante (*Provv.* 8 maggio 2008 [doc. *web* n. 1521716]).

Comunicazioni ex art. 39 del Codice

Un ente comunale ha informato l'Autorità, ai sensi dell'art. 39 del Codice, di voler trasmettere i dati personali contenuti in una graduatoria formata per l'assunzione di educatori di asilo nido al fine di consentire ad un comune limitrofo, che ne aveva fatto richiesta, di reperire personale supplente anche per il proprio servizio comunale. In questo caso, l'operazione di comunicazione, non prevista da alcuna norma di legge o regolamento, è stata ritenuta praticabile in quanto necessaria all'amministrazione ricevente per la gestione dei servizi sociali e l'instaurazione di rapporti di lavoro. Tuttavia il comune che intende effettuare la comunicazione deve rendere un'idonea informativa alle persone incluse nella graduatoria, ponendo in evidenza, in particolare, il diritto di opporsi per motivi legittimi al trattamento dei dati che li riguardano (*Nota* 9 maggio 2008).

Cedolini dello stipendio

Con riferimento ad una segnalazione inoltrata da alcune organizzazioni sindacali, l'Ufficio ha sollecitato l'Amministrazione dell'interno-Dipartimento della pubblica sicurezza a adottare opportune cautele nelle modalità di predisposizione e consegna ai dipendenti dei *cd. "cedolini"* dello stipendio (*Nota* 7 novembre 2008). Andrebbero infatti predisposte modalità di consegna dei cedolini idonee a limitare l'immediata accessibilità delle informazioni ivi contenute al solo interessato e agli incaricati del trattamento (*v. Parere* 31 dicembre 1998 [doc. *web* n. 39324], *Provv.* 31 ottobre 2007 [doc. *web* n. 1459297]).

L'amministrazione ha assicurato di essere determinata ad adottare nell'imminente futuro le modalità di recapito della busta paga in formato elettronico ai singoli dipendenti in conformità a quanto previsto dalla legge 30 dicembre 2004, n. 311 (art. 1, comma 197). L'Ufficio si è riservato di verificare la conformità ai princìpi del Codice della prassi adottata dall'amministrazione di riportare sulla busta paga l'indicazione della sigla del sindacato (art. 11 del Codice).

Forze armate e di polizia. Foglio matricolare

Muovendo da un ricorso e da una segnalazione riguardanti la trascrizione sul foglio matricolare degli appartenenti alla Polizia di Stato dei dati relativi a diagnosi e a prognosi contenuti nei certificati medici prodotti dagli interessati per giustificare le assenze dal servizio per

malattia, l'Ufficio è intervenuto presso il Ministero dell'interno-Dipartimento della pubblica sicurezza richiamando quanto già affermato dal Garante circa la non conformità ai princìpi di proporzionalità e indispensabilità della prassi di trascrivere sul foglio matricolare i dati relativi alle patologie *"sofferte durante il servizio"* (il *cd.* quadro *"M"*), benché lecitamente raccolti ai sensi dell'art. 61 del d.P.R. 28 ottobre 1985, n. 782 (*v.* da ultimo il *Provv.* del 14 giugno 2007, recante *"Linee-guida"* in materia di pubblico impiego, punto 8.2 pubblicato in *G.U.* 13 luglio 2007 [doc. *web* n. 1417809]; *v.* anche *Provv.* 24 maggio 2007 [doc. *web* n. 1426782] e, con riferimento al servizio matricolare del Corpo della Guardia di finanza, *Provv.* 19 ottobre 2005 [doc. *web* n. 1185148]) (*Nota* 4 settembre 2008).

In proposito, l'Amministrazione dell'interno ha rappresentato all'Ufficio di voler adeguare ai princìpi del Codice e alle pronunce del Garante il trattamento dei dati sanitari del personale finalizzato alla tenuta del foglio matricolare. Sul punto l'Ufficio, nel valutare positivamente le determinazioni assunte dall'amministrazione, ha chiesto alla medesima di valutare la possibilità di diramare opportune istruzioni transitorie agli organi interessati, volte ad assicurare prontamente il rispetto dei diritti e della dignità degli interessati in attesa dell'elaborazione di nuove indicazioni sul tema (*Nota* 21 ottobre 2008).

Diagnosi sui certificati medici

Con *provvedimento* del 30 ottobre 2008 [doc. *web* n. 1569552], adottato a seguito della segnalazione di un sindacato, il Garante ha vietato al Ministero della giustizia-Dipartimento dell'amministrazione penitenziaria il trattamento dei dati personali idonei a rilevare lo stato di salute del personale del Corpo della polizia penitenziaria relativi all'indicazione della diagnosi sui certificati di malattia.

Nella decisione il Garante ha ribadito che, in assenza – come nel caso di specie – di specifiche disposizioni, il lavoratore assente per malattia è tenuto a fornire un certificato contenente esclusivamente la prognosi con la sola indicazione dell'inizio e della durata dell'infermità.

Contestualmente al divieto di trattamento dei dati, il Garante ha prescritto al Ministero della giustizia-Dipartimento dell'amministrazione penitenziaria di impartire le disposizioni opportune al fine di conformare il trattamento dei dati alle vigenti disposizioni in materia di protezione dei dati personali.

Carta multiservizi della difesa

Il trattamento dei dati personali effettuato mediante la Carta multiservizi della difesa è stato sottoposto all'attenzione dell'Ufficio che ha avviato i necessari approfondimenti presso lo Stato maggiore della difesa aderendo ad un tavolo di lavoro per l'esame preliminare delle specifiche questioni connesse alla protezione dei dati personali (*Note* 7 maggio 2008 e 10 febbraio 2009). Tali profili di interesse attengono, in particolare, ai presupposti di liceità del trattamento, anche con riferimento al rispetto dei princìpi di necessità, proporzionalità, finalità e alle modalità di funzionamento della carta, nonché all'adempimento dell'obbligo di informativa e alle misure di sicurezza applicate (*v.* anche *Provv.* del Garante del 27 ottobre 2005 sul progetto di carta multiservizi della giustizia [doc. *web* n. 1185160] e *Provv.* 17 giugno 2007, in particolare punto 7 [doc. *web* n. 1417809]).

Trattamento di dati relativi all'infezione da Hiv

Un militare affetto da Hiv ha lamentato che presso il luogo di lavoro presso cui presta servizio non verrebbero adottate adeguate cautele nel trattamento delle informazioni riguardanti le persone sieropositive o affette da Hiv, specie nell'ambito delle verifiche sull'idoneità al servizio degli interessati ad opera delle commissioni medico legali. Considerato il particolare regime di protezione previsto dalla legge n. 135/1990 e dal Codice per i dati sulla salute, e, in particolare, per quelli riguardanti l'Hiv, gli elementi acquisti dall'Ufficio hanno riguardato l'informativa agli interessati, specie in relazione all'indicazione circa la natura obbligatoria o facoltativa del conferimento delle informazioni sullo stato di salute da parte degli interessati, le modalità utilizzate per la trasmissione dell'esito delle visite medico-legali ad altri organi o uffici dell'amministrazione della difesa per i necessari adempimenti in materia di sanità pubblica o di stato giuridico del personale, nonché le misure di sicurezza adottate (*Nota* 19 dicembre 2008).

10.4.2. Rapporto di lavoro in ambito privato

Cedolino elettronico

Con una segnalazione sono stati chiesti chiarimenti sulla conformità alla disciplina di protezione dei dati personali delle modalità *"telematiche"* con le quali una società comunicava il prospetto paga ai dipendenti. Dagli approfondimenti svolti non sono emersi specifici profili di violazione della disciplina, avuto particolare riguardo alle misure di sicu-

rezza adottate dalla società per prevenire indebiti accessi da parte di terzi ai dati contenuti nel *"cedolino elettronico"* (*strong authentication* basata su certificati digitali).

Nondimeno, si è rilevato, da un lato, che la legge n. 4/1953 pone in capo ai datori di lavoro privati l'*"obbligo di consegna"* del prospetto paga ai propri dipendenti onde consentire loro, all'atto della corresponsione della retribuzione, una puntuale verifica in ordine alla correttezza dell'importo erogato; dall'altro, che le modalità telematiche adottate dalla società non fornivano garanzie in tal senso. Pertanto, è stata interessata della questione (anche alla luce della risposta del Ministero del lavoro, della salute e delle politiche sociali ad una recente istanza di interpello) la Direzione provinciale del lavoro territorialmente competente, anche in considerazione dell'ampia utilizzazione dello strumento telematico nel rapporto di lavoro (*cfr. Nota* del 9 aprile 2009).

"Buoni pasto"

Una segnalazione ha evidenziato l'indicazione, sui documenti *"buoni pasto"* forniti da una banca, di alcune informazioni (in particolare, nome e cognome) riferite ai dipendenti che ne fruivano.

La vigente disciplina in materia individua gli specifici requisiti da riportare sui *"buoni pasto"*, ma non include tra questi il nome e il cognome dell'utente (art. 5, d.P.C.M. 18 novembre 2005, attuativo dell'art. 14 *vicies-ter* della legge n. 168/2005). Si è, pertanto, rilevato che tale indicazione risulta idonea a fornire a soggetti terzi (tra i quali la società di emissione del titolo, gli esercizi convenzionati ed eventuali ulteriori possessori del *"buono pasto"*) informazioni attinenti all'attività lavorativa dell'utente medesimo attraverso l'associazione del nominativo dell'interessato alla ragione sociale del datore di lavoro, in violazione del principio di non eccedenza dei dati trattati, sancito dall'art. 11, comma 1, lett. *d*), del Codice. Ciò, tenuto anche conto che le esigenze di correttezza nell'utilizzo del documento di legittimazione previste dalla normativa sopra richiamata possono essere perseguite anche senza indicare il nominativo dell'utente (*ad es.*, attraverso la sottoscrizione dell'utilizzatore già prevista dalla disciplina vigente, eventualmente associata al numero progressivo di identificazione del buono pasto e/o alla ragione sociale o al codice fiscale del datore di lavoro).

Peraltro, in considerazione della disponibilità mostrata dalla società a modificare le

proprie metodologie di predisposizione del documento di fatturazione, non è stata promossa l'adozione di un *provvedimento* da parte del Garante (*Nota* del 27 agosto 2008).

Tesserini identificativi

Da alcune segnalazioni concernenti l'utilizzo – in attuazione di specifiche normative di settore – di tesserini identificativi contenenti le generalità dei lavoratori, sono emerse preoccupazioni per alcune categorie professionali (segnatamente, le *"guardie particolari giurate"*) esposte, per la natura dell'attività espletata, a pericoli per la propria incolumità personale. All'esito degli approfondimenti svolti e alla luce di alcune recenti pronunce in materia, non sono emersi specifici profili di violazione della disciplina in materia di protezione dei dati personali, considerato che il trattamento può essere lecitamente svolto in difetto del consenso degli interessati se effettuato dal titolare in esecuzione di specifici obblighi di legge (*cfr.* art. 24, comma 1, lett. *a*), del Codice). Nondimeno, nel ritenere comunque condivisibili le preoccupazioni espresse in merito all'applicazione delle richiamata normativa di settore a talune categorie di lavoratori *"a rischio"*, l'Autorità ha interessato della questione, per i profili di propria competenza, anche il Ministero del lavoro, della salute e delle politiche sociali (peraltro, in parte, già pronunciatosi con la risposta ad istanza di interpello del 3 ottobre 2008, prot. 25/I/0013426 in riferimento ad un caso similare) (*cfr.*, a titolo esemplificativo, *Nota* del 13 marzo 2009).

Comunicazione dati personali da parte di OO.SS.

Un segnalante ha lamentato che un'organizzazione sindacale, nell'esercizio delle proprie prerogative sindacali, avesse comunicato alcuni dati personali (segnatamente, la qualifica di agente di pubblica sicurezza rivestita e il quantitativo di ore di straordinario accordatogli dall'amministrazione di appartenenza), mediante posta elettronica (il cui utilizzo era stato regolarmente autorizzato dall'amministrazione per finalità di comunicazione con i dipendenti), a tutto il personale.

Al riguardo, premettendo che, contrariamente a quanto richiesto dall'interessato, non rientra tra i compiti dell'Autorità *"ordinare"* all'organizzazione sindacale di diffondere comunicazioni di rettifica sull'asserita divulgazione di dati personali, si è precisato che il *"diritto di affissione"* riconosciuto alle rappresentanze sindacali dall'art. 25 della legge n. 300/1970 può essere esercitato anche a mezzo di *"comunicati inerenti a materie di interesse sindacale e del lavoro"* (circostanza, questa, ritenuta ricorrente nel caso di specie,

anche alla luce dell'assai ampia accezione al riguardo recepita dalla giurisprudenza). Infine, è stato chiarito che ai sensi del combinato disposto di cui agli artt. 136, comma 1, lett. *c*), e 137, comma 3, del Codice, i trattamenti temporanei effettuati per finalità di pubblicazione o diffusione occasionale di *"articoli, saggi e altre manifestazioni del pensiero"* (tra i quali è stata ritenuta annoverabile anche la comunicazione sindacale) non sono soggette a talune disposizioni del Codice (nel caso di specie, per quanto di interesse, al consenso dell'interessato) (*Nota* 11 dicembre 2008).

Comunicazione a terzi di dati relativi alle condizioni di salute di un minore

Un padre ha segnalato un trattamento illecito di dati della figlia minore, portatrice di disabilità grave, da parte della società presso la quale lavora la madre della medesima. In particolare, la struttura di amministrazione del personale, nell'ambito della procedura interna di riconoscimento alla dipendente di un periodo di congedo straordinario per disabilità grave, avrebbe posto illecitamente a conoscenza del superiore gerarchico della madre alcuni dati personali, quali nome, cognome, data di nascita e stato di disabilità dell'interessata.

In base alla documentazione acquisita, non è risultata comprovata l'*"indispensabilità"* del trattamento, richiesta dall'autorizzazione generale n. 1/2007 [doc. *web* n. 1429762], anche in rapporto alle funzioni che il superiore gerarchico poteva svolgere nel caso concreto. Comunque quest'ultimo avrebbe potuto essere coinvolto con modalità meno invasive e parimenti efficaci (*ad es.*, rendendolo edotto solo dell'assenza della dipendente e del relativo intervallo temporale, e non anche della ragione della stessa).

Alla luce di tali considerazioni – e tenuto conto che dalle ragioni dell'assenza possono risultare desumibili informazioni e circostanze afferenti alla sfera privata del lavoratore non rilevanti ai fini della valutazione dell'attitudine professionale del medesimo (art. 8, l. n. 300/1970) – il trattamento di dati personali della minore è stato ritenuto in violazione del principio di pertinenza e di non eccedenza (art. 11, comma 1, lett. *d*), del Codice), oltre che del principio di indispensabilità di cui all'autorizzazione generale n. 1/2007, sicché è stato vietato alla società l'ulteriore messa a disposizione dei dati relativi alla figlia minore del segnalante (*Provv.* 6 novembre 2008, doc. *web* n. 1571485).

Dati relativi alle condizioni di salute e loro conoscibilità all'interno di una società

In un'altra segnalazione, una ex dipendente di una società ha lamentato l'avvenuta comunicazione a terzi (nel caso rappresentato, la sorella) di dati relativi alla propria condizione di salute da parte della società, in assenza del proprio consenso.

In proposito, questa Autorità ha ricordato che il trattamento di dati sensibili può avvenire senza il consenso dell'interessato quando questi, per impossibilità fisica, incapacità di agire o incapacità di intendere e di volere non sia in grado di prestarlo e il trattamento risulti necessario per la salvaguardia della sua incolumità personale (art. 26, comma 4, lett. *b*), del Codice) o per specifici obblighi di legge in materia di sicurezza sul lavoro (art. 26, comma 1, lett. *d*), del Codice). Non risultando la ricorrenza di tali circostanze, l'Autorità ha vietato l'ulteriore comunicazione a terzi dei dati relativi alle condizioni di salute della segnalante (*Provv.* 2 aprile 2008 [doc. *web* n. 1519902]).

Trattamento di dati personali raccolti in occasione di programmi di fidelizzazione e loro utilizzo per fini disciplinari nell'ambito del rapporto di lavoro

Due dipendenti di due distinte società (che gestiscono, alcuni esercizi commerciali) hanno contestato l'utilizzo, da parte dei rispettivi datori di lavoro, di propri dati personali (raccolti per finalità di *marketing*, fidelizzazione e fini statistici) per promuovere un procedimento disciplinare nei loro confronti culminato nel licenziamento (in quanto gli interessati, nella veste di dipendenti dei menzionati esercizi commerciali, *"caricavano"* sulla propria carta di fidelizzazione gli acquisti effettuati dalla clientela).

Dall'istruttoria è emerso che le società, nel perseguire una pur legittima finalità (ovvero l'accertamento di un comportamento ritenuto illegittimo di un lavoratore relativo all'uso indebito di una carta), hanno violato la disciplina di protezione dei dati personali che prevede una preventiva informativa agli interessati sulle concrete modalità di utilizzo dei dati che li riguardano. I dati acquisiti, anziché essere stati trattati nel solo ambito del programma di fidelizzazione (come dichiarato nell'informativa fornita agli interessati), sono stati infatti utilizzati anche per assumere decisioni relative alla gestione del rapporto di lavoro. L'Autorità, non risultando agli atti che in sede di adesione al programma di fidelizzazione gli interessati fossero stati informati sull'utilizzo dei dati raccolti anche per controllare l'esecuzione della prestazione lavorativa e l'osservanza dell'obbligo di fedeltà dei dipendenti, ha vietato alle due società di effettuare, nel contesto del rapporto di lavoro, ulteriori operazioni di trattamento dei dati connessi all'utilizzo della carta di fidelizzazione in viola-

zione dei princìpi di liceità e finalità (art. 11, comma 1, lett. *a*) e *b*), del Codice) (*Provv.* 2 aprile 2008 [doc. *web* n. 1519679] e *Provv.* 6 novembre 2008 [doc. *web* n. 1573780]).

Trattamento di dati personali connesso all'utilizzo di strumenti elettronici

Con un reclamo un'organizzazione sindacale ha contestato l'avvenuta fornitura ai dipendenti, da parte della compagnia aerea di appartenenza, di *computer* portatili (denominati *"e-flight bags"*) idonei non solo all'invio di comunicazioni aziendali in formato elettronico, ma anche a svolgere funzioni ulteriori, tra cui la formazione tecnico-specialistica del personale. In particolare, tale fornitura sarebbe avvenuta, stanti le potenzialità di controllo a distanza dell'attività dei lavoratori insite nello strumento, senza l'osservanza delle procedure a tal fine richieste dall'art. 4 della l. n. 300/1970, oltre che in assenza dell'informativa agli interessati e del loro consenso in ordine al trattamento di dati personali connesso all'utilizzo dello strumento.

Dalla documentazione è emersa l'idoneità dello strumento a controllare a distanza l'attività lavorativa dei dipendenti, in ragione delle funzioni di tracciamento e registrazione degli accessi al corso di formazione (oltre che della relativa durata) utili al monitoraggio dell'andamento del processo formativo degli interessati. Rispetto a tale funzionalità, ritenuta compatibile con le esigenze organizzative dell'azienda, la società non ha comprovato l'avvenuto espletamento delle procedure di cui all'art. 4 della l. n. 300/1970, presupposto indefettibile per la liceità e correttezza del trattamento dei dati (artt. 11, comma 1, lett. *a*) e 114 del Codice). L'Autorità ha quindi disposto, nelle more dell'eventuale espletamento di tali procedure, il blocco dell'ulteriore trattamento dei dati personali riferiti ai dipendenti, limitatamente alle informazioni connesse all'utilizzo dello strumento per finalità formative (*Provv.* 2 aprile 2008 [doc. *web* n. 1519695]).

Trattamento di dati personali svolto nell'ambito di attività investigative interne alla società

Con altro reclamo è stata contestata una procedura interna volta a verificare il corretto operato del reclamante, all'epoca dei fatti amministratore delegato di detta società. L'attività di verifica, avviata a seguito di una denuncia anonima pervenuta al *chief executive officer* della capogruppo estera – che avanzava sospetti di comportamenti illeciti nei confronti del *management* italiano dell'azienda – sarebbe stata condotta dalla società e da un apposito *team* investigativo esterno e avrebbe determinato, all'esito della stessa (peraltro infruttuoso), le dimissioni del reclamante. Tra le operazioni contestate dall'interessato figura, in

particolare, l'acquisizione della corrispondenza a lui indirizzata, estratta dall'account di posta elettronica dal medesimo utilizzato e contenente (a detta del reclamante) anche informazioni comuni e sensibili a lui relative. Il reclamante ha pertanto chiesto all'Autorità la cancellazione e/o distruzione dei messaggi di posta elettronica e il divieto di trattare ulteriormente tali dati.

La società resistente, all'esito di articolate deduzioni, ha invece chiesto la sospensione del procedimento amministrativo sul reclamo innanzi all'Autorità, previa valutazione del rapporto di connessione e pregiudizialità con il giudizio contestualmente pendente presso l'Autorità giudiziaria ordinaria, e ha chiesto in via riconvenzionale il blocco del trattamento delle informazioni riconducibili a terzi e alla medesima società prodotte davanti al giudice ordinario.

L'Autorità ha chiarito che il principio di alternatività tra azione giudiziaria e tutela amministrativa innanzi al Garante è contemplato dal Codice nella sola ipotesi della presentazione di ricorsi, che il reclamo in via riconvenzionale non è previsto e che al Garante non competono valutazioni sulla rilevanza e l'ammissibilità di atti e documenti prodotti in giudizio (neppure per i profili inerenti il trattamento di dati personali) (art. 160, comma 6, del Codice).

Nel merito lo scambio di corrispondenza elettronica con soggetti esterni (siano o meno essi estranei) all'attività lavorativa configura, già di per sé, un'operazione idonea a rendere conoscibili talune informazioni personali relative all'interessato (*ad es.*, i nominativi dei mittenti e/o dei destinatari delle *e-mail*, che possono per sé sole fornire, come i dati di traffico telefonico, indicazioni rilevanti in ordine ai contatti in essere degli interessati e, quindi, essere considerati dati personali ai medesimi relativi). Le operazioni effettuate dalla società sulla corrispondenza elettronica del reclamante, comprovate in atti, integrano quindi un trattamento di dati personali ai sensi dell'art. 4, comma 1, lett. *a*), del Codice, peraltro avvenuto in difformità dalla vigente disciplina di protezione dei dati.

Alla luce della documentazione acquisita, il trattamento effettuato dalla società non è rispettoso dei princìpi di liceità e correttezza (art. 11, comma 1, lett. *a*), del Codice), non essendo stato comprovato che il reclamante fosse stato reso edotto della possibilità di con-

trolli sulla casella di posta elettronica da lui utilizzata, né delle procedure prescritte per il controllo a distanza dell'attività lavorativa (art. 4, legge n. 300/1970).

Inoltre, nel richiamare quanto previsto dal Codice (art. 23, comma 3) e da alcuni recenti provvedimenti in materia (da ultimo *Provv.* 1° marzo 2007 [doc. *web* n. 1387522]), l'Autorità ha ribadito che il consenso dell'interessato si considera validamente prestato solo se manifestato in relazione a un trattamento *"chiaramente"* individuato: circostanza, questa, non desumibile in relazione al caso di specie, non risultando in atti documentata la puntuale conoscenza, da parte del reclamante, delle finalità e delle modalità della raccolta della corrispondenza a sé riferita.

Le risultanze istruttorie hanno poi evidenziato che la società ha comunicato al *project manager* della società incaricata dell'attività investigativa i dati personali del reclamante senza la prescritta informativa e l'eventuale designazione di questi quale responsabile del trattamento (né è risultata provata l'esistenza di altro presupposto di liceità del trattamento per la comunicazione dei dati personali riferiti al reclamante).

Per tali ragioni, è stato vietato alla società l'ulteriore trattamento dei dati personali riferiti all'interessato contenuti nella corrispondenza estratta dall'account di posta elettronica (fatta comunque salva la loro conservazione per la tutela di diritti in sede giudiziaria nei limiti di cui all'art. 160, comma 6, del Codice) (*Provv.* 2 aprile 2008 [doc. *web* n. 1519703]).

Titolare-responsabile

In un quesito, una società specializzata nell'elaborazione e stampa di cedolini paga dei dipendenti per conto terzi (attività che può comportare il trattamento di dati sensibili dei dipendenti medesimi) ha chiesto chiarimenti sull'effettiva necessità di essere designata, da parte delle società *"clienti"*, solitamente in forza di contratti di servizio, quale responsabile del trattamento.

Al riguardo, è stato ribadito che la designazione del responsabile del trattamento, ancorché non obbligatoria (art. 29, comma 1, del Codice), può divenire una soluzione obbligata quando una parte – sia pure strumentale – dei trattamenti necessari per perseguire le finalità del titolare è curata da un soggetto esterno (*Parere* 19 dicembre 1998 [doc. *web* n. 41941]) ad esempio, nell'ambito di un contratto di servizio sottoscritto dal titolare-utilizzatore con la società fornitrice del servizio stesso.

La disciplina vigente riconosce comunque in capo al solo *"titolare"* del trattamento le decisioni in ordine alle finalità e alle modalità dello stesso (art. 4, comma 1, lett. *f*), del Codice), finalità e modalità che, nel caso di specie, non sono state ritenute riconducibili a preventive determinazioni da parte della società richiedente (*Nota* del 20 giugno 2008).

Geolocalizzazione ed *event data recorder*

Una società di trasporto pubblico locale ha presentato un'istanza di verifica preliminare (ai sensi dell'art. 17 del Codice) relativa al trattamento di dati personali dei conducenti dei veicoli in dotazione – nonché di quelli a disposizione delle società controllate – conseguente all'utilizzo di un sistema satellitare di localizzazione basato su tecnologia *Gps* (*Global positioning system*). Il sistema (comprensivo della gestione di una banca dati e del relativo portale di accesso, messi a disposizione della società di trasporto dal fornitore del servizio) risulterebbe idoneo a raccogliere un elevato numero di informazioni, tra cui la localizzazione, la velocità e la direzione dei veicoli, l'osservanza da parte dei conducenti della normativa in tema di circolazione stradale e delle relative prescrizioni aziendali, le condotte di guida degli autisti, il consumo di carburante, la dinamica di eventuali sinistri (mediante dispositivo di registrazione e trasmissione dei dati: *cd. "event data recorder"*), eventuali anomalie tecnico-meccaniche dei veicoli.

Una delle finalità del trattamento sarebbe quella di garantire la sicurezza dei passeggeri e del mezzo. Le informazioni, acquisite automaticamente dal sistema di bordo secondo criteri previamente concordati con il fornitore del servizio (all'accensione e allo spegnimento del veicolo; ogni cinque minuti con veicolo fermo o in movimento; ogni cinque km con veicolo in movimento; all'inizio e al termine di ogni fermata), confluirebbero in una banca dati gestita dal fornitore medesimo. Gli stessi dati, unitamente al servizio per la loro elaborazione (*ad es.*, il tracciato del percorso effettuato), sarebbero resi fruibili all'azienda dal fornitore attraverso un portale ad accesso riservato.

La società ha inoltre dichiarato che le informazioni ottenute e relative alla *"condotta di guida"*, per finalità connesse al rispetto delle prescrizioni normative di marcia in strada e al fine di riconoscere trattamenti economici premianti in favore dei lavoratori sarebbero acquisite solo in forma di indici medi e non sulla base di dati analitici.

L'Autorità ha precisato che i dati che consentono di identificare, anche indirettamente, i

conducenti e quelli relativi allo *"stile di guida"* o registrati mediante l'*"event data recorder"* (in quanto riconducibili, anche in un secondo momento, ad azioni poste in essere dai medesimi) devono ritenersi informazioni personali (art. 4, comma 1, lett. *b*), del Codice). I trattamenti devono comunque avvenire con modalità rispettose, in concreto, dei diritti e delle libertà fondamentali, nonché della dignità degli interessati (art. 2, comma 1, del Codice) e in conformità all'art. 11, comma 1, lett. *a*) del medesimo Codice, con le garanzie e procedure espressamente previste a tutela dei lavoratori dall'art. 4 della legge n. 300/1970.

L'Autorità ha inoltre invitato la società a designare il fornitore (esterno) del servizio di geolocalizzazione quale responsabile del trattamento ai sensi dell'art. 29 del Codice, tenuto conto che la decisione sulle finalità perseguibili nel caso di specie risulta in capo alla sola società di trasporto.

La finalità del trattamento con il sistema *Gps* delle informazioni relative alla localizzazione dei veicoli è stata ritenuta lecita dall'Autorità anche nella prospettiva di potenziale incremento della sicurezza del conducente e delle persone trasportate e della maggiore efficienza del servizio di trasporto pubblico locale. L'Autorità ha poi valutato conforme al principio di necessità (art. 3 del Codice) l'adozione di specifici accorgimenti, come i codici cifrati, funzionali a non rendere conoscibile al fornitore del servizio i dati identificativi dei conducenti.

Parimenti lecito è risultato il trattamento relativo alla "condotta di guida" osservata (sintetizzata in forma di indici medi) per finalità connesse al rispetto delle prescrizioni normative di marcia su strada. Tali informazioni possono essere trattate nel rispetto delle specifiche disposizioni di legge in materia (*cfr.* il d.lg. n. 285/1992 *"Nuovo codice della strada"* e successive modifiche e integrazioni), anche per riconoscere premi in favore dei lavoratori che conformino il proprio stile di guida agli *standard* fissati dalla stessa società. Quest'ultima deve tuttavia selezionare le informazioni pertinenti e non eccedenti ai fini del calcolo degli indici medi da utilizzare per gli anzidetti premi, tenendo presenti i limiti posti dalla normativa di settore (in particolare, il divieto per le imprese di trasporto di *"concedere premi o maggiorazioni di salario in base alle distanze percorse* […], *di natura tale da mettere in pericolo la sicurezza stradale"* (art. 10, reg. Ce n. 561/2006 del 15 marzo 2006).

Anche la *cd. "black box"* (dispositivo di registrazione e trasmissione dei dati) è stata ritenuta lecita dall'Autorità, a condizione che la società espliciti in modo più dettagliato negli atti attuativi le finalità che intende perseguire. Infatti, l'acquisizione di elementi volti alla ricostruzione di un sinistro, può rivelarsi utile anche per accertare condotte non conformi alla disciplina in materia di sicurezza stradale ed eventuali responsabilità in capo ai conducenti.

Per tutte le finalità indicate nel *provvedimento*, il Garante ha comunque prescritto alla società: di fornire ai lavoratori gli elementi previsti dall'art. 13 del Codice in tema di informativa, unitamente a compiuti ragguagli sulla natura dei dati trattati e sulle caratteristiche del sistema, tenuto conto delle diverse finalità perseguite; di consentire l'accesso ai dati riferiti ai conducenti, concernenti la localizzazione o inerenti alle *"condotte di guida"*, ai soli incaricati della società che possono prenderne legittimamente conoscenza in ragione delle mansioni svolte (*ad es.*, in relazione alla circolazione dei veicoli, al personale incaricato di coordinare il servizio di trasporto pubblico nei diversi turni di lavoro; nel caso degli indici medi utili a misurare la *"condotta di guida"*, agli incaricati operanti nella gestione delle risorse umane); di non conservare i dati personali per un tempo superiore a quello necessario al conseguimento delle finalità indicate (avuto particolare riguardo alle informazioni relative alla localizzazione – opportunamente anonimizzate – che potranno essere trattate per le attività di monitoraggio e pianificazione del servizio di trasporto pubblico solo se in forma aggregata); di notificare il trattamento al Garante, con specifico riferimento ai dati relativi alla localizzazione dei lavoratori (*Provv.* 5 giugno 2008 [doc. *web* n. 1531604]).

Trattamento di dati giudiziari dei dipendenti e attività di *rating*

A seguito di una richiesta presentata, ai sensi dell'art. 41 del Codice, da una società di *rating* (controllata da altra società con sede negli Stati uniti d'America) riguardante il trattamento dei dati giudiziari relativi ai propri dipendenti (per adempiere così all'obbligo di registrazione previsto dal *Credit Rating Agency Reform Act* of 2006 e ottenere lo *status* di *"Nationally Recognized Statistical Rating Organisation" - Nsro*), il Garante ha autorizzato la società a trattare i dati giudiziari richiesti limitatamente al solo personale operante nel relativo dipartimento e per la sola finalità dichiarata, nel rispetto, per quanto non diver-

samente stabilito con l'autorizzazione ad hoc, delle prescrizioni di cui all'autorizzazione n. 7/2007 (*Provv.* 31 gennaio 2008 [doc. *web* n. 1488729]).

In sede di rinnovo delle autorizzazioni generali si sono inseriti specifici riferimenti al trattamento di dati giudiziari di lavoratori effettuati da società di rating nell'ambito delle previsioni di cui all'autorizzazione generale n. 7/2008 (*Provv.* 19 giugno 2008, in *G.U.* 21 luglio 2008, n. 169 [doc. *web* n. 1529557]).

10.4.3. Previdenza

Permessi per l'assistenza a familiari disabili

Anche a seguito degli approfondimenti sollecitati dall'Ufficio alla luce dei princìpi di pertinenza, non eccedenza e indispensabilità, come già anticipato nella *Relazione* 2007, l'Inps ha fornito nuove istruzioni (*cfr.* Circolare 29 aprile 2008, n. 53) alle proprie articolazioni organizzative circa la documentazione da presentare per richiedere i permessi per l'assistenza ai familiari disabili in situazione di gravità da parte di dipendenti che lavorano o risiedono in luoghi distanti da quello della persona da assistere (art. 33 legge 5 febbraio 1992, n. 104). Le nuove istruzioni, adottate anche in considerazione delle difficoltà riscontrate nell'attuazione delle precedenti indicazioni, stabiliscono che le sedi dell'istituto si astengano dall'acquisire il *cd. "Programma di assistenza"* a firma congiunta del lavoratore e del disabile, che doveva contenere una pianificazione motivata delle modalità con cui il lavoratore intendeva assistere il familiare.

10.5. ATTIVITÀ DI *MARKETING* E FIDELIZZAZIONE

Con *provvedimento* adottato il 19 giugno 2008 [doc. *web* n. 1526724], recante misure di semplificazione in relazione alle attività amministrative e contabili (più ampiamente illustrato *infra*, al n. 10.8), in applicazione dell'istituto del bilanciamento degli interessi (art. 24, comma 1, lett. *g*), è stata individuata, in tema di *marketing*, un'ipotesi nella quale non va richiesto il consenso dell'interessato.

Il titolare del trattamento che abbia già venduto un prodotto o prestato un servizio, nel quadro dello svolgimento di ordinarie finalità amministrative e contabili, potrà utilizzare i recapiti di posta cartacea forniti dall'interessato medesimo, per inviare ulteriore mate-

riale pubblicitario, promuovere una vendita diretta, compiere ricerche di mercato o per comunicazioni commerciali.

Tale soluzione considera le difficoltà rappresentate da alcuni operatori economici nel conservare un proprio diretto *"canale comunicativo"* con i soggetti con i quali abbiano già instaurato un rapporto contrattuale; tiene al tempo stesso conto del diritto dell'interessato a non essere disturbato mediante comunicazioni promozionali, in base a garanzie analoghe a quelle previste dalla legge per l'uso della posta elettronica (art. 130, comma 4; *v.* anche, con riguardo alle comunicazioni postali, l'art. 58, comma 2, d.lg. n. 206/2005).

Vendita a domicilio e trattamento di dati per finalità di *marketing*

Sono stati effettuati accertamenti presso la sede legale di una società che effettua vendite a domicilio, per verificare l'osservanza della disciplina di protezione dei dati sia nella fornitura di beni e servizi attraverso vendite a distanza previste dalla legge, sia in eventuali operazioni di trattamento volte a verificare l'affidabilità e solvibilità economica della clientela.

È risultato che la società in questione – che commercializza oggetti per la casa – raccoglie le informazioni personali riferite all'utenza e rende l'informativa alla clientela sia con contatti telefonici, sia mediante compilazione di modelli resi disponibili *on-line*, nonché in occasione degli incontri dimostrativi e dell'eventuale stipula del contratto. In quest'ultima circostanza, viene altresì acquisito il consenso al trattamento dei dati personali per le diverse finalità perseguite dalla società. È inoltre risultato che i dati riferiti alla clientela (che ha effettuato acquisti) vengono conservati a tempo indeterminato (attesa la garanzia a vita, contrattualmente prevista, gravante sui beni commercializzati) e vengono utilizzati dalla società anche per finalità di *telemarketing*. Non sono risultati prefissati, invece, i tempi di conservazione dei dati relativi ai clienti che non hanno provveduto ad effettuare acquisti (dati comunque utilizzati dalla società per contatti volti a comprendere le ragioni del mancato acquisto).

Valutati gli elementi in atti, il Garante ha vietato alla società l'ulteriore trattamento dei dati relativi alla clientela utilizzati per finalità di *telemarketing*, atteso che la modulistica impiegata dalla società prevede il rilascio di un unico consenso, manifestato nell'ambito di un più ampio contesto (comprensivo tanto delle attività di *marketing* che di quelle relative alla gestione del rapporto precontrattuale ed, eventualmente, contrattuale), volto ad

autorizzare una pluralità di trattamenti invero ben distinti. La formulazione presente nella modulistica utilizzata dalla società non è risultata dunque idonea a soddisfare i requisiti previsti (posto che il consenso informato deve essere manifestato specificamente in riferimento ad un trattamento chiaramente individuato: art. 23, comma 1, del Codice), ragion per cui il trattamento per finalità di *marketing* è risultato essere stato svolto dalla società in violazione di legge.

L'Autorità ha altresì prescritto alla società l'adozione di alcune misure volte a conformare i trattamenti dei dati riferiti alla clientela alla disciplina di protezione dei dati. Al riguardo, non è infatti risultata idonea l'informativa resa *on-line* – nella sua duplice versione presente sul sito – in quanto carente di alcuni elementi previsti dall'art. 13 del Codice e, quindi, tale da non rappresentare, in modo agevole e trasparente, le varie fasi del trattamento posto in essere dalla società. In proposito, l'Autorità già in passato aveva dettagliatamente evidenziato l'esigenza di rendere in modo chiaro e trasparente l'informativa agli interessati (*Provv.* 13 gennaio 2000 [doc. *web* n. 42276]) anche prescrivendo che l'informativa inserita all'interno di moduli sia adeguatamente evidenziata e collocata in modo autonomo e unitario in un apposito riquadro che la renda agevolmente individuabile (*Provv.* 24 febbraio 2005 [doc. *web* n. 1103045]).

Parimenti, è risultata carente anche l'informativa resa in occasione del contatto telefonico mediante *call center* (contenente l'indicazione di una sola delle finalità del trattamento e priva della menzione dei diritti degli interessati). L'Autorità ha dunque prescritto alla società di integrare le informative (sia quella fornita *on-line* sia quella resa tramite *call center*), con gli elementi mancanti. Ha inoltre prescritto alla società di adottare misure necessarie all'individuazione di tempi massimi certi per la conservazione dei dati personali riferiti alla clientela (salva l'osservanza di espresse disposizioni di legge), nonché la cancellazione o anonimizzazione dei dati la cui conservazione non risulti giustificata (art. 11, comma 1, lett. *e*), del Codice) (*Provv.* 19 maggio 2008 [doc. *web* n. 1526956]).

Consenso dell'interessato

Con un reclamo presentato nei confronti di una concessionaria automobilistica è stata lamentata l'indebita utilizzazione di dati personali per finalità di *marketing*, in assenza di adeguata informativa e di consenso dell'interessato per tale finalità (al quale la modulistica

predisposta riconosceva la sola facoltà di negare il consenso all'uso dei dati). Su tali basi, pertanto, il reclamante ha ricevuto da parte della concessionaria, una volta acquistato il veicolo, alcuni messaggi pubblicitari sia presso il proprio domicilio, con comunicazioni postali, sia mediante *Sms*, sul proprio telefono cellulare.

Gli elementi acquisiti hanno confermato che l'informativa resa al reclamante era carente di taluni elementi prescritti dall'art. 13 del Codice e che non era stato acquisito il consenso espresso dell'interessato ai sensi dell'art. 23, comma 1, del Codice per le finalità di *marketing*. L'Autorità ha quindi disposto che i dati del reclamante non potevano più essere utilizzati per il perseguimento di detta finalità (art. 11, comma 2, del Codice), dando prescrizioni volte a rendere l'informativa conforme all'art. 13 del Codice (*Provv.* 31 gennaio 2008 [doc. *web* n. 1500829]).

10.6. ALTRE ATTIVITÀ IMPRENDITORIALI

Vicenda Alitalia/Cai: cessione in blocco di beni e contratti

Alitalia/Cai hanno rivolto congiuntamente all'Autorità un'istanza, in relazione all'intervenuta cessione di beni e contratti perfezionatisi tra le parti, per chiedere l'esonero dall'obbligo di rendere individualmente l'informativa agli interessati (in quanto comportante un impiego di mezzi sproporzionato rispetto ai diritti tutelati) e la contestuale indicazione di eventuali misure appropriate ai sensi dell'art. 13, comma 5, lett. *c*), del Codice. Le società Cai si sono rese cessionarie, oltre che di complessi di beni e contratti, di interi *database* organizzati in ragione delle diverse categorie di soggetti censiti (equipaggi, soggetti manutentori e certificatori della flotta di aeromobili, oltre quattromila fornitori e alcuni milioni di clienti) facenti capo alle società cedenti, con conseguente mutamento della titolarità in ordine ai trattamenti derivanti dalla cessione.

Il trattamento dei dati (secondo quanto dichiarato dalle società istanti, di regola anagrafici o relativi a transazioni di natura economica) riferito alle menzionate tipologie di interessati sarebbe proseguito in termini sostanzialmente invariati quanto a finalità e modalità; le informazioni rese disponibili dalle società Alitalia alle società Cai per effetto dell'intervenuta cessione, infatti, sarebbero destinate a trattamenti compatibili con gli scopi per i quali le stesse sono state in precedenza raccolte e trattate.

Le società istanti hanno altresì richiesto a questa Autorità, in assenza di altri presupposti di liceità del trattamento (art. 24 del Codice), di trattare i dati personali degli interessati senza il loro consenso; ciò, tenuto conto dell'asserita impossibilità – derivante, oltre che dalla complessità delle citate operazioni di cessione, dal ridotto periodo di tempo a disposizione e dall'elevato numero di soggetti coinvolti nei diversi trattamenti – di richiedere e acquisire il consenso di ciascuno degli interessati, nonché delle immutate finalità e modalità dei trattamenti rientranti nella complessa operazione economica.

Con specifico riferimento all'informativa da rendere agli interessati, l'Autorità, anche in considerazione dell'immutata finalità dei trattamenti dei dati oggetto di cessione e della già ampia notorietà acquisita dalla vicenda, ha accolto la richiesta formulata dalle società, autorizzandole a rendere l'informativa (avente per contenuto gli elementi previsti all'art. 13 del Codice e non già noti agli interessati) mediante la pubblicazione di un annuncio sui siti *web* delle società coinvolte nella cessione e, anche in un unico contesto, su quattro quotidiani previamente individuati, nonché dandone comunicazione agli interessati in occasione della prima circostanza utile di contatto successiva alla cessione.

Per quanto concerne la richiesta di trattare i dati personali degli interessati in assenza del loro consenso, l'Autorità ha ritenuto opportuno distinguere i profili in funzione dei soggetti censiti.

Relativamente alle operazioni di cessione in blocco dei rapporti in essere riferiti sia a clienti creditori di prestazioni derivanti dalla partecipazione a programmi di fidelizzazione delle società Alitalia (quale il programma *"Millemiglia"*), sia a clienti creditori di prestazioni di trasporto successive alle operazioni di cessione (che hanno per lo più già pagato il corrispettivo dovuto), l'Autorità ha ritenuto giustificato il bilanciamento di interessi (art. 24, comma 1, lett. *g*), del Codice), prevedendo la facoltà di prescindere dall'acquisizione del consenso di ciascuno dei *"clienti non volati"* interessati ai fini della comunicazione (e del successivo trattamento) dei dati personali necessari all'esecuzione delle prestazioni destinate ad essere eseguite dalle società Cai, atteso che queste ultime si sono contrattualmente accollate dette obbligazioni (per la cui efficacia, peraltro, l'ordinamento prescinde dal consenso del creditore). Ciò, anche in ragione dell'immutata finalità del trattamento dei dati oggetto

delle operazioni di cessione, del vantaggio derivante in capo agli aderenti a programmi di fidelizzazione (che vedono preservate eventuali pretese maturate o maturande) e, in relazione ai clienti che abbiano già acquistato un titolo di viaggio, considerate le esigenze di speditezza e continuità del servizio pubblico essenziale di trasporto aereo.

Per quanto attiene ai dati personali coinvolti nella cessione e riferiti a contratti intercorrenti tra le società Alitalia e Cai (indicati analiticamente nel contratto di cessione), l'Autorità ha ritenuto integrata la fattispecie prevista nell'art. 24, comma 1, lett. *b*), del Codice, sì che il trattamento dei dati personali riferibili ai contraenti ceduti che abbiano prestato il consenso alla cessione del contratto che li legava alle società Alitalia (cedenti) deve ritenersi lecito (in relazione alle medesime finalità originariamente perseguite) anche in assenza del loro consenso.

Con riferimento, ancora, alla comunicazione di informazioni personali relative a contratti di trasporto già eseguiti (*cd. "clienti volati"*), come pure relativi a fornitori che hanno prestato i propri servizi nei confronti delle società Alitalia, l'Autorità ha ritenuto integrati gli estremi di cui all'art. 24, comma 1, lett. *a*), del Codice. Infatti, tali informazioni (organizzate in distinti *database*) sono state oggetto di apposita pattuizione tra le parti, concorrendo alla complessiva valutazione dell'operazione dal punto di vista economico. Al riguardo, in considerazione del fatto che il commissario straordinario è tenuto, a liquidare le poste attive e a trasferire le utilità suscettibili di essere annoverate, secondo la valutazione delle parti, nell'ambito della *"cessione di beni e contratti"* (alla luce dell'articolato quadro normativo vigente), l'Autorità ha ritenuto lecita la comunicazione delle informazioni contenute nei predetti *database* in assenza del consenso degli interessati, stante la citata previsione normativa di cui all'art. 24, comma 1, lett. *a*), del Codice. Peraltro l'Autorità ha comunque atto del fatto che il trattamento sarà limitato unicamente all'esecuzione, in forma aggregata, di indagini di mercato e per eseguire proiezioni di tipo statistico e di ricerca (come da dichiarazioni delle società istanti).

Anche in relazione ai dati personali riferiti agli equipaggi, ai soggetti manutentori e ai certificatori della flotta di aeromobili, il trattamento è stato ritenuto lecito dall'Autorità in assenza del consenso degli interessati (purché nel rispetto del principio di finalità); ciò,

in base alla previsione contenuta nel citato art. 24, comma 1, lett. *a*) del Codice. Infatti, tali informazioni corrispondono sostanzialmente a quelle previste per la regolare tenuta dei registri di aeronavigabilità di cui al Regolamento (Ce) 2042/2003 della Commissione europea del 20 novembre 2003 e le medesime sono oggetto, altresì, di apposita previsione (in relazione alla tenuta e conservazione del quaderno tecnico di bordo) nel Regolamento tecnico adottato dall'Ente nazionale per l'aviazione civile-Enac, adottato ai sensi dell'art. 687 del r.d. 30 marzo 1942, n. 327 (codice della navigazione).

L'Autorità si è comunque riservata di svolgere eventuali verifiche in relazione agli altri trattamenti di dati personali effettuati dalle società Cai (*Provv.* 8 gennaio 2009 [doc. *web* n. 1580603]).

10.7. ATTIVITÀ DI IMPRESA E CONTROLLI

Trattamento di dati personali nell'ambito di una procedura di rimborso di biglietti aerei

Una segnalazione ha lamentato che le procedure previste da una compagnia aerea per il rimborso dei biglietti acquistati via Internet mediante carta di credito richiedevano, tra i documenti da allegare, anche copia dell'estratto conto della carta di credito dell'acquirente.

Al riguardo, la società ha precisato che le informazioni richieste (peraltro non riferite all'intera movimentazione bancaria del cliente, ma solo ed esclusivamente all'operazione di acquisto del biglietto da rimborsare) risultavano necessarie per identificare l'effettivo titolare della carta di credito, unico soggetto deputato a ricevere l'accredito dell'importo versato per l'acquisto del titolo di viaggio. La medesima società ha inoltre attestato la presenza, all'interno del proprio sito *web*, di una *privacy policy* aziendale, nella quale sono enunciate e spiegate in maniera chiara e puntuale le finalità della raccolta e del trattamento dei dati personali dell'interessato (cliente/passeggero), ivi compresi i profili di trattamento correlati alle procedure di rimborso dei biglietti. Le dichiarazioni e la documentazione prodotte – unitamente al fatto che il modulo disponibile sul sito della compagnia aerea reca espressamente l'informativa fornita agli interessati in ordine al trattamento dei propri dati personali connesso alle procedure di rimborso – non hanno reso opportuna l'adozione di un provvedimento da parte dell'Autorità (artt. 14, comma 2, e 11, comma 1, lett. *d*), regolamento del Garante n. 1/2007) (*Nota* del 30 ottobre 2008).

"Recupero crediti"

Nonostante il *provvedimento* generale del 30 novembre 2005 [doc. *web* n. 1213644] continuano a pervenire numerose segnalazioni che, al di là del relativo esito, evidenziano la necessità per l'Autorità e per gli operatori del settore di mantenere alta la soglia di attenzione di questa delicata tematica.

Anche per queste ragioni e alla luce delle recenti modifiche apportate all'art. 115 del r.d. n. 773/1931 (Tulps) – che abilitano le società di recupero dei crediti allo svolgimento delle proprie attività *"senza limiti territoriali"* (art. 4 l. 6 giugno 2008 n. 101; Circ. Ministero interno n. 557/pas/11858.12015 dell'8 gennaio 2008) – l'Autorità, con nota del 27 novembre 2008, ha richiamato l'attenzione del Ministero dell'interno sul fenomeno in oggetto (comunicando allo stesso il *provvedimento* generale) anche in vista dell'adozione di eventuali iniziative di sua competenza, con riserva di inoltrare alle singole questure territorialmente interessate le specifiche segnalazioni, per consentire opportune verifiche anche in relazione all'applicazione della disciplina contenuta nel Tulps. A seguito di tale comunicazione vi sono stati proficui contatti tra l'Ufficio del Garante e rappresentanti del Ministero dell'interno volti ad identificare le aree di possibile interferenza tra le discipline di rispettiva competenza e di possibile collaborazione.

10.8. SEMPLIFICAZIONI NEGLI ADEMPIMENTI CONTABILI E AMMINISTRATIVI

Finalità amministrative e contabili

Nel 2008, nel solco di iniziative adottate in passato, il Garante è nuovamente intervenuto in materia di semplificazione, snellendo gli adempimenti nei trattamenti per finalità amministrative e contabili, le procedure relative alle misure minime di sicurezza, nonché introducendo ulteriori semplificazioni al modello utilizzato per effettuare la notificazione al Garante.

Il primo *provvedimento*, adottato il 19 giugno 2008 [doc. *web* n. 1526724], reca misure di semplificazione per l'intero settore pubblico e privato in relazione alle attività amministrative e contabili, in particolare nei riguardi di piccole e medie imprese, liberi professionisti e artigiani.

In esso vengono individuate soluzioni concrete per agevolare ulteriormente l'ordinaria attività di gestione amministrativa e contabile, in modo particolare nei casi in cui non

sono trattati dati di carattere sensibile o giudiziario, per rendere più snelle le procedure burocratiche e più semplici i moduli dell'informativa, favorendo una più agevole comprensione dei cittadini sulle modalità e finalità del trattamento dei dati personali.

Il Garante ha inoltre fornito indicazioni specifiche per la redazione di un'informativa unica per il complesso dei trattamenti di dati personali a fini esclusivamente amministrativi e contabili. Gli operatori potranno anche redigere una prima informativa breve rinviando ad un testo più articolato disponibile su siti Internet, reti Intranet, in bacheche o presso gli sportelli al pubblico del titolare del trattamento.

Le associazioni di categoria sono state invitate a predisporre informative-tipo per determinati settori o categorie di trattamenti, prevedendo la messa a disposizione, gratuitamente, di un *kit* di istruzioni concrete e *fac-simili* per facilitare l'opera di semplificazione degli adempimenti previsti.

Alle indicazioni relative all'informativa si aggiungono quelle relative al consenso, che deve essere acquisito solo nei casi veramente necessari.

Il Garante, considerati i princìpi di efficacia e proporzionalità e in relazione agli artt. 2, 18, comma 4, 24, comma 1, e 154, comma 1, lett. *c*), del Codice, ha chiarito che il consenso non deve essere richiesto in particolare, quando:

- il trattamento dei dati in ambito privato è svolto per adempiere a obblighi contrattuali o normativi o, comunque, per ordinarie finalità amministrative e contabili;
- i dati trattati provengono da pubblici registri ed elenchi pubblici conoscibili da chiunque o sono relativi allo svolgimento di attività economiche dell'interessato.

Misure di sicurezza

L'art. 29 del decreto-legge 25 giugno 2008, n. 112 (convertito in legge il 6 agosto 2008, n. 133) ha modificato gli artt. 34 e 38 del Codice.

In particolare, nell'art. 34 è stato aggiunto il comma 1-*bis*, in base al quale per tutte le imprese che trattano soltanto dati personali non sensibili e che trattano solo i dati sensibili relativi allo stato di salute dei dipendenti e collaboratori (certificati medici senza indicazione della relativa diagnosi) ovvero all'adesione ad organizzazioni sindacali, la tenuta di un aggiornato documento programmatico sulla sicurezza è sostituita dall'obbligo di autocertificazione, resa dal titolare del trattamento ai sensi dell'art. 47 del t.u. di cui al d.P.R. 28 dicembre 2000, n. 445.

Inoltre, il citato comma 1-*bis* ha demandato al Garante la semplificazione del Disciplinare tecnico in materia di misure minime di sicurezza.

In attuazione di tale previsione, gli adempimenti a carico dei titolari del trattamento sono stati rimodulati in funzione delle effettive caratteristiche dimensionali o di struttura delle imprese, della natura dei trattamenti, nonché in considerazione di esigenze di riduzione dei costi (*Provv.* 27 novembre 2008 [doc. *web* n. 1571218]. Le nuove garanzie, adottate sentito il Ministro per la semplificazione normativa, interessano:

a) amministrazioni pubbliche e società private che utilizzano dati personali non sensibili (nome, cognome, indirizzo, codice fiscale, numero di telefono) o che trattano come unici dati sensibili dei dipendenti quelli relativi allo stato di salute o all'adesione a organizzazioni sindacali;

b) piccole e medie imprese, liberi professionisti o artigiani che trattano dati solo per fini amministrativi e contabili.

In base al *provvedimento* del Garante, le categorie interessate:

- possono impartire anche oralmente le istruzioni agli incaricati in materia di misure minime;
- possono utilizzare per l'accesso ai sistemi informatici un qualsiasi sistema di autenticazione basato su un username e una *password*; lo username deve essere disattivato quando viene meno il diritto di accesso ai dati;
- in caso di assenze prolungate o di impedimenti del dipendente possono mettere in atto procedure che consentano comunque l'operatività e la sicurezza del sistema (*ad es.*, l'invio automatico delle *e-mail* ad un altro recapito accessibile);
- devono aggiornare i programmi di sicurezza (antivirus) almeno una volta l'anno ed effettuare *backup* dei dati almeno una volta al mese.

Con il *provvedimento*, inoltre, il Garante ha fornito a piccole e medie imprese, artigiani, liberi professioni, soggetti pubblici e privati che trattano dati solo a fini amministrativi e contabili, alcune indicazioni per la redazione di un documento programmatico per la sicurezza semplificato.

Procedure semplificate sono state indicate anche per chi tratta dati senza l'impiego di sistemi informatici.

Notificazione

Nel nuovo testo dell'art. 38 del Codice è stato sostituito il comma 2, precisando e circoscrivendo il contenuto del modello che deve essere utilizzato per effettuare la notificazione.

Insieme con quello sulle misure minime di sicurezza, il Garante ha adottato in data 22 ottobre 2008 [doc. *web* n. 1571196] un *provvedimento* che, in linea con le semplificazioni già adottate in precedenza snellisce ulteriormente il modello utilizzato per effettuare le notificazioni, e che non comporta l'obbligo di modificare le notificazioni già presentate.

11. Trasferimento di dati personali all'estero

La tematica delle *cd.* "*Binding corporate rules* (*Bcr*)" (Norme vincolanti d'impresa, *v. infra*, *par.* 20.1 e 20.7) ha formato oggetto di intenso lavoro anche nel corso del 2008, in particolare con riferimento alle numerose richieste, pervenute da parte di altre autorità di controllo, nell'ambito dell'attivazione di procedure di cooperazione concernenti alcuni progetti di *Bcr* elaborati da vari gruppi societari di carattere multinazionale.

L'Autorità italiana ha intensificato l'attività di verifica della richiesta, avanzata nel 2007 (*v. Relazione* 2007, *p.* 115) da un gruppo bancario italiano, volta a instaurare la procedura di coordinamento per l'approvazione di *Bcr* innanzi al Garante in qualità di *lead authority*, in ordine al trattamento di dati relativi al personale dipendente.

Constatata la sussistenza dei presupposti ad agire nell'ambito della procedura di cooperazione (in conformità al documento WP 107 del Gruppo art. 29) e ottenuta conferma, da parte delle altre Autorità interessate, a procedere in veste di *lead authority*, il Garante ha intrapreso una puntuale attività di analisi del testo preliminare di *Bcr* presentato dal gruppo societario, al fine di verificarne la conformità con i criteri di adeguatezza sanciti dai documenti del Gruppo art. 29 (*cfr.* WP 74 e 153). Tale riflessione ha determinato l'attiva partecipazione della società, cui sono state fornite diverse indicazioni volte a suggerire alcune modifiche al menzionato progetto di *Bcr*, soprattutto in vista dell'approvazione di alcuni nuovi documenti in ambito europeo (*cfr.* WP 153, 154 e 155) e della recente modifica legislativa al Codice (*cfr.* art. 44, lett. *a*), del Codice, come modificato dalla legge 6 agosto 2008, n. 133).

Nel 2008 si è, infatti, assistito all'intensificazione delle attività di approfondimento in materia di *Bcr* da parte del Gruppo art. 29, attraverso l'approvazione di tre documenti (*v.* anche, *par.* 20.1), volti a precisare alcuni aspetti di fondamentale importanza.

A tali nuovi sviluppi in sede europea si è accompagnato il recente intervento legislativo di modifica dell'art. 44 del Codice, già invocato dal Garante con apposita segnalazione al Parlamento e al Governo adottata nel corso del 2007 (*cfr. Relazione* 2007, *p.* 115).

Il nuovo testo, nell'includere le regole di condotta osservate all'interno di gruppi di società tra gli strumenti considerati adeguati ai fini del trasferimento dei dati personali al

di fuori dell'Ue e dello Spazio economico europeo, ha determinato l'entrata a pieno titolo del Garante nel novero delle Autorità in grado di rilasciare un'autorizzazione al trasferimento dei dati personali verso Paesi terzi, che non offrano adeguate garanzie di tutela, tramite lo strumento delle *Bcr*.

La norma non risolve tutte le questioni relative all'efficacia vincolante dello strumento delle *Bcr* nell'ordinamento italiano, pur collocandosi in un'ottica garantista volta ad imporre alle società l'obbligo di assicurare agli interessati l'esercizio dei propri diritti nell'ambito del territorio dello Stato italiano, in ordine all'inosservanza delle *Bcr* medesime (*cfr.* art. 44, lett. *a*), secondo capoverso del Codice).

12. Attività forense

Anche nel 2008 si è registrato un incremento dell'attività legata alle segnalazioni e ai reclami pervenuti in materia di attività forense, con riferimento al trattamento di dati personali, spesso sensibili, effettuato dagli avvocati e dalle agenzie investigative nell'ambito di procedimenti giudiziari civili e penali, specie in materia di separazione tra coniugi.

Di particolare rilievo appare la sottoscrizione, avvenuta il 27 ottobre 2008 da parte delle associazioni rappresentative dell'avvocatura e degli investigatori privati, del *"Codice di deontologia e di buona condotta per il trattamento di dati personali effettuato per svolgere le investigazioni difensive o per far valere o difendere un diritto in sede giudiziaria"* (*G.U.* 24 novembre 2008, n. 275, in vigore dal 1° gennaio 2009 e allegato al Codice [doc. *web* n. 1565171]).

In materia di attività forense l'attenzione del Garante si è concentrata sulle modalità di acquisizione e utilizzazione delle prove dedotte in giudizio da parte degli avvocati.

È emersa infatti l'esigenza di richiamare gli operatori del settore ad un più attento rispetto dei princìpi di liceità, correttezza ed essenzialità del trattamento posto in essere, con riferimento alle modalità di acquisizione e raccolta dei dati stessi, soprattutto nell'ambito del processo civile e nei casi di giudizi di separazione tra coniugi.

In risposta a segnalazioni pervenute l'Autorità ha comunque ribadito che valutare la validità, l'efficacia e l'utilizzabilità nel procedimento giudiziario di documenti e provvedimenti, anche se basati su un trattamento di dati personali non legittimo, spetta al giudice e non al Garante.

Il codice di deontologia e di buona condotta

Gli aspetti di maggiore novità introdotti dal codice per le indagini difensive, il cui rispetto costituisce, come noto, condizione essenziale per la liceità e la correttezza dei trattamenti di dati personali (art. 12, comma 3, del Codice), riguardano l'ambito di applicazione, i tempi di conservazione delle informazioni, i rapporti con i terzi e la stampa e le modalità di trattamento dei dati personali per le finalità sopra richiamate.

In particolare, gli avvocati e gli investigatori privati possono informare la clientela anche oralmente in modo semplice e colloquiale sull'uso che verrà fatto dei loro dati personali. L'informativa scritta potrà anche essere affissa nello studio o pubblicata sul sito *web*.

I soggetti destinatari del codice deontologico devono fornire istruzioni al personale di studio in modo da adottare speciali cautele in caso di utilizzo di registrazioni audio/video, di tabulati telefonici, di perizie e di ogni altra documentazione utilizzata, e vigilare affinché si eviti l'uso ingiustificato di informazioni che potrebbero comportare gravi rischi per il cliente. Atti e documenti, una volta estinto il procedimento o il mandato, possono essere conservati, in originale o in copia, solo se necessari per altre esigenze difensive della parte assistita o dell'avvocato.

Gli investigatori, da parte loro, non possono intraprendere di propria iniziativa investigazioni, ricerche o altre forme di raccolta dei dati. Le investigazioni sono lecite solo se l'incarico è conferito per iscritto da un difensore o da un altro soggetto. L'incarico ricevuto va eseguito personalmente: ci si può avvalere di altri investigatori privati se nominati all'atto del conferimento oppure successivamente purché tale possibilità sia stata prevista. Conclusa l'attività investigativa, e comunicati i risultati al difensore o a chi ha conferito l'incarico, i dati raccolti devono essere cancellati. L'archivio deve essere periodicamente controllato e contenere solo informazioni pertinenti ed indispensabili.

Dati genetici e difesa in giudizio

Con *provvedimento* del 27 novembre 2008 [doc. *web* n. 1581365] il Garante si è pronunciato in materia di trattamento di dati genetici da parte di avvocati e investigatori privati.

Il *provvedimento* trae origine da una vicenda in cui, su incarico del legale del genitore, un'agenzia di investigazioni ha prelevato campioni genetici del figlio, all'insaputa di questi, poi sottoposti, senza informare l'interessato, al *test* per appurare la compatibilità genetica tra figlio e genitore. Venuto a conoscenza del fatto al momento della proposizione dell'azione di disconoscimento di paternità proposta dal padre, il figlio si è rivolto al Garante. La società di investigazioni e l'avvocato si sono difesi affermando che la legge garantirebbe la possibilità di effettuare analisi genetiche senza richiedere il consenso dell'interessato qualora si tratti di far valere o difendere un diritto in sede giudiziaria.

L'Autorità ha invece ritenuto violati i diritti del figlio e ha vietato al genitore e al suo legale l'ulteriore trattamento dei dati genetici acquisiti, salvo quelli già depositati in giudizio.

Ha ricordato che, anche sulla base delle prescrizioni impartite dal Garante con le autorizzazioni generali al trattamento dei dati genetici, la raccolta e il trattamento di tale tipologia di dati, di natura particolarmente delicata, può avvenire esclusivamente con il consenso informato, *"manifestato previamente e per iscritto"*, dell'interessato. Si può derogare all'obbligo del previo consenso per far valere o difendere un proprio diritto in sede giudiziaria, ma solo nel caso in cui l'accertamento sia assolutamente *"indispensabile"*, circostanza che non ricorreva nel caso di specie.

13. Trattamento dei dati personali in ambito condominiale

Continuano a pervenire numerose segnalazioni, dal contenuto più vario, relative ad attività connesse all'amministrazione dei condomìni, già oggetto del *provvedimento* generale 18 maggio 2006 [doc. *web* n. 1297626] (Per quanto riguarda la videosorveglianza in ambito condominiale si rimanda al *par.* 15.3).

Dati personali nel regolamento condominiale

In una segnalazione la proprietaria di un immobile ha lamentato l'avvenuta indicazione, nell'atto di deposito del regolamento di condominio, del proprio stato civile (di persona legalmente separata) da parte dell'impresa costruttrice dell'immobile stesso. Invitata a fornire chiarimenti, la società in questione ha precisato che l'indicazione dello stato civile nella nota di trascrizione del regolamento condominiale risultava necessaria in quanto l'art. 2659 c.c. impone al richiedente la trascrizione di un atto tra vivi di presentare presso la conservatoria dei registri immobiliari una nota contenente anche il *"regime patrimoniale"* delle parti. Di qui la necessità di indicare la condizione di legalmente separata della segnalante, in quanto funzionale all'indicazione dello stesso regime patrimoniale di separazione dei beni della stessa. Alla luce di tale disposizione l'Autorità dopo aver richiesto alla segnalante eventuali ulteriori elementi di valutazione, non ha ravvisato violazioni della disciplina in materia di protezione dei dati personali (*Nota* del 3 ottobre 2008).

Dati personali nelle tabelle relative alle spese di riscaldamento

In una segnalazione una condòmina ha contestato che nella tabella di ripartizione delle spese di riscaldamento fosse indicata la sua qualità di ex moglie di altro condomino. Poiché il condominio (tramite l'amministratore) ha dichiarato di essersi attivato ai fini della rettifica dell'anagrafica del riparto del riscaldamento non si è ritenuto necessario promuovere l'adozione di un provvedimento da parte dell'Autorità (artt. 14, comma 2, e 11, comma 1, lett. *d*), reg. Garante n. 1/2007) (*Nota* 31 ottobre 2008).

Partecipazione di terzi all'assemblea condominiale

In un caso, è stato chiesto di verificare se la partecipazione di alcuni soggetti non appartenenti alla compagine condominiale a due assemblee di condominio fosse conforme alla disciplina di protezione dei dati. Dalle risultanze istruttorie non è risultato chiaro a che titolo uno dei predetti soggetti avesse partecipato ad una delle due assemblee. Nondimeno, considerato che l'amministratore di condominio ha dichiarato, ai sensi dell'art. 168 del Codice, di aver preso atto delle indicazioni fornite dall'Autorità e di averne

fatto puntuale applicazione nei confronti dei soggetti attualmente amministrati, non si sono ravvisati gli estremi per promuovere l'adozione di un provvedimento da parte dell'Autorità (artt. 14, comma 2, e 11, comma 1, lett. *d*), reg. Garante n. 1/2007) (*Nota* 20 gennaio 2009).

L'Autorità è intervenuta anche nei confronti di due reclamanti che hanno lamentato, nel corso di un'assemblea condominiale tenutasi nel 2005, l'avvenuta comunicazione ad estranei alla compagine condominiale di dati personali relativi al loro contenzioso con il condominio, nonché alla loro condizione di morosità. Dagli elementi acquisiti non è risultato provato che i soggetti estranei (un tecnico e il rappresentante legale di una ditta appaltatrice di lavori condominiali) avessero assistito solamente alla trattazione del punto all'ordine del giorno che li riguardava, poiché il verbale non dava conto di tale circostanza. L'Autorità ha quindi ravvisato nel caso una comunicazione a terzi dei dati personali dei reclamanti, in violazione del principio di pertinenza e non eccedenza (art. 11, comma 1, lett. *d*), del Codice), oltre che in assenza del consenso degli interessati (ovvero di altro presupposto di liceità del trattamento: art. 24 del Codice). Il titolare del trattamento è stato pertanto invitato a fornire riscontro (regolarmente pervenuto) in ordine alle misure adottate per evitare, in futuro, il ripetersi di eventi analoghi (*Nota* 16 aprile 2008).

Comunicazione di dati personali in occasione di contratti di fornitura di beni e servizi

Alcuni rappresentanti dell'Anaci hanno formulato a questa Autorità un quesito (occasionato dalla sentenza Cass. S.u. 8 aprile 2008, n. 9148) sulla liceità della comunicazione nei confronti di fornitori di beni e servizi condominiali (di regola a cura dell'amministratore) di dati personali dei condomini. Richiamati preliminarmente i princìpi sanciti nel *Provv.* del 18 maggio 2006 [doc. *web* n. 1297626], è stato rappresentato che, anche a seguito della richiamata sentenza, non sono ravvisabili ostacoli alla menzionata comunicazione. Infatti, questa può essere effettuata in assenza del consenso degli interessati per dare esecuzione agli obblighi derivanti da un contratto stipulato dai partecipanti alla compagine condominiale, ancorché di regola per il tramite dell'amministratore (art. 24, comma 1, lett. *b*), del Codice), ed eventualmente per far valere o difendere un diritto in sede giudiziaria (art. 24, comma 1, lett. *f*), del Codice). Le informazioni comunicate devono essere comunque pertinenti e non eccedenti (tali possono ritenersi quelle che con-

sentono di identificare i condòmini obbligati al pagamento di corrispettivi dei contratti, le rispettive quote millesimali ed eventuali ulteriori informazioni necessarie a determinare le somme individualmente dovute) (*Nota* 26 settembre 2008).

Affissione di dati personali in spazi condominiali accessibili al pubblico

Il conduttore di una stanza di un appartamento di proprietà di un condominio ha lamentato l'avvenuta diffusione della notizia relativa alla scadenza prossima del suo contratto di locazione e la contestuale intimazione al rilascio dell'immobile da parte della stessa compagine condominiale, ancorché per il tramite dell'amministratore. L'avviso avrebbe potuto essere comunicato agli altri condomini con modalità alternative all'affissione nella bacheca condominiale, quali l'inserimento nelle cassette postali di una comunicazione individualizzata.

Il condominio (in persona dell'amministratore), invitato ad adeguarsi alle prescrizioni del *Provvedimento* 18 maggio 2006 [doc. *web* n. 1297626], ha dichiarato di aver immediatamente sostituito il predetto avviso con altro privo di indicazione di dati personali. Il segnalante ha però contestato che il *"nuovo"* avviso, benché privo di riferimenti espressi, conteneva tuttavia indicazioni idonee a renderlo identificabile, ancorché indirettamente (art. 4, comma 1, lett. *b*) del Codice).

L'Autorità, ritenendo fondata la segnalazione (anche in ragione del fatto che la disdetta del contratto di locazione avrebbe potuto essere comunicata con modalità tali da non renderne edotti soggetti estranei alla compagine condominiale), ha vietato al condominio l'ulteriore diffusione dei dati personali riferiti anche indirettamente al segnalante e relativi alla scadenza del contratto di locazione (*Provv.* 20 novembre 2008 [doc. *web* n. 1576139]).

Assemblea condominiale e divulgazione dati personali

Alcuni condòmini hanno lamentato un'illecita divulgazione della loro situazione debitoria nei confronti del costruttore del medesimo immobile a fronte della fornitura, resa loro in passato di servizi per l'erogazione di energia elettrica da parte dell'amministrazione condominiale, che avrebbe allegato all'avviso di convocazione dell'assemblea di condominio un prospetto contenente anche i predetti dati. A detta dei segnalanti la predetta situazione debitoria sarebbe stata ascrivibile a spese afferenti non la gestione condominiale, ma servizi fruiti uti singuli dagli interessati. L'istruttoria espletata ha confermato la fondatezza di questa prospettazione, sicché le modalità di comunicazione sono risultate in contrasto

con la disciplina applicabile (art. 23 del Codice; *Provv.* 18 maggio 2006 [doc. *web* n. 1297626]). Il condominio (tramite dell'amministratore) è stato invitato ad adeguarsi ai princìpi di protezione dei dati personali richiamati nel menzionato *provvedimento* generale; a seguito del riscontro fornito non sono stati ravvisati presupposti per l'adozione di un provvedimento da parte dell'Autorità (art. 14, comma 2, e 11, comma 1, lett. *d*), reg. Garante n. 1/2007) (*Nota* 26 giugno 2008).

14. Sicurezza dei dati e dei sistemi

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

Il Garante, anche nel 2008 ha seguito con attenzione le questioni legate al tema della conservazione dei dati di traffico telefonico e telematico sia per finalità di accertamento e repressione dei reati sia per altre finalità ordinarie.

Nella *Relazione* 2007 si è riferito del *provvedimento* del 17 gennaio 2008 (*G.U.* 5 febbraio 2008 n. 30 [doc. *web* n. 1482111]), con il quale l'Autorità ha prescritto ai fornitori di servizi di comunicazione elettronica accessibili al pubblico, ai sensi degli artt. 17, 123 e 132 del Codice, l'adozione entro il 31 ottobre 2008 di specifici accorgimenti e misure in grado di garantire un elevato livello di protezione dei predetti dati di traffico.

Il *provvedimento* del 17 gennaio è stato successivamente aggiornato con quello del 24 luglio 2008 (*G.U.* 13 agosto 2008, n. 189 [doc. *web* n. 1538224]), in ragione delle modifiche nel frattempo apportate alla normativa di riferimento da diversi interventi legislativi quali, in particolare, il d.lg. 30 maggio 2008, n. 109 e la l. 18 marzo 2008, n. 48.

Con tale *provvedimento* il Garante ha inoltre accolto – in ragione della complessità degli interventi necessari per adeguare i sistemi informativi dei fornitori alle prescrizioni del *provvedimento*, nonché delle predette modifiche normative – la richiesta presentata singolarmente da alcuni gestori, nonché dall'associazione Asstel, di un differimento del suindicato termine del 31 ottobre 2008.

Il termine è stato così prorogato al 30 aprile 2009 con riferimento alle nove prescrizioni previste per i trattamenti di dati per finalità di accertamento e repressione dei reati, nonché alle cinque prescrizioni relative ai trattamenti di dati ai sensi dell'art. 123 del Codice. È stato infine differito al 30 giugno 2009, il termine riguardante la *strong authentication* riferita agli incaricati che accedono ai dati di traffico nell'ambito dell'attività di *call center*.

Successivamente, nel mese di aprile 2009 sono pervenute all'Autorità numerose richieste da parte di alcune associazioni rappresentative del mondo delle telecomunicazioni, con

le quali è stata descritta una situazione di sostanziale, ma non ancora integrale, adeguamento, per la quasi totalità dei fornitori, alle prescrizioni contenute nel *provvedimento* del 24 luglio 2008 in materia di *data retention*, con particolare riferimento alle misure e agli accorgimenti prescritti alla lettera *a*), nn. 3, 6 e 9 e alla lettera *c*) dello stesso.

Le medesime associazioni hanno, quindi, richiesto al Garante un rinvio dei termini indicati nel *provvedimento*, al fine di realizzare il completamento dell'attuazione delle richiamate prescrizioni.

Il Garante in ragione dell'elevato numero di piattaforme e sistemi aziendali coinvolti negli adempimenti previsti dal *provvedimento*, e, quindi, della complessità degli interventi necessari ha accordato la richiesta proroga, limitatamente alle misure specificamente indicate.

L'Autorità, pertanto, con il *provvedimento* del 29 aprile 2009 (in corso di pubblicazione nella *G.U.* [doc. *web* n. 1612508]), ha fissato il nuovo termine al 15 dicembre 2009, prevedendo altresì che, entro la medesima data, tutti i titolari del trattamento interessati debbano dare conferma al Garante delle misure e degli accorgimenti adottati, attestandone l'integrale adempimento (*cfr.* lett. *b*) del *provvedimento* 24 luglio 2008).

Come si è detto, il quadro normativo in materia di conservazione dei dati di traffico (*v.* anche, *par.* 2.1.) a partire dall'entrata in vigore del Codice, ha subito numerose modificazioni ad opera di altrettanti interventi legislativi, che hanno fissato di volta in volta differenti tempi di conservazione dei dati di traffico telefonico e telematico.

L'art. 132 del Codice, modificato prima della sua entrata in vigore dal d.l. n. 354/2003 (convertito in legge, con modificazioni, dall'art. 1 della l. n. 45/2004), ha introdotto un distinto obbligo, per i fornitori di servizi di comunicazione elettronica, di conservare per finalità di accertamento e repressione dei reati i dati di traffico telefonico relativi ai servizi offerti per due periodi di ventiquattro mesi ciascuno.

Un successivo provvedimento d'urgenza del 2005 (d.l. n. 144/2005, convertito in legge, con modificazioni, dall'art. 1 della l. n. 155/2005) ha poi introdotto: l'obbligo di conservazione dei dati di traffico telematico, escludendone i contenuti, per due periodi di sei mesi ciascuno; l'obbligo di conservazione dei dati relativi alle chiamate telefoniche

senza risposta; particolari modalità di acquisizione dei dati 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.

Il predetto provvedimento d'urgenza ha, inoltre, introdotto 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, fissando il termine al 31 dicembre 2007. Questo è stato successivamente prorogato al 31 dicembre 2008 dal d.l. n. 248/2007 (convertito in legge, con modificazioni, dall'art. 1 della l. n. 31/2008).

Successivamente, è intervenuta in materia la Direttiva 2006/24/Ce, la quale contiene specifiche indicazioni sia sui tempi di conservazione dei dati di traffico (minimo sei mesi e massimo due anni), sia sulla corretta e uniforme individuazione delle categorie di dati da conservare, in relazione ad alcuni specifici servizi offerti dai fornitori (telefonia di rete fissa e telefonia mobile, accesso a Internet, posta elettronica in Internet e telefonia via Internet).

In attuazione della Direttiva 2006/24/Ce della quale, come si è detto, il Garante aveva già tenuto conto nell'adozione del provvedimento del 17 gennaio 2008, il d.lg. 30 maggio 2008 n. 109, modificando l'art. 132 *citato*, ha previsto un periodo unico di conservazione pari a ventiquattro mesi per i dati di traffico telefonico, a dodici mesi per i dati di traffico telematico e a trenta giorni per i dati relativi alle chiamate senza risposta, senza ulteriori distinzioni in base al tipo di reato.

La legge n. 48/2008, di ratifica della Convenzione del Consiglio d'Europa sulla criminalità informatica stipulata a Budapest il 23 novembre 2001, ha poi nuovamente modificato l'art. 132 del Codice, prevedendo una specifica ipotesi di conservazione temporanea dei dati relativi al traffico telematico a fini di svolgimento di investigazioni preventive o di accertamento e repressione di reati.

Sulla materia è successivamente intervenuto il d.l. 2 ottobre 2008, n. 151 (convertito in legge, con modificazioni, dall'art. 1 della l. n. 186/2008), il quale, introducendo alcune modifiche e integrazioni nell'art. 6 del citato d.lgs. 109/2008, ha prorogato al 31 marzo

2009 il regime transitorio sopra descritto, che consente di conservare i dati di traffico telefonico e telematico, differendo così ulteriormente l'applicazione della disciplina contenuta nella Direttiva 2006/24/Ce.

14.2. MISURE DI SICUREZZA

Sicurezza dei dati e dei sistemi

In riscontro a taluni quesiti della Federazione nazionale agricoltura (Fna-Confsal), l'Autorità è tornata a fornire chiarimenti sulle misure di sicurezza prescritte dal Codice (artt. 31 e *ss.* ed Allegato B. al Codice).

Muovendo dalla preliminare necessità di chiarire – anche in base all'atto costitutivo o allo statuto – se i soggetti indicati dall'associazione operino quali titolari del trattamento (artt. 4, comma 1, lett. *f*) e 28 del Codice) l'Autorità ha precisato che: le *cd. "misure minime di sicurezza"* vanno applicate con una diversa gradazione a seconda che i trattamenti di dati personali, siano effettuati con o senza l'ausilio di strumenti elettronici (artt. 33-35 del Codice e Allegato B.); il documento programmatico sulla sicurezza (Dps) deve essere redatto da ogni titolare, anche attraverso il responsabile, se designato (regola 19 dell'Allegato B. *cit.*), se i dati sensibili e/o giudiziari sono trattati con strumenti elettronici (art. 34, comma 1, lett. *g*), del Codice e regola 19 dell'Allegato B. al Codice) considerando, ove opportuno, la *"Guida operativa"*, curata dal Garante (doc. *web* n. 1007740) e le recenti semplificazioni introdotte dall'art. 29 del decreto-legge 25 giugno 2008, n. 112 (delle quali il Garante ha tenuto conto nell'adottare il *provvedimento* del 27 novembre 2008 [doc. *web* n. 1571218]. Tali disposizioni si applicano ai trattamenti con strumenti elettronici di dati non sensibili o dei soli dati sensibili inerenti allo stato di salute di dipendenti e collaboratori, senza indicazione della relativa diagnosi, ovvero di dati relativi all'adesione a organizzazioni sindacali. In tali casi, la tenuta di un aggiornato dps è stata sostituita da un'autocertificazione (resa dal titolare del trattamento ai sensi dell'articolo 47 del d.P.R. 28 dicembre 2000, n. 445) che attesta che il trattamento riguarda soltanto tali dati personali nell'osservanza delle altre misure di sicurezza prescritte come modificato dalla legge di conversione 6 agosto 2008, n. 133). La Federazione può predisporre un unico modello di dps recepibile dai titolari del trattamento che ad essa afferiscono, ciascuno tenendo conto delle

operazioni in concreto effettuate e delle modalità di trattamento utilizzate; ciascun titolare può designare uno o più *"responsabili del trattamento"* purché in possesso dei requisiti prescritti dall'art. 29 del Codice (*Nota* 3 febbraio 2009).

14.3. PRESCRIZIONI SULLA SICUREZZA DEI DATI NEGLI UFFICI GIUDIZIARI

È stato riferito nella *Relazione* 2007 che con *provvedimento* del 15 novembre 2007 (doc. *web* n. 1480605) il Garante ha indicato al Tribunale ordinario di Roma la necessità di apportare alcune modificazioni e integrazioni alle misure di sicurezza adottate, volte a rafforzare il livello di protezione dei dati personali trattati ai sensi dell'art. 47, comma 2, del Codice.

Nel dare tempestivo riscontro al *provvedimento*, il Tribunale ha rappresentato di avere dato attuazione solo parziale a tali indicazioni, adducendo, per le misure non realizzate, attinenti alla complessiva organizzazione e funzionamento dei servizi, la mancanza di spazi disponibili e la cronica mancanza di personale, e comunicando, quanto all'adozione delle misure di natura informatica, di avere interessato le competenti strutture del Ministero della giustizia (già destinatario di copia del *provvedimento* del 15 novembre 2007).

Il Garante ha quindi adottato il *provvedimento* del 13 ottobre 2008 [doc. *web* n. 1565790] con il quale, preso atto della mancata realizzazione delle misure prescritte, e considerato che tale attuazione dipende per lo più da misure strutturali e dalla disponibilità delle indispensabili risorse finanziarie, ha indicato al Ministero della giustizia la necessità di fornire al Tribunale ordinario di Roma le risorse materiali, tecniche e umane idonee a consentire al Tribunale stesso di apportare le modificazioni e integrazioni indicate nel *provvedimento* del novembre 2007.

14.4. SICUREZZA DEI DATI RELATIVI A RIFIUTI ELETTRICI ED ELETTRONICI

Disciplina di protezione dei dati personali e rifiuti elettrici ed elettronici (Raee)

A seguito di alcune segnalazioni (relative al rinvenimento di dati personali all'interno di apparecchiature cedute a rivenditori per la dismissione o per far valere la garanzia) e di notizie di stampa sul rinvenimento di dati bancari di oltre un milione di individui in un disco rigido usato commercializzato attraverso un sito Internet, il Garante ha adottato un

provvedimento generale sui rischi derivanti dalla circolazione di componenti elettroniche "usate" contenenti dati personali, con particolare riguardo all'eventuale accesso di terzi ai dati memorizzati all'interno di apparecchiature destinate alla dismissione (o oggetto di nuova commercializzazione). Ciò anche in ragione dell'adozione del d.lg. 25 luglio 2005, n. 151 (attuativo di normativa comunitaria in materia), che prevede misure volte a favorire il reimpiego, il riciclaggio e altre forme di recupero di tali rifiuti.

La menzionata disciplina (e la normativa secondaria che ne è derivata) – che non si occupa dei profili di protezione dei dati personali – lascia impregiudicati gli obblighi gravanti sui titolari del trattamento relativamente alle misure di sicurezza adottate. Ne consegue che ogni titolare è tenuto ad adottare misure organizzative e tecniche per garantire l'effettiva cancellazione o trasformazione in forma non intelligibile dei dati personali contenuti nei supporti elettrici ed elettronici in occasione della dismissione di apparati elettrici ed elettronici (art. 31 e *ss.* del Codice). Ciò, anche incaricando soggetti tecnicamente qualificati (che attestino l'esecuzione di tali operazioni o si impegnino ad effettuarle), qualora il titolare non sia in grado di cancellare effettivamente i dati o di anonimizzarli. L'Autorità ha anche indicato ai titolari dei trattamenti alcune procedure (suscettibili di aggiornamento alla luce dell'evoluzione tecnologica) ritenute idonee a garantire che, in sede di reimpiego, riciclaggio, ovvero di smaltimento di apparecchiature elettriche ed elettroniche, siano effettivamente cancellati (o resi anonimi) i dati personali ivi memorizzati (*Provv.* 13 ottobre 2008 [doc. *web* n. 1571514]).

14.5. IL RUOLO DEGLI AMMINISTRATORI DI SISTEMA NELLA SICUREZZA DEI TRATTAMENTI

Individuazione degli amministratori di sistema e controllo del loro operato

Il ruolo dell'amministratore di sistema, rilevante per alcuni profili nel diritto penale (*v.* artt. 615-*ter*, 635-*bis*, *ter*, *quater* e *quinquies*, nonché 640 del c.p.) e nella disciplina di protezione dei dati previgente al Codice del 2003, non ha avuto adeguata disciplina, nonostante la sua particolare delicatezza, tenuta in considerazione nell'ambito di piani di sicurezza o di documenti programmatici elaborati da aziende e organizzazioni. L'attività ispettiva svolta dal Garante rispetto a banche dati di grande rilievo, ma anche in sistemi di minore complessità, ha consentito tuttavia di rilevare preoccupanti sottovalutazioni

dei rischi e carente consapevolezza delle criticità insite nello svolgimento di tali delicate mansioni.

Pertanto l'Autorità è intervenuta (*Provv.* 27 novembre 2008, in *G.U.* 24 dicembre 2008, n. 300 [doc. *web* n. 1577499]) per richiamare tutti i titolari di trattamenti effettuati, anche solo in parte, mediante strumenti elettronici, alla necessità di prestare massima attenzione ai rischi e alle criticità implicite nell'affidamento degli incarichi di amministratore di sistema, fissando nel contempo le regole per l'adozione da parte di enti, amministrazioni pubbliche e società private delle misure tecniche e organizzative che riguardano tale peculiare figura.

Sono stati compresi nella definizione di *"amministratore di sistema"* i soggetti chiamati a svolgere funzioni di gestione e manutenzione di un impianto di elaborazione che possono comportare la possibilità tecnica di accesso a tutti i dati personali memorizzati o trasmessi tramite i sistemi informatici; pertanto sono stati considerati equivalenti, e compresi nella definizione ai fini del *provvedimento*, gli amministratori di basi di dati, di reti e di apparati di sicurezza, di sistemi *software* complessi.

Le misure sono dirette ad agevolare la verifica sull'attività degli amministratori da parte di chi ha la titolarità delle banche dati e dei sistemi informatici, e non riguardano i trattamenti di dati effettuati a fini amministrativo contabili, che pongono minori rischi per gli interessati e che sono stati oggetto di misure di semplificazione.

Tra le misure prescritte è compresa la registrazione degli accessi (autenticazioni informatiche) degli amministratori ai sistemi di elaborazione e agli archivi elettronici, da conservare per un periodo non inferiore a sei mesi. Analogamente a quanto avviene per i responsabili del trattamento, l'operato degli amministratori di sistema deve essere verificato, ma con periodicità annuale, dai titolari del trattamento, mentre i loro estremi identificativi e l'elenco delle funzioni loro attribuite devono essere riportati in un documento da rendere disponibile in caso di accertamenti da parte del Garante, anche nel caso in cui la funzione sia svolta a qualsiasi titolo da soggetti esterni all'organizzazione, ovunque operanti. Quale misura di trasparenza interna alle aziende e alle organizzazioni, è stata poi prevista l'instaurazione di un regime di conoscibilità dell'identità degli amministratori di

sistema addetti a trattamenti di dati personali che riguardino i lavoratori operanti a qualsiasi titolo in aziende e in organizzazioni.

Il Garante, in ragione della complessità degli interventi organizzativi e tecnici necessari, su richiesta di alcune associazioni di operatori interessati ha prorogato i termini per gli adempimenti. In particolare, dopo l'unificazione dei termini e il differimento al 30 giugno 2009 (*Provv.* 12 febbraio 2009, in *G.U.* n. 45 24 febbraio 2009 [doc. *web* n. 1591970]), ha avviato una consultazione pubblica (*Provv.* 21 aprile 2009 – in corso di pubblicazione in *Gazzetta Ufficiale* – per *"acquisire osservazioni e commenti da parte dei titolari del trattamento ai quali il provvedimento si rivolge con esclusivo riferimento a quanto prescritto al punto 2 del dispositivo del provvedimento del 27 novembre 2008"*), fornendo nel contempo, tramite il proprio sito, le risposte alle domande più frequenti (*faq*).

15. La videosorveglianza e la biometria

15.1. Videosorveglianza in ambito pubblico

Anche nel 2008 l'Autorità è stata chiamata a fornire indicazioni sull'applicazione del *provvedimento* generale in materia di videosorveglianza del 29 aprile 2004 (doc. *web* n. 1003482).

Più volte è stata richiamata l'attenzione sulle garanzie da osservare nell'ambito dei rapporti di lavoro anche quando gli impianti siano utilizzati per esigenze organizzative e dei processi produttivi, ovvero siano richiesti per la sicurezza del lavoro (punto 4.1 del *cit. provvedimento* generale) (*Note* 3 marzo 2008, 13 marzo 2008, 30 aprile 2008, 2 settembre 2008, 24 novembre 2008 e 9 gennaio 2009).

Ad un ente locale che aveva installato impianti di videosorveglianza attraverso *web cam*, diffondendo le immagini in tempo reale sul suo sito istituzionale, è stato fatto presente che non risulta di regola giustificata un'attività di sorveglianza rivolta non al controllo di eventi, situazioni e avvenimenti, ma a fini promozionali-turistici o pubblicitari, attraverso *web cam* o *cameras-on-line* che consentano di individuare i tratti somatici delle persone che figurano nei campi visuali ripresi, rendendole identificabili (*cfr.* punto 2.3 del citato *provvedimento* e *Provv.* 14 giugno 2001 [doc. *web* n. 41782]) (*Nota* 15 maggio 2008).

Nel corso di un accertamento ispettivo disposto dal Garante su segnalazione era emerso che delle cinque telecamere installate presso uno studio medico, due riprendevano le immagini dell'ingresso ai locali e tre erano posizionate all'interno dei luoghi destinati a spogliatoio. Alla luce delle vigenti disposizioni in tema di interferenze illecite nella vita privata, di tutela della dignità, del domicilio e degli altri luoghi cui è riconosciuta analoga tutela (*Provv.* 29 aprile 2004, punto 2.1.), il trattamento svolto attraverso l'installazione di telecamere negli spogliatoi non è risultato effettuato in modo lecito.

In particolare, è stato valutato che la collocazione di telecamere operanti in modo continuo negli spogliatoi di un ambulatorio medico determina un'intromissione ingiustificata nella vita privata delle persone che vi si recano risultando, pertanto, essere lesiva della loro riservatezza e dignità. Sono stati conseguentemente vietati all'ambulatorio, ai sensi del-

l'art. 154, comma 1, lett. *d*), del Codice, ulteriori trattamenti illeciti aventi per oggetto i dati personali raccolti mediante il descritto sistema di videosorveglianza installato negli spogliatoi (*Provv.* 4 dicembre 2008 [doc. *web* n. 1576125]).

Ad un'azienda sanitaria locale, che aveva formulato un quesito sull'installazione di un sistema di videosorveglianza presso alcune sedi operative dei Servizi per le tossicodipendenze dislocate sul territorio provinciale, è stato fatto presente che il sistema avrebbe potuto evidenziare anche profili inerenti le condizioni di salute dei pazienti. Pertanto, 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 rendendo accessibili le immagini unicamente ai soggetti specificamente autorizzati (*ad es.*, personale medico ed infermieristico).

Nei casi in cui l'impiego di un sistema di videosorveglianza degli accessi sia utilizzato a salvaguardia del patrimonio aziendale e per monitorare le zone nevralgiche e a rischio per la sicurezza dei pazienti e dei visitatori, dati idonei a rilevare lo stato di salute, l'appartenenza etnica o razziale e le convinzioni religiose possono essere rilevati incidentalmente anche attraverso la ripresa dei tratti somatici o dell'abbigliamento degli interessati o il contesto in cui è effettuata la ripresa (*v.* art. 20, comma 2, del Codice; scheda n. 41 dell'Allegato B.; schema tipo di regolamento per il trattamento dei dati sensibili e giudiziari di competenza delle regioni, delle province autonome, delle aziende sanitarie, degli enti regionali/provinciali e degli enti vigilati e controllati dalle regioni e dalle province autonome, sul quale, in data 13 aprile 2006, l'Autorità ha espresso parere favorevole [doc. *web* n. 1272225]; punto 4.2 del *cit. Provv.* 29 aprile 2004) (*Nota* 30 gennaio 2009).

Da ultimo, si menziona la segnalazione di un nucleo operativo dei Carabinieri di una regione, relativa al trattamento di dati effettuato da taluni comuni con apparecchiature elettroniche per il rilevamento automatico di infrazioni al codice della strada. In particolare, si lamentava la mancata designazione, quali responsabili ed incaricati del trattamento, dei soggetti coinvolti nell'installazione e nel funzionamento delle apparecchiature in questione.

Sulla base degli elementi ottenuti dai comuni, in un caso l'Ufficio ha evidenziato, in particolare, che il titolare del trattamento deve specificare analiticamente e per iscritto i

compiti affidati al responsabile, con particolare riferimento al trattamento dei dati personali, ed è tenuto a vigilare sul rispetto delle vigenti disposizioni, ivi compreso il profilo relativo alla sicurezza, anche tramite verifiche periodiche (art. 29, commi 4 e 5, del Codice). In mancanza di tali designazioni, la trasmissione di dati personali da parte di soggetti pubblici a soggetti esterni privati si configura come una comunicazione ed è, in quanto tale, assoggettata alle norme più stringenti previste per tale operazione (art. 19, comma 3, del Codice) (*Note* 26 maggio 2008, 24 luglio 2008 e 28 luglio 2008).

Videosorveglianza a bordo taxi

A seguito di notizie di stampa – che evidenziavano l'installazione di sistemi di videosorveglianza all'interno delle autovetture adibite al servizio taxi, in attuazione di progetti pubblici volti a promuovere la sicurezza nell'ambito del menzionato servizio – l'Autorità ha richiesto informazioni ad alcune compagnie/cooperative di radio-taxi per valutare la liceità dei trattamenti. Solo due compagnie hanno dichiarato di avere in corso l'installazione (in via di completamento entro la fine del 2008) di un sistema di videosorveglianza dotato di minicamera a infrarossi e relativa interfaccia di acquisizione delle foto (denominata "*black box*"). La menzionata minicamera scatterebbe fotografie ai clienti memorizzate nella *black box* in formato criptato (destinate ad essere sovrascritte dopo circa 24 ore dalla loro acquisizione); solo in caso di allarme lanciato dal tassista (*ad es.*, in caso di aggressione) le immagini raccolte a partire dai dieci minuti antecedenti l'allarme verrebbero trasmesse dal sistema mediante protocollo radio non accessibile a terzi (oltre a poter essere *"scaricate"* direttamente dalla *black box*) e rese fruibili a un incaricato della centrale radio-taxi dotato di *chip card* di autenticazione per consentire di contattare le autorità di polizia. L'impianto, predisposto nel rispetto del principio di necessità (verrebbero rese utilizzabili le sole foto scattate nei dieci minuti antecedenti alla sua attivazione, in caso di emergenza, da parte del tassista), sarebbe altresì provvisto di accorgimenti *hardware* e *software* ritenuti in grado di rendere inaccessibile i dati a tassisti, installatori, e ad altri soggetti non autorizzati; solo la compagnia/cooperativa potrebbe accedere ai dati registrati in caso di richiesta delle informazioni da parte delle forze dell'ordine (debitamente autorizzate dall'autorità giudiziaria). Il sistema di videosorveglianza e il conseguente trattamento dei dati personali verrebbe segnalato alla clientela mediante apposita vetrofania, visibile anche

all'esterno del veicolo raffigurante l'icona della telecamera conforme a quella presente sul sito dell'Autorità. Sono in corso gli opportuni approfondimenti sulla liceità del trattamento.

15.2. BIOMETRIA IN AMBITO PUBBLICO

Nel corso dell'anno numerose richieste hanno evidenziato l'interesse dei soggetti pubblici per i sistemi di rilevazione automatica per il controllo degli accessi al luogo di lavoro mediante il riconoscimento dei dati biometrici dei dipendenti. Si è reso necessario, quindi, ribadire le indicazioni contenute nel *provvedimento* generale recante *"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]).

In cinquantaquattro casi sono pervenute richieste di verifica preliminare relative all'utilizzo di dati biometrici; nella quasi totalità di essi non era richiesta tale procedura, prevista nel Codice all'art. 17, con riferimento ai trattamenti di dati personali – diversi da quelli sensibili e giudiziari – che presentano rischi specifici per i diritti e le libertà fondamentali, nonché per la dignità dell'interessato.

Due richieste sono state definite con *provvedimento* favorevole (Azienda Policlinico Umberto I, *Provv.* 15 aprile 2008 [doc. *web* n. 1523435]; Azienda ospedaliera civile Maria Paternò Arezzo di Ragusa (*Provv.* 19 giugno 2008 [doc. *web* n. 1532480]) mentre altre tre sono ancora all'esame del Collegio in ragione della particolare delicatezza dei casi sottoposti, che ha reso necessario un supplemento di istruttoria.

Per quanto riguarda l'Azienda Policlinico Umberto I, la richiesta era incentrata sull'installazione di lettori biometrici per: 1) permettere l'accesso a locali ed aree a rischio; 2) autenticazione informatica; 3) verificare la presenza del personale in servizio. Al riguardo, il Garante ha fornito prescrizioni e accorgimenti nei primi due casi, non ritenendo invece proporzionato l'utilizzo di tecniche biometriche nel terzo.

L'Azienda ospedaliera civile Maria Paternò Arezzo di Ragusa aveva invece avanzato richiesta di verifica preliminare per la raccolta di dati biometrici, desunti dall'impronta digitale, di pazienti e personale sanitario da associare alle sacche di sangue destinate alla tra-

sfusione, per prevenire errori dei identificazione di pazienti o delle unità di sangue in sede di trasfusione, fonti di conseguenze gravissime. Il *provvedimento* favorevole del Garante ritiene proporzionata allo scopo la modalità del trattamento prospettata dall'Azienda, ed indica alcuni accorgimenti da adottare, in particolare per quanto attiene alla conservazione dei dati.

In più occasioni, il Garante ha ricordato 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; ha fatto altresì presente che 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 (*Note* 24 giugno 2008, 3 settembre 2008, 14 novembre 2008 e 11 dicembre 2008).

In due occasioni il Garante ha precisato che, di regola, tali sistemi possono essere attivati soltanto per particolari esigenze di controllo dell'accesso a speciali aree dei luoghi di lavoro ad esempio, perché l'aerea è destinata allo svolgimento di attività aventi carattere di segretezza, ovvero che comportano la necessità di trattare informazioni rigorosamente riservate (*ad 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), nonché alla conservazione di oggetti di particolare valore o la cui disponibilità deve essere circoscritta in quanto un utilizzo improprio può determinare un rischio grave e concreto per la salute e l'incolumità dei dipendenti o di terzi (*ad es.*, ambienti ove sono custodite sostanze stupefacenti o psicotrope) (*Note* 17 ottobre 2008, 30 gennaio 2009 e 13 febbraio 2009).

Nelle medesime occasioni è stato altresì ricordato che il trattamento di dati relativi alle impronte digitali è ammesso a condizione che sia sottoposto con esito positivo – di regola a seguito di un interpello del titolare – alla verifica preliminare prevista dall'art. 17 del Codice anche per determinate categorie di titolari o di trattamenti; che venga effettuata preventivamente la notificazione al Garante (artt. 37, comma 1, lett. *a*) e 38 del Codice); che non sia comunque registrata l'immagine integrale dell'impronta digitale, bensì solo il

modello di riferimento da essa ricavato (*template*); che 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); che sia fornita ai dipendenti interessati un'informativa specifica per il trattamento in questione (art. 13 del Codice).

Ad una agenzia per il diritto allo studio universitario è stato fatto presente che la raccolta e la registrazione di impronte digitali e dei codici numerici da esse ricavati, e successivamente utilizzati per effettuare il confronto tra il *"modello"* di impronta digitale memorizzato nel *microchip* del tesserino rilasciato allo studente e quello di volta in volta elaborato dal programma di gestione sulla base della rilevazione dell'impronta digitale, sono operazioni di trattamento di dati personali riconducibili ai singoli interessati (art. 4, comma 1, lett. *b*), del Codice). Pertanto, trovando applicazione la normativa contenuta nel Codice, il trattamento con tali modalità volto al controllo degli accessi alla mensa universitaria non sarebbe risultato, allo stato degli atti, effettuato in modo lecito (*Nota* 1° dicembre 2008).

15.3. VIDEOSORVEGLIANZA IN AMBITO PRIVATO

Salvo quanto si dirà di seguito sui trattamenti effettuati in ambito condominiale mediante sistemi di videosorveglianza, deve rilevarsi che la materia continua a formare oggetto di numerose segnalazioni (esaminate alla luce della legge e del *provvedimento* generale del 29 aprile 2004 [doc. *web* n. 1003482]), come pure di controlli da parte dell'Autorità, spesso con l'ausilio della Guardia di finanza. Peraltro, la disciplina di protezione dei dati personali non trova applicazione, ai sensi dell'art. 5, comma 3, del Codice, in caso di trattamenti di dati per fini esclusivamente personali – e i rapporti di vicinato rientrano per lo più in quest'ambito – salvo che le immagini registrate non siano oggetto di comunicazione sistematica o diffusione. In tal caso, sussistendone i presupposti, l'interessato può far valere i propri diritti avanti all'autorità giudiziaria ordinaria, anche a mente del divieto sanzionato penalmente relativo all'indebita raccolta (mediante l'uso di strumenti di ripresa visiva o sonora, nonché alla rivelazione e alla diffusione) di immagini atti-

nenti alla vita privata che si svolgono nell'abitazione altrui o in un altro luogo di privata dimora (art. 615-*bis* c.p. - Interferenze illecite nella vita privata).

Videosorveglianza e condominio

A seguito di alcuni quesiti e segnalazioni è stata inviata una segnalazione al Parlamento e al Governo sull'eventualità di disciplinare con norme apposite alcuni profili relativi alla videosorveglianza all'interno di edifici condominiali e nelle relative pertinenze. Tale tematica, con particolare riferimento alle condizioni di liceità del trattamento, ai soggetti deputati a manifestare la volontà per svolgerlo e alle eventuali maggioranze da rispettare, non è stata oggetto di valutazione specifica nei due provvedimenti di carattere generale adottati in materia di videosorveglianza (*Provv.* 29 novembre 2000 [doc. *web* n. 31019], 29 aprile 2004 [doc. *web* n. 1003482]).

Al riguardo, è emersa l'esistenza di due contrapposti interessi: da un lato, l'esigenza di preservare la sicurezza di persone e la tutela di beni comuni; dall'altro, la preoccupazione che, nel rendere più agevolmente conoscibili a terzi abitudini e stili di vita individuali e familiari, si incida sulla libertà degli interessati di muoversi, non controllati, nel proprio domicilio e all'interno delle aree condominiali.

Considerato che il profilo in esame non trova regolamentazione specifica e che gli orientamenti giurisprudenziali sull'utilizzo delle aree comuni non appaiono sufficienti a dissolvere tutti i dubbi al medesimo relativi, l'Autorità, anche alla luce di quanto previsto dalla disciplina penalistica in tema di interferenze illecite nella vita privata, ha auspicato un eventuale intervento normativo chiarificatore (anche nell'ambito di alcuni più ampi disegni di legge già oggetto di attenzione da parte di entrambi i rami del Parlamento) per un equo contemperamento tra i diritti fondamentali delle persone coinvolte e le legittime esigenze di difesa e protezione di persone e cose (Segnalazione al Parlamento e al Governo 13 maggio 2008 [doc. *web* n. 1523997]).

Esercizi commerciali e videosorveglianza

Sono pervenute due distinte segnalazioni relative all'installazione, presso un esercizio commerciale, di un sistema di videosorveglianza in asserita violazione della disciplina di protezione dei dati personali. Dall'istruttoria (anche con accertamenti in *loco*) è risultato che il titolare del trattamento non ha designato il soggetto incaricato di mantenere l'impianto quale responsabile del trattamento (art. 29 del Codice), ancorché unico soggetto

autorizzato ad accedere alle immagini registrate; ciò ha configurato la possibilità di una comunicazione a terzi (ai sensi dell'art. 4, comma 1, lett. *l*), del Codice) da parte del medesimo titolare del trattamento in assenza del consenso informato degli interessati (artt. 13 e 23 del Codice) o di un altro presupposto equipollente di liceità (art. 24 del medesimo Codice). In proposito, il Garante ha prescritto di designare il manutentore del sistema quale responsabile del trattamento, disponendo nelle more il blocco della comunicazione a tale soggetto delle immagini registrate. È inoltre emerso che il sistema consente la registrazione audio della voce degli interessati. Al riguardo – a prescindere da eventuali profili di liceità penale (artt. 617, 617-*bis* e 623-*bis* c.p.) – l'Autorità ha vietato l'ulteriore trattamento della voce degli interessati, in assenza di idonei e comprovati elementi giustificativi, in quanto effettuato in violazione del principio di finalità (secondo cui il trattamento deve essere effettuato per finalità determinate, esplicite e legittime – art. 11, comma 1, lett. *b*), del Codice – che non sono risultate ricorrere nella fattispecie) (*Provv.* 2 ottobre 2008 [doc. *web* n. 1581352]).

Videosorveglianza e difesa in giudizio

In un reclamo è stata contestata l'installazione in aree condominiali di un sistema di videosorveglianza (e la successiva produzione in giudizio di immagini riferite al reclamante acquisite attraverso il menzionato sistema) da parte di uno studio di consulenza avente sede nel condominio. Dagli elementi acquisiti è risultato che l'impianto era stato installato dallo studio (in passato oggetto di atti vandalici e intimidatori) per finalità di sicurezza dei propri beni patrimoniali e di deterrenza. Tale impianto (peraltro disattivato all'epoca della richiesta di informazioni) aveva in passato consentito di acquisire in ordine all'autore dei predetti atti (individuato nel medesimo reclamante) informazioni successivamente depositate presso la competente autorità giudiziaria nell'ambito di un procedimento penale al riguardo instaurato. Tenuto conto che le immagini (fatte salve quelle depositate presso la procura) non sono state conservate dal titolare e che sull'utilizzabilità di quelle prodotte in giudizio ogni valutazione spetta all'autorità giudiziaria (artt. 47 e 160, comma 6, del Codice), non sono stati ravvisati i presupposti per un intervento da parte dell'Autorità (art. 11, comma 1, lett. *b*), reg. Garante 1/2007). Nondimeno, l'Autorità ha richiamato il titolare del trattamento, in caso di eventuale riattivazione del

sistema, al rispetto dei princìpi evidenziati nel *provvedimento* del 29 aprile 2004 (con specifico riferimento all'angolo visuale di ripresa) (*Nota* del 16 aprile 2008).

15.4. BIOMETRIA IN AMBITO PRIVATO

Trattamenti di dati biometrici per finalità di rilevazione della presenza dei lavoratori

Alcuni accertamenti ispettivi svolti tramite la Guardia di finanza hanno evidenziato l'esistenza presso due società di sistemi di rilevazione dei dati biometrici per accertare la presenza dei dipendenti sui luoghi di lavoro.

In termini generali, l'utilizzo di dati biometrici nel contesto lavorativo può risultare giustificato solo per presidiare accessi ad *"aree sensibili"* (in ragione delle attività ivi svolte) (*cfr. Provv.* 21 luglio 2005 [doc. *web* n. 1150679]; *"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. 1364939]), non per finalità connesse all'ordinaria gestione del rapporto di lavoro.

Le società sono state perciò invitate a fornire riscontro sulle misure volte ad adeguare il trattamento dei dati biometrici riferiti ai lavoratori ai princìpi richiamati nei menzionati provvedimenti.

La prima società ha precisato di aver installato in sostituzione del pregresso sistema biometrico (per le finalità di gestione delle presenze e degli orari del personale in servizio) appositi *badge* per la timbratura del cartellino elettronico (*cfr. Nota* del 30 ottobre 2008).

La seconda ha dichiarato di essersi adoperata, per installare un nuovo sistema di rilevazione delle presenze in sostituzione del precedente che rilevava i dati biometrici dei dipendenti.

Tenuto conto delle affermazioni rese dalla società (secondo cui il sistema installato risulterebbe idoneo ad essere configurato come un normale terminale di rilevazione delle presenze in grado di leggere i *badge* passivi di prossimità), non è stata promossa l'adozione di un *provvedimento* da parte dell'Autorità (*cfr. Nota* del 18 novembre 2008). La società ha peraltro fatto successivamente sapere di essersi dotata di un sistema *"tradizionale"* di rilevazione delle presenze dei lavoratori.

Sono pervenute anche nel 2008 alcune richieste di verifica preliminare sul trattamento di dati personali biometrici dei dipendenti. In un caso la richiesta era stata avanzata da una fondazione bancaria con sede in un immobile di alto valore artistico con più accessi, che renderebbero possibile a estranei di introdursi all'interno del palazzo senza essere visti. La finalità perseguita, consistente nell'assicurare la sicurezza di un immobile di elevato valore (anche per le opere d'arte in esso contenute) è risultata lecita, anche alla luce delle linee-guida sul trattamento di dati personali per la gestione del rapporto di lavoro (*Provv.* 23 novembre 2006 [doc. *web* n. 1364099]). Nel fornire, pertanto, alcune indicazioni affinché il trattamento fosse conforme alla disciplina di protezione dei dati personali, non si è ritenuto necessario un *provvedimento ad hoc* (*Nota* 18 aprile 2008).

L'adozione di un *provvedimento* è, invece risultata opportuna a seguito di una richiesta, avanzata da una società che gestisce servizi idrici, per trattare i dati biometrici dei dipendenti al fine di controllarne gli accessi a impianti di potabilizzazione e alle sedi centrale e periferiche della società. Il sistema, che prevede il consenso dei dipendenti, si basa su una raccolta di dati biometrici mediante apparecchiature dotate di lettore di impronte digitali e di un apposito *software*; l'impronta digitale verrebbe trasformata in un codice numerico (*template*), memorizzato su *smart card* e utilizzato esclusivamente per la raccolta e il successivo trattamento dei dati ai fini predetti. A livello centralizzato verrebbero memorizzati per sette giorni i dati personali relativi all'orario degli accessi giornalieri e i codici numerici che consentono alla società di risalire al dipendente.

Il trattamento è stato ritenuto lecito, tenendo conto della finalità di incrementare la sicurezza dell'impianto idrico anche con misure preventive a tutela della qualità delle acque (peraltro oggetto del d.lg. 2 febbraio 2001, n. 31, recante *"Attuazione della Direttiva 98/83/Ce relativa alla qualità delle acque destinate al consumo umano"*) e di assicurare così, mediatamente, la salute pubblica.

Si è, tuttavia, ravvisata l'esigenza di trattare i dati biometrici solo dei lavoratori per i quali, a seguito di una ricognizione preventiva, la società constati e documenti l'effettiva necessità di accedere alle aree meritevoli di protezione. A tal fine, il meccanismo da utilizzare deve essere basato sulla lettura delle impronte digitali cifrate su uno strumento

disponibile per il lavoratore (*smart card* o analoghi dispositivi), senza creare un archivio centralizzato dei *template* derivati dall'analisi delle impronte digitali. Il Garante ha comunque rappresentato la necessità del previo assolvimento degli obblighi previsti dall'art. 4 dello Statuto dei lavoratori (*Provv.* 15 febbraio 2008 [doc. *web* n. 1497675]).

Biometria e luoghi di lavoro

L'Autorità ha vietato ad una società, perché illegittimo e invasivo, l'ulteriore trattamento dei dati raccolti attraverso un sistema di rilevazione di dati biometrici ricavati dalle impronte digitali installato in alcune sedi di lavoro solo per commisurare la retribuzione agli orari di lavoro effettivi. Nel caso (segnalato da uno dei dipendenti interessati) non sono, infatti, emerse ragioni concrete e specifiche in grado di giustificare l'utilizzo di dati biometrici. Il trattamento non è risultato conforme neanche alle indicazioni in materia contenute nelle *"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"* (*Provv.* 23 novembre 2006 [doc. *web* n. 1364099]). Inoltre, non era stata rispettata la procedura prescritta dall'art. 4 della legge n. 300/1970, da osservare (*cfr.* Ca*ss.* 17 luglio 2007, n. 15892) nel caso in cui le apparecchiature consentano di controllare il rispetto degli orari di entrata e uscita e la presenza sul luogo di lavoro da parte dei dipendenti (*Provv.* 2 ottobre 2008 [doc. *web* n. 1571502]).

In un altro caso, all'esito di verifiche, anche ispettive, presso una società di trasporti campana, il trattamento di dati biometrici è risultato svolto in termini non compatibili con le suddette linee-guida del 23 novembre 2006 [doc. *web* n. 1364099]. La società, invitata ad attenersi al rispetto di tali prescrizioni, ha ritenuto eccessivamente onerosi gli investimenti a tal fine necessari, comunicando all'Autorità la dismissione degli apparati di rilevazione biometrica sperimentalmente installati. Essa è stata, in ogni caso, richiamata all'osservanza di quanto prescritto dagli articoli 16, comma 1, e 38, comma 4, del Codice per la cessazione del trattamento dei dati biometrici dei lavoratori (*Nota* 11 dicembre 2008).

Riconoscimento vocale e credenziali di autenticazione

A seguito di un'istanza di verifica preliminare ai sensi dell'art. 17 del Codice, il Garante ha autorizzato, per l'autenticazione degli accessi ai sistemi informativi di una società, il trattamento di dati personali dei dipendenti della società medesima, basato sul riconoscimento dei dati biometrici degli interessati. Il sistema si basa sulle impronte vocali criptate

in forma di modello algoritmico, con l'ausilio di una società esterna (che memorizzerebbe alcune informazioni personali degli utenti su un proprio *server*) e sarebbe funzionale alla reimpostazione automatica delle parole-chiave riferite agli utenti, confrontando quelle di volta in volta pronunciate con il modello vocale ai medesimi riferito.

In proposito, le impronte vocali, unitamente ai dati da esse ricavati, costituiscono informazioni personali ai sensi dell'art. 4, comma 1, lett. *b*), del Codice con conseguente loro applicazione della disciplina in materia (*Provv.* 19 novembre 1999 [doc. *web* n. 42058] e *Provv.* 21 luglio 2005 [doc. *web* n. 1150679]; *v.* pure il documento di lavoro sulla biometria del Gruppo art. 29, Direttiva 95/46/Ce -WP80-, punto 3.1).

L'Autorità, ferma restando la necessità del consenso degli interessati (art. 23 del Codice; *cfr.* altresì *Provv.* 1° febbraio 2007, punto 3.3. [doc. *web* n. 1381983]; *Provv.* 26 luglio 2006, punto 3.3. [doc. *web* n. 1318582]; *Provv.* 15 giugno 2006, punto 3.2. [doc. *web* n. 1306523]) e la predisposizione di sistemi alternativi per la reimpostazione della *password*, ha comunque prescritto alcuni accorgimenti a garanzia degli utenti, con particolare riguardo alle istruzioni a disposizione degli utilizzatori del sistema, alle misure organizzative per prevenire rischi di impiego abusivo dei dati raccolti e alla cancellazione dei dati vocali dei lavoratori successivamente alla cessazione del rapporto di lavoro o di collaborazione (*Provv.* 28 febbraio 2008 [doc. *web* n. 1501094]).

16. Il registro dei trattamenti

Tra i compiti del Garante, rientra la tenuta del Registro dei trattamenti (art. 154, comma 1, lett. *l*) del Codice) formato sulla base delle notificazioni ricevute. Come previsto dall'art. 37, comma 4, il Registro è accessibile a chiunque e la sua consultazione gratuita avviene per via telematica attraverso il sito *web* dell'Autorità.

Nel perseguire le finalità di semplificazione e accelerazione delle procedure amministrative l'art. 29 del d.l. n. 112/2008, come modificato dalla legge di conversione n. 133/2008, ha modificato l'art. 38 del Codice relativo alle modalità di notificazione. Il Garante, che sin dal 2004 aveva posto in essere profondi cambiamenti in relazione alla procedura di notificazione, ha operato una ulteriore drastica semplificazione dei contenuti e delle modalità di compilazione del modello informatico.

Con il *provvedimento* a carattere generale del 22 ottobre 2008 (*G.U.* 9 dicembre 2008, n. 287 [doc. *web* n. 1571196]), il Garante ha infatti approvato un nuovo modello di notificazione che è stato reso disponibile e operativo sul sito Internet dell'Autorità già all'inizio di gennaio 2009, entro la metà dei previsti sessanta giorni.

L'introduzione del nuovo modello non ha comportato l'obbligo di effettuare una nuova notificazione da parte dei soggetti che l'avevano già effettuata.

Tra gli elementi di novità, oltre ad una generale riorganizzazione senza alcun aggravio di carattere tecnico o procedurale per i notificanti, si segnala la limitazione dei casi di obbligatorietà dell'indicazione del luogo principale di custodia dei dati e la sottrazione all'obbligo del pagamento dei diritti di segreteria nel caso di modifica di elementi quali il numero telefonico, di *fax* e l'indirizzo di posta elettronica.

Né l'utilizzazione del modello in vigore dal 2004, né quella del nuovo hanno evidenziato significative difficoltà da parte dei notificanti. Lo sperimentato servizio di assistenza *on-line*, tramite messaggi di posta elettronica sia di tipo automatico che personalizzato, affiancato dal tradizionale supporto telefonico hanno fornito anche nell'anno 2008 riscontri fortemente positivi in termini di soddisfazione dell'utenza. Il controllo in tempo reale della procedura da parte del dipartimento ha assicurato una soluzione estremamente rapida delle problematiche più comuni rilevate dagli utenti ed un'opera di

costante prevenzione delle possibili disfunzioni del sistema.

Rispetto al passato ha segnato un netto miglioramento la soluzione dei problemi relativi all'apposizione della firma digitale, per una maggiore familiarità dell'utenza con tale strumento.

Si è mantenuto costante il numero dei cittadini interessati al contenuto del Registro che si sono avvalsi del servizio di ausilio svolto dal Dipartimento. Sono altresì significativamente aumentati i casi di accesso diretto al Registro da parte degli utenti con una media giornaliera di circa novanta accessi.

L'aumento di tale modalità di fruizione delle notificazioni è particolarmente soddisfacente, quale segno della effettiva realizzazione del dettato dell'art. 37, comma 4, del Codice che ha a suo tempo stabilito la consultazione telematica gratuita del Registro e che si accompagna alla ulteriore possibilità di stampa integrale delle notificazioni di interesse del cittadino.

Si sottolinea come, anche per le notificazioni presentate in data antecedente al 1° gennaio 2004, si sia provveduto a semplificare al massimo l'*iter* di richiesta al dipartimento e si sia in grado di effettuare invii *on-line* di *file* in formato *pdf* contenenti l'immagine delle notificazioni che venivano a suo tempo presentate su supporto cartaceo. Tale tipo di supporto comportava nel passato l'invio di copie conformi all'originale con tempi decisamente più lenti e modalità di invio estremamente complesse rispetto alle attuali ed ovviamente alle esigenze degli interessati.

Si è ulteriormente consolidata l'attività di controllo delle notificazioni effettuate e di accertamento delle violazioni all'obbligo di notificazione, in vista delle attività ispettive del Garante.

Il 2008 ha fatto registrare una inversione di tendenza rispetto al numero delle notificazioni presentate, con un aumento del 30% rispetto all'anno precedente.

Risultano in contrazione le notificazioni di trattamenti relativi a dati idonei a rivelare lo stato di salute e la vita sessuale, trattati per le specifiche finalità previste dall'art. 37, comma 1, lett. *b*), del Codice, mentre aumentano notevolmente i trattamenti di dati trattati con strumenti elettronici e volti a definire il profilo o la personalità dell'interessato o

ad analizzarne abitudini o scelte di consumo. I descritti scostamenti si riflettono anche sulle statistiche generali del periodo 2004-2008, che presentano infatti un significativo scarto dei valori percentuali di incidenza sul totale dei trattamenti notificati, per queste specifiche tipologie di trattamento.

17. La trattazione dei ricorsi

17.1. Il procedimento dei ricorsi a dieci anni dalla sua entrata in vigore

La presentazione della *Relazione* 2008 consente di tracciare un bilancio dei primi dieci anni di applicazione della specifica disciplina che ha introdotto e regolamentato il ricorso al Garante per la tutela di quel complesso di situazioni giuridiche soggettive che trovano ora collocazione nell'art. 7 del Codice. Solo con l'entrata in vigore del d.P.R. 31 marzo 1998 n. 501 (avvenuta il 16 febbraio 1999), ed in particolare degli artt. 17-20 di tale testo normativo – a due anni di distanza dalla nascita del Garante e dall'approvazione della prima legge organica italiana in tema di *data protection* – questo strumento alternativo di tutela trovò infatti piena cittadinanza nell'ordinamento giuridico.

Un percorso iniziato in sordina con i primi timidi tentativi della primavera del 1999: procedimenti peraltro già significativi sol che si pensi che fin dalla decisione del 19 aprile 1999 l'Autorità si pronunciò su una rilevante questione concernente la lesione dell'identità personale di una ricorrente, posta in essere da un quotidiano di rilievo nazionale (pronuncia che diede luogo anche, a distanza di tempo, ad una delle prime decisioni della Corte di cassazione sulla legge n. 675/1996, pienamente confermativa dell'orientamento espresso dall'Autorità).

Da allora sono ormai quasi quattromila i ricorsi esaminati, istruiti e decisi dal Garante che ha così avuto modo di "toccare", attraverso la miriade di fattispecie analizzate, i più diversi settori connessi, talora in modo sorprendente e inaspettato, al concetto ampio e multiforme di dato personale. Dalla varietà delle fattispecie è però possibile ricavare problematiche ricorrenti e linee di tendenza che, anche con riferimento all'ultimo anno, possono essere riassunte attorno ad alcune parole chiave.

17.2. I ricorsi nel 2008: temi ricorrenti e linee di tendenza

17.2.1. Accesso ai dati personali e trasparenza delle informazioni

L'esigenza di ogni interessato di conoscere tutte le informazioni che lo riguardano (non solo quelle più comuni, ma tutti i dati relativi al proprio stato di salute, alla propria situa-

zione contabile e finanziaria, alla propria collocazione professionale…), unitamente alla necessità di "seguire" e controllare l'*iter* di tali dati, resta l'esigenza primaria rispetto alla quale gli strumenti giuridici offerti dal Codice hanno sicuramente aperto una nuova pagina di trasparenza che si affianca così alle potenzialità dischiuse, a partire dal 1990 e in riferimento all'operato delle pubbliche amministrazioni, dalla legge n. 241. Ecco perché il diritto di accesso (esercitato da solo o assieme alle altre situazioni giuridiche di cui all'art. 7 del Codice) resta il cardine della tutela assicurata dal ricorso al Garante e quasi per antonomasia ne condensa e ne riassume le finalità.

17.2.2. La crescita esponenziale dei trattamenti sulla rete

Internet incide sempre più spesso e profondamente sulla dimensione della protezione dei dati personali e interessa in modo crescente anche la realtà dei ricorsi, sfidando frequentemente le categorie giuridiche tradizionali e mettendo in risalto i limiti di legislazioni nazionali alle prese con fenomeni globali che oltrepassano le dimensioni ordinarie di spazio e di tempo. Dai problemi connessi al fenomeno dello *spam*, al controllo della posta elettronica e della navigazione *web* dei lavoratori, fino ai temi correlati alla rintracciabilità *"infinita"* dei dati tramite i motori di ricerca, emerge in maniera sempre più forte la difficoltà di controllare la diffusione delle informazioni e di assicurare spazi di protezione al singolo sia nella sua dimensione personale sia in quella professionale.

17.2.3. Privacy *e manifestazione del pensiero*

Le cennate potenzialità della rete Internet accrescono la sensibilità degli interessati che hanno, anche nel 2008, moltiplicato i ricorsi che pongono al centro il conflitto (noto nelle premesse ma sempre nuovo nelle manifestazioni) fra la tutela della riservatezza del singolo e le esigenze connesse al diritto/dovere di informare e di essere informati, nell'ambito di un corretto esplicarsi del diritto di cronaca e di critica. Anche in questo ambito il ricorso ex art. 145 del Codice ha acquisito un suo spazio riconoscibile – affiancandosi alle più tradizionali forme di tutela imperniate sulle disposizioni dei codici (civile e penale) e sul dettato della *cd. "legge sulla stampa"* (l. 8 febbraio 1948, n. 47) – offrendo agli interes-

sati le varie possibilità di intervento previste dall'art. 7 del Codice ed in particolare l'arma dell'opposizione per motivi legittimi al (futuro) trattamento dei dati. Strumento prezioso, quello del ricorso in ambito giornalistico, ma sicuramente problematico. Basti pensare al complesso rapporto tra tutela della riservatezza (in coerenza con il dettato degli artt. 136 e *ss.* del d.lg. n. 196/2003 e del codice di deontologia in materia di attività giornalistica) e princìpi di cui all'art. 21 della Costituzione.

Esaminando la casistica concreta emerge come un numero sempre più elevato di casi riguardi l'ambito televisivo (ivi comprese le trasmissioni di carattere non strettamente giornalistico, ma ad esse assimilate, come le "inchieste d'assalto" di note trasmissioni satiriche, di cui è esempio, tra gli altri, il *provvedimento* del 5 giugno 2008 [doc. *web* n. 1542403]). Si tratta di fattispecie nelle quali (prima e più del dato contenutistico) il tema in discussione è rappresentato dalle modalità di raccolta dei dati personali. Ciò, con riferimento all'uso di telecamere nascoste o all'agire di intervistatori che celano il loro vero ruolo al fine di mantenere un carattere di *"genuinità"* alla situazione fatta oggetto di inchiesta, contando sull'effetto sorpresa. Sono ipotesi delicate, da vagliare sicuramente caso per caso, con speciale riferimento all'art. 2, comma 1, del codice deontologico dei giornalisti ed alla necessità di valutare se le modalità di raccolta e diffusione siano proporzionate e realmente giustificate rispetto ad uno scopo informativo altrimenti non conseguibile (*v.* la decisione del 3 febbraio 2009). Nel caso citato risultavano, ad esempio, essere state adottate misure idonee a rendere non identificabili gli interessati ripresi dalle telecamere (inquadrature limitate, oscuramento del volto, mascheramento della voce, *ecc.*), anche se il servizio televisivo non era poi stato trasmesso per autonoma scelta editoriale degli autori.

Ricorsi delicati hanno poi riguardato la diffusione giornalistica di dati personali relativi a minori (vedi decisioni del 2 ottobre 2008 [doc. *web* n. 1557470] e del 27 novembre 2008 [doc. *web* n. 1582436]). È questo un ambito sul quale l'Autorità è ripetutamente intervenuta tenendo conto della particolare attenzione riservata al tema dalle disposizioni del codice deontologico di settore (che riprende al riguardo le elaborazioni della *"Carta di Treviso"*) nonché da quelle del codice di procedura penale (in particolare l'art. 114, comma 6) e dalle norme specifiche sul processo minorile. Tutte disposizioni che

mirano a precludere la divulgazione di notizie o immagini idonee a consentire l'identificazione dei minori coinvolti in vicende di cronaca (non solo penale). In questo ambito una situazione ricorrente è quella dei *"pezzi"* giornalistici nei quali non compaiono direttamente i dati identificativi dei minori coinvolti ma sono presenti elementi che possono portare alla loro *"identificabilità"* secondo il dettato dell'art. 4, comma 1, lett. *b*), del Codice (riferimenti, *ad es.*, a età, scuole frequentate, luoghi di residenza o di villeggiatura, attività professionale dei genitori, *ecc.*). Ciò, tenendo conto, a tutela dei minori, che il rischio che si verifichi tale identificabilità deve essere evitato specie in relazione ad ambiti locali, nei quali è più forte l'attenzione della pubblica opinione ed occorre assolutamente evitare che la stampa finisca per assecondare forme di curiosità anche morbosa.

17.2.4. Identità personale

È un altro dei concetti chiave attorno a cui ruotano molte decisioni degli ultimi mesi. È sicuramente il segno di una maturazione e di una consapevolezza nuova che vede la protezione dei dati non come un complemento, ma appunto come un elemento costitutivo che può incidere significativamente sull'identità della persona.

Ne sono esempio le numerose decisioni sul trattamento dati svolto dalle società di informazione commerciale in relazione agli *"accostamenti"* (giudicati in diverse ipotesi illegittimi dal Garante) di dati relativi a società commerciali con le informazioni più strettamente riferite alle persone fisiche che a vario titolo avevano operato all'interno delle stesse. Accostamenti capaci di proiettare (in maniera impropria) ombre negative sull'affidabilità, sulla solidità patrimoniale e, spesso, anche sulla serietà professionale di numerosi operatori economici.

Basti citare, tra le tante, la decisione del 12 giugno 2008 ([doc. *web* n. 1537684] *v. par.* 10) adottata nei confronti del maggiore operatore italiano nel settore delle informazioni commerciali (Cerved S.p.A.). Nel caso citato il Garante è intervenuto disponendo la sospensione della visibilità dei dati dell'interessato in ragione di due distinti profili. Anzitutto in ordine ai citati *"accostamenti"* che creavano, nel *"dossier persona"* relativo al ricorrente, un pericoloso *"corto circuito"* fra la persona dell'interessato e la vicenda del fallimento

di una società di cui lo stesso era stato socio accomandante. Ciò, considerato che l'evento fallimento è relativo ad un terzo (appunto la società fallita) e che l'ordinamento prevede una responsabilità personale dei soci accomandanti solo in casi residuali e accertabili giudizialmente (*cfr.* artt. 2314 e 2320 c.c.), che non si erano verificati nel caso di specie.

La censura dell'Autorità si è appuntata poi su un ulteriore aspetto, la formulazione dell'*"indice di rilevanza storica dei fenomeni di insolvibilità"*, un dato di tipo valutativo elaborato con l'ausilio di procedimenti informatici mediante l'attribuzione di un peso ponderato ad una serie di eventi. Al riguardo il Garante pur riconoscendo, in termini generali, la legittimità dell'espressione di giudizi di tipo valutativo riferiti a soggetti economici, ha però sottolineato l'esigenza che gli stessi siano basati su dati esatti, completi, pertinenti e non eccedenti e che i giudizi medesimi siano fondati su procedure trasparenti e verificabili tali da assicurare la necessaria qualità dei dati.

Nella nuova realtà tecnologica, peraltro, l'identità personale non è solo valore da affermare e tutelare nella dimensione sociale e relazionale ma elemento (o insieme di elementi), costitutivi della persona, che possono essere anche oggetto di indebita appropriazione e di illecito utilizzo. È il tema, sempre più attuale, del *cd. "furto d'identità"* di cui qualche ricorso (*v. ad es.*, le decisioni del 13 ottobre [doc. *web* n. 1562822] e del 6 novembre 2008 [doc. *web* n. 1571531]) ha messo in luce la frequenza e la pericolosità. Ciò, quando profili biografici artatamente ricostruiti vengono utilizzati per porre in essere contratti di acquisto o di finanziamento (finalizzati alla truffa) impiegando informazioni personali che poi finiscono, con indicazione *"negativa"* a carico di persone inconsapevoli, negli archivi di qualche centrale rischi.

17.2.5. Conservazione della memoria e riservatezza

Molti degli aspetti sopra evidenziati (diffusione dei dati sulla rete, indicizzabilità degli stessi tramite i motori di ricerca, esigenze di tutela degli interessati con particolare riguardo alla necessità di proteggere l'attuale identità di una persona evitando che *"tracce"* e *"scorie"* della sua esistenza rimangano perennemente associate alla sua persona) si ritrovano contemporaneamente implicate in un problema di recente emersione e che sta

dando luogo ad un vivace contenzioso: la diffusione di dati conseguente alla libera disponibilità degli archivi storici *on-line* dei principali quotidiani. Si tratta di un'iniziativa che sfruttando le più recenti tecnologie dilata le possibilità di rapida ricerca e acquisizione di materiale documentario che, fino a tempi recenti, era acquisibile solo attraverso la faticosa consultazione di archivi cartacei.

Ciò peraltro comporta (attraverso gli automatismi indotti dai motori di ricerca) che fatti e notizie anche molto risalenti nel tempo possano essere facilmente rintracciati in rete riportando all'attenzione dei *"navigatori"* del *web* episodi e situazioni (legati spesso alla cronaca giudiziaria) che possono proiettare oggi un'immagine negativa su alcuni dei protagonisti, specie quando il tempo trascorso aveva invece, portato, ad un naturale oblio su tali vicende. È evidente il contrasto anche lacerante che può così aprirsi fra le esigenze conoscitive che postulano la più ampia disponibilità di dati e informazioni (a fini di documentazione giornalistica o di ricostruzione storica) e le contrapposte esigenze di tutela della riservatezza (richiamate da soggetti che, non essendo persone note o personaggi pubblici, invocano il ritorno ad un anonimato che li sottragga alle conseguenze di quella nuova forma di gogna elettronica rappresentata dagli istantanei risultati delle ricerche in rete). Di queste problematiche è esempio significativo, fra gli altri, il ricorso deciso l'11 dicembre 2008 [doc. *web* n. 1583162]. Accogliendo, seppur in parte, le richieste del ricorrente, che contestava la diffusione sull'archivio storico *on-line* del principale quotidiano italiano di un articolo risalente al 1995 che riferiva del suo coinvolgimento in un'indagine giudiziaria, il Garante ha preso posizione su questo tema delicato. Lo ha fatto considerando, fra l'altro, il tempo trascorso dalla vicenda oggetto dell'articolo e tenendo conto che con il passare degli anni le persone coinvolte hanno intrapreso nuovi percorsi di vita personale e sociale che potrebbero essere compromessi dal continuo ritorno di *"un passato che non passa"*. Va pertanto valutato il rischio che la rappresentazione istantanea e cumulativa di fatti ormai risalenti, derivante dalle ricerche operate appunto tramite i motori di ricerca, continui a riverberare i propri effetti sugli interessati. Per evitare questo rischio, che comporterebbe un sacrificio sproporzionato dei diritti degli interessati, si è ordinato all'editore di adottare ogni misura tecnicamente idonea ad evitare che le generalità del ricorrente

contenute nell'articolo in questione continuino ad essere rinvenibili direttamente attraverso l'utilizzo dei motori di ricerca generalisti, ferma rimanendo la possibilità di consultare la versione integrale dell'articolo medesimo accedendo direttamente al sito *web* dell'editore.

Si tratta di una soluzione che cerca di realizzare il faticoso contemperamento fra due interessi confliggenti sulla quale sicuramente il Garante avrà modo di tornare per verificare, al contatto con la molteplicità delle fattispecie concrete, la tenuta di queste indicazioni di primo orientamento.

Già con la decisione del 12 febbraio 2009 [doc. *web* n. 1601624] il Garante ha offerto alcune nuove puntualizzazioni in ordine alla diffusione in un archivio storico *on-line* di un articolo risalente al 2001 concernente una truffa di rilevanti proporzioni. In questo caso le richieste del ricorrente sono state ritenute infondate. Ciò in ragione del breve lasso di tempo intercorso dai fatti e dai successivi sviluppi giudiziari della questione che sono tali da far ritenere non ancora cessata, allo stato, l'opportunità di un'ampia conoscibilità dei fatti in questione.

Va peraltro rilevato che i primi riscontri a queste decisioni da parte dei titolari del trattamento sono positivi. Accogliendo un'indicazione presente nella stessa decisione citata, RCS Quotidiani S.p.A. ha manifestato interesse e disponibilità alla convocazione di un tavolo di lavoro (allargato alla partecipazione dell'Ordine dei giornalisti, delle associazioni rappresentative degli editori e di quelle dei gestori dei motori di ricerca) per valutare le molteplici implicazioni sottese da queste prime decisioni.

17.2.6. Protezione dei dati e tutela giurisdizionale

Sempre più spesso il ricorso al Garante viene proposto non come uno strumento di tutela fine a se stesso ma come procedimento pensato e utilizzato nell'ambito di una più ampia strategia di difesa o comunque di tutela dei propri diritti e interessi. In questo quadro la *"strumentalità"* (efficace) del ricorso appare sia dal punto di vista dell'esercizio del diritto d'accesso (con riferimento a tutte le ipotesi nelle quali vi sia l'interesse ad arricchire o completare il quadro conoscitivo e probatorio), sia dal punto di vista dell'utilizzo degli

altri diritti di cui all'art. 7 (con particolare riferimento alle ipotesi nelle quali si manifesti l'opposizione al trattamento di determinati dati o si chieda, in caso di violazione di legge, la cancellazione degli stessi).

In questa seconda ipotesi, che più concretamente esprime il ruolo strumentale che il ricorso può assumere, le richieste dell'interessato sono spesso volte, all'opposto del caso precedente, non ad arricchire gli elementi di conoscenza ma a privare la controparte di informazioni che a vario titolo (nella gestione di un rapporto di lavoro, in un confronto in un'aula di giustizia, *ecc.*) possono danneggiare l'interessato.

Molti sono i contesti in cui il ricorso si è posto come tappa nell'ambito di un più vasto contenzioso tra le parti, coinvolgendo il Garante nell'esame di fattispecie, anche innovative, che hanno poi fornito lo spunto per l'elaborazione di provvedimenti e di linee-guida di portata generale.

Ne è stata esempio significativo negli ultimi anni la materia del rapporto di lavoro dove più volte – in relazione a contestazioni disciplinari o a procedimenti scaturiti a seguito del licenziamento di un lavoratore – il Garante è stato chiamato a pronunciarsi sul trattamento dati connesso all'utilizzo della posta elettronica o dell'apparecchio telefonico d'ufficio o a valutare la liceità di operazioni di accesso da parte del datore di lavoro alle informazioni concernenti, ad esempio, i siti Internet visitati dal dipendente durante l'orario di lavoro. Né sono mancati i casi in cui è stato sottoposto al vaglio della disciplina del Codice l'utilizzo – al fine di controllare l'eventuale svolgimento di attività incompatibili con l'asserito stato di malattia o con i doveri di fedeltà del lavoratore – di investigatori privati.

Ma è la dinamica più propriamente processuale che ha offerto esempi significativi. Basti pensare alle vicende connesse all'asserita acquisizione illecita di dati contabili presso istituti di credito da parte di soggetti non legittimati e all'eventuale successivo utilizzo degli stessi (in evidente danno della controparte) nell'ambito, ad esempio, di un giudizio incentrato sui profili economici di una separazione fra coniugi. È in questi contesti che possono acquistare un peso significativo norme come l'art. 11, comma 2, del Codice in base al quale *"i dati personali trattati in violazione della disciplina rilevante in materia di trattamento dei dati personali non possono essere utilizzati"* ma anche il comma 6 del-

l'art. 160 che, in un equilibrato rapporto con i poteri riservati all'autorità giurisdizionale, precisa che *"la validità, l'efficacia, l'utilizzabilità di atti, documenti … basati sul trattamento di dati personali non conforme a disposizioni di legge o di regolamento restano disciplinate dalle pertinenti disposizioni processuali nella materia civile e penale"*.

Non sono naturalmente mancate le ipotesi in cui si è, per così dire, estremizzato l'utilizzo degli strumenti di tutela dell'art. 7 e sulla base, ad esempio, di un'asserita risoluzione per inadempimento di un contratto (sul cui accertamento, peraltro, l'autorità giudiziaria doveva ancora pronunziarsi) si è preteso (in modo dall'Autorità giudicato infondato) di ottenere la cancellazione di tutti i dati relativi al rapporto contrattuale in questione. Risultato, questo, che avrebbe ovviamente inciso in maniera grave sul diritto di difesa di controparte che invece, come affermato dal Garante, ben poteva continuare a trattare questi dati senza consenso sia in relazione all'esecuzione del contratto medesimo sia per le citate ed evidenti ragioni di difesa: ciò sulla base dei presupposti equipollenti di cui all'art. 24 del Codice (*Provv.* 27 novembre 2008 [doc. *web* n. 1580262]).

Molto comune è poi il tentativo (infondato) di ottenere il blocco o addirittura la cancellazione di una intera serie di dati sulla base della denunciata violazione di un limitato aspetto del trattamento in questione. Può essere al riguardo illuminante il caso deciso il 19 maggio 2008 [doc. *web* n. 1523347] nel quale – in relazione ad un controverso trattamento posto in essere dal Ministero dell'interno nei confronti di un proprio dipendente – è stato messo in luce che la raccolta, l'elaborazione e la conservazione di una nutrita serie di informazioni concernente le asserite prestazioni lavorative non autorizzate era avvenuta lecitamente, mentre la contestata comunicazione a terzi di alcuni dati costituiva un'autonoma operazione di trattamento la cui eventuale illiceità non comportava però l'illiceità dell'intero trattamento dei dati da parte dell'amministrazione resistente e il conseguente diritto del ricorrente a ottenerne la cancellazione o il blocco.

Particolare rilievo ha poi assunto, nell'ambito della ricerca degli elementi utili a costruire una strategia processuale, assicurando il migliore esercizio del diritto di difesa, l'accesso finalizzato all'acquisizione di dati personali, sia in *"entrata"* che in *"uscita"*, contenuti nei *cd. "tabulati di traffico telefonico"*. La relativa disciplina (con particolare

riguardo all'estensione temporale del periodo di conservazione di tali dati) costituisce uno dei punti più travagliati dell'intero Codice. L'art. 132, che disciplina tale particolare aspetto con riferimento a finalità diverse da quelle di fatturazione, ha subito infatti molteplici modifiche che hanno più volte profondamente mutato la relativa disciplina, sia con riguardo ai tempi di conservazione dei dati (progressivamente ridotti) sia in relazione alle modalità di acquisizione degli stessi.

Ciò spiega perché anche decisioni che si sono succedute a breve distanza di tempo facciano riferimento a cornici normative differenti (*ad es.*, *Provv.* 29 maggio 2008 [doc. *web* n. 1531594] e *Provv.* 13 novembre 2008 [doc. *web* n. 1573708]) che hanno trovato, all'attualità, un momento di (almeno apparente) sintesi con la disciplina dettata dal d.lg. n. 109/2008 con la quale il nostro Paese si è adeguato, quanto ai tempi di conservazione dei dati, alle indicazioni del legislatore comunitario.

17.3. I ricorsi esaminati nell'anno 2008: brevi considerazioni statistiche

Eterogeneità delle situazioni rappresentate e varietà dei diritti fatti valere sono stati la costante della trattazione dei ricorsi anche nell'anno passato. Ne sono testimonianza immediata le tabelle statistiche (*v. cap.* 23) che ben fotografano questa realtà.

Dal punto di vista numerico emerge come, dopo tre anni di diminuzione, è ritornato a crescere il totale dei ricorsi decisi dal Garante (anche se di poche unità rispetto all'anno precedente, trecentoventuno rispetto ai trecentosedici del 2007): segno di un assestamento delle cifre complessive che ormai si attestano sui 300/400 ricorsi all'anno.

Peraltro, nonostante i dieci anni trascorsi, le potenzialità dello strumento *"ricorso"* non appaiono ancora pienamente esplicitate come dimostra l'approccio *"pionieristico"* e le incertezze che ancora contraddistinguono molti degli atti (anche redatti da professionisti legali) che pervengono all'Autorità.

Va peraltro evidenziato come negli ultimi anni sia anche molto cresciuto il ricorso alla tutela giurisdizionale delle posizioni giuridiche garantite dal Codice. Ciò, attraverso la particolare procedura di cui all'art. 152 del Codice medesimo cui si affianca appunto, in chiave di alternatività, lo strumento del ricorso. La tutela dei diritti di cui all'art. 7 del

Codice non è più quindi confinata alle decisioni direttamente adottate dall'Autorità ma sta lentamente penetrando nella pratica ordinaria degli uffici giudiziari contribuendo a quella diffusione dei concetti chiave della disciplina di cui tuttora si ravvisa la necessità e si avverte la carenza.

Anche l'esame del tipo di decisioni adottate nell'ultimo anno consente alcune osservazioni. Si conferma anzitutto come largamente predominante la conclusione dei procedimenti attraverso la declaratoria di *"non luogo a provvedere"*. Si tratta della situazione tipica nella quale la realizzazione dei diritti dell'interessato consegue appunto alla presentazione del ricorso e al successivo intervento dell'Autorità che attiva il relativo procedimento. L'impressione al riguardo è che spesso solo il passaggio alla fase contenziosa assicura quell'effettiva tutela dell'interessato che il sistema affiderebbe piuttosto al diretto esercizio dei diritti da parte dell'interessato stesso.

Va peraltro rilevato come spesso le iniziali mancate risposte dei titolari del trattamento celino piuttosto, con riferimento alle realtà organizzative complesse, problemi di coordinamento interno e persistenti ritardi nell'individuare con prontezza le istanze ex art. 7 del Codice e apprestare le relative, idonee risposte.

Al riguardo sono emblematici gli esiti di parecchie richieste di accesso a dati personali detenuti da istituti di credito, spesso inizialmente istruite in modo erroneo come richieste formulate ai sensi dell'art. 119 del *"Testo unico bancario"*, norma che disciplina il distinto diritto di acquisizione di copia di documenti bancari.

Sempre esaminando il tipo di decisioni adottate appare particolarmente significativo il numero di casi (complessivamente più di cinquanta) di accoglimento totale o parziale delle istanze del ricorrente: segno sicuro dell'esistenza di una *"richiesta di giustizia"* che trova soddisfazione di fronte al Garante, chiamato con frequenza ad interpretare ed applicare la normativa di riferimento in ambiti inediti.

Speculare a questo aspetto è il numero (che rimane ancora significativo) dei ricorsi dichiarati inammissibili. Ciò evidenzia spesso (al di là dei casi di carenza dei requisiti formali minimi previsti dal Codice) il desiderio e la volontà di utilizzare gli strumenti previsti dalla disciplina in materia di protezione dei dati anche oltre i confini fissati dalla legge

stessa. È un pò il riflesso (sul piano dell'attività contenziosa) della situazione che vede il Garante destinatario di una miriade di segnalazioni e richieste di intervento, indirizzate ad un'Autorità identificata o percepita come il difensore di ogni reale o supposta turbativa della *"tranquillità"* individuale.

Ripercorrendo i ricorsi decisi nel 2008 è non meno significativo l'esame delle categorie di titolari di trattamento nei cui confronti sono stati proposti i ricorsi.

Emerge come largamente predominante l'ambito corrispondente all'attività economica privata ed in particolare alla sfera dei rapporti con il sistema creditizio. Ma se negli anni passati spiccava come maggioritario il tema delle richieste di cancellazione dei dati rivolte alle *cd. "centrali rischi private"*, il quadro statistico riferito all'anno 2008 mette in luce una realtà più variegata. Emerge infatti un uso sempre più intenso del diritto di accesso finalizzato alla ricostruzione di complesse situazioni contabili o alla definizione precisa dei cespiti ereditari (sfruttando le potenzialità insite nell'art. 9, comma 3, concernente l'acquisizione dei dati delle persone defunte), non disgiunto, in diversi casi, da connesse richieste di aggiornamento, integrazione o addirittura cancellazione dei dati. Ma è sicuramente il momento della patologia nell'utilizzo degli strumenti di pagamento e nella gestione dei contratti bancari o la conseguenza dei ritardi nel rimborso delle rate dei finanziamenti che ispira i molti ricorsi proposti nei confronti dei sistemi di informazioni creditizie o quelli che vengono indirizzati nei riguardi degli istituti di credito in relazione all'inserimento di informazioni (*"negative"* dal punto di vista dell'affidabilità economica dei soggetti interessati) nella Centrale dei rischi istituita presso la Banca d'Italia o nella Centrale d'allarme interbancaria (*cd. "archivio Cai"*), con specifico riferimento alle segnalazioni connesse all'emissione di assegni senza provvista o senza autorizzazione.

Ma la ragnatela degli archivi (ormai in larghissima parte informatizzata) che racchiudono informazioni di tipo economico è vastissima. Basti pensare al registro informatico dei protesti, al registro delle imprese, alle informazioni contenute nei registri immobiliari. Poiché si tratta di archivi caratterizzati da un regime di ampia pubblicità è evidente come diventi particolarmente delicato il trattamento dati svolto da quei soggetti che, professionalmente, si occupano di aggregare e ponderare queste informazioni, fornendo valuta-

zioni sulla solidità e solvibilità di molti operatori economici. Ecco dunque la ragione dei numerosi ricorsi proposti nei confronti delle società di informazioni commerciali cui si è fatto cenno. È un settore (ed un ambito di trattamento) delicato in un mercato competitivo attraversato per giunta dalle ricadute della crisi economica globale. L'esigenza di definire al riguardo regole di comportamento certe e definite è forte e lascia ipotizzare la possibilità (e forse l'opportunità) di arrivare a forme di regolamentazione condivise attraverso, ad esempio, l'elaborazione di un codice deontologico di settore.

Non si può infine non segnalare il rilevante numero di ricorsi proposti nei confronti degli operatori economici che con modalità tradizionali (posta fisica) o con strumenti più moderni e tecnologici (uso massivo del telefono e della posta elettronica) esercitano attività di *marketing*.

Di fronte all'entità massiva del fenomeno ed alle incertezze al riguardo dello stesso quadro normativo l'arma (sempre prevista dall'art. 7) dell'opposizione ai trattamenti per fini promozionali e pubblicitari resta uno dei pochi ma sicuri strumenti per riconquistare (seppur faticosamente, atteso l'elevato numero di soggetti con i quali occorre *"ingaggiare battaglia"*) una porzione di tranquillità perduta.

18. Il contenzioso giurisdizionale

18.1. Considerazioni generali

Anche nel 2008 si è confermata l'utilità del ricorso previsto dall'art. 152 del Codice, volto alla tutela giurisdizionale del diritto alla protezione dei dati personali in alternativa al ricorso presentato in sede amministrativa al Garante.

Nel corso dell'anno sono stati notificati all'Autorità centoventisette ricorsi, dimensione quantitativa analoga a quella riscontrata nel 2007, nel quale era stato registrato un incremento notevolissimo.

Atteso l'elevato numero di tali controversie, assume sempre maggiore utilità l'obbligo di notifica al Garante di tutti i ricorsi presentati all'autorità giudiziaria (art. 152, comma 7) e l'obbligo – purtroppo non sempre puntualmente adempiuto – per le cancellerie di trasmettere al Garante copia dei provvedimenti emessi dall'autorità giudiziaria in relazione a quanto previsto dal Codice o in materia di criminalità informatica (art. 154, comma 6).

La disponibilità di tali strumenti consente al Garante di avere un'ampia informazione sull'evoluzione della giurisprudenza in materia di protezione dei dati personali e di segnalare al Parlamento e al Governo gli interventi normativi necessari per la tutela dei diritti degli interessati (come previsto dall'art. 154, comma 1, lett. *f*), del Codice).

18.2. I profili procedurali

In base all'art. 152 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).

In tema di giurisdizione, contrariamente a quanto accaduto nel 2007, nel corso del 2008 l'Autorità non ha avuto notizia di ricorsi concernenti il trattamento dei dati personali proposti avanti al giudice amministrativo.

In tema di competenza territoriale, il Tribunale di Sorrento (provvedimento del 25 ottobre 2008) e il Tribunale di Grosseto (sentenza n. 163 del 7 dicembre 2005) in applicazione del disposto di cui all'art. 152, comma 2, del Codice, hanno dichiarato la loro

incompetenza territoriale a conoscere delle controversie ivi azionate, in favore del tribunale del luogo dove risiede il titolare del trattamento (rispettivamente il Tribunale di Milano e di Firenze).

In tema di competenza per materia, il Tribunale di Ferrara (sentenza n. 1946 del 24 gennaio 2008) ha dichiarato che spetta al giudice ordinario, ai sensi dell'art. 152, commi 1 e 3, del Codice, e non al giudice della volontaria giurisdizione, la competenza a trattare i giudizi concernenti l'applicazione del Codice.

Nel 2008 sono stati proposti due ricorsi straordinari al Presidente della Repubblica nei confronti di provvedimenti del Garante.

Nel primo caso il Consiglio di Stato, accogliendo la tesi sostenuta dall'Autorità, ha dichiarato inammissibile il ricorso (parere n. 4468/2007). Pur ricordando che la giurisprudenza dello stesso Consiglio ha ritenuto ammissibile in via di principio, avverso gli atti amministrativi illegittimi, sia il ricorso straordinario al Presidente della Repubblica, sia l'azione avanti al giudice ordinario (Ad. Gen. n. 988 del 29 maggio 1998), il giudice amministrativo ha però escluso la possibilità di ricorso straordinario avverso gli atti dell'amministrazione oggetto di forme di tutela giurisdizionale, quale quella prevista dall'art. 152, comma 1, del Codice, qualificabile come esclusiva e funzionale.

Con tale decisione il Consiglio di Stato ha modificato il precedente orientamento, di cui si è dato conto nella *Relazione* 2006, in base al quale aveva invece ritenuto ammissibile il ricorso straordinario al Capo dello Stato proposto nei confronti di un provvedimento adottato dal Garante in materia di trattamento di dati personali (parere n. 2265/2005).

Altro ricorso straordinario, attualmente in attesa di decisione, è stato proposto per l'annullamento del *provvedimento* del 23 gennaio 2008 ([doc. *web* n. 1487903], *v. Relazione* 2007, *par.* 12.2) con il quale il Garante ha disposto nei confronti del Consiglio dell'ordine degli avvocati di Santa Maria Capua Vetere il divieto del trattamento, in qualunque forma, di dati personali biometrici di alcuni praticanti avvocati.

18.3. I PROFILI DI MERITO

Alcune pronunce emesse dall'autorità giudiziaria, in fattispecie in cui non erano in discussione provvedimenti adottati dal Garante, evidenziano come ancora non si presti sufficiente attenzione alla tutela dei minori nella pubblicazione di notizie attraverso i mezzi di informazione.

Con ricorso al Tribunale di Paola, i genitori di una minore disabile hanno lamentato la pubblicazione della notizia della deliberazione comunale con la quale era stata concessa una forma di assistenza in favore della figlia, della quale era stata rivelata l'identità.

Il Tribunale ha ricordato che in base al codice di deontologia relativo al trattamento dei dati personali in ambito giornalistico il diritto del minore alla riservatezza è primario rispetto al diritto di cronaca. Ha specificato inoltre che disposizioni del codice vietano la pubblicazione dei nomi dei minori comunque coinvolti in fatti di cronaca, tanto più ove vengano rivelati dati sensibili, in quanto idonei a rivelarne lo stato di salute, e che comunque la pubblicazione dell'identità della minore non era essenziale al fine di descrivere l'avvenuta adozione della delibera.

Il Tribunale ha quindi condannato il direttore editoriale del periodico al risarcimento del danno (sentenza n. 574 del 17 aprile 2007).

Il Tribunale di Torino si è invece pronunciato in ordine alla pubblicazione su di un periodico di un articolo contenente i dati identificativi, corredati da fotografia, di un minore coinvolto in un procedimento giudiziario. Anche in tale caso il Tribunale, citando un pronunciamento del Garante, ha ricordato la priorità accordata dal codice deontologico relativo al trattamento dei dati personali in ambito giornalistico al diritto alla riservatezza del minore rispetto al diritto di cronaca. Nella specie, inoltre, particolari disposizioni contenute anche nel Codice (art. 50), vietano espressamente la pubblicazione di dati idonei a consentire l'identificazione di un minore coinvolto in un procedimento giudiziario. Il Tribunale (sentenza n. 4244 del 2 luglio 2008) ha quindi vietato alla testata giornalistica l'ulteriore diffusione di notizie o immagini idonee a consentire l'identificazione del minore, condannando i responsabili al risarcimento del danno.

18.4. LE OPPOSIZIONI AI PROVVEDIMENTI DEL GARANTE

L'anno 2008 ha registrato un netto incremento delle opposizioni a provvedimenti del Garante: a fronte dei diciotto ricorsi del 2007, nel 2008 sono state proposte trentadue opposizioni, di cui dodici nei confronti di decisioni assunte a seguito di ricorso.

Tale incremento va ascritto principalmente all'aumento delle opposizioni nei confronti di ordinanze ingiunzioni concernenti il pagamento di sanzioni amministrative comminate dall'Autorità sulla base dell'accertamento della violazione di disposizioni del Codice. La casistica indica quattordici opposizioni di tale natura (nel 2007 erano state solo due). Due dei relativi giudizi sono giunti a definizione in sede di merito.

Nel corso del 2008 l'Autorità ha avuto notizia di dieci decisioni dell'autorità giudiziaria relative ad opposizioni a provvedimenti del Garante, che si è sempre costituito.

Per quanto riguarda le opposizioni a ordinanze ingiunzioni, il Tribunale di Roma (sentenza n. 21303 del 29 ottobre 2008) ha accolto il ricorso proposto da un laboratorio di analisi al quale è stata comminata la sanzione amministrativa per non aver provveduto alla notificazione del trattamento con le modalità previste dall'art. 8 del Codice. Avverso tale decisione il Garante ha proposto ricorso per Cassazione.

In senso favorevole all'Autorità si è invece concluso il giudizio avanti al Tribunale di Treviso (sentenza n. 68 del 2 aprile 2008), che ha rigettato l'opposizione avverso l'ordinanza con cui il Garante ha ingiunto a un'azienda sanitaria il pagamento di una sanzione amministrativa per la violazione dell'art. 163 del Codice.

Due opposizioni sono state proposte in materia di trattamenti di dati effettuati nel settore del credito.

Un primo caso ha riguardato il *provvedimento* del Garante del 21 dicembre 2006 [doc. *web* n. 1378399] con il quale l'Autorità ha ordinato a un istituto di credito, nonché alla Banca d'Italia, la cancellazione dalla *"Centrale allarme interbancaria centrale"* (Cai) dei dati della società che ne aveva fatto istanza. Il Tribunale di Roma (sentenza n. 24504 del 14 dicembre 2007) ha accolto l'opposizione proposta dalla Banca d'Italia per carenza di legittimazione passiva. Il Garante avverso tale sentenza ha proposto ricorso in Cassazione.

Con altra pronuncia il Tribunale di Bologna (sentenza n. 20412 del 4 dicembre 2008) ha invece rigettato l'opposizione proposta avverso il *provvedimento* del 4 maggio 2006 [doc. *web* n. 1302311] con il quale il Garante ha vietato alla società che gestisce un sistema di informazioni creditizie di comunicare a fornitori di servizi di comunicazione elettronica dati contenuti nel sistema. Con il *provvedimento* l'Autorità ha, altresì, vietato il trattamento delle informazioni relative all'utilizzo irregolare delle carte di pagamento e dei dati ricavati dalle liste elettorali.

Dopo avere riconosciuto il pieno rispetto da parte del Garante della normativa che presiede al corretto espletamento del procedimento amministrativo, il Tribunale, nel confermare integralmente il provvedimento opposto, ha in particolare escluso che i fornitori di servizi di comunicazione elettronica possano avere accesso al sistema di informazioni creditizie, non avendone titolo, in base al disposto dell'art. 117 del Codice e di alcune disposizioni del codice deontologico del settore.

Per quanto attiene al trattamento effettuato in ambito giornalistico devono essere segnalate tre pronunce, tutte favorevoli all'Autorità.

Due decisioni sono state adottate dal Tribunale di Milano.

Nel primo caso (sentenza n. 7463 del 9 giugno 2008) il Tribunale ha respinto il ricorso proposto contro il *provvedimento* del 13 settembre 2007 [doc. *web* n. 1620926] con il quale l'Autorità ha vietato l'ulteriore trattamento delle immagini di un noto uomo politico fotografato all'interno di un parco di sua proprietà, pubblicate da un settimanale. Condividendo gli argomenti espressi dal Garante, il Tribunale ha ritenuto illecita l'acquisizione delle immagini pubblicate, per contrasto con norme del Codice e del codice deontologico relativo al trattamento dei dati personali nell'esercizio dell'attività giornalistica: il fotografo aveva infatti violato il domicilio dell'interessato – dovendosi ritenere il parco quale pertinenza dell'abitazione – utilizzando mezzi tecnici particolarmente invasivi, costituiti da potenti teleobiettivi. La società editrice del settimanale ha proposto ricorso per Cassazione avverso tale decisione.

Nel secondo caso (sentenza n. 2646 del 28 febbraio 2008) il Tribunale ha respinto il ricorso proposto avverso il *provvedimento* del Garante del 15 luglio 2006 [doc. *web*

n. 1310796] con cui l'Autorità ha vietato l'ulteriore diffusione di dati personali anche sensibili relativi alle tragiche circostanze della morte di una persona nota.

Si sono infine conclusi i due giudizi – trattati congiuntamente dall'autorità giudiziaria – con i quali una società concessionaria di reti televisive aveva proposto opposizione nei confronti di due noti *provvedimenti*, entrambi del 14 dicembre 2006, con i quali l'Autorità aveva disposto il divieto del trattamento di dati personali di alcuni parlamentari [doc. *web* n. 1370954] e di alcuni clienti di una discoteca [doc. *web* n. 1370781] (*v. Relazione* 2006 e 2007). Il Tribunale di Roma ha rigettato i ricorsi (sentenza n. 9055 del 30 aprile 2008).

Riguardo ai controlli del datore di lavoro sull'uso di strumenti elettronici da parte dei lavoratori, va registrata la pronuncia del Tribunale di Palermo (sentenza n. 4607 del 17 dicembre 2007) che ha respinto l'opposizione avverso il *provvedimento* del 2 febbraio 2006 (doc. *web* n. 1229854] con il quale il Garante ha vietato il trattamento da parte di una casa di cura dei dati relativi alla navigazione in Internet del dipendente. Il titolare del trattamento ha proposto ricorso per Cassazione.

Solo una decisione ha riguardato il settore del *marketing*: l'opposizione era stata proposta avverso il *provvedimento* del Garante del 7 dicembre 2006 [doc. *web* n. 1379101] con il quale è stato vietato ad una società editoriale l'invio di materiale pubblicitario. Il Tribunale di Milano ha respinto il ricorso (sentenza n. 5967 dell'8 febbraio 2008).

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.

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 e sugli esiti delle vicende processuali.

19. L'ATTIVITÀ ISPETTIVA E LE SANZIONI

19.1. LA PROGRAMMAZIONE DELL'ATTIVITÀ ISPETTIVA

L'Autorità ha proseguito, anche nell'anno 2008, il processo di sviluppo dell'attività ispettiva, già avviato nell'anno 2007. 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;
- effettuare controlli per categorie omogenee di titolari del trattamento secondo una metodologia predefinita denominata *"a progetto"*.

Sotto il primo profilo, nell'anno 2008 si è registrato un ulteriore incremento delle attività (+10% rispetto al 2007) in linea con la tendenza generale di aumento dell'attività di controllo, già evidenziata negli anni precedenti.

Anno	2002	2003	2004	2005	2006	2007	2008
Ispezioni	40	69	100	230	350	452	500

Delle cinquecento attività ispettive, trecentottantacinque sono state effettuate di iniziativa, sulla base di programmi ispettivi semestrali disposti dall'Autorità e centoquindici nell'ambito di istruttorie connesse a reclami, segnalazioni e ricorsi presentati dai cittadini.

Come dimostrano i dati sopra riportati, grande importanza riveste l'attività di prevenzione effettuata "*motu proprio*" dall'Autorità (anche in assenza cioè 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 il 75%).

In relazione a tale attività, il Collegio determina, con cadenza semestrale, le linee di indirizzo attraverso delibere 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 dell'attività di controllo consente, attraverso verifiche effettuate 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 degli operatori appartenenti ad 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 la 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 2008, 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 in riferimento a profili di interesse generale per categorie di interessati nell'ambito di:

- trattamenti di dati personali effettuati dall'amministrazione finanziaria, mediante il sistema informativo della fiscalità, con particolare riferimento alle misure adottate per garantire l'accesso ai dati da parte degli enti esterni;
- trattamenti di dati personali effettuati da istituti di credito, relativamente alla legittimità della consultazione e del successivo utilizzo dei dati da parte dei soggetti aventi diritto, anche in riferimento al tracciamento degli accessi e a correlate misure di protezione;
- trattamenti di dati personali effettuati da una società operante nel settore delle informazioni commerciali, con riferimento all'utilizzo di dati pubblici e di conservatoria, nonché alle informazioni necessarie a verificare l'affidabilità, la solvibilità e la struttura economico-finanziaria dell'impresa;
- trattamenti di dati personali effettuati da società di telecomunicazione in relazione all'invio di *Sms* e *fax* indesiderati.

Con riferimento, invece, al periodo luglio-dicembre 2008, l'attività ispettiva di iniziativa è stata finalizzata ad accertamenti nell'ambito di:

- trattamenti di dati personali effettuati dall'amministrazione finanziaria, mediante il sistema informativo della fiscalità, con particolare riferimento alle misure adottate per garantire l'accesso ai dati da parte degli enti esterni;
- trattamenti di dati personali effettuati da parte di operatori di telecomunicazione, con finalità di profilazione dei clienti, mediante dati di traffico;
- trattamenti di dati personali effettuati da parte delle Camere di commercio, con particolare riguardo agli aggiornamenti delle informazioni camerali;
- trattamenti di dati personali effettuati da una società in relazione all'introduzione di carte di fidelizzazione in farmacia;
- trattamenti di dati personali effettuati da una società con finalità di profilazione dei medici per l'attività di informazione del farmaco;
- trattamenti di dati personali effettuati da società con finalità di *marketing;*
- trattamenti di dati personali effettuati da società in relazione al credito al consumo;
- trattamenti di dati personali effettuati da società con riferimento al riutilizzo commerciale di dati pubblici, in particolare liste elettorali e dati di conservatoria.

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 2008 è risultato determinante, nel settore ispettivo, il rapporto con la Guardia di finanza che ha consentito all'Autorità di poter disporre di risorse qualificate per espletare l'attività di controllo affidata dalla legge.

Il protocollo di intesa siglato nel 2005 consente al Garante di avvalersi del Corpo attraverso:

- la partecipazione di 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.

In pratica il Garante, ogni qualvolta ritenga necessaria la collaborazione del Corpo, attiva il Nucleo speciale *privacy* con sede a Roma che, disponendo di personale specializzato, provvede direttamente ad effettuare gli accertamenti, avvalendosi anche, ove necessario, dei 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. Qualora nell'ambito dell'ispezione emergano 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 2008, le attività tese a realizzare un maggior coinvolgi-

mento nell'attività di controllo della componente territoriale della Guardia di finanza (nuclei di polizia tributaria, gruppi, compagnie e tenenze).

L'obiettivo è quello di disporre di un dispositivo di controllo flessibile ed 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 anche i reparti territoriali della Guardia di finanza.

In questo ambito, è stata effettuata una particolare attività di controllo denominata *"progetto videosorveglianza"*. Per attività *"a progetto"* si intende un'attività complessa di carattere operativo, rientrante nell'attuazione di linee strategiche definite di concerto con il Comando generale della Guardia di finanza, che comporta l'esecuzione di compiti interrelati da parte di unità organizzative della componente speciale e di quella territoriale del Corpo, con obiettivi, tempi e assorbimento di risorse definiti.

Questa tipologia di controllo che la Guardia di finanza effettua utilizzando innovativi processi di lavoro modellati sulle tecniche di *project management*, è stata effettuata sulla base dell'elaborazione congiunta, da parte dell'Ufficio del Garante e del Nucleo speciale *privacy* della Guardia di finanza, di una guida per l'accertamento. Nell'ambito di tale guida sono stati definiti, in modo estremamente analitico, i passi che i *team* di ispettori avrebbero successivamente dovuto effettuare e le liste dei controlli da eseguire *in loco*.

Nell'ambito del *"progetto videosorveglianza"* gli accertamenti, effettuati alla fine del mese di settembre, sono stati indirizzati alla verifica del rispetto delle disposizioni previste dal Codice, in relazione anche a quanto previsto nel *provvedimento* generale del 29 aprile 2004 (doc. *web* n. 1003482), nei confronti di quaranta sistemi di videosorveglianza installati, su tutto il territorio nazionale, da comuni, scuole, ospedali, società private, istituti di vigilanza che trattano dati personali anche per conto terzi e altri soggetti.

I soggetti da sottoporre ad ispezione sono stati individuati tenendo conto della dimensione dei sistemi di videosorveglianza, della loro incidenza in aree aperte al pubblico con una elevata presenza di persone e di minori, dell'utilizzo di tecnologie particolarmente sofisticate o di telecamere non facilmente rilevabili.

Ai quaranta controlli delegati dal Garante si sono aggiunti anche ulteriori accertamenti effettuati autonomamente dalla Guardia di finanza nell'ambito delle ordinarie attività di controllo.

L'attività ha consentito di rilevare in trentanove violazioni dell'obbligo di fornire l'informativa al pubblico sulla presenza del sistema di videosorveglianza, in circa trenta casi un periodo di conservazione delle immagini eccessivo rispetto a quanto previsto nel *provvedimento* del Garante e, in due casi, violazioni relative all'utilizzo di tali sistemi in contrasto con quanto previsto dall'art. 4 dello Statuto dei lavoratori che hanno comportato la segnalazione all'autorità giudiziaria in relazione alla sanzione penale prevista dall'art. 171 del Codice.

19.3. I SETTORI OGGETTO DEI CONTROLLI E I CASI PIÙ RILEVANTI

Nel 2008 sono state effettuate, suddivise per settore, le seguenti attività ispettive:

- quaranta controlli nei confronti di soggetti pubblici e privati che utilizzano sistemi di videosorveglianza, per verificare la liceità del trattamento e il rispetto del *provvedimento* generale del Garante sullo specifico tema;
- trenta controlli nei confronti di cliniche private che trattano dati sensibili, con riferimento all'adozione delle misure minime di sicurezza;
- venti controlli nei confronti di circoli sportivi per verificare le modalità di trattamento dei dati degli associati;
- venti controlli nei confronti di villaggi turistici, per verificare le modalità di trattamento dei dati dei clienti acquisiti anche tramite siti *web*;
- venti controlli nei confronti di agenzie assicurative, per verificare le modalità di trattamento dei dati, anche sensibili, degli assicurati;
- venti controlli nei confronti di agenzie di viaggio, per verificare le modalità di trattamento dei dati dei clienti acquisiti anche tramite siti *web*;
- venti controlli nei confronti di Internet *Point/Cafè*, per verificare le modalità dei trattamenti dei dati di traffico telefonico e telematico;
- venti controlli nei confronti di dottori commercialisti, per verificare le modalità di trattamento dei dati, anche sensibili, dei clienti;

- venti controlli nei confronti di dottori psichiatri e psicologi, per verificare le modalità di trattamento dei dati, anche sensibili, dei clienti;
- venti controlli nei confronti di videoteche, per verificare le modalità di trattamento dei dati dei clienti acquisiti anche tramite siti *web*;
- venti controlli nei confronti di società che effettuano attività di fidelizzazione, profilazione e *marketing*, per verificare le modalità di trattamento dei dati dei clienti;
- dieci controlli nei confronti di società finanziarie, per verificare le modalità di trattamento dei dati dei clienti, in relazione al credito al consumo ed alla solvibilità;
- dieci controlli nei confronti di società che effettuano attività di vendita *on-line*, per verificare le modalità di trattamento dei dati dei clienti acquisiti tramite siti *web*;
- dieci controlli nei confronti di società di *service providers*, per verificare le modalità dei trattamenti dei dati di traffico telefonico e telematico;
- dieci controlli nei confronti di medici dentisti, per verificare le modalità di trattamento dei dati, anche sensibili, dei clienti;
- dieci controlli nei confronti di istituti scolastici, per verificare le modalità di trattamento dei dati degli studenti acquisiti anche tramite siti *web*;
- dieci controlli nei confronti di medici oculisti, per verificare le modalità di trattamento dei dati, anche sensibili, dei clienti acquisiti anche tramite siti *web*;
- dieci controlli nei confronti di centri di chirurgia estetica, per verificare le modalità di trattamento dei dati, anche sensibili, dei clienti acquisiti anche tramite siti *web*;
- dieci controlli nei confronti di società che effettuano concorsi a premi *on-line* per verificare le modalità di trattamento dei dati dei clienti acquisiti tramite siti *web*;
- nove controlli nei confronti di società di *dealers*, in relazione alle modalità di acquisizione del consenso, connesso alla profilazione, all'atto dell'attivazione di schede telefoniche;
- otto controlli nei confronti di soggetti vari a completamento di istruttorie già avviate in precedenza;
- quattro controlli nei confronti di laboratori di analisi genetica che effettuano trattamenti per i quali è prevista la notificazione al Garante;

- novantacinque controlli nei confronti di soggetti vari in relazione a specifiche segnalazioni trasmesse dai dipartimento giuridici;
- un controllo nei confronti di una società farmaceutica, in relazione all'introduzione di carte di fidelizzazione in farmacia;
- un controllo nei confronti di una società farmaceutica in relazione alla profilazione dei medici presso i quali le società farmaceutiche svolgono attività promozionale;
- venticinque controlli nei confronti di soggetti pubblici che utilizzano i sistemi informativi della fiscalità mediante *"anagrafe tributaria"*;
- quindici controlli nei confronti di istituti di credito, relativamente alla legittimità della consultazione e del successivo utilizzo dei dati da parte dei soggetti aventi diritto, anche in riferimento al tracciamento degli accessi e a correlate misure di protezione;
- quattro controlli nei confronti di società con riferimento al riutilizzo commerciale di dati pubblici, in particolare liste elettorali e dati di conservatoria;
- tre controlli nei confronti di compagnie telefoniche in relazione al trattamento di dati personali effettuati sui dati di traffico con finalità di profilazione e *marketing*;
- cinque controlli nei confronti di società che effettuano trattamenti di dati personali con finalità di profilazione e *marketing*.

In relazione a quanto emerso dagli accertamenti, sono state effettuate circa cento proposte di adozione di prescrizioni, per conformare il trattamento alla legge e/o di provvedimenti inibitori, a fronte delle quali l'Autorità ha adottato alcuni provvedimenti di particolare rilievo per le garanzie nei confronti dei cittadini.

Tra i più rilevanti si segnalano:

- il provvedimento nei confronti di una società che opera nel settore alberghiero in relazione a dati personali trattati senza specifico consenso a fini di *marketing*, di rilevazione di informazioni su gusti abitudini o preferenze dei clienti (*Provv.* 31 gennaio 2008 [doc. *web* n. 1490553]);
- il provvedimento nei confronti di una società che effettua servizi di *call center*, per una compagnia telefonica, in relazione all'invio di *fax* promozionali (*Provv.* 13 maggio 2008 [doc. *web* n. 1520217]);

- il provvedimento nei confronti di una società che effettua servizi di *marketing*, per conto di varie società, in relazione all'invio di *fax* promozionali (*Provv.* 13 maggio 2008 [doc. *web* n. 1520243]);
- il provvedimento nei confronti di una società che effettua servizi di *marketing* mediante sito *web*, per diverse società, in relazione all'invio di messaggi promozionali (*Provv.* 13 maggio 2008 [doc. *web* n. 1521775]);
- cinque provvedimenti nei confronti di diverse società che raccolgono e vendono elenchi di soggetti (banche dati), in relazione all'utilizzo degli stessi per chiamate promozionali e all'invio di messaggi promozionali (*Provv.* 26 giugno 2008 [doc. *web* nn. 15443315, 15443326 e 15443338]; *Provv.* 25 settembre 2008 [doc. *web* nn. 1562758 e 1562780]);
- il provvedimento nei confronti di una società che effettua la vendita di prodotti per la casa a domicilio per il trattamento di dati a fini di *marketing* in violazione di legge (*Provv.* 19 maggio 2008 [doc. *web* n. 1526956]);
- le linee-guida per i trattamenti di dati personali nell'ambito delle sperimentazioni cliniche di medicinali (*Provv.* 24 luglio 2008 [doc. *web* n. 1533155]);
- il provvedimento nei confronti dell'anagrafe tributaria in relazione al trattamento dei dati e agli accessi da parte degli enti esterni (*Provv.* 18 settembre 2008 [doc. *web* n. 1549548]);
- due provvedimenti nei confronti di una società, in relazione al trattamento dei dati personali per finalità di informazioni commerciali (*Provv.* del 13 ottobre 2008 [doc. *web* n. 1571459] e *Provv.* 30 ottobre 2008 [doc. *web* n. 1570327]).

19.4. L'ATTIVITÀ SANZIONATORIA DEL GARANTE

19.4.1. Violazioni penali e procedimenti relativi alle misure minime di sicurezza

In conseguenza delle ispezioni effettuate, sono state inviate all'autorità giudiziaria dodici informative (di cui sette da parte del Dipartimento attività ispettive e sanzioni dell'Autorità e cinque da parte della Guardia di finanza).

Le violazioni penali hanno riguardato: mancata adozione delle misure minime di sicu-

rezza (5), mancato adempimento di una deliberazione del Garante (1), trattamento illecito dei dati (1), falsità nelle dichiarazioni e notificazioni al Garante (3) e altre fattispecie (2).

Ventisei 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, come noto, 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 impartirsi alla persona individuata come responsabile della predetta violazione, verificato il ripristino delle misure violate, possa ammettere i destinatari della prescrizione al pagamento pari a 1/4 del massimo della sanzione prevista corrispondenti a 12.500 euro. L'adempimento alla prescrizione ed il pagamento della somma, vengono comunicati all'autorità giudiziaria competente per le valutazioni in ordine all'estinzione del reato.

L'attività di cui sopra ha riguardato venti persone (in qualità di titolari/responsabili dei trattamenti), per un totale di sanzioni applicate pari a 335.329 euro.

19.4.2. Sanzioni amministrative

In conseguenza delle ispezioni effettuate, sono stati avviati trecentotrentotto procedimenti sanzionatori amministrativi (di cui centocinquantacinque ad opera del Dipartimento e centottantatre da parte della Guardia di finanza e altri organi accertatori).

Come evidenziano i dati di seguito riportati, anche per quanto attiene l'attività sanzionatoria, nell'anno 2008, si è registrato un notevole incremento.

Anno	2002	2003	2004	2005	2006	2007	2008
Violazioni contestate	46	27	27	94	158	228	338

Le sanzioni amministrative contestate, per un totale compreso tra un minimo di 1.113.000 e un massimo di 6.678.000 euro, hanno riguardato:

- omessa o inidonea informativa (311);

- omessa notificazione (12);

- omessa risposta alle richieste del Garante (15).

A fronte delle contestazioni notificate sono stati riscossi 1.061.843 euro a titolo di definizione in via breve.

L'incidenza delle violazioni, sia penali che amministrative, riscontrate è stato pari a circa al 67% sul totale delle ispezioni.

L'adempimento più sanzionato è quello relativo alla violazione dell'obbligo di fornire all'interessato tutte le informazioni riguardanti il trattamento dei dati al fine di renderlo pienamente consapevole dell'effettivo utilizzo dei suoi dati personali.

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 es.*, 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.

Delle contestazioni effettuate per l'omessa o inidonea informativa, circa il 32% sono da riferirsi a segnalazioni relative a trattamenti effettuati, attraverso *call center*, da compagnie telefoniche in relazione all'attivazione di servizi non richiesti, a riprova dello straordinario sforzo compiuto nel 2008 dall'Autorità per contrastare tale fenomeno.

19.4.3. Il nuovo apparato sanzionatorio

Il decreto-legge n. 207/2008, convertito nella legge 27 febbraio 2009, n. 41, ha apportato significative modifiche all'apparato sanzionatorio del Codice. Le modifiche si sono concentrate, in massima parte, sulle sanzioni amministrative mentre è rimasto sostanzialmente inalterato l'impianto sanzionatorio penale.

In linea generale, gli interventi hanno comportato: un aumento delle pene pecuniarie previste per ciascuna violazione; la previsione di nuove ipotesi sanzionatorie; la creazione di meccanismi per consentire una maggiore modulabilità della sanzione in rapporto al

caso concreto in ragione della minore o maggiore gravità, della circostanza che le violazioni siano state commesse in relazione a banche di dati di particolare rilevanza o dimensioni, del coinvolgimento di un maggior numero di interessati e delle condizioni economiche del contravventore.

Fra le nuove fattispecie sanzionatorie amministrative sono state previste, all'art. 162, comma 2-*bis*, le ipotesi di trattamento illecito e di omissioni nell'adozione delle misure minime di sicurezza (già sanzionate penalmente dagli artt. 167 e 169 del Codice, articoli tuttora vigenti).

La sanzione amministrativa (da 20.000 euro a 120.000 euro) potrà essere contestata in tutti i casi di violazione delle disposizioni richiamate dall'art. 167 nonché nei casi di violazione delle misure minime di sicurezza previste dal Codice e, per quanto riguarda le misure minime di sicurezza, senza la possibilità di avvalersi dell'estinzione del procedimento sanzionatorio con il pagamento in misura ridotta.

È stata inoltre introdotta, all'art. 162, comma 2-*ter*, una specifica fattispecie sanzionatoria amministrativa (da 30.000 euro a 180.000 euro) nei casi di inottemperanza ai provvedimenti del Garante che prescrivono, anche d'ufficio, ai titolari del trattamento le misure necessarie o opportune al fine di rendere il trattamento conforme alle disposizioni vigenti o che prevedono il blocco o il divieto del trattamento.

La norma rafforza la cogenza delle determinazioni dell'Autorità, fino ad oggi garantita, limitatamente alla violazione dei provvedimenti di blocco e di divieto del trattamento nonché di quelli relativi alla decisione dei ricorsi, dalla sanzione penale prevista dall'art. 170 del Codice.

Per quanto riguarda i meccanismi introdotti al fine di modulare le sanzioni amministrative, va evidenziato in primo luogo che l'art. 164-*bis*, comma 1, prevede la possibilità di contestare le sanzioni accertate applicando una riduzione a due quinti dei limiti minimo e massimo previsto per ciascuna violazione, nei casi di minore gravità della violazione stessa o in relazione alla natura economica e sociale dell'attività svolta dal contravventore.

Di contro, i commi 2 e 3 del medesimo articolo prevedono delle particolari *"aggravanti"* che determinano un sensibile aumento delle sanzioni:

- in caso di più violazioni di un'unica o di più disposizioni commesse, anche in tempi diversi, in relazione a banche di dati di particolare rilevanza o dimensioni (sanzione da 50.000 euro a 300.000 euro senza la possibilità di avvalersi dell'estinzione del procedimento sanzionatorio con il pagamento in misura ridotta);
- in altri casi di maggiore gravità e, in particolare, di maggiore rilevanza del pregiudizio per uno o più interessati, ovvero quando la violazione coinvolge numerosi interessati, con aumento dei limiti minimo e massimo delle sanzioni previste per ciascuna violazione in misura pari al doppio.

Tutte le sanzioni possono essere, inoltre, ai sensi dell'art. 164-*bis*, comma 4, aumentate fino al quadruplo quando possono risultare inefficaci in ragione delle condizioni economiche del contravventore.

20. Le relazioni internazionali

La mancata entrata in vigore del Trattato di Lisbona ha rallentato i progetti delle autorità di protezione dei dati personali europee, riunite nel Gruppo art. 29 e nel Gruppo di lavoro Polizia e Giustizia, di valutare l'impatto delle nuove previsioni in materia di protezione dei dati personali. Il Trattato infatti richiama espressamente ed ingloba nel quadro giuridico le disposizioni della *"Carta dei diritti fondamentali"*, che, com'è noto, all'art. 8 ha introdotto il diritto fondamentale delle persone alla tutela dei dati personali, affiancandolo all'art. 7 che riguarda il diritto alla riservatezza. Sempre il Trattato, nel prevedere la fine della divisione in pilastri dell'ordinamento comunitario, chiede un quadro di riferimento tendenzialmente unico in materia di trattamento dei dati personali. Giova ricordare che oggi nell'ambito del *cd. "primo pilastro"* – che riguarda i settori coperti dal diritto comunitario – esiste un quadro armonizzato di princìpi che, nel garantire la libera circolazione dei dati personali tra i Paesi dell'Unione europea, assicura agli individui un elevato livello di tutela, costituito dalla Direttiva 95/46/Ce sulla tutela delle persone rispetto al trattamento di dati personali e sulla libera circolazione di tali dati e dalla 2002/58/Ce che specifica i princìpi della direttiva generale in relazione al trattamento dei dati personali nell'ambito delle comunicazioni elettroniche. Nessun principio esiste al momento per quanto riguarda i trattamenti di dati che si svolgono nel *cd. "secondo pilastro"* (politica estera e di sicurezza comune), mentre è recentemente stata adottata una decisione quadro sulla protezione dei dati personali trattati nell'ambito della cooperazione giudiziaria e di polizia in materia penale che dovrà essere attuata dai Paesi dell'Unione entro la fine di novembre 2010. L'attenzione delle Autorità si è comunque mantenuta sul quadro giuridico generale per valutarne la tenuta e migliorarne l'attuazione, ovvero intervenire sulle modifiche proposte, ad esempio alla direttiva sulla *privacy* nelle comunicazioni elettroniche, o al nuovo programma di lavoro in materia di polizia e sicurezza, che sostituirà il *cd. "Programma de L'Aja"*.

Il Garante ha attivamente partecipato a diversi gruppi di lavoro cooperando con le autorità europee e mondiali di protezione dei dati personali (*v. par.* 20.1 e seguenti). In alcuni casi ha anche svolto, come per il Gruppo di lavoro polizia e giustizia, un determinante e propositivo ruolo di iniziativa.

Da segnalare che il cons. Giovanni Buttarelli, che ha svolto il ruolo di segretario generale dal momento dell'istituzione dell'Autorità, nel dicembre 2008 è stato nominato Garante europeo aggiunto dei dati personali.

Occorre evidenziare gli importanti contatti intercorsi tra il Garante e il Parlamento europeo, nonché con il Commissario per i diritti umani del Consiglio d'Europa in particolare in relazione alle iniziative del Governo italiano per utilizzare i poteri di emergenza di protezione civile in alcune aree metropolitane (Napoli, Roma, Milano) in cui vivono popolazioni nomadi. L'annuncio del censimento rom ha destato preoccupazioni forti in tutta Europa e la Commissione europea è intervenuta richiedendo non solo al Governo, ma anche al Garante, di indicare l'impatto di tali iniziative sui diritti fondamentali ed in particolare sul diritto alla protezione dei dati personali. Il Parlamento europeo, dopo aver adottato una risoluzione critica nel luglio 2008 ha inviato componenti della Commissione Libe, per incontri con le autorità. Il Garante ha nell'occasione descritto al Comitato le azioni svolte per accertare il tipo di trattamento di dati e, successivamente, per definire le modalità idonee ad assicurare il rispetto dei princìpi di protezione dei dati.

Il Garante, infatti, anche sulla base di notizie di stampa circa l'eventuale ricorso a forme di rilevazione anche biometriche (impronte digitali) estese ai minori, per finalità di identificazione o di censimento di comunità di nomadi, ha chiesto informazioni, in particolare ai Prefetti di Roma, Milano e Napoli, rilevando tra l'altro che l'adozione di tali misure potrebbe determinare l'insorgere di delicati problemi discriminatori, potenzialmente lesivi della dignità delle persone e specialmente dei minori.

Al riguardo, il Ministero dell'interno ha informato l'Autorità dell'intenzione di promuovere l'adozione di alcune linee-guida rivolte ai prefetti in merito alla raccolta dei dati relativi al censimento delle comunità nomadi.

Con il *provvedimento* del 17 luglio 2008 [doc. *web* n. 1537659] l'Autorità ha quindi espresso il proprio parere favorevole sullo schema di linee-guida messe a punto dal Ministero dell'interno per l'attuazione delle ordinanze adottate dal Presidente del Consiglio dei ministri il 30 maggio 2008 concernenti insediamenti di comunità nomadi nelle regioni Campania, Lazio e Lombardia. Le linee-guida stabiliscono i princìpi fonda-

mentali e le modalità da seguire nell'identificazione di chi risiede nei campi nomadi e tengono conto delle indicazioni e delle raccomandazioni in precedenza formulate dall'Autorità.

Anche l'incontro con il Commissario Hammarberg ha avuto come oggetto l'iniziativa del Governo italiano ed il ruolo svolto dal Garante.

L'Ufficio ha anche seguito con particolare attenzione le attività dei ministeri degli affari esteri e dell'interno sia per definire ed attuare le misure necessarie per l'emissione dei passaporti elettronici ed integrare nel *chip* le impronte digitali del titolare, come prescritto dai regolamenti comunitari, sia per la costruzione della parte nazionale del sistema Vis (sistema informativo visti) e la preparazione degli uffici consolari alle relative procedure.

Ha inoltre posto in essere le azioni necessarie per gli accertamenti preliminari sulla legittimità dei trattamenti svolti nella parte nazionale dei sistemi europei di informazione, partecipando alle decisioni adottate dalle Autorità di controllo Europol, Schengen, Eurodac ed alle azioni di *enforcement* avviate dal Gruppo art. 29.

Conferenze delle autorità su scala internazionale

La 30ma Conferenza internazionale delle autorità di protezione dati si è tenuta a Strasburgo dal 15 al 17 ottobre, organizzata congiuntamente dall'Autorità francese per la protezione dei dati (Cnil) e dall'Autorità federale tedesca (Bfd), per celebrare il trentennale dell'istituzione dei due organismi. La partecipazione è stata consistente, con oltre cinquecento iscritti provenienti da sessanta Paesi che si sono confrontati su tematiche legate da un unico filo conduttore: "*come tutelare la privacy in un mondo che non conosce più frontiere*".

Le prime due giornate, articolate in sei sessioni, hanno affrontato temi assai diversi quali l'equilibrio fra *privacy* e sicurezza, le opportunità di trasformare la tutela della *privacy* in un bene primario anche per le imprese, i rischi legati alle *social network*, le debolezze e i punti di forza dell'attuale quadro normativo regionale ed internazionale. La terza giornata è stata riservata, come è prassi, alla discussione fra le sole autorità di protezione dei dati e all'adozione di documenti e risoluzioni.

Fra queste ultime ricordiamo, in particolare, la Risoluzione sulla *privacy on-line* dei minori e la Risoluzione sull'urgenza di tutelare la *privacy* in un mondo senza frontiere. La prima sottolinea la necessità di educare e sensibilizzare alla protezione dei dati personali

ed invita *provider* e operatori in genere, ad applicare il principio di minimizzazione nel trattamento di dati relativi a minori. La seconda mira alla creazione di un gruppo di lavoro, comprendente anche l'Autorità italiana e coordinato dall'Autorità nazionale spagnola, per definire *standard* internazionali in materia di *privacy* sulla base dei princìpi già definiti in altri strumenti di varie regioni del mondo – in particolare la Convenzione 108/1981 del Consiglio d'Europa ed i princìpi Ocse ed Apec.

Ancora va menzionata la Risoluzione sulla costituzione di un Comitato che rappresenti la conferenza in occasione di incontri internazionali, che prevede la creazione di un Comitato ristretto (comprendente anche l'Autorità italiana) per far ottenere alla Conferenza lo *status* di *"osservatore"* presso vari organismi internazionali quali Ocse, Iso, Apec, Itu, Unesco.

Infine, la Risoluzione sulla tutela della *privacy* nei servizi di *social network*, all'interno della quale, anche alla luce del cosiddetto *"Memorandum di Roma"*, adottato dal Gruppo di Berlino durante l'incontro ospitato a Roma nel mese di marzo 2008 (*v. Relazione* 2007 *p.* 173), si invitano gli utenti a valutare con attenzione se e cosa pubblicare in rete, e si ricorda ai fornitori di tali servizi l'obbligo di informare adeguatamente gli utenti sulla natura dei trattamenti effettuati in rete e sui rischi possibili. Inoltre, la Risoluzione suggerisce l'applicazione di idonee misure (anche tecniche) per evitare che i dati personali siano estratti dai profili contenuti all'interno di siti di *social network* senza il consenso degli utenti (*ad es.*, attraverso gli algoritmi dei motori di ricerca esterni). La Risoluzione, infine, contiene ulteriori raccomandazioni che riguardano, in particolare, la necessità di consentire agli utenti di limitare la visibilità dell'intero profilo e di recedere facilmente dal servizio cancellando ogni informazione pubblicata sul *social network*; cautele ancora maggiori devono essere messe in atto qualora l'utente (come spesso avviene in questi casi) sia un minore.

20.1. LA COOPERAZIONE TRA AUTORITÀ GARANTI NELL'UE: IL GRUPPO ART. 29

Il Gruppo art. 29 (che riunisce i rappresentanti delle autorità europee in materia di protezione dei dati personali, ed è stato istituito ai sensi dell'art. 29 della Direttiva 95/46/Ce),

ha proseguito l'attuazione del programma biennale di attività adottato nel 2007 (*cfr.* *Relazione* 2007, *p.* 160).

In particolare, con riferimento al miglioramento dell'applicazione della Direttiva 95/46/Ce, sono stati previsti interventi volti a chiarire l'interpretazione di alcuni aspetti chiave, primi tra tutti la nozione di "*data controller*" e quella di "*data processor*". L'analisi, approfondita nell'ambito di uno specifico gruppo di lavoro, si è posta l'obiettivo di meglio definire la portata applicativa delle nozioni di *"titolare"* e di *"responsabile"* del trattamento, in particolare in vista dell'allocazione della relativa responsabilità, dell'individuazione dei rispettivi ruoli in caso di *outsourcing*, nonché delle ipotesi di contitolarità del trattamento.

In ordine alla protezione dei dati nell'ambito dei trasferimenti internazionali, particolare rilevanza è stata attribuita all'analisi di strumenti quali le *binding corporate rules* e l'accordo *Safe Harbor*. In questo contesto, si sono inserite le attività di approfondimento e di riflessione volte alla delineazione di linee-guida per le imprese e alla modifica della procedura di cooperazione in materia di *Bcr* (*v.* prosieguo), nonché le valutazioni relative all'implementazione dell'accordo *Safe Harbor*, intensificatesi in occasione del *Workshop on international transfers of personal data* (Bruxelles, 21.10.08). Parimenti, è stato confermato l'impegno del Gruppo ad esprimersi, come richiesto dalla Commissione, in merito alla valutazione di adeguatezza di Israele, Andorra, Nuova Zelanda ed Ecuador.

In materia di nuove tecnologie, diversi sono gli obiettivi rilanciati dai Garanti europei; in particolare, si ricorda l'impegno a completare il lavoro già intrapreso con riferimento ai motori di ricerca e ai *social network*; quello di giungere a una seconda opinione sulla direttiva *e-privacy*; quello di proseguire le riflessioni in materia di *Rfid* e di profilazione.

Tra gli impegni assunti, si collocano anche alcuni di carattere interno, relativi al miglioramento dell'efficacia dell'attività con azioni volte, in particolare, all'instaurazione di buone pratiche di lavoro, al perfezionamento della comunicazione tra le autorità, all'implementazione del regolamento sulle procedure interne di funzionamento dei sottogruppi (*cfr.* WP 157).

Infine, tra le priorità del programma di lavoro, sono state inserite le tematiche relative

a dati sanitari e trattamenti per finalità epidemiologiche, "*pre-trial discovery*", protezione dei dati e minori, "*credit histories*".

Per migliorare ed affinare le verifiche interne della corretta applicazione dei princìpi di protezione dei dati, è stato inserito nel programma di attività l'avvio di una nuova azione comune di verifica nel settore della conservazione dei dati di traffico telefonico e telematico, scelto in connessione con l'entrata in vigore della *cd. "direttiva Frattini"* 2006/24/Ce.

Diversi sono stati i documenti adottati dal Gruppo art. 29: di seguito si segnalano i principali.

Parere 3/2008 sugli *standard* Wada in materia di *anti-doping*

Il Gruppo art. 29 ha espresso un parere sul progetto di s*tandard* internazionale elaborato dall'Agenzia mondiale *anti-doping* (*World Anti-Doping Agency*-Wada), volto a fissare le regole in materia di protezione dei dati trattati da organizzazioni e soggetti che operano nel settore dell'*anti-doping* sportivo (*cfr.* WP 156).

Il Gruppo ha accolto con favore l'iniziativa della Wada anche alla luce dell'estensione geografica (globale) della sua applicazione. Tuttavia, non ha sostenuto interamente le previsioni degli *Standard*, considerata la presenza al loro interno di non poche lacune rispetto al livello minimo di tutela richiesto dalla normativa europea in materia di protezione dei dati.

Particolari raccomandazioni sono state suggerite con riguardo alle definizioni, ai princìpi di necessità e di proporzionalità, al trattamento dei dati sensibili, al consenso dell'interessato, all'informativa, alle attività di comunicazione e di conservazione dei dati e all'esercizio dei diritti da parte degli interessati.

Inoltre, particolare attenzione è stata dedicata all'implementazione della banca dati Adams, con sede in Canada, nella quale dovrebbero confluire ed essere conservati i dati che gli atleti sono tenuti a comunicare alle diverse organizzazioni *anti-doping*.

Sempre nell'ambito del progetto di s*tandard* internazionale per la protezione dei dati personali, il Gruppo art. 29 ha istituito un sottogruppo, per approfondire gli aspetti maggiormente problematici ed elaborare un secondo parere in materia.

Tra tali questioni si sono in particolare segnalate: il funzionamento del *database* Adams; l'individuazione della base giuridica del trattamento; le modalità del trattamento di dati

sensibili e le tipologie dei dati trattati; la pubblicazione in Internet delle decisioni in materia di *anti-doping*; il trasferimento dei dati; la tipologia delle informazioni richieste agli atleti da inserire nel *cd. "modulo whereabouts"* volto a consentire la reperibilità degli atleti ai fini di controlli *anti-doping*; l'individuazione del titolare del trattamento; l'informativa da prestare agli interessati (*v. par.* 20.3)

Parere sulla ricerca di *"pre-trial discovery"*

Il Gruppo dei Garanti europei ha adottato un documento di lavoro (*cfr.* WP 158) volto a delineare le linee-guida in materia di trattamento di dati personali nell'ambito delle richieste di informazioni, provenienti per lo più dagli Stati uniti, relative alle attività di *"pre-trial discovery"* (ovvero le attività di ricerca della prova connesse all'instaurazione di un procedimento giudiziario).

Tale intervento è stato reso necessario dal crescente aumento delle attività di trasferimento transfrontaliero di dati personali collegato all'attuazione di ordini di trasmissione o di esibizione dei documenti emanati da giudici statunitensi.

La questione ha coinvolto in particolare società, spesso sussidiarie o controllate di gruppi multinazionali aventi sede legale negli Stati uniti, cui è stato richiesto, dalla capogruppo, di fornire informazioni (comprensive anche di dati personali relativi a dipendenti, clienti o fornitori) considerate rilevanti nell'ambito delle investigazioni difensive o delle attività pre-contenziose di ricerca della prova connesse all'instaurazione di un procedimento giudiziario. Il recente aumento di richieste di tal tipo, che, tra l'altro, comportano un trasferimento di dati personali, anche sensibili, verso paesi che non offrono adeguate garanzie di protezione, ha evidenziato la presenza di non poche problematiche in considerazione dell'applicazione della disciplina prevista dalla 95/46/Ce.

I Garanti europei hanno, dunque, rappresentato l'esigenza di contemperare le esigenze difensive, come disciplinate dalla normativa statunitense in materia di *"pre-trial discovery"*, con i princìpi europei di protezione dei dati personali sanciti dalla Direttiva 95/46/Ce.

Sono state così emanate alcune linee-guida, indirizzate ai titolari del trattamento stabiliti in uno Stato membro, volte a ribadire che alle richieste di informazioni connesse ad esigenze difensive nell'ambito di procedimenti civili si applicano le norme in materia di protezione dei dati personali (il documento non si riferisce al processo penale).

Il testo (*cfr.* WP 158) dedica particolare attenzione alle finalità del trattamento, individuate con riferimento all'utilizzo delle informazioni così raccolte (conservazione, comunicazione, successivi trasferimenti o usi ulteriori), soprattutto in vista dell'applicazione dei princìpi di proporzionalità e di stretta finalità del trattamento, nonché delle previsioni della direttiva in materia di conservazione dei dati.

Speciale rilevanza è, inoltre, riservata alla determinazione della base giuridica del trattamento, la quale può essere alternativamente individuata, a seguito di un'analisi effettuata caso per caso, nel consenso dell'interessato (purché sia possibile dimostrarne la manifestazione libera e informata), nell'adempimento di un obbligo di legge (nei soli casi in cui all'interno dello Stato membro, in cui i dati sono raccolti, viga un obbligo normativo di conformarsi ad un ordine giudiziario proveniente da un giudice straniero), nel perseguimento di un legittimo interesse del titolare o di un terzo a condizione che non siano pregiudicati i diritti e le libertà fondamentali dell'interessato (operando una valutazione che tenga conto della effettiva rilevanza dell'informazione personale rispetto alle esigenze di difesa in giudizio).

Inoltre, il documento ribadisce i princìpi in materia di modalità del trattamento (art. 6 della Direttiva 95/46/Ce), di rilascio di una preventiva informativa agli interessati, in particolare tenendo conto della circostanza che i dati, nella maggior parte delle ipotesi, non sono raccolti presso l'interessato (artt. 10-11 della Direttiva 95/46/Ce), di esercizio dei diritti (artt. 12-15 della direttiva) e di adozione di adeguate misure di sicurezza (art. 17).

Infine, un'attenta riflessione è stata condotta con riferimento all'applicazione degli artt. 25-26 della direttiva in materia di trasferimenti transfrontalieri di dati personali. In tale contesto, il Gruppo dei Garanti europei ha incoraggiato l'adesione all'accordo *Safe Harbor*, nonché l'adozione di *standard contractual clauses* o di *binding corporate rules*, precisando però la necessità che il trasferimento di tali dati per finalità di difesa in giudizio sia espressamente ricompreso tra quelli coperti dagli strumenti sopracitati. La deroga di cui all'art. 26 (1), lett. *d*), della direttiva ("tr*asferimento per finalità di esercizio di un diritto in giudizio*") non può, infatti, costituire una base giuridica sufficiente a legitti-

mare trasferimenti *"in massa"* di dati personali verso paesi che potrebbero non assicurare una tutela adeguata.

Le *Binding corporate rules*

Particolarmente intensa è stata l'attività del Gruppo dei Garanti europei in materia di *"Binding corporate rules (Bcr)"*.

Tale strumento, che trae la propria efficacia giuridica dal rilascio di specifiche autorizzazioni nazionali al trasferimento dei dati personali verso Paesi terzi, ha richiesto un'attenta riflessione volta a chiarirne la natura giuridica e a meglio definirne le modalità di applicazione.

Il lavoro del Gruppo art. 29 è stato, in particolare, dedicato all'analisi dello strumento delle *Bcr* e alla sua effettiva diffusione nell'ambito dei grandi gruppi multinazionali d'impresa. In questo contesto è stata valutata l'opportunità di rilanciarne l'efficacia, semplificare gli oneri connessi al loro utilizzo e rendere una maggiore trasparenza con riferimento alle relative procedure di adozione.

Sono state così predisposte alcune linee-guida esemplificative per le società, comprensive di una *check list* contenente tutti gli elementi necessari alla redazione delle *Bcr* da parte degli organismi coinvolti (*cfr.* WP 153); la redazione di specifiche Faq volte a chiarire caratteristiche e contenuto delle *Bcr* medesime (*cfr.* WP 155); l'individuazione di un *"modello"* esemplificativo di *Bcr*, in grado di costituire una guida utile per le società interessate (*cfr.* WP 154).

Parimenti, è stato intrapreso un lavoro di approfondimento e di semplificazione della procedura amministrativa di rilascio delle autorizzazioni nazionali al trasferimento dei dati personali tramite *Bcr*, soprattutto con riferimento alla fase di *"cooperazione"* tra le Autorità in materia di protezione dei dati prevista dai documenti del Gruppo art. 29 (*cfr.* WP 107 e WP 133). L'applicazione concreta ha, infatti, reso evidente l'opportunità di prevedere meccanismi di cooperazione più rapidi e trasparenti, in grado di velocizzare anche i tempi di definizione delle procedure di autorizzazione. È stata, in questo senso, intrapresa un'attività di revisione del WP 107, volta a migliorarne l'efficacia.

In tale linea alcune Autorità, tra cui il Garante, hanno aderito ad un accordo volto alla predisposizione di una procedura di *"stretta cooperazione"* in materia di procedura di rila-

scio delle autorizzazioni ai trasferimenti di dati personali tramite *Bcr*, con l'obiettivo di semplificare gli adempimenti posti a carico delle società e di definire in tempi più rapidi le attività di analisi dei testi di *Bcr* sottoposti a valutazione.

Privacy e minori

Il Gruppo ha approvato il documento di lavoro n. 1/2008 sulla tutela dei dati relativi ai minori (WP 147).

Il documento è stato sottoposto a consultazione pubblica, e ha costituito la base del successivo parere 2/2009 (WP 160) adottato l'11 febbraio 2009.

Come nel documento di lavoro, il parere è suddiviso in due parti: la prima volta ad individuare i princìpi fondamentali in materia di protezione del minore con specifico riferimento alla tutela dei dati, e la seconda relativa all'attuazione dei princìpi di protezione dati nell'ambito scolastico, luogo assai significativo per lo sviluppo del minore e in cui si svolgono molte delle sue attività quotidiane.

Particolare attenzione è prestata al principio dell'interesse primario del minore (*cd.* "*best interest of the child*"), elemento fondamentale per la risoluzione dei conflitti che possono insorgere anche tra i minori e i loro rappresentanti. Ampio spazio è inoltre dedicato al principio di rappresentanza (da parte dei genitori o di chi abbia titolo) nonché alla necessità che nelle decisioni concernenti il minorenne si tenga conto del suo livello di maturità, coinvolgendolo progressivamente nelle scelte che lo riguardano.

Con specifico riferimento alla protezione dei dati, il parere ricorda che i princìpi di protezione dati e, in particolare, di qualità dei dati, di correttezza e di proporzionalità del trattamento devono essere rispettati soprattutto laddove il trattamento riguardi i minori. A tal proposito viene anche menzionato il diritto all'oblìo, particolarmente significativo considerato che le informazioni che riguardano il minorenne sono suscettibili di divenire presto obsolete ed eccedenti rispetto all'originario scopo della raccolta.

Con riferimento all'informativa, il parere si sofferma sulla necessità di utilizzare criteri di sinteticità e di semplicità in grado di accrescere, con un linguaggio adeguato, la consapevolezza del minore sul trattamento dei dati che lo riguardano.

La seconda parte del parere riguarda principalmente l'applicazione delle regole in materia di protezione dei dati nelle scuole. In particolare, sono enunciati i princìpi ai quali si

devono ispirare i trattamenti dei dati che confluiscono nei *dossier* scolastici suscettibili di causare discriminazione tra gli studenti. Il parere si sofferma inoltre sulla comunicazione a soggetti terzi da parte delle scuole dei dati relativi agli alunni per finalità di *marketing*, nonché sulla disciplina dei risultati scolastici, caratterizzata da una certa difformità tra gli Stati membri che optano per il principio di trasparenza dei risultati e quelli che ne privilegiano invece la confidenzialità.

Grande attenzione è prestata all'impiego delle nuove tecnologie nella vita scolastica. L'impiego di dispositivi biometrici per l'accesso alle scuole, di videosorveglianza, e di *badge* muniti di *Rfid* devono ispirarsi al rigoroso rispetto del princìpi di necessità e di proporzionalità, anche tenendo conto che forme di controllo eccessive possono incidere sullo sviluppo del minore stesso.

Vengono dettati princìpi sull'uso di siti *web* scolastici, sulla pubblicazione di foto di minori anche su Internet, e apposite precauzioni per l'uso di videofonini.

Il parere richiama l'attenzione dei diversi soggetti coinvolti (insegnanti, scuole, autorità competenti, *ecc.*) sulla necessità di garantire un'adeguata protezione dei dati relativi ai minori e di avviare un processo di sensibilizzazione dei minori stessi riguardo ai rischi derivanti dal trattamento dei dati che li riguardano e all'esercizio dei loro diritti.

Protezione dei dati e attività dei motori di ricerca

Del parere del 4 aprile 2008 (WP 148), sulla protezione dei dati in relazione alle attività dei motori di ricerca si è riferito nella *Relazione* 2007 (*p.* 164).

Dopo la pubblicazione del parere tutti i principali gestori dei motori di ricerca hanno contattato il Gruppo per manifestare la propria disponibilità a valutare con attenzione le indicazioni fornite dalle autorità europee. *Google*, inoltre, ha iniziato un dialogo molto serrato con il *Data Protection Commissioner* irlandese, avendo stabilito in Irlanda il proprio *data center*. Attraverso tale dialogo, *Google* ha inteso affrontare in modo dettagliato molte delle questioni sulle quali il Gruppo aveva sollecitato una presa di posizione da parte dei motori di ricerca. Le risposte di *Google* si sono concretizzate in una *"lettera aperta"* in cui l'azienda informava di aver ridotto il periodo di conservazione dei *file* di *log* degli utenti da diciotto a nove mesi, per venire incontro alle sollecitazioni del Gruppo art. 29 (che comunque aveva indicato un periodo non superiore ai sei mesi). *Google*

affrontava tutti i punti sollevati nel parere del Gruppo art. 29 sui *"motori di ricerca"*, con particolare riguardo alla natura di dato personale dell'indirizzo Ip (contestata da *Google*, che comunque non escludeva la necessità di un'analisi specifica, caso per caso, al fine di valutare l'effettiva rintracciabilità dell'interessato attraverso l'indirizzo Ip); all'applicazione delle disposizioni della Direttiva 2002/58/Ce rispetto ai *cookie* utilizzati per tenere traccia degli utenti ed alla titolarità del trattamento (*Google Inc.* non riteneva che i trattamenti effettuati dalle controllate europee, principalmente per finalità di natura commerciale, consentissero di estendere le norme della direttiva Ue ai trattamenti effettuati attraverso il motore di ricerca, pur riconoscendo che vi è un margine di apprezzamento in materia); alla liceità delle operazioni di trattamento effettuate da *Google*. Il Gruppo art. 29 ha quindi deciso di tenere un'audizione pubblica per sollecitare chiarimenti su queste ed altre problematiche (*ad es.*, le modalità di anonimizzazione delle stringhe di ricerca), invitando i principali gestori di motori di ricerca (*Google*, *Yahoo!* e *Microsoft*) ed un meta-motore di ricerca (*Ixquick*); l'audizione si è tenuta durante la riunione plenaria del febbraio 2009.

Il Gruppo si è successivamente dato alcune settimane di tempo per riflettere sulle risposte fornite e valutare l'opportunità di altre iniziative congiunte. Va rilevato che nel frattempo anche *Microsoft* e *Yahoo!* hanno segnalato la propria disponibilità a ridurre i tempi di conservazione dei *file* di *log* degli utenti, pari a diciotto mesi per quanto riguarda *Microsoft* (che si è dichiarata disposta a scendere a sei mesi) e a novanta giorni per quanto concerne *Yahoo!* (anche se i *log*, di fatto, vengono conservati in forma non anonima per sei mesi per finalità di lotta contro frodi ed altre forme di criminalità).

Privacy e comunicazioni elettroniche

Come accennato nella *Relazione* 2007 (*v. p.* 165), il Gruppo art. 29 si è occupato delle proposte di revisione della Direttiva 2002/58/Ce, presentate dalla Commissione il 13 novembre 2007, in materia di *privacy* e comunicazione elettroniche. Va sottolineato che il pacchetto di proposte della Commissione comprendeva anche una *"proposta di Regolamento"* concernente l'istituzione di un'Autorità europea di regolazione del mercato delle comunicazioni, fra i cui compiti rientrerebbe la definizione di *standard* di sicurezza paneuropei (con ciò accogliendo in parte la proposta formulata dal Gruppo art. 29 nel suo

contributo alla consultazione pubblica del 2006). Tale proposta è stata, però, successivamente bocciata dal Consiglio e dal Parlamento europeo.

Il Gruppo ha pubblicato quindi un parere (WP 150 del 15 maggio 2008) indirizzato in via primaria alla Commissione europea, ma rivolto anche al Parlamento ed al Consiglio. In sintesi, il parere sottolinea la necessità di garantire più efficacemente la sicurezza delle reti e facilitare l'esercizio dei diritti degli utenti. In particolare, esso condivide alcune delle osservazioni contenute nel documento pubblicato sullo stesso tema dal Garante europeo per la protezione dei dati (10 aprile 2008); i Garanti concordano sull'opportunità di guardare alle reti in una prospettiva più ampia, data la natura sempre più spesso "mista" (pubblica/privata) delle reti di comunicazione elettronica, nonché sulla valutazione positiva di alcuni emendamenti proposti dalla Commissione – soprattutto il chiarimento relativo all'applicabilità delle disposizioni della direttiva a tecnologie quali l'*Rfid*, in quanto utilizzino "reti di comunicazione elettronica disponibili al pubblico" per veicolare i segnali di trasmissione, e l'attribuzione del diritto di intraprendere azioni legali in caso di violazioni della normativa nazionale (*ad es.*, in materia di *spam*) anche a soggetti non direttamente colpiti, ma comunque direttamente interessati, quali i fornitori di servizi Internet.

Il Gruppo art. 29 ha proposto, tuttavia, ulteriori emendamenti che riguardano, in modo particolare, l'estensione dell'obbligo per i fornitori di servizi di comunicazione di notificare violazioni e/o rischi per la sicurezza delle reti a tutti gli *"utenti"* dei servizi di comunicazione elettronica (anziché ai soli *"abbonati"* a tali servizi); ciò dovrà avvenire secondo un approccio equilibrato che tenga conto dei costi e dell'impatto che tali notifiche possono esplicare sull'attività dei fornitori (*ad es.*, in termini di danno di immagine). Inoltre, il Gruppo ha segnalato l'opportunità di ampliare la definizione di *"sistemi di chiamata"* contenuta nella Direttiva 2002/58/Ce (art. 13) includendovi i sistemi di *"comunicazione"* (per tenere conto degli sviluppi tecnologici legati, ad esempio, alla tecnologia *Bluetooth*, il cui funzionamento è difficilmente assimilabile ad una *"chiamata"* sul terminale dell'utente); ciò consentirebbe di garantire una protezione più efficace nei confronti delle comunicazioni indesiderate. Per lo stesso motivo, l'estensione del *"diritto di intra-*

prendere azioni legali" dovrebbe comprendere le violazioni dell'articolo 5.3 della direttiva, ossia l'uso e l'installazione, per esempio, di *spyware*. Il parere ricorda, inoltre, l'esigenza di garantire l'applicazione del principio di necessità (o minimizzazione) nell'utilizzo e nella gestione dei servizi di comunicazione elettronica, attraverso la realizzazione dell'approccio definito *"privacy by design"*, nonché l'obbligo per i *provider* di assicurare, più in generale, la riservatezza delle comunicazioni a prescindere dalla configurazione fisica delle reti utilizzate per la trasmissione di tali comunicazioni – quindi tenendo conto di eventuali accordi tecnologici stipulati con soggetti o imprese di Paesi terzi rispetto ai flussi di dati in partenza dall'Ue.

L'iter comunitario è successivamente proseguito con l'adozione da parte del Parlamento europeo, il 24 settembre 2008, delle proposte di modifica del pacchetto comunicazioni elettroniche. Riguardo alla Direttiva 2002/58/Ce, il Parlamento ha seguito solo parte delle indicazioni contenute nel parere del Gruppo articolo 29; peraltro, alcune delle proposte presentate dai gruppi parlamentari introducevano obblighi ulteriormente stringenti (*ad es.*, relativamente alla segnalazione di rischi o violazioni reali della sicurezza in rete da parte dei *provider* di servizi di comunicazione elettronica). Come accennato, il Parlamento ha respinto la proposta di costituire un'autorità unica europea incaricata di vigilare e legiferare sulla sicurezza delle reti di comunicazione elettronica. Le modifiche del Parlamento, inoltre, proponevano di estendere il campo di applicazione della direttiva ai *"servizi della società dell'informazione"*, e non ai soli servizi di comunicazione elettronica accessibili al pubblico, e consentivano agli *Isp* di utilizzare i dati di traffico anche per finalità connesse alla *"sicurezza"* delle reti e delle comunicazioni.

Conformemente alla procedura di codecisione, si è quindi avuta, il 28 novembre 2008, l'adozione della proposta modificata del Consiglio Ue relativa al pacchetto normativo in oggetto. Il Consiglio ha recepito solo una parte degli emendamenti del Parlamento ed ha tenuto conto in misura ridotta delle osservazioni contenute in un documento di compromesso presentato dalla Commissione il 7 novembre 2008. In base al testo del Consiglio, le principali modifiche al testo attuale della Direttiva 2002/58/Ce riguarderebbero gli obblighi di notifica delle violazioni della sicurezza che coinvolgano dati personali (limi-

tate alle violazioni *"gravi"*, non meglio definite, secondo un meccanismo in tre tempi che prevede anche la notifica alle autorità di protezione dati, e solo con riguardo agli *"abbonati"* interessati); l'estensione della possibilità di trattare dati di traffico per non meglio precisati *"scopi di sicurezza"* (secondo quanto indicato nel nuovo comma 6a dell'articolo 6); l'estensione della possibilità di ottenere tutela (giuridica o di altra natura) contro violazioni degli obblighi concernenti le comunicazioni indesiderate (*spam*: articolo 13) a tutte le persone fisiche e giuridiche, compresi quindi gli stessi fornitori dei servizi di comunicazione elettronica, e con riguardo agli *"utenti"* di tali servizi (non soltanto, dunque, agli *"abbonati"* come attualmente previsto). Il Consiglio ha specificato l'ambito delle comunicazioni indesiderate (indicando che *"electronic mail"* comprende anche *Sms* e *Mms*). La Commissione europea, attraverso il Commissario Reding, si è espressa negativamente su tale proposta di compromesso, ritenuta troppo timida; il Garante europeo ha successivamente reso pubblico un secondo parere sulle proposte di modifica (9 gennaio 2009) contenente numerose e dettagliate osservazioni, in buona parte critiche.

Anche il Gruppo art. 29 ha adottato un nuovo parere, il 10 febbraio 2009, relativo al testo licenziato dal Consiglio e, in parte minore, agli emendamenti proposti dal Parlamento europeo.

I Garanti plaudono all'estensione (proposta dal Parlamento europeo) dell'ambito di applicazione della direttiva ai *"servizi della società dell'informazione"*; inoltre, chiedono di chiarire sia le modalità di notificazione delle violazioni della sicurezza dei sistemi telematici, sia i soggetti coinvolti (suggerendo di indirizzare la notifica anche agli utenti solo in caso di violazioni che comportino *"conseguenze avverse"* per la protezione dei loro dati personali), sia il concetto di *"grave"* violazione della sicurezza informatica. Peraltro, il parere giudica superflua e potenzialmente lesiva della *privacy* individuale l'introduzione, da parte del Consiglio, del comma 6a nell'art. 6 della direttiva; tale comma prevederebbe la possibilità di trattare dati di traffico *"per scopi di sicurezza delle reti e delle informazioni"* non meglio precisati. Vengono ritenuti inopportuni anche alcuni emendamenti proposti dal Parlamento europeo (e non accettati dal Consiglio) quali, in particolare, la previsione di ritenere la configurazione di *default* dei programmi di navigazione (*browser*) come

manifestazione del consenso espresso dell'interessato rispetto alla ricezione di, ad esempio, *cookies* o altri programmi; quanto all'obbligo di segnalare alle autorità di protezione dati le richieste di accesso ai dati di traffico telematico da parte delle autorità giudiziarie e di polizia, che il Parlamento proponeva di introdurre su base automatica nei confronti dei *provider*, il Gruppo ha ritenuto preferibile chiedere la predisposizione di un rapporto annuale, redatto sulla base di criteri comuni e uniformi, così da consentire alle singole autorità di valutare la necessità di accertamenti ulteriori. Fra gli aspetti del testo del Consiglio sui quali il Gruppo esprime il proprio apprezzamento, occorre ricordare la possibilità per le persone giuridiche di far valere i propri diritti in caso di comunicazioni indesiderate ed i chiarimenti, contenuti nei *"considerando"* aggiunti al testo della direttiva, relativi alla natura di *Sms*, *Mms* ed altre modalità di comunicazione elettronica.

Enforcement

Il Gruppo ha conferito mandato al sottogruppo *Enforcement* di impostare l'attività di verifica relativa all'applicazione della direttiva sulla conservazione dei dati a fini di lotta alla criminalità (Direttiva 2006/24/Ce sulla *data retention*). Sono stati designati come *rapporteurs* l'autorità italiana e quella cipriota. Superate le iniziali difficoltà sull'impostazione dell'azione di *enforcement* (la direttiva non è stata attuata ancora in molti paesi), il sottogruppo ha acquisito, attraverso le autorità di protezione dei dati, informazioni di base sull'organizzazione del settore, sul tipo di società – nazionali o transnazionali – che erogano i servizi, sui poteri delle autorità stesse di supervisione e controllo dei trattamenti di dati. Successivamente ha definito i criteri per la selezione delle società fornitrici di reti e di servizi di comunicazioni elettroniche cui rivolgersi. Il campione selezionato sarà chiamato a fornire adeguata risposta alle domande formulate in un apposito questionario comune. Nel caso specifico il Gruppo ha scelto un campione rappresentativo limitato nel numero e formulato questioni molto precise soprattutto sulla sicurezza dei dati e dei sistemi. La prima fase a livello nazionale sarà basata sulla somministrazione di un questionario, conciso e preciso, e sarà seguita da una seconda fase di controllo *in loco* delle risposte fornite, ove ritenuto necessario dall'autorità di protezione dei dati. L'azione si svolgerà nel corso del 2009 e dovrebbe concludersi, con il rapporto finale e le considerazioni del Gruppo art. 29, nei primi mesi del 2010.

Diverse le attività svolte in connessione alle vicende *Pnr*.

Pnr Usa: il Gruppo art. 29 ha approvato il nuovo testo dell'informativa breve, lunga ed extrabreve per le compagnie aeree e le agenzie di viaggio, anche ai fini delle prenotazioni effettuate telefonicamente, in rapporto al nuovo accordo *Pnr* del luglio 2007.

La visita negli Usa per la revisione congiunta dell'applicazione degli accordi non si è effettuata, perché la nuova amministrazione americana ha chiesto tempo per prepararsi. Peraltro non è chiaro quale presenza e ruolo assumeranno nella delegazione europea le autorità di protezione dei dati personali.

Pnr europeo: continuano i lavori di *follow up* del parere congiunto adottato nel dicembre 2007 dal Gruppo art. 29 e dal *Working Party on Police and Justice* (*Wppj*) sulla proposta di *"proposta di decisione-quadro"* che istituisce un sistema europeo di raccolta ed analisi delle informazioni che obbliga i vettori aerei a mettere a disposizione delle autorità competenti per la prevenzione e repressione dei reati in anticipo rispetto all'effettuazione dell'imbarco i dati dei passeggeri raccolti fin dal momento della prenotazione del volo. Da segnalare il parere legale dell'ufficio giuridico del Consiglio, che ha indicato l'opportunità di modificare la base giuridica scelta per la redazione della proposta di decisione-quadro sul *Pnr* europeo e di garantire un migliore rispetto dei diritti di protezione dati; in questo caso, il servizio giuridico suggerisce una modifica della Direttiva 95/46/Ce che estenda il suo ambito di applicazione ai trattamenti di terzo pilastro. I lavori di analisi e discussione della proposta sono in corso presso il Consiglio, che intenderebbe mantenere la base giuridica scelta. Il Gruppo ha deciso la preparazione di un secondo parere, sempre congiuntamente al *Wppj*.

Follow-up Pnr Canada: la revisione congiunta dell'applicazione degli accordi si è svolta nell'autunno del 2008 con la collaborazione delle autorità canadesi.

La delegazione era formata anche da rappresentanti delle autorità di protezione dei dati personali. Nell'occasione, anche su sollecitazione scritta rivolta dal Gruppo alla Commissione per chiedere chiarimenti e sottolineare che le attività di *matching*, controlli, *ecc.* previste dal *Memorandum* non sembrano essere conformi all'accordo *Pnr* raggiunto fra Ue e Canada, è stato sollevato anche il problema del *Memorandum of understanding* Canada (*Passenger Protect Program*) / Compagnie aeree europee.

Il Gruppo ha anche adottato un documento che fissa alcuni *standard* generali rispetto al trasferimento di dati relativi a passeggeri (*Pnr*) (WP 151). Il documento si era reso necessario considerate le crescenti richieste di tali dati formulate da diversi Paesi (quali India, Corea, Australia) e le conseguenti pressioni sulle compagnie aeree. Il documento potrebbe servire non solo per i negoziatori comunitari (Consiglio e Commissione) con i Paesi summenzionati, ma anche per influenzare l'Icao a migliorare i global *standard* già elaborati.

Il Gruppo ha anche espresso dubbi e perplessità in una lettera alla Commissione relativamente alle richieste americane di un nuovo sistema di controllo degli ingressi (Esta: *Electronic System for Travel Authorization*).

Il sistema prevede che chi intende recarsi negli Usa invii in anticipo un formulario elettronico contenente gli stessi elementi oggi richiesti in formato cartaceo. Il passaggio da un sistema cartaceo ad uno elettronico, anche per gli effetti sulla legge applicabile, presenta alcune criticità, evidenziate alla Commissione per consentirle le opportune iniziative prima che la proposta entri in vigore.

Anche per quanto riguarda l'introduzione in Europa di un analogo sistema, che sembra potersi evincere dal sopra ricordato pacchetto di iniziative per il rafforzamento dei controlli alle frontiere esterne, il Gruppo ha inviato una lettera al Commissario Barrot per richiamare l'attenzione della Commissione sulla necessità di valutare l'effettiva applicazione di disposizioni comunitarie già in essere prima di procedere all'introduzione di ulteriori obblighi in materia di raccolta e trattamento dei dati relativi a passeggeri.

20.2. LA COOPERAZIONE DELLE AUTORITÀ DI PROTEZIONE DEI DATI NEL SETTORE LIBERTÀ, GIUSTIZIA E AFFARI INTERNI

Da segnalare in particolare due elementi: da un lato l'intensificarsi e lo strutturarsi dei lavori del Gruppo di lavoro Polizia e giustizia (*Wppj*) sotto la guida del presidente del Garante; dall'altro, il crescente coordinamento con il Gruppo art. 29, volto a favorire una valutazione possibilmente completa degli aspetti di protezione dei dati personali delle iniziative che non si esauriscono nell'ambito di uno dei pilastri in cui si articolano le competenze dell'Unione: un caso classico riguarda l'uso dei dati dei passeggeri aerei, raccolti

per la prestazione del servizio di trasporto, ma oggetto di crescenti pressioni ed interventi normativi per rendere i relativi *database* di immediato e pieno accesso per le forze di polizia e giudiziarie a fini di *"valutazione del rischio"* e profilazione. Analogamente per i tabulati relativi alle utenze e al traffico telefonico e telematico.

Come si è già rilevato, per il modo di elaborazione e per la frammentarietà delle competenze in materia in seno all'Unione, molte nuove iniziative dell'Unione europea che riguardano dati personali sono tuttora sottratte al controllo delle autorità di protezione dei dati, alcune perché riguardano materie di terzo pilastro, altre perché non rientrano in modo netto in uno dei tradizionali pilastri dell'Ue.

Il Gruppo art. 29 ed il Gruppo di lavoro polizia e giustizia, oltre a rivolgersi al Parlamento europeo che svolge peraltro un ruolo ancora limitato nelle materie non facenti parti del *cd. "primo pilastro"* hanno, come ricordato sopra, cooperato ad iniziative congiunte.

Le autorità di protezione dei dati hanno segnalato con preoccupazione sempre maggiore il progressivo venir meno di *"momenti istituzionalizzati"* presso il Consiglio ed anche, in parte, presso la Commissione, che favorissero la necessaria valutazione dell'impatto delle nuove iniziative sui diritti fondamentali della persona e, più specificamente, sulla tutela dei dati personali; il ritardo dell'entrata in vigore del nuovo trattato non ha certamente giovato.

Tra le iniziative legislative in ambito europeo va finalmente registrata la decisione quadro sui princìpi per il trattamento dei dati personali nel terzo pilastro, elemento richiamato dal *"Programma de L'Aja"* come necessario di riferimento per le attività di cooperazione tra forze di polizia e magistratura, al fine di prevenire e reprimere reati (GU L350 del 30 dicembre 2008).

Il testo della decisione quadro tuttavia, come ricordato, è stato modificato *in pejus* durante la discussione in Consiglio, rispetto all'originaria proposta della Commissione, e non contiene più alcuna previsione circa la creazione di un organismo parallelo a quello del Gruppo art. 29 con ruolo indipendente e consultivo. Altri aspetti su cui le autorità di protezione dati hanno rilevato la debolezza dell'impianto normativo e delle tutele previ-

ste, riguardano: il campo di applicazione, limitato a disciplinare i soli scambi di dati tra i Paesi Ue e non direttamente applicabili ai trattamenti di dati nazionali, i meccanismi che consentono l'ulteriore trasferimento dei dati a Paesi ed organismi terzi, i diritti di accesso ed informazione delle persone interessate e le modalità del trattamento dei dati sensibili. Si tratta di aspetti di grande rilievo, suscettibili di incidere negativamente sul raggiungimento di quell'elevato livello di tutela che la decisione quadro dichiara di voler garantire agli interessati, ribaditi nel comunicato stampa del Gruppo polizia e giustizia, soprattutto allo scopo di ricordare che i princìpi devono essere coerenti in tutti gli Stati.

Va menzionato poi che nel terzo pilastro, a parte l'attività del Gruppo polizia e giustizia, è continuata l'attività in particolare delle Autorità comuni di controllo Schengen, Europol e Dogane, organismi di supervisione e controllo istituiti da specifiche convenzioni.

È continuata anche l'attività di supervisione a livello europeo sul funzionamento del sistema Eurodac, coordinata dal Garante europeo.

Questo modello di supervisione sarà applicato, una volta entrati in funzione, anche per il Vis (sistema informativo visti) – la cui entrata in funzione è prevista per la fine del 2009 – nonché per il SIS II che sarà invece operativo verso la seconda metà del 2010, essendo emersi problemi di notevole complessità.

Sulle modalità attuative del Vis sembra essere stato raggiunto l'accordo interistituzionale per assoggettare all'obbligo di fornire le impronte digitali i bambini a partire dai dodici anni, sia per la richiesta di visti, sia per altri tipi di documenti, attraverso la definizione di "modelli *standard*" europei e per disciplinare le procedure presso gli uffici consolari e gli altri uffici abilitati al rilascio dei visti di breve soggiorno (*cd. "visti Schengen"*).

L'Italia ha presentato, ed è tuttora in discussione presso il Parlamento, il disegno di legge di ratifica del *cd. "Trattato di Prüm"* (d.l. n. 586) che prevede tra l'altro l'istituzione della banca dati Dna. Nel frattempo, su forte pressione della presidenza di turno del Consiglio sono stati adottati e pubblicati i testi delle due decisioni del Consiglio che trasformano in iniziativa legislativa dell'Unione gran parte delle disposizione del Trattato di Prüm e delle disposizioni applicative (Decisione 2008/615/GAI del 23 giugno 2008 in GU L210 - Decisione 2008/616/GAI del 23 giugno 2008 in GU L210).

Le relative disposizioni entreranno in vigore nel luglio 2009.

Su tali temi il Garante ha elaborato spunti e proposte per garantire il necessario rispetto dei princìpi di protezione dei dati personali nell'elaborazione e nell'attuazione delle disposizioni suindicate.

Europol: l'attività dell'Autorità di controllo comune e i casi di contenzioso

Nel periodo considerato l'Acc ha continuato la sua attività sulla proposta di decisione per l'integrazione di Europol tra le strutture dell'Unione e sulla definizione del quadro generale di riferimento per lo svolgimento della sua attività e le norme attuative della proposta medesima.

Il testo della proposta 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. Il Consiglio ha raggiunto l'accordo sul testo che è stato quindi adottato senza discussione e pubblicato nel mese di aprile 2009 (Decisione 2009/371/GAI del 6 aprile 2009 in GU L121). L'entrata in vigore è prevista per il 1° gennaio 2010 e per quella data dovranno essere completate le modifiche per adattare le vigenti disposizioni alle nuove previsioni: si tratta ad esempio delle regole per l'apertura del *file* di analisi, per la trasmissione a Stati ed organismi terzi di dati nell'ambito di una procedura che richiede il parere dell'Acc Europol, ma che determinano anche la necessità per la stessa Acc di modificare il suo regolamento interno.

Per quanto in particolare riguarda il lavoro di supervisione, si conferma l'importanza dell'attività ispettiva, condotta annualmente, dell'Acc e affidata ad un gruppo che comprende esperti degli aspetti tecnologici.

L'ispezione si svolge di regola nel mese di marzo. Nel corso dell'ultima i partecipanti hanno focalizzato le verifiche sul contenuto e qualità dei dati trattati nei *file* di analisi e nel sistema di informazione Europol, sulla valutazione del funzionamento di quest'ultimo, sull'infrastruttura tecnica utilizzata e sull'attuazione delle raccomandazioni formulate dall'Acc nelle precedenti ispezioni. Con l'occasione sono stati svolti accertamenti sui dati detenuti da Europol relativi a procedure di ricorso aperte presso l'appo-

sito comitato dell'Acc, nonché nel funzionamento e contenuti dei progetti "*Check the web*" ed Oasis.

Dall'esito dell'ispezione e dagli accertamenti svolti anche in sede nazionale dalle autorità di protezione dei dati, incluso il Garante, è risultato che va maggiormente verificata la legittimità dell'inserimento di dati nel sistema di informazione Europol legata ad operazioni Frontex. Pertanto pur se l'Acc ha riconosciuto l'alto grado di adeguamento alle raccomandazioni formulate da parte di Europol, sono state rappresentate preoccupazioni per un uso del sistema che potrebbe essere non pienamente rispettoso delle regole esistenti.

L'Acc ha continuato a seguire, anche attraverso i risultati dell'ispezione, l'uso del sistema "*check the web*", un portale che mette a disposizione degli Stati partecipanti le informazioni ed i *link* ai siti *web* utili ai fini della lotta alla criminalità e l'uso di OASIS, progetto messo a punto per consentire analisi strategiche e di sistema al di là dei limiti imposti dai singoli *file* di analisi ritenuti troppo angusti.

Attività consultiva dell'Acc: l'Acc ha espresso parere sull'apertura di un *file* di analisi e su due richieste di autorizzare il direttore di Europol ad aprire negoziati con Paesi terzi per la trasmissione di dati personali. Nell'occasione l'Acc ha analizzato sulla base delle informazioni fornite da Europol il livello di adeguatezza dei due Paesi in questione, ravvisando problemi più importanti rispetto all'apertura di negoziati con uno di essi (la Russia); per l'altro, (Israele), invece, i pur rilevanti problemi riscontrati potrebbero incidere sulla stipula di un accordo per la trasmissione dei dati da Europol.

Nella conferenza, tenuta a Bruxelles il 9 ottobre, per celebrare i dieci anni di attività dell'Acc, i risultati finora raggiunti e le sfide future, il presidente del Garante, quale presidente del Gruppo polizia e giustizia ha offerto diversi spunti sulle attività svolte nel settore giustizia, sicurezza e libertà, evocando possibili futuri scenari per la cooperazione tra le autorità di protezione dei dati nel settore.

Attività del Comitato ricorsi: il Comitato ha definito un caso basato su una richiesta di accesso e verifica dei propri dati. In ragione delle circostanze emerse il Comitato ha chiesto ad Europol di riconsiderare la decisione iniziale di non rivelare l'esistenza o meno di dati relativi all'interessato ed ha ottenuto che questi ottenesse una risposta chiara in

merito. Un altro caso è tuttora pendente. L'Acc ha quindi discusso ed approvato la relazione di attività relativa al biennio 2006-2008, in corso di pubblicazione.

Le attività dell'Acc, inclusi i pareri adottati e le iniziative svolte sono comunque disponibili anche in italiano sul sito dell'Acc.

Il Sistema informativo doganale: l'attività dell'Autorità di controllo comune

In base alla Convenzione istitutiva, il Sistema informativo doganale (Sid) è formato da una base di dati centrale cui si può accedere tramite terminali in ogni Stato membro. Alla Commissione europea è affidata la gestione tecnica dell'infrastruttura del sistema.

La vigilanza sul corretto funzionamento del Sid è affidata ad una autorità comune di controllo, composta, per ciascun Paese, da due rappresentanti delle autorità nazionali di protezione dei dati.

L'Acc Dogane ha esaminato nel 2008 la bozza di rapporto sul funzionamento del sistema chiedendo di evidenziare alcuni aspetti di criticità emersi nell'ispezione svolta nel 2007, in particolare sui profili di sicurezza.

Le raccomandazioni dell'Acc richiedono di chiarire che ai fini del corretto adempimento degli obblighi del trattamento dei dati personali la responsabilità deve essere attribuita congiuntamente ad Olaf, l'organismo antifrode della Commissione europea, ed agli Stati membri; di migliorare la procedura per mantenere la registrazione dei diritti e credenziali attribuiti agli operatori e la valutazione periodica di queste, nonché una politica comune per la gestione delle *password* e il miglioramento della *management policy* del sistema per garantire la qualità e l'integrità dei dati. L'Acc ha anche richiesto di sviluppare azioni in materia di formazione del nuovo SIS basato sul *web*, fornendo la necessaria attenzione agli aspetti di protezione dei dati, preparando linee-guida ed istruzioni su aspetti specifici.

L'Acc ha inoltre completato la verifica del rispetto delle condizioni per la raccolta e trattamento dei dati personali iniziata lo scorso anno, 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; prima di intraprendere un'azione comune finalizzata a verificare la liceità dei trattamenti di dati personali, ha suggerito agli Stati di svolgere un ruolo più attivo per far individuare e se possibile, prevenire problemi di sicurezza.

A tal fine l'Acc ha sviluppato una sorta di *kit* di autovalutazione che il Regno Unito, la Grecia e la Slovacchia stanno sperimentando. Al termine della sperimentazione un nuovo questionario/*test* sarà messo a punto quale base, per le autorità di protezione dei dati, delle attività nazionali di supervisione.

Va infine segnalato che l'Acc sarà chiamata a fornire il suo parere su una proposta di atto comunitario, probabilmente una decisione, sull'uso delle tecnologie dell'informazione a scopi doganali che sostituirà la Convenzione indicata sopra.

Schengen

L'attività dell'Acc Schengen pur continuando a seguire gli sviluppi del SIS ed il passaggio dal vecchio al nuovo sistema, si è maggiormente incentrata sul funzionamento dell'attuale sistema.

L'integrazione di nove dei dieci Paesi entrati a far parte dell'Unione nel 2004 nel SIS e l'abolizione delle frontiere con questi nuovi Stati è il fatto più importante degli ultimi anni. Anche la Svizzera ed il Liechtenstein sono oggi considerati a pieno titolo nella cooperazione Schengen.

L'Acc Schengen ha pertanto ritenuto opportuno completare le verifiche nazionali sulla legittimità dei trattamenti di dati in relazione alle segnalazioni inserite nel SIS in base agli articoli 97 e 98, nonché procedere ad un aggiornamento della guida all'esercizio del diritto di accesso ai dati contenuti nel SIS, anche in vista dell'entrata in funzione del SIS II prevista per la seconda metà del 2010.

La Commissione europea, che avrà la responsabilità della gestione tecnica del SIS II sta predisponendo, con la collaborazione delle autorità nazionali di protezione dei dati, una campagna informativa per i cittadini.

L'Acc ha iniziato a seguire la migrazione dei dati dal SIS al SIS II e lo scenario futuro della supervisione e controllo (che passerà dall'Acc all'Edps con le autorità di protezione dati).

L'Acc ha inoltre adottato un parere in relazione all'attuazione dell'articolo 102 a) della Convenzione.

È stato altresì predisposto ed approvato il rapporto di attività, che copre il triennio 2005-2008 (*Schengen Joint Authority - Activity Report - Dec. 2005 - Dec. 2008*).

In relazione all'azione comune di verifica in ciascuno dei Paesi partecipanti della rego-

larità delle segnalazioni inserite nel sistema con riferimento all'art. 99 della Convenzione (sorveglianza discreta e controllo specifico), il Garante ha ampliato l'attività di verifica rispetto a quanto deliberato dall'Acc. A conclusione della parte nazionale dell'accertamento, è stato adottato un provvedimento con le prescrizioni ritenute necessarie a conformare il trattamento alle disposizioni della Convenzione. Si nota tuttavia una certa difficoltà da parte del Ministero dell'interno ad adeguarsi alle prescrizioni del Garante, in particolare per quanto riguarda la corretta individuazione dei casi in cui possono essere inserite nel SIS segnalazioni basate su questo articolo, che fa riferimento al concetto di *"reati particolarmente gravi"* assunto come non esistente in Italia. Altri aspetti tuttora aperti concernono la supervisione delle misure di sicurezza: si attende il completamento della migrazione in altra sede di tutto il sistema per procedere ad una verifica *in loco*.

Eurodac

L'attività di coordinamento del Garante europeo per la protezione dei dati personali, dopo l'adozione del primo rapporto, prosegue con gli approfondimenti necessari a valutare le procedure seguite dagli Stati sia per definire l'età (dodici anni) oltre la quale le impronte possono essere inserite nel sistema, sia per informare le persone dell'uso che sarà fatto delle impronte, nonché sulle modalità di trattamento dei dati in *Dublinet*.

Al termine degli accertamenti svolti (*v. Relazione* 2007, *pp.* 168-169) è stato adottato un *provvedimento* [doc. *web* n. 1537606] contenente le prescrizioni considerate per conformare il trattamento alle norme vigenti. Molte raccomandazioni formulate nel rapporto del Garante europeo sono state riprese dal Garante e fatte oggetto di apposita prescrizione.

Anche in questo caso gli accertamenti sono stati estesi 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.

Il Garante è intervenuto in particolare per verificare l'uso delle *cd. "ricerche speciali"* (richieste di accesso ai dati che il regolamento Eurodac consente permettere l'esercizio dei diritti della persona interessata). A seguito dell'intervento del Garante l'uso di tali categorie è cessato, risultando essere frutto di un errore. Tuttavia, il mancato esercizio da parte degli interessati del diritto di accesso ai propri dati determina incertezza sulla compren-

sione delle informazioni fornite per iscritto e sull'utilizzo di tale facoltà. Il *provvedimento* adottato dal Garante richiede specificamente che l'informativa sia data nei modi e nei tempi più idonei a far comprendere gli obiettivi e l'impatto del trattamento dei dati ed a consentire il pieno esercizio dei diritto di accesso e degli altri diritti collegati.

Altre prescrizioni hanno riguardato l'adeguamento delle misure di sicurezza.

La Commissione europea ha presentato all'inizio di dicembre due proposte di regolamento (Com (2008)825 e Com (2008)242) per modificare il quadro giuridico esistente, facendo seguito all'attività di valutazione svolta in relazione alla gestione della banca dati Eurodac ed alle procedure di asilo.

Un punto particolarmente delicato dell'agenda della Commissione, che non ha formato oggetto per il momento di una proposta di iniziativa legislativa specifica, concerne la possibilità per le forze di polizia di accedere ad Eurodac; le autorità di protezione dei dati personali hanno avuto modo di occuparsi di tale questione attraverso l'attività del *Working Party Police and Justice* (*v. infra*).

Working Party on Police and Justice

L'attività del Gruppo di lavoro polizia e giustizia è proseguita con grande intensità nel 2008 consolidando, sotto la presidenza del presidente del Garante, l'efficiente cooperazione tra le autorità di protezione dei dati europee ed accrescendo l'incisività dell'azione svolta. Molta attenzione è stata posta per cercare di accreditare la voce del Wppj nelle sedi appropriate e soprattutto stimolare ed intensificare i contatti con il Parlamento europeo, da sempre sensibile al tema del rispetto dei diritti che segue in particolare attraverso la Commissione Libe.

Pur essendo ancora un organismo informale, con le opportune sinergie con le Acc sopra ricordate e la possibilità di fare riferimento al segretariato comune di queste il Wppj ha tenuto quattro riunioni plenarie nel corso dell'anno; ciò ha permesso di decidere le azioni da intraprendere ed adottare i relativi atti in tempi sufficientemente brevi. La strutturazione di appositi sottogruppi, secondo quanto previsto dal regolamento interno, ha anche consentito di poter contare su prime bozze di elevato livello qualitativo.

L'attività del Wppj, seppur con le limitazioni richiamate, consente alle autorità di protezione dei dati di esprimersi anche in mancanza di un quadro legale definito a livello

europeo e di esplorare, con sempre maggior successo, le possibilità di sviluppare azioni (reazioni) congiunte con il Gruppo art. 29 sui temi che presentano una duplice valenza.

Il Wppj sempre per facilitare l'adempimento dei compiti attribuitigli dalle *Spring Conference* di Cipro ha adottato un programma di lavoro per il 2008 anche introducendo nuovi argomenti, quali ad esempio gli approfondimenti sugli accordi bilaterali tra gli Stati europei in materia di cooperazione giudiziaria e di polizia in materia penale (lotta al terrorismo, alla criminalità, allo sfruttamento dell'immigrazione illegale o alla pedo-pornografia) che prevedano forme di trasmissione di dati personali; le disposizioni nazionali di attuazione della Convenzione del Consiglio d'Europa sul *cybercrime* che possono avere un importante impatto nell'applicazione dei princìpi introdotti dalla decisione quadro sulla protezione dei dati personali nell'ambito della cooperazione giudiziaria e di polizia in materia penale (*v. supra, par.* 20).

Nella *Spring Conference* di Roma, il Wppj ha presentato una prima informale sintesi dell'attività svolta e la bozza di regolamento interno, che è stata formalmente approvata. Nella stessa occasione il Wppj ha presentato la dichiarazione poi adottata dalla stessa Conferenza relativa alla proposta sulla strategia europea di sorveglianza generalizzata dei viaggiatori (*v. Relazione* 2007, *p.* 161).

Altri temi trattati:

- la conservazione ed utilizzo a fini di polizia dei dati *Api* e *Pnr* raccolti da vettori aerei per fornire servizi commerciali. Dopo l'adozione di un parere congiunto con il Gruppo art. 29 (WP 145), trasmesso alla Commissione ed al Consiglio Ue, il Wppj si è riservato di intervenire nuovamente sul punto. Si è riferito nella *Relazione* 2007 (*p.* 169) delle posizioni critiche assunte dal Gruppo sull'argomento, che resta prioritario nell'agenda europea.

  Su richiesta italiana è inoltre stato sollevato il problema della compatibilità con la Direttiva 2004/82/Ce, ed in generale con gli obblighi derivanti dal diritto comunitario, delle richieste – formulate a pena di sanzione – ai vettori aerei di fornire dati *Api* (e *Pnr*) relativi a passeggeri di voli intracomunitari;
- il potenziamento della cooperazione transfrontaliera, con particolare riguardo al

contrasto del terrorismo e della criminalità transnazionale ("*progetto di decisione del Consiglio sul Trattato di Prüm*"). Come si è detto (*v. supra, par.* 20.2) sono state pubblicate nella *Gazzetta Ufficiale* della Unione europea il 6 agosto 2008 sia la decisione che reca disposizioni in materia di scambio di informazioni fra autorità giudiziarie e di polizia (*cd. "Trattato di Prüm"*), sia l'atto che ne fa applicazione (atti n. 615 e 616); le relative disposizioni dovranno essere applicate dagli Stati a partire dal luglio 2009. La discussione per la ratifica e l'entrata in vigore del Trattato di Prüm è in corso presso il Parlamento.

- il *cd. "Pacchetto Frattini"*, di cui si è riferito nella *Relazione* 2007 (*v. p.* 170).

Sulla base dei risultati del questionario interno si è deciso di continuare a lavorare ad uno strumento comune per lo svolgimento di *audit* ed ispezioni nel settore, sottoposto per la definitiva approvazione alla *Spring Conference* del 2009, tenutasi ad Edimburgo, (23-24 aprile).

Il Wppj ha avviato, inoltre, sulla base di questionari predisposti dall'autorità italiana, un'attività di approfondimento e verifica dell'impatto a livello nazionale della ratifica della Convenzione del Consiglio d'Europa sulla criminalità informatica ed un inventario degli accordi bilaterali (o multilaterali) stipulati in materia di *law enforcement* dai singoli Stati nazionali.

Il Wppj ha definito ed approvato il primo rapporto annuale di attività, presentato per la definitiva adozione alla *Spring Conference* di Edimburgo.

Nell'occasione la relazione del presidente si è soffermata anche sul seguito del programma di lavoro per il 2008/2009 (con particolare riguardo all'impatto del Trattato di Lisbona sulla materia attinente al *"terzo pilastro"* ed all'attività delle autorità di protezione dati, all'entrata in vigore del nuovo quadro di princìpi relativi al trattamento dei dati nella cooperazione di polizia e giustizia ed all'impatto sugli accordi bi e multilaterali in vigore tra i Paesi dell'Unione).

La *Spring Conference* ha anche rinnovato il mandato del presidente del Garante italiano quale Presidente del WPPJ.

20.3. LA PARTECIPAZIONE AD ALTRI COMITATI E GRUPPI DI LAVORO

"Case Handling Workshop"

Il diciottesimo incontro del *"Case Handling Workshop"*, organizzato dall'Autorità di protezione dei dati slovacca a Bratislava, ha costituito, come già in passato, l'occasione per focalizzare l'attenzione su una pluralità di temi, alcuni dei quali di particolare interesse per le autorità dei paesi di nuova adesione all'Ue.

L'agenda ha dato spazio dapprima, come consueto, a una presentazione dell'Autorità ospite e delle sue attività.

In tale ambito, particolare rilievo è stato dato alla descrizione delle attività ispettive, con riguardo sia all'avvio e allo svolgimento delle ispezioni (è stato costituito un registro nel quale vengono annotati i *"ricorsi"* che giungono e le attività che a seguito di questi vengono svolte), sia all'introduzione nell'ordinamento slovacco della figura del *"data protection official"* (incaricato aziendale per la protezione dei dati: obbligatorio nel caso di soggetti giuridici con più di 6 dipendenti). Quest'ultimo consente, a giudizio dell'autorità slovacca, di responsabilizzare i titolari del trattamento con riferimento alla protezione dei dati, pur con la difficoltà di individuare persone adeguate al ruolo che deve essere svolto (nessun particolare supporto è fornito dall'Autorità slovacca per la scelta e la formazione di tali figure) e che assicurino la dovuta indipendenza.

L'incontro ha quindi offerto l'occasione per analizzare l'esperienza che è derivata all'autorità slovacca dal suo ingresso nell'area Schengen: dopo la descrizione del funzionamento dell'ufficio SIRENE, sono stati presentati gli esiti di alcune ispezioni che l'Autorità ha condotto all'interno dei consolati slovacchi in alcuni Paesi terzi (Russia, Bielorussia) con riferimento alle modalità ivi utilizzate per il trattamento dei dati personali in occasione della richiesta e del rilascio di visti Schengen.

I lavori del *workshop* sono proseguiti con una discussione sul difficile rapporto tra protezione dei dati e *mass media*. Ha introdotto la sessione una breve analisi (presentata dall'autorità ceca) degli ordinamenti europei (pochi) nei quali la disciplina di protezione dei dati trova applicazione anche con riferimento ai trattamenti svolti per finalità di giornalismo e manifestazione del pensiero. Tra le presentazioni (oltre a quella spagnola che si è

soffermata su due recenti raccomandazioni in materia di pubblicazione di dati personali nella *Gazzetta Ufficiale* di Madrid e trattamento dei dati nell'ambito dei servizi di *e-government*), interessante quella belga che ha manifestato la propria preoccupazione per il diffondersi di programmi televisivi sempre più invasivi delle libertà individuali (*cfr.*, *ad es.*, i classici programmi di *candid camera* o i sempre più diffusi *reality show*). La sessione è stata l'occasione per presentare tre recenti casi affrontati dall'Autorità italiana in materia di giornalismo e, in particolare, i delicati aspetti relativi alla pubblicazione *on-line* degli archivi storici delle principali testate italiane.

I lavori della prima giornata si sono chiusi con una sessione dedicata alle misure di sicurezza e con la presentazione dei servizi di due società di consulenza che operano nel settore.

Il *whistleblowing* (ossia la possibilità per i dipendenti di aziende o di altre strutture di segnalare, eventualmente in forma anonima o comunque protetta, irregolarità o violazioni delle quali vengano a conoscenza in rapporto all'attività lavorativa) è stato il tema più controverso affrontato nella seconda giornata di lavori del *workshop*. Dopo la presentazione delle esperienze svedese, danese e francese (incentrate per lo più su vicende che vedono interessate società con legami con gli Stati Uniti e quindi in qualche modo vincolate dal *Sarbanes-Oxley Act*, *cfr. www.sarbanes-oxley.com*), l'attenzione si è focalizzata sul crescente numero di richieste rivolte alle autorità nazionali da società *"totalmente europee"* al fine di introdurre tali schemi nella propria organizzazione aziendale e non solo per reati di natura fiscale e contabile. La questione, di forte interesse, sarà probabilmente argomento di discussione anche nel prossimo *workshop*.

Le altre sessioni hanno affrontato il tema del trattamento dei dati personali sul luogo di lavoro (con due presentazioni del Garante europeo dedicate ai controlli proposti dalla Commissione europea sul funzionamento del meccanismo denominato *"flexitime"*, che consente ai funzionari di indicare in modo flessibile le ore lavorate in ambito settimanale, e alla raccolta di dati relativi al fascicolo personale dei dipendenti per quanto attiene ad eventuali precedenti di natura penale e/o giudiziaria in genere) e le problematiche connesse alla videosorveglianza, anche con riguardo all'attività lavorativa (tema questo già più

volte affrontato nel corso dei precedenti incontri). Interessante, a tale riguardo, il divieto del Commissario di protezione dei dati del Liechtenstein di proseguire l'utilizzo di un sistema di videosorveglianza che l'autorità municipale di Vaduz aveva installato nel centro storico della città per finalità di sicurezza di beni e persone. Il sistema è stato considerato sproporzionato dal momento che riprendeva costantemente tutta l'attività della zona senza che fosse stata data prova della sua effettiva necessità.

Iwgdpt

Il "Gruppo di Berlino" (*International Working Group on Data Protection in Telecommunication*) si è riunito il 13 e il 14 ottobre a Strasburgo.

In occasione dell'incontro è stato organizzato il seminario pubblico "*Privacy in the age of social network services*", dal quale è risultato confermato l'uso crescente dei *social network* quale strumento di socializzazione e comunicazione.

Il seminario è stato occasione per riflettere sulle diverse problematiche relative al trattamento dei dati nell'ambito delle reti sociali. In particolare, è stato posto l'accento sulla categorie di soggetti (diversi da quelli abilitati dall'interessato) che possono avere interesse ad acquisire informazioni personali attraverso i *social network* (datori di lavoro, insegnanti, genitori, forze di polizia, *ecc.*) e sulla necessità che i soggetti pubblici (in particolare le *cd. "law enforcement agencies"* e l'*intelligence*) assicurino basi legali per ogni raccolta di dati, evitando la creazione di profili segreti (*ad es.*, associati all'elaborazione di "*risk ratings*").

È stato inoltre affrontato il tema della titolarità del trattamento in un ambito in cui gli stessi utenti immettono informazioni sul proprio conto e sui terzi. Sono stati ribaditi gli obblighi degli stessi servizi di *social network* di tener fede alle proprie *privacy policies*, procedere ad *audit*, essere trasparenti sulle pratiche seguite, prestare attenzione nel ricorrere a profilazione e *scoring*, segnalare, infine, i rischi connessi alla commercializzazione dei dati. È stato infine fatto riferimento anche alle interazioni tra il *social network* e altri servizi del *web* (ad esempio, le mappe offerte da *Google* che possono essere facilmente inserite in questi siti), nonché alla possibilità di esportate il proprio profilo in altri *social network* (*cd. "open social"*).

Tra i problemi segnalati, si evidenziano il potenziale conflitto tra *privacy* e tutela della

libertà di espressione, il diritto all'oblio, i profili attinenti alla legge applicabile e alla giurisdizione competente.

La riunione del *Iwgdpt* è stata l'occasione per riflettere sulle nuove tecniche di crittazione biometrica e di videosorveglianza, sui primi sistemi che si stanno presentando in attuazione della *European electronic toll service directive* 2004/52, alla luce dell'obbligatorietà di questo strumento, con particolare riferimento alla disposizione delle unità per procedere al pagamento (preferendo rispetto a sistemi centralizzati, *on board unit* con uso di *Gps* o di sistemi radio), nonché sulle questioni relative alla realizzazione di *Google Street View*, ed in particolare sulle assicurazioni della società che dalle mappature in corso nelle strade verranno rimossi i numeri di targa e anonimizzati i volti dei passanti.

Consiglio d'Europa

Nel corso del 2008 l'autorità italiana ha continuato a seguire i lavori del Comitato consultivo (T-Pd) della Convenzione 108/1981 del Consiglio d'Europa, partecipando anche agli incontri del *Bureau*, gruppo ristretto che si riunisce ogni quattro mesi assicurando continuità ai lavori del T-Pd.

Profilazione

Il T-Pd ha proseguito l'approfondimento del tema della profilazione, una particolare tecnica di trattamento che permette di desumere informazioni relative a una persona a partire dai dati (anonimizzati o meno) relativi ad un gruppo di individui al quale l'interessato appartiene o si suppone appartenga (*v. Relazione* 2007, *p.* 174). Sulla base dello studio commissionato ad esperti scientifici, il T-Pd ha lavorato alla predisposizione di un quadro di garanzie per gli individui oggetto di profilazione, in vista di una raccomandazione in materia. Il progetto di raccomandazione (che pure mira a fornire princìpi che valgano per i diversi settori) guarda con particolare attenzione alle nuove tecnologie che consentono di immagazzinare enormi quantità di dati e di procedere con estrema rapidità all'elaborazione automatica di decisioni e valutazioni sull'individuo sulla base di criteri predeterminati senza l'intervento dell'intelligenza umana. In un simile quadro si è discusso sull'opportunità di garantire il diritto di opposizione, di fornire agli individui una adeguata informativa sulla profilazione di cui siano oggetto, di vietare, di regola, profilazioni basate su dati sensibili, di realizzare un bilanciamento degli interessi coinvolti.

Agenzia mondiale *anti-doping* (Adams)

Del parere rilasciato sulla compatibilità del documento *"International Standards for the Protection of Privacy and Data Protection"*, elaborato dalla *"World Anti-doping Agency"* (Wada), con i princìpi sulla protezione dei dati del Consiglio d'Europa (T-Pd-BUR(2008)04 fin), si è riferito nella *Relazione* 2007 (*p.* 174).

Nel corso dell'anno è stata anche avviata la discussione sull'opportunità di elaborare un protocollo addizionale alla Cedu per inserire nel catalogo dei diritti fondamentali il diritto alla protezione dati. Anche a fronte dei dibattiti complessi avviati a livello nazionale si è deciso di attendere le sorti del Trattato di Lisbona, e di ridiscutere il tema durante la riunione del T-Pd del 2009.

Il T-Pd è poi tornato a discutere delle iniziative volte a dare applicazione all'art. 1 del Protocollo addizionale alla Convenzione 108 sulle autorità indipendenti. È stata in particolare sottolineata l'esigenza di redigere un rapporto che faccia luce sulla situazione attuale delle diverse autorità nazionali e di concentrare l'analisi sui requisiti di indipendenza delle autorità.

Il T-Pd ha inoltre deciso di conferire lo *status* di osservatore alle proprie riunioni sia all'"Associazione delle autorità francofone di protezione dei dati personali" (Afapdp), sia alla "Rete Iberoamericana di protezione dei dati" (Ripd).

Anche nel 2008 il Consiglio d'Europa ha svolto la propria attività di coordinamento riguardo al *"Data protection day"*. In particolare, il Consiglio d'Europa, con il supporto della Commissione europea, ha dato pubblicità, anche attraverso il proprio sito *web*, alle diverse iniziative intraprese dalle autorità interessate, tra cui il Garante, volte a sensibilizzare i cittadini sulle tematiche della *privacy* e della protezione dei dati (*v. par.* 21.6).

Ocse

In ambito Ocse, particolarmente approfondita è stata la riflessione sulle tematiche di Internet, specie nelle sue interazioni con altre tecnologie come la *Rfid*.

In tale settore, un evento rilevante, al quale il *Working Party on Information Security and Privacy* (Wpisp) ha dedicato particolare attenzione (*v. Relazione* 2007, *p.* 175), è stata la Conferenza Ministeriale di Seul del 17 e 18 giugno 2008, sul tema *"Il futuro di Internet"*.

Durante la Conferenza è stata messa in evidenza l'importanza di rilanciare un dialogo di respiro internazionale sulle problematiche di Internet in relazione al settore privato. In

tale occasione, è stata adottata da trentanove paesi, tra cui l'Italia, la *"Seul Declaration for the future of Internet economy"*, con la quale le Parti hanno affermato il loro impegno a lavorare insieme alle imprese, la società civile, e gli esperti tecnici per stimolare l'innovazione, la concorrenza, e gli investimenti nelle tecnologie della comunicazione, costruendo un clima di fiducia nell'economia di Internet. Nella Dichiarazione, tra l'altro, si sottolinea l'impegno delle Parti a: facilitare la convergenza delle reti e dei servizi digitali; promuovere la creatività nell'uso e nelle applicazioni di Internet garantendo un flusso libero di informazioni, di ricerca e di innovazione; rafforzare la sicurezza della rete e la fiducia nei suoi utilizzatori, in particolare assicurando la sicurezza dei sistemi e la protezione dell'identità digitale e della *privacy* dei navigatori della rete; garantire lo sviluppo di un'economia di Internet che sia realmente globale anche attraverso *policy*, frutto della cooperazione tra i diversi Paesi, volte a migliorare la *privacy* di utenti e in particolare dei minori.

Significativa, nel quadro delle attività dell'Ocse in materia di nuove tecnologie, anche l'elaborazione dei due documenti *"Rfid application, impacts and country initiatives"* (18 aprile 2008), che evidenzia le applicazioni e le iniziative prese dai diversi paesi in materia di *Rfid*, e *"Measuring security and trust in the on-line environment"* (29 gennaio 2008), che si propone di analizzare in quale misura le preoccupazioni riguardo alla sicurezza *on-line* siano di ostacolo allo sviluppo della rete e con quali modalità i soggetti (persone fisiche e società) che utilizzano la rete proteggono reti e dispositivi informatici.

Il Gruppo Wpisp nel 2008 ha proseguito la sua attività sulla *Digital Identity*, in particolare con riferimento al rapporto tra personalità e identità digitale nella società dell'informazione. Ha altresì seguito le tematiche relative alla protezione dei minori *on-line* anche in vista del Convegno organizzato dall'Apec e l'Ocse di Singapore del 15 aprile 2009 sulle iniziative volte a promuovere una Internet più sicura per i minori, tema che pure rientra tra gli obiettivi della Dichiarazione di Seul. I rappresentanti del Gruppo hanno concordato un ampio scambio di informazioni sulle politiche e le *best practices* dei diversi paesi riguardo la protezione dei minori dai rischi derivanti dall'uso di Internet, in particolare relativi ai contenuti lesivi della rete e ai problemi di *privacy* e sicurezza dei dati.

21. Le attività di comunicazione, studio e ricerca

21.1. La comunicazione del Garante: profili generali

L'attività di comunicazione e informazione svolta nel 2008 è stata principalmente volta a sviluppare nell'opinione pubblica la consapevolezza che la protezione dei dati personali non è un *"lusso"* del sistema, ma un diritto fondamentale nell'odierna società globalizzata e tecnologica.

È stata privilegiata un'informazione ed una comunicazione tanto più divulgativa, quanto attenta all'uso di un linguaggio rigoroso, in particolare sui grandi temi legati alla protezione dei dati quali: la messa in sicurezza delle grandi banche dati pubbliche e private; la conservazione dei dati di traffico telefonico; le intercettazioni; le investigazioni difensive; gli archivi di consulenti e periti dei magistrati; il ricorso sempre più massiccio a sistemi di videosorveglianza per finalità di sicurezza, soprattutto in ambito locale; la protezione delle reti di telecomunicazione e comunicazione elettronica; la tutela dei minori su Internet e il fenomeno *social network*; l'uso dei dati genetici; il ricorso sproporzionato o generalizzato a tecniche di raccolta di dati biometrici.

Medesimo impegno è stato posto anche riguardo a questioni di più immediato interesse sociale quali, ad esempio: lo stop alla diffusione su Internet dei redditi dei contribuenti; le misure a protezione dell'Anagrafe tributaria; la regolamentazione della propaganda elettorale; il rispetto della dignità delle persone nelle strutture sanitarie; le sperimentazioni cliniche; la tutela della riservatezza negli alberghi; il corretto uso dei dati dei condòmini; la profilazione dei gusti e delle abitudini dei consumatori e le *"carte di fedeltà"*; l'informazione televisiva e il disagio sociale; immigrazione e censimento dei campi nomadi.

L'Autorità ha mantenuto ancora un alto livello di attenzione ed informazione a tutela dei lavoratori, tenendo comunque conto delle esigenze di semplificazione degli adempimenti per imprese e pubbliche amministrazioni.

Costante, infine, è stato l'impegno nel ricercare il giusto equilibrio nel delicato rapporto tra diritto di cronaca e diritti fondamentali della persona e massima attenzione è stata posta alla tutela di donne e minori vittime di violenze sessuali.

Alcune cifre

La presenza sui *media* delle tematiche riguardanti la protezione dei dati personali ed in particolare l'attività del Garante, ha mantenuto una costante crescita. Nel periodo dal 1 gennaio al 31 dicembre 2008 il Servizio relazioni con i mezzi di informazione ha selezionato oltre ventiquattromila articoli di interesse dell'Autorità. Sulla base della rassegna stampa prodotta giornalmente, le pagine dei maggiori quotidiani e periodici nazionali, dei principali quotidiani locali e dei *media on-line*, che hanno dedicato spazio alle questioni legate generalmente alla *privacy*, sono state oltre ottomilaquattrocento, delle quali tremilaottocento dedicate esclusivamente all'attività del Garante. Le prime pagine rivolte ai temi della protezione dei dati personali sono state circa ottocentoventotto (di cui quattrocentotrentuno riguardanti la sola Autorità). Numerose sono state le interviste, gli interventi e le dichiarazioni pubblicate sulla carta stampata (quattrocentoquattordici) e andate in onda su tv e radio nazionali e locali (centotrentacinque).

21.2. I PRODOTTI INFORMATIVI

Nel 2008 l'Autorità ha diramato cinquantaquattro Comunicati stampa e diciannove *Newsletter*.

La *Newsletter*, giunta al suo 10° anno di pubblicazione (per un totale di trecentodiciassette numeri e millenovantanove notizie) è lo strumento giornalistico del quale il Garante si avvale per informare, in modo ampio ed approfondito, dei provvedimenti adottati e della propria attività nazionale ed internazionale. La consultazione *on-line* e l'invio telematico ad un numero sempre crescente di abbonati (istituzioni, pubbliche amministrazioni, imprese, liberi professionisti, privati cittadini) hanno notevolmente ampliato la diffusione della *Newsletter* e favorito l'apprezzamento da parte di un vasto pubblico.

Il *Cd-rom* del Garante *"Il Garante e la protezione dei dati personali"* giunto alla XVIII edizione si apre con una presentazione multimediale dell'attività, le funzioni e l'organizzazione dell'Autorità. Al suo interno sono disponibili diverse informazioni sull'Autorità, il Glossario e una sezione *"Temi"* con schede informative su argomenti di particolare interesse o attualità. Come nelle precedenti edizioni, nell'archivio aggiornato sono disponibili, in forma integrale e nell'originaria veste editoriale, le pubblicazioni dell'Autorità.

Altre due aree tematiche, *"Normativa"* e *"Informazione"*, permettono di accedere ai testi della normativa nazionale ed internazionale, ai comunicati stampa ed alla raccolta completa delle *Newsletter*. L'archivio ipertestuale realizzato in formato *pdf* consente la consultazione con funzioni di ricerca *"full text"*.

Il *Cd-rom* rappresenta un strumento ormai conosciuto ed atteso da amministrazioni pubbliche, imprese, liberi professionisti e cittadini. In occasione della Conferenza dei Garanti europei, svoltasi a Roma in primavera, il Servizio relazioni con i mezzi di informazione ha realizzato un *Cd-rom* in lingua inglese contenente la raccolta della normativa italiana ed europea sulla protezione dei dati personali, distribuito ai numerosi ospiti internazionali intervenuti alla Conferenza.

L'impegno per una comunicazione semplice e diretta principalmente al cittadino trova concreta applicazione nella realizzazione dei *dépliant* divulgativi in grado di illustrare i diversi temi connessi alla protezione dei dati personali. Ai nove pieghevoli finora realizzati si è aggiunto quello dedicato alla difesa della *privacy* in ambito sanitario: il pieghevole è stato tradotto anche in lingua inglese, francese e tedesca per essere fruibile anche dai molti cittadini stranieri presenti sul nostro territorio. Il progetto di comunicazione istituzionale proseguirà con la realizzazione di una ulteriore serie di *dépliant* relativi a diverse tematiche (*social network*, scuola, lavoro, condominio).

21.3. I PRODOTTI EDITORIALI

Il notiziario bimestrale "*Garante privacy.it"*, giunto al sesto anno, e destinato a personalità del mondo istituzionale ed 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 apre con un editoriale che affronta argomenti di attualità, a firma di uno dei quattro componenti del Garante.

L'Autorità già da alcuni anni – al fine di contribuire ulteriormente all'approfondimento dei temi legati alla *privacy* ed ai princìpi posti dalla normativa nazionale e comunitaria – ha realizzato la collana *"Contributi"*, nella quale sono pubblicati testi di appro-

fondimento sulle problematiche riguardanti la tutela della dignità della persona e la protezione dei dati personali. Attualmente la raccolta è composta da sette volumi.

21.4. GLI INCONTRI INTERNAZIONALI

Nel 2008 il Garante ha ospitato l'annuale Conferenza europea delle autorità garanti per la protezione dei dati personali (*Spring Conference*). L'incontro si è svolto a Roma il 17 e 18 aprile ed ha visto la partecipazione dei rappresentanti di trentotto Paesi. I lavori – articolati in sei sessioni ciascuna introdotta da un contributo video affidato a personalità del mondo delle istituzioni, del diritto e della ricerca – si sono focalizzati su tre grandi temi: sicurezza, nuove tecnologie, globalizzazione dell'economia.

La globalizzazione e l'uso delle nuove tecnologie portano con sé, oltre a nuove potenzialità, anche nuove minacce per i diritti delle persone: a fronte di una maggiore richiesta di sicurezza si tende, sempre più, ad estendere l'uso dei dati personali. Il presidente Francesco Pizzetti ha sottolineato, in questa sede, come il necessario livello di controllo e sorveglianza non deve diventare un ostacolo alla circolazione o restringere gli spazi di libertà.

Ad ottobre, in Lussemburgo, il presidente Pizzetti – in qualità di presidente del "*Working Party on Police and Justice*", Wppj (Gruppo che riunisce i Garanti europei incaricato di seguire le problematiche connesse all'attività di collaborazione giudiziaria) – ha incontrato Jacques Barrot, vice presidente della Commissione europea e commissario europeo per la Giustizia, la libertà e la sicurezza. Al centro dei colloqui, il lavoro svolto dai Garanti europei per la protezione dei dati personali nell'ambito della cooperazione giudiziaria e di polizia tra i Paesi dell'Ue e le prospettive aperte dal Trattato di Lisbona.

Dal 15 al 17 ottobre il Collegio dell'Autorità ha partecipato a Strasburgo alla 30° Conferenza Internazionale delle Autorità Garanti, dedicata quest'anno al tema "*Proteggere la privacy in un mondo senza confini*". Alla Conferenza, che ogni anno riunisce le Autorità per la protezione dei dati personali provenienti da ogni continente, sono stati affrontati numerosi temi che vanno dalle problematiche di natura economica (*privacy* come risorsa e non come ostacolo per le imprese), al rapporto fra *privacy* e crescente pubblicità delle informazioni personali (*social network*); dalla corsa verso la creazione di banche dati sem-

pre più estese per finalità di sicurezza, all'esigenza di mettere in atto strategie mirate di informazione e sensibilizzazione per i più giovani.

Il presidente Pizzetti a febbraio, a Sofia, ha partecipato al seminario sulla Protezione dei dati personali in Europa, organizzato dall'Autorità spagnola e bulgara; a maggio, a Parigi, è intervenuto al Convegno sulla Protezione dei dati personali nella ricerca biomedica e farmacologica.

Il segretario generale Giovanni Buttarelli, a maggio, ha partecipato all'incontro *"Doing no evil"* presso il Parlamento europeo. In tale occasione il cons. Buttarelli ha espresso forte preoccupazione per possibili future minacce per la protezione dei dati personali, che potrebbero derivare dalla possibilità di navigare in Internet attraverso il cellulare.

21.5. LE RELAZIONI CON IL PUBBLICO

Profili di carattere generale

L'Ufficio relazioni con il pubblico cura la conoscenza della disciplina in materia di trattamento dei dati personali e si pone come struttura di raccordo tra il cittadino e l'Autorità.

Gli uffici per le relazioni con il pubblico sono stati istituiti, come è noto, dall'art. 12 del d.lg. 3 febbraio 1993, n. 29 (ora art. 11, del d.lg. 30 marzo 2001, n. 165), quale risposta a una duplice esigenza, già messa in luce dalle precedenti leggi 7 agosto 1990, n. 241, e 8 giugno 1990, n. 142: da un lato, dare veste istituzionale all'emergente cultura della trasparenza amministrativa e della qualità dei servizi; dall'altro, fornire uno strumento organizzativo adeguato alle esigenze di attuazione delle funzioni di comunicazione istituzionale e contatto con i cittadini.

Successivamente, la legge 7 giugno 2000, n. 150, portando a compimento l'evoluzione normativa avviata con le riforme degli anni '90, individua nell'Urp, uno dei principali strumenti organizzativi attraverso cui le amministrazioni pubbliche possono espletare le funzioni di comunicazione e relazione con il pubblico.

Il personale preposto all'Ufficio delle relazioni con il pubblico ha il compito di dare piena visibilità all'attività dell'Autorità, garantendo al cittadino sia la possibilità di partecipare e accedere alle diverse fasi procedimentali attraverso le forme di coinvolgimento

espressamente regolamentate, sia il costante aggiornamento sulle tematiche di interesse dell'Autorità.

In particolare l'Urp del Garante per la protezione dei dati personali svolge compiti:

- di informazione sulle disposizioni normative in materia di protezione dati personali, in particolare sugli adempimenti previsti dal Codice e sulle forme di tutela attivabili davanti all'Autorità;
- di comunicazione esterna attraverso una vera e propria attività di diffusione della cultura della *privacy* e di formazione degli utenti;
- propedeutici all'accesso dei cittadini agli atti amministrativi;
- di ascolto e misurazione della qualità dei servizi forniti;
- di comunicazione interna;
- di comunicazione interistituzionale, attraverso l'attivazione di flussi informativi tra gli uffici per le relazioni con il pubblico delle diverse Autorità ed amministrazioni.

Sempre più rilevante e di grande ausilio è la strumentazione tecnologica, grazie alla quale è stata attuata una nuova modalità di comunicazione telematica sia nei rapporti con l'utente che internamente tra gli uffici della stessa Autorità.

La soddisfazione degli utenti dell'Ufficio è legata innanzitutto alla continuità del servizio nonché alla celerità e completezza delle informazioni fornite.

Nel corso dell'anno sono state ricevute numerose manifestazioni di gradimento, che permettono di confermare una stretta correlazione tra *"qualità erogata"* e *"qualità percepita"*.

L'attività dell'Ufficio relazioni con il pubblico

L'attività dell'Urp si può suddividere in tre grandi aree:

- semplificazione, ovvero agevolazione del rapporto con il cittadino, dall'accesso ai documenti, alla semplificazione dei messaggi rivolti all'utenza (modulistica), all'avvio dei procedimenti per la tutela dei diritti davanti al Garante;
- comunicazione e gestione integrata dei rapporti con l'utenza, come la raccolta delle segnalazioni e delle istanze e la pubblicizzazione dell'attività dell'Autorità, in un rapporto di scambio continuo e circolare;
- informazione, con particolare cura nei messaggi direttamente riferiti all'utenza tra-

mite mezzi di comunicazione ordinari e anche più diretti come il contatto telefonico o la posta elettronica, compreso il sito *web*.

L'attività dell'Ufficio relazioni con il pubblico si è consolidata nel 2008 con l'entrata in vigore del Regolamento n. 1 del 2007 (*G.U.* 9 gennaio 2008, n. 7 [doc. *web* n. 1477480]) concernente le procedure interne all'Autorità aventi rilevanza esterna, finalizzato allo svolgimento dei compiti demandati al Garante, il cui art. 18 disciplina la trattazione dei quesiti e delle richieste di parere.

Si conferma anche per il 2008 l'interesse della pubblica opinione per le tematiche legate alla *privacy*. Siffatto interesse è rilevabile dal crescente numero dei contatti registrati nel corso dell'anno, specie in occasione di fatti che hanno suscitato grande risonanza sui mezzi d'informazione, con numerose richieste di chiarimenti da parte dei cittadini, anche semplicemente mossi dal desiderio di esprimere le proprie posizioni o rimostranze.

Si richiamano, a mero titolo esemplificativo, le centinaia di *e-mail* di commento e/o di richiesta di intervento pervenute all'Urp in occasione della diffusione, tramite il sito *web* dell'Agenzia delle Entrate, dei dati concernenti le dichiarazioni dei redditi per l'anno 2005 dei contribuenti italiani sia prima che dopo i correlati ripetuti interventi del Garante.

È sempre molto alta l'attenzione dei cittadini verso l'attività del Garante rivolta a stroncare il fenomeno delle telefonate pubblicitarie, dette anche telefonate indesiderate.

Numerose segnalazioni continuano a pervenire al riguardo all'Ufficio relazioni con il pubblico che, d'intesa con il dipartimento competente, ha avviato una prima fase d'istruttoria, volta alla verifica/integrazione degli elementi necessari per aprire la procedura.

Molti sono, inoltre, gli episodi di cronaca che, per il clamore suscitato e la grande rilevanza dei temi, hanno indotto l'Autorità a intervenire, talvolta a più riprese e in maniera decisa. Così, il caso della studentessa inglese trovata uccisa a Perugia il 2 novembre 2007, le inchieste di 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 per ricevere le diverse istanze dei cittadini.

I contatti complessivamente registrati nel periodo di riferimento, trentaseimilatrecen-

tottanta, sono diversamente distribuiti rispetto al 2007: così, mentre rimane sostanzialmente invariato il numero dei contatti telefonici (intorno ai quindicimila) sono leggermente diminuiti i visitatori (millecento a fronte dei millecinquecentocinquanta del 2007), segno di un evidente preferenza per i contatti a mezzo del telefono e della posta elettronica. L'entrata in vigore del Regolamento sulle procedure interne sopra citato ha comportato un notevole incremento dei fascicoli trattati (ottocentottantatre nel 2008 a fronte dei seicentottantanove relativi all'anno 2007).

L'attività del servizio relazioni con il pubblico è frutto di un'attenta progettazione, sia in fase strategica, sia in fase operativa, in funzione delle specificità che caratterizzano il contesto di riferimento. Il pacchetto di servizi, gli strumenti operativi, i processi di lavoro, le professionalità impiegate, ed anche la logistica e l'arredo fan parte di un progetto complessivo contribuendo in modo sinergico all'assolvimento di funzioni definite e obiettivi organizzativi prestabiliti.

Tematiche d'interesse

Le tematiche più ricorrenti che, nel periodo in esame, sono state oggetto di richieste da parte dei cittadini e delle amministrazioni pubbliche sono quelle relative agli adempimenti previsti dal Codice, al *marketing*, alle telefonate e alle *e-mail* pubblicitarie, alla propaganda elettorale (che ha impegnato l'ufficio in occasione delle elezioni politiche e amministrative avvenute nel mese di aprile 2008), al lavoro, al condominio ed alla videosorveglianza, cui l'ufficio ha provveduto dando pronto riscontro attraverso la predisposizione di note tipo o attraverso il contatto telefonico.

In sintesi è stata riscontrata una notevole affluenza del pubblico presso la sede dell'Ufficio in prossimità delle numerose scadenze correlate agli adempimenti previsti dal Codice. In particolare, in prossimità della scadenza annuale dei termini relativi alle nuove misure minime di sicurezza, si continua a registrare un rilevante incremento di quesiti specifici e di richieste di chiarimenti, anche alla luce delle recenti modifiche normative intervenute con la legge n.133 del 2008, il cui art. 29 ha modificato tra l'altro, l'art. 34 del Codice, prevedendo, per taluni titolari di trattamento, misure di sicurezza semplificate (art. 34 comma 1-*bis* del Codice).

Anche quest'anno numerosi sono stati i quesiti pervenuti dagli enti locali in materia

di accesso agli atti amministrativi e, in particolare, di accesso da parte dei consiglieri comunali.

Tra le tematiche che hanno suscitato maggiore interesse il trattamento dei dati personali dei lavoratori per finalità di gestione del rapporto di lavoro, nonché il trattamento dei dati personali della clientela in ambito bancario, soprattutto con riguardo all'accesso alla documentazione bancaria.

Si segnala, infine, la delicata problematica relativa alle intercettazioni e divulgazioni di comunicazioni telefoniche. In numerose occasioni il Garante ha richiamato i mezzi d'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.

Nella seconda metà dell'anno di riferimento, sono pervenute molte segnalazioni sul trattamento dei dati nei cosiddetti *"Social network"* (*Facebook*, *MySpace*, *ecc.*), che rappresentano importanti strumenti d'innovazione sociale, e di scambio di opinioni ed informazioni per un numero crescente di persone, ma che comportano gravi rischi ed incognite che vanno dall'uso distorto dei dati a veri e propri furti d'identità.

21.6. LE MANIFESTAZIONI E LE CONFERENZE

Per promuovere la conoscenza della legge il Garante ha confermato – anche nel corso del 2008 – la sua presenza in importanti manifestazioni.

A maggio, con il proprio *stand*, l'Autorità ha partecipato alla XIX edizione del *Forum Pa*. Sulla base dei dati forniti dagli organizzatori, la manifestazione ha registrato complessivamente l'afflusso di circa trentaseimila visitatori e lo *stand* del Garante è stato visitato da una media giornaliera di circa trecento/quattrocento visitatori.

Il segretario generale Buttarelli, è intervenuto al convegno *"Tecnologie e privacy nel rapporto di lavoro pubblico. Il corretto utilizzo degli strumenti tra esigenze di efficienza ed economicità e diritti della personalità"*.

Il vice presidente dell'Autorità, Giuseppe Chiaravalloti, ad ottobre è intervenuto al *workshop* organizzato da *"Consumers' Forum"*, dedicato quest'anno al tema *"Authority:*

quali strategie per i prossimi anni"; a novembre ha partecipato in qualità di relatore al XXVIII Convegno nazionale sul "*Sistema demografico: risorsa per la semplificazione, la sicurezza dello Stato e la convivenza civile*".

Il 28 gennaio è stata celebrata in tutta Europa la seconda *"Giornata europea della protezione dei dati personali"*. 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 volta a sensibilizzare i cittadini europei sui diritti legati alla tutela della vita privata e delle libertà fondamentali di ciascun individuo. L'Autorità italiana, per celebrare questo secondo appuntamento dedicato al tema *"Privacy e mondo della scuola"*, ha organizzato, in collaborazione con il Ministero della pubblica istruzione, incontri con le scuole superiori presso alcuni uffici scolastici regionali. Francesco Pizzetti a Torino, Giuseppe Chiaravalloti a Catanzaro, Mauro Paissan a Roma e Giuseppe Fortunato a Napoli, hanno trattato le tematiche della protezione dei dati personali legate al mondo giovanile, per stimolare l'attenzione dei giovani ad un uso consapevole delle nuove tecnologie. Durante gli incontri, ai quali hanno partecipato dirigenti scolastici, insegnanti e studenti è stato proiettato anche un video divulgativo sull'attività del Garante e sui temi generali legati alla *privacy*. A tutti gli intervenuti sono stati distribuiti *gadget* realizzati per l'evento.

Al *Data Privacy Day 2008*, equivalente americano della Giornata europea, svoltosi presso la Duke University (North Carolina) ha partecipato il segretario generale Buttarelli.

Il Laboratorio *Privacy* e Sviluppo (*v. par.* 21.9), istituito presso il Garante su iniziativa dell'avv. Giuseppe Fortunato e da lui stesso coordinato, è entrato a far parte dei cento *"casi di successo"* segnalati nel Terzo rapporto Eurispes sulle eccellenze in Italia.

21.7. IL SERVIZIO STUDI E DOCUMENTAZIONE

La redazione della Relazione annuale

Come negli anni scorsi, il Servizio studi ha coordinato la predisposizione del testo della *Relazione* annuale per la presentazione al Parlamento, avvalendosi della preziosa collaborazione della Redazione *web*.

L'attività in parola, specifico compito istituzionale del Garante, ha costituito occasione di analisi degli atti e delle iniziative adottati, nonché di catalogazione dei provvedimenti

e dei documenti nazionali e comunitari relativi all'anno in corso, utile anche alla pubblicazione dei testi medesimi sul sito istituzionale del Garante.

La versione pubblicata sul sito, come negli anni precedenti, è stata redatta in modo da consentire un collegamento ipertestuale con i documenti e la normativa citata, per garantire agli utenti qualità e rapidità della consultazione.

La funzione di studio e di supporto giuridico

Il Servizio studi ha continuato a svolgere attività di studio e ricerca, quale supporto interno, su materie di interesse dell'Autorità, anche su impulso del Collegio e del segretario generale.

In particolare sono stati svolti approfondimenti in materia di diritti dei detenuti, libertà di stampa e dignità degli indagati, Ced e dati concernenti trascrizioni di terreni, sanzioni amministrative (in particolare le modifiche al d.lg. n. 196/2003 introdotte dal d.l. n. 207/2008).

Tale attività ha riguardato anche provvedimenti e documenti di rilievo comunitario e internazionale, come nel caso dei pareri resi sulle *binding corporate rules*, strumenti utilizzabili nelle pratiche commerciali soprattutto dalle multinazionali, volti a garantire un livello adeguato di protezione dei diritti degli interessati nei Paesi terzi (vedi *par.* 11).

Gli approfondimenti sono stati effettuati, in collaborazione con i servizi interessati, su specifici punti problematici, quali la legge regolatrice applicabile e la giurisdizione competente anche alla luce del novellato art. 44 del Codice (*cfr.* art. 29, d.l. n. 112/2008).

Tali profili delle *binding corporate rules* sono stati altresì oggetto di un seminario, curato in collaborazione con il Servizio Relazioni Comunitarie e Internazionali, in ragione della novità e complessità della materia, nonché del prevedibile coinvolgimento dell'Ufficio sull'istruttoria funzionale all'adozione delle autorizzazioni di cui al citato art. 44 del Codice.

Il Servizio ha inoltre fornito una valutazione sull'opportunità di intervento in giudizio da parte della Presidenza del Consiglio dei Ministri sulla questione sollevata dal Tribunale di Roma circa la legittimità costituzionale dell'art. 137, comma 2, del d.lg. n. 196/2003 in relazione all'art. 15 della Costituzione, esprimendo dubbi sulla rilevanza della questione. La vicenda attiene alla pubblicazione a mezzo stampa di un articolo relativo alla

corrispondenza epistolare tra una detenuta e la sorella; il dubbio di costituzionalità del citato art. 137, comma 2, riguarda l'omessa esplicita previsione della necessità del consenso dell'interessato al trattamento dei dati relativi alla corrispondenza epistolare nell'esercizio dell'attività giornalistica.

Il Servizio ha altresì espresso un articolato parere negativo sulla richiesta di un operatore economico di accedere, ai sensi della legge n. 241/90, a documentazione attinente un *provvedimento* emesso dal Garante nei confronti di un operatore concorrente del richiedente, in relazione al trattamento di dati della clientela.

I pareri sulle leggi regionali

Nell'arco dell'anno il Servizio studi ha altresì fornito valutazioni idonee a formulare, unitamente a quelle dei servizi interessati, pareri alla Presidenza del Consiglio dei Ministri sulla conformità delle leggi regionali alla normativa nazionale in materia di protezione dei dati personali ai fini dell'impugnativa davanti alla Corte costituzionale ai sensi dell'art. 127 Cost..

Al riguardo si registra, come nei due anni precedenti, un sostanziale corretto svolgimento della potestà legislativa regionale, nonostante la difficoltà di individuare i confini della materia e quindi degli ambiti di titolarità tra Stato e Regioni.

In taluni casi, è stata segnalata la necessità di integrare il testo legislativo, suscettibile di applicazione non pienamente conforme alla normativa nazionale, con un atto di natura regolamentare ai sensi degli articoli 19 e 20 del Codice. In un solo caso, relativo ad una legge regionale in materia sanitaria, sono stati espressi dubbi di legittimità sulla prevista pubblicazione sul sito *web* dei nominativi e dei *curricula* degli aspiranti alle cariche dirigenziali e di alcune informazioni epidemiologiche, soprattutto in ragione dei limiti posti al legislatore regionale dalla normativa nazionale in materia di protezione dei dati personali.

I servizi interni di documentazione

Il Servizio studi ha continuato a curare la documentazione e l'aggiornamento del personale attraverso il costante monitoraggio della normativa nazionale e comunitaria nonché di quella internazionale, della giurisprudenza e della letteratura giuridica. Al riguardo ha utilizzato un criterio molto ampio per l'identificazione delle materie di interesse al fine di assicurare all'Ufficio un servizio efficace e tempestivo idoneo a costituire un utile strumento di lavoro e di riflessione.

In particolare ha curato la diffusione interna, tendenzialmente a cadenza bimestrale, del "*Repertorio di documentazione su diritti, libertà fondamentali e dignità della persona*", denominato "*Osservatorio privacy*" ovvero una raccolta delle sentenze pubblicate e dei commenti e riflessioni dottrinarie riguardante oltre che la protezione dati, profili istituzionali e questioni attinenti a personale ed amministrazione.

Con specifici *alert*, denominati *"Servizio studi news"*, sono state tempestivamente segnalate novità normative, giurisprudenziali e dottrinali, anche attraverso fonti giornalistiche, in materia di diritti e libertà delle persone e di protezione dei dati personali.

21.8. LA BIBLIOTECA

La Biblioteca, unità di articolazione della Segreteria generale, ha potenziato servizi e funzioni nell'ambito di un progetto di *Digital Library* e di *"organizzazione tecnologica delle conoscenze"*. Il progetto, pianificato in più fasi nell'arco del triennio 2008-2010, ha una duplice finalità: creare una nuova infrastruttura informatica di supporto del lavoro istruttorio dei dipartimenti; dare impulso alle attività di ricerca e di analisi nel campo degli interessi specifici della presidenza e del Collegio.

L'infrastruttura informatica, ideata in stretta collaborazione con il Dipartimento delle risorse tecnologiche, ha previsto almeno due livelli complementari di sostegno alla produttività dell'Ufficio: la modifica del sito *web* della Biblioteca, consultabile sulla rete Intranet del Garante, e centrato sulla integrazione delle risorse elettroniche disponibili *on-line*; la costruzione di una rete Intranet locale, accessibile nelle sale attrezzate della Biblioteca, e centrata sulla differenziazione delle risorse elettroniche in base agli interessi dell'utenza.

Questo vasto processo di razionalizzazione dell'informazione selezionata e gestita dalla Biblioteca si è concretizzato nell'allestimento di un *"portale"* Intranet strutturato sotto forma di un centro di servizi interdipartimentale e suddiviso in tre sezioni:

- il catalogo Opac *on-line* (per un totale di oltre quarantamila notizie bibliografiche), arricchito da un sistema sperimentale di classificazione costruito su un *thesaurus* di oltre mille termini e parole chiave associati alla *"protezione dei dati"*;

- i collegamenti integrati alle banche dati giuridiche italiane di primaria importanza sul piano generale;
- i collegamenti integrati su rete Intranet locale alle riviste elettroniche e alle principali banche dati giuridiche italiane e straniere ad elevato profilo specialistico.

La pianificazione della qualità della documentazione ha costituito anche il presupposto delle attività di studio e di elaborazione di *report* e *dossier* che la Biblioteca ha occasionalmente condotto e curato su indicazione della presidenza e dei componenti del Collegio: la duttilità dei dispositivi tecnologici di *"organizzazione delle conoscenze"* in tema di protezione dei dati si è dimostrata funzionale alla messa a punto di efficaci modelli interpretativi dei fenomeni, spesso contraddittori, che caratterizzano le tendenze attuali in questo settore.

Il patrimonio cartaceo della Biblioteca consiste attualmente di circa quattordicimila titoli monografici (circa seimiladuecento titoli sono in lingua italiana) con un incremento di oltre duemila unità rispetto al 2007 e di circa quattrocento titoli di periodici, dei quali centodieci correnti.

Il patrimonio della Biblioteca ha continuato ad essere cresciuto da alcune donazioni. Si segnala, al riguardo, la nuova donazione da parte del prof. Stefano Rodotà, presidente dell'Autorità dal 1997 al 2005, di circa cinquecento volumi a incremento del fondo costituito nel 2006.

Nel 2008 la Biblioteca ha riscontrato circa quattromila richieste di titoli in lettura da parte di utenti interni (+38% rispetto al 2007); circa duecento domande di accesso (-10%) e circa millecinquecento richieste di titoli in lettura da parte di utenti esterni (-17%); circa seimila contatti sul catalogo Opac (+50%) e circa ottomila ore di consultazione di banche dati da parte degli utenti esterni e interni (+430%).

21.9. Altre iniziative di comunicazione e ricerca

21.9.1. Il Laboratorio Privacy Sviluppo

Il Laboratorio *Privacy* Sviluppo, avviato con il favore del Collegio e coordinato dall'avv. Giuseppe Fortunato parallelamente alla sua attività istituzionale presso l'Autorità,

dal novembre 2006 si occupa dell'*"altra faccia della privacy"*: la 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 di ciascuno liberamente determinati. Il Laboratorio è un *"luogo"* di ricerca e studio al quale ciascuno può dare il proprio apporto 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 i lavori del Laboratorio hanno avuto inizio, è stato ancora arricchito nei contenuti, ma al tempo stesso, pur nella complessità degli argomenti, snellito nella forma e reso di più agevole consultazione. Il testo, efficacemente illustrato in un *Dvd* multimediale, è stato alla base di un nuovo percorso di incontri presso le Università italiane (fra cui Università Cattolica del Sacro Cuore, Centro Universitario Collalto, Università La Sapienza, Università di Chieti "G. D'Annunzio", Università LUM di Bari, Università di Modena e Reggio Emilia, Università Europea di Roma, Università di Campobasso, Sede italiana dell'Università di Washington). Uno specifico Seminario di due giorni è stato svolto presso il *master* in Gestione delle risorse umane della LUMSA Università di Roma. Sono, inoltre, continuati gli incontri presso gli Istituti superiori – e in qualche caso anche scuole elementari, come in istituti di Ercolano e Montesarchio – che hanno avuto l'apprezzamento della Commissione bicamerale per l'infanzia. Si sono altresì effettuati incontri presso Comuni (Foggia, Cagliari, Livorno, Montesarchio) e Ordini professionali. Uno stimolante evento si è svolto su *Second Life* (nella virtuale *"Piazza di Spagna"*) con ampia partecipazione dei fruitori di tale piattaforma *web*, prevalentemente giovani.

Il Laboratorio è divenuto un'iniziativa internazionale con la partecipazione delle Autorità nazionali per la protezione dei dati personali di Spagna, Grecia, Irlanda, Islanda, Malta, Inghilterra, Israele, Polonia, Repubblica Ceca, Thailandia, Nuova Zelanda, Cipro, Croazia, Lettonia, Ungheria, Macedonia, Romania, Slovenia, Slovacchia, Bulgaria, Lituania, Estonia, e anche autorità regionali come quelle della Comunità di Madrid e della Catalogna.

Il Garante Europeo per la protezione dei dati personali ha voluto sostenere l'iniziativa con un messaggio ufficiale con cui ha definito l'iniziativa *"originale e interessante"*.

All'avv. Giuseppe Fortunato, coordinatore del Laboratorio, sono state affidate a Madrid le conclusioni nel *Seminar on Data Protection Best Practices in European Public Services* anche in seguito al quale sono pervenuti, nel corso del 2008, apprezzati contributi da numerose personalità. Le tematiche del Laboratorio, anche tramite la traduzione in inglese dell'apposito inserto della *Newsletter* del Garante, sono state oggetto di diffusione presso le *Law School* dell'Università di Miami e dell'Università di Washington (Seattle).

Con l'Università di Barcellona, il Laboratorio ha superato le selezioni, articolate in più fasi, di apposito Programma Jean Monnet della Commissione Europea.

Il Laboratorio è stato premiato nel *"Rapporto Nostra Eccellenza"* dell'Eurispes quale caso di eccellenza per i risultati raggiunti.

Sul testo LA SVOLTA sono state proficuamente discusse undici tesi di laurea e di *master* presso varie Università in varie discipline e sono state coinvolte associazioni professionali o comunque dedite alla tutela della persona.

Fra le oltre 4000 associazioni che partecipano attualmente alle attività del Laboratorio, riunite nella coalizione *"Civicrazia"*, le venti che garantiscono permanentemente i maggiori *standard* di impegno fanno parte del Comitato Guida del Laboratorio. LA SVOLTA, con il suo 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).

Molteplici personaggi del mondo della cultura, delle arti e dello spettacolo (le cui interviste sono state pubblicate nel sito *web* del Laboratorio) hanno espresso il proprio apprezzamento all'iniziativa.

Con la nuova partecipazione dell'avv. Giuseppe Fortunato alla trasmissione *"10 minuti di …"* su Rai Uno è stato illustrato il concetto di *privacy*, inteso non più e non solo come *"libertà da"*, ma anche come *"libertà per"* e, in particolare, come lo sviluppo della propria personalità sia condizione essenziale per l'esercizio delle libertà fondamentali.

Agli accordi con la Scuola superiore della pubblica amministrazione locale si sono

aggiunte Convenzioni del Laboratorio con il Consiglio nazionale dell'Ordine dei giornalisti, con il Consiglio nazionale dell'Ordine degli psicologi, con la Federazione relazioni pubbliche italiane, con il Coordinamento delle libere attività professionali, con l'Agenzia autonoma per la gestione dell'albo dei segretari comunali, con l'Unione dei segretari comunali e provinciali, che hanno comportato comuni attività di promozione del messaggio LA SVOLTA e di sviluppo della Civicrazia nell'ambito delle specifiche attività professionali.

La Conferenza Nazionale dei Garanti delle persone detenute ed ex detenute ha inserito nel suo statuto la partecipazione al Laboratorio e l'adesione al messaggio LA SVOLTA e molteplici sono stati gli approfondimenti in tale ambito per favorire il recupero e il reinserimento sociale.

Il Laboratorio, anche tramite il proprio sito *web www.laboratorioprivacysviluppo.it* raccoglie i contributi di quanti aderiscono alle sue iniziative e ne valorizzano il messaggio di piena espressione della persona umana, di sinergie associative e di pubbliche istituzioni sempre più al servizio del cittadino.

Lo sviluppo di tali attività ha comportato una strutturazione territoriale con appositi referenti in ciascuna Regione presso università, ordini professionali o enti locali.

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 di 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 2008 le entrate di competenza ammontano complessivamente a 20,9 milioni di euro, con un incremento di 0,3 milioni di euro rispetto al precedente esercizio.

La voce più significativa, pari a euro 18,2 milioni di euro, è rappresentata dal contributo erogato dallo Stato che ha fatto registrare, tuttavia, una riduzione di circa 0,6 milioni di euro rispetto al 2007, per effetto delle restrizioni previste dalla legge finanziaria e dai relativi provvedimenti di attuazione. Tale riduzione, tuttavia, risulta compensata da un corrispondente incremento di proventi propri e rimborsi che hanno consentito all'Autorità di registrare, nel complesso, somme in entrata di poco superiori a quelle del precedente esercizio.

Le spese ascrivibili alla competenza del 2008 sono state pari a complessivi 19,7 milioni di euro, delle quali la parte più significativa, pari a circa 19,1 milioni di euro, attiene alle spese correnti per il funzionamento dell'Ufficio e per il corretto svolgimento delle attività istituzionali, mentre la restante parte, pari a 0,6 milioni di euro, riguarda le somme destinate agli acquisti di beni durevoli.

L'entità della spesa fa registrare un incremento rispetto all'anno precedente nella misura di circa 1,3 milioni di euro, dovuto in misura prevalente agli oneri per il perso-

nale, per effetto sia dell'immissione in organico di nuove unità, sia del riconoscimento delle indennità di fine rapporto al personale cessato dal servizio nel corso dell'anno, sia dell'adeguamento delle tabelle retributive.

Ulteriori incrementi di spesa, di natura non ricorrente, sono ascrivibili agli oneri sostenuti per l'organizzazione dell'annuale conferenza tra le autorità europee che nel 2008 si è svolta a Roma.

Ha contribuito, infine, all'incremento degli oneri complessivi di funzionamento la spesa sostenuta per l'acquisizione in locazione di una nuova unità immobiliare nello stesso stabile sede del Garante, per sopperire ad ineludibili esigenze di ampliamento degli uffici, a seguito del completamento di procedure di selezione avviate da tempo.

Il rispetto degli indirizzi di contenimento della spesa previsti dalle recenti leggi finanziarie non ha comportato ridimensionamenti significativi dell'attività amministrativa, in quanto si è avuta la possibilità di sopperire alle minori risorse finanziarie correnti assicurate dal finanziamento statale mediante maggiori risorse proprie e attraverso l'utilizzo di una parte delle economie realizzate negli anni pregressi.

L'ultima tabella allegata alla presente *Relazione* riassume sinteticamente i valori finanziari di competenza dell'esercizio 2008 e di quello precedente.

In particolare, sono evidenziate le risorse finanziarie complessivamente accertate, tra cui quelle trasferite dallo Stato, nonché le somme complessivamente impegnate nel periodo di riferimento.

La gestione amministrativa, pur nel rispetto dei vincoli di bilancio dettati dalle disposizioni legislative emanate sulla materia, è stata indirizzata ad un generale miglioramento delle funzionalità operative dell'Ufficio e ad un potenziamento di alcuni settori strategici dell'Autorità quali quello della vigilanza e del controllo, da un lato, e degli affari giuridici, legali e normativi, dall'altro lato.

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 che ha affiancato il personale in organico.

È proseguita, inoltre, la collaborazione con il Nucleo speciale funzione pubblica e *pri-*

vacy, operativo presso la stessa Guardia di finanza, il cui personale specializzato procede direttamente all'esecuzione delle attività ispettive.

Le entrate connesse all'attività ispettiva e di controllo spettanti al Garante, ancorché non incassate nell'anno di riferimento, ammontano a circa 0,3 milioni di euro e fanno registrare nel 2008 un tendenziale *trend* di crescita rispetto agli anni precedenti. Tale importo, tuttavia, continua ad assumere un valore marginale rispetto all'entità complessiva delle entrate che affluiscono al bilancio dell'Autorità.

Va evidenziato, in proposito, che le risorse destinate al bilancio del Garante per effetto delle sanzioni irrogate in sede di controllo scontano rallentamenti procedurali, non dipendenti dagli adempimenti posti in essere dall'Ufficio, che hanno determinato in più occasioni l'impossibilità di recuperare la quota parte delle somme teoricamente spettanti. Tali difficoltà si ritiene possano essere superate alla luce delle disposizioni contenute nel decreto-legge 30 dicembre 2008, n. 207, convertito, con modificazioni, dalla legge 27 febbraio 2009, n. 14, sia in ordine alla rideterminazione delle modalità di acquisizione delle somme, sia riguardo all'entità delle sanzioni stesse.

Tra le attività rientranti negli obiettivi programmatici dell'Autorità, una particolare attenzione ed un impegno significativo sono stati dedicati 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.

A tal fine l'Autorità ha partecipato attivamente ad eventi e manifestazioni, anche di rilievo internazionale, per divulgare la conoscenza e promuovere idonee campagne informative sui diritti dei cittadini, ed ha organizzato l'importante conferenza svoltasi in primavera a Roma tra i rappresentanti delle Autorità europee.

L'attività contrattuale per il 2008 si è svolta, come di consueto, al servizio delle esigenze dell'Ufficio, principalmente nelle aree delle risorse tecnologiche, delle relazioni con i *media* e delle attività di manutenzione della sede.

Fra le attività più rilevanti si evidenziano:

- il contributo allo svolgimento della *Spring Conference* dei Garanti della Comunità Europea a Roma, in sinergia costante con la società organizzatrice, individuata nel-

l'anno precedente mediante ricerca di mercato, e con le varie funzioni interne coinvolte;

- la gara europea volta a selezionare un nuovo fornitore del servizio di trasporto con conducente;
- una ricerca di mercato per la realizzazione, nel nuovo e molto più capiente formato *Dvd*, della banca dati del Garante, elemento fondamentale dell'attività di comunicazione dell'Ufficio; nell'occasione si è definito, in collaborazione con il Servizio interessato, un nuovo capitolato, che, insieme alle caratteristiche intrinseche del nuovo supporto fisico, consentisse di porre le premesse per un salto di qualità del prodotto;
- il coordinamento delle attività di adeguamento tecnologico alle specifiche esigenze dell'Ufficio degli impianti (elettrico, di rete e telefonico) di un appartamento da condurre in locazione;
- il rinnovo del contratto di telefonia mobile, che ha portato ad una marcata diminuzione delle tariffe di traffico in voce (con previsione a consuntivo di un risparmio del 40% circa su dodici mesi), al noleggio a titolo gratuito e per una durata di due anni dei cellulari, coperti da polizza *kasko*, e a nuove e più economiche tariffe per il traffico dati, in funzione dei volumi di traffico sviluppati, particolarmente convenienti per il collegamento alla rete tramite *pc* portatile;
- la revisione dei capitolati relativi alle manutenzioni e le conseguenti ricerche di mercato, che hanno portato ad un ampio cambiamento dei fornitori e ad un contestuale miglioramento del servizio.

22.2. LE NOVITÀ LEGISLATIVE E REGOLAMENTARI E L'ORGANIZZAZIONE DELL'UFFICIO

Si è riferito nel paragrafo 2.2 delle modifiche apportate alla durata del mandato del Presidente e dei componenti il Collegio del Garante (sette anni non rinnovabili). Di pare durata deve intendersi anche il mandato del segretario generale (art. 7 del regolamento 1/2000 [doc. *web* n. 1098801]), incarico rivestito dal marzo 2009 dal consigliere di Stato Filippo Patroni Griffi.

Nel 2008 l'Autorità ha dato concreta attuazione alla *deliberazione* di incremento della pianta organica [doc. *web* n. 1429691] che, in conformità a quanto previsto dalla legge finanziaria 2007 (l. 27 dicembre 2006, n. 296), ha potenziato di venticinque unità la dotazione organica dell'Ufficio.

Come già rilevato nella *Relazione* 2007, tale incremento è prioritariamente volto a perseguire il migliore espletamento dei compiti istituzionali demandati al Garante e, in particolare, di quelli di controllo e vigilanza sul rispetto della normativa in materia di trattamento dei dati personali (art. 154, comma 1, lett. *a*), del Codice), dando ulteriore impulso alle iniziative finalizzate ad accrescere 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.

L'articolato programma di assunzioni predisposto dall'Autorità e, in parte già attuato nel corso dello stesso 2008, persegue l'obiettivo di potenziare la capacità di risposta dell'Ufficio del Garante, incrementando anche le risorse professionali disponibili nei settori della sicurezza informatica e della comunicazione elettronica. In coerenza con questo obiettivo, l'Autorità – come si dirà in seguito – ha bandito nuovi concorsi e procedure selettive per diverse qualifiche e tipologie contrattuali, per complessivi ventitrè posti.

Il consolidamento dell'organico dell'Autorità costituisce il presupposto per una successiva operazione di semplificazione e razionalizzazione del modello organizzativo dell'Ufficio, per taluni profili già avviata attraverso una ricognizione dei compiti e delle procedure svolte dai dipartimenti amministrativi.

La riorganizzazione della struttura esistente prevede altresì, all'esito di una breve sperimentazione esauritasi nel corso del 2008, la contestuale riduzione delle unità temporanee di primo livello anche in attuazione dei regolamenti adottati dal Garante nel dicembre del 2007 (*G.U.* 9 gennaio 2008, n. 7) recanti la disciplina dei procedimenti posti a tutela degli interessati secondo ben precise linee di priorità, modalità procedurali e termini.

È stata altresì avviata la procedura di modifica della pianta organica volta ad incrementare la dotazione organica dei funzionari.

22.3. IL PERSONALE E I COLLABORATORI ESTERNI

Agli inizi del 2008 sono stati banditi concorsi pubblici finalizzati al reclutamento di personale appartenente alle aree, rispettivamente, dirigenziale nella misura di un'unità, direttiva nella misura di sette unità – di cui cinque per l'area giuridico-amministrativa e due per l'area informatica – e operativa nella misura di otto unità.

In alcuni dei predetti bandi sono state previsti alcuni posti riservati (nella misura di due posti in quello per funzionario giuridico-amministrativo e di un posto in quello per funzionario informatico, nonché di tre posti in quello per 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, o 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 finalizzate al reclutamento, con contratto a tempo determinato, di due funzionari con profilo informatico 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.

Le predette procedure, ad eccezione di quella da ultimo citata, si sono concluse tra la fine del 2008 e gli inizi del 2009. Ciò ha consentito di realizzare l'importante obiettivo di incrementare l'esiguo organico di cui l'Autorità ha potuto disporre nell'immediato passato.

Nel periodo considerato si sono svolti alcuni *stage* in collaborazione con diverse università.

Al 31 dicembre 2008 l'Ufficio poteva contare su un organico, a diverso titolo, di novantaquattro unità, di cui novanta in servizio, al quale va aggiunto un contingente di personale a contratto di tredici unità, alcune delle quali peraltro assunte per brevi periodi.

A fronte di questi dati, l'incremento realizzatosi all'esito delle predette procedure con-

corsuali e selettive appare particolarmente significativo ove si consideri che sono state immesse in servizio complessivamente diciotto unità, di cui solo tre con contratto a tempo determinato, mentre sono *in itinere* ulteriori due assunzioni e le procedure per incrementare di quattro unità la dotazione organica dei funzionari.

Nel periodo considerato si è reso necessario ricorrere ad alcuni incarichi di collaborazione occasionali, in particolare per la predisposizione dei flussi documentali necessari per attuare i regolamenti interni del Garante sui procedimenti aventi rilevanza esterna previsti dal Codice, nonché per attività di supporto ai dipartimenti amministrativi in tema di bilanci e di trattamenti pensionistici e ai componenti del Garante.

L'Autorità si è avvalsa delle convenzioni Consip, conferendo in *insourcing* alcune attività di natura esecutiva che non richiedono un apporto lavorativo di elevato contenuto professionale (*ad es.*, per l'attività di portineria e per compiti ausiliari).

Nel periodo considerato, l'Autorità si è avvalsa, altresì, di un servizio 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.

22.4. IL SETTORE INFORMATICO E TECNOLOGICO

Nel 2008 il Dipartimento risorse tecnologiche ha continuato l'attività strumentale volta allo sviluppo del sistema informativo dell'Autorità, di cui ha curato direttamente la manutenzione e il funzionamento, fornendo assistenza agli utenti, pur nel crescente coinvolgimento nei processi lavorativi dell'Autorità, in forma di consulenza interna nell'ambito della trattazione di procedimenti o nell'elaborazione di provvedimenti e pareri dell'Autorità, in collaborazione con le unità organizzative dell'Ufficio competenti dell'area giuridica.

Il personale del Dipartimento ha partecipato nel contempo alle attività ispettive, in collaborazione con il Dipartimento attività ispettive e sanzioni, con la realizzazione di accessi a banche dati, con l'analisi e lo studio dei materiali acquisiti e con la stesura di rapporti. Rilevante è stata anche la partecipazione a gruppi di lavoro, seminari e convegni

internazionali, in collaborazione con il Servizio relazioni comunitarie e internazionali, e alle attività di divulgazione e comunicazione dell'Autorità.

Sviluppo del sistema informativo e dei servizi ICT

Successivamente all'approvazione dei regolamenti sui procedimenti amministrativi dell'Autorità, nel giugno 2008 è stata avviata l'implementazione del sistema informatico per la gestione del *workflow* documentale, che si integrerà con il sistema di protocollo informatico già disponibile consentendo, una ancora più agevole trattazione informatica dei procedimenti.

È stata ulteriormente sviluppata la piattaforma di reportistica *on-line* per l'Ufficio, integrandola con i *database* e con i sistemi applicativi in funzione di una maggiore fruibilità delle informazioni sulle prestazioni, mentre è stata avviata la digitalizzazione dei servizi della Biblioteca, con particolare riferimento ai *database on-line* e alle opere fruibili in abbonamento sulla rete.

È proseguita con accresciuta intensità l'attività di *help-desk* interno e di assistenza tecnica per l'intero sistema informativo e per le esigenze informatiche dell'Ufficio.

Di particolare rilievo, nell'ambito degli sviluppi del sistema informativo, l'adesione dell'Autorità al Sistema pubblico di connettività (Spc) previsto dal codice dell'amministrazione digitale, che consente un efficiente funzionamento dei servizi *on-line* dell'Autorità, mentre con l'adesione al progetto Cns (Carta nazionale dei servizi) del Cnipa, si è perseguito il fine di dotare tutto il personale di *smart card* avanzate con possibilità di gestire certificati digitali emessi da diverse *Certification Authority*, anche interne, per scopi di firma digitale e *strong authentication*, oltre che fungere da *badge* per il rilevamento delle presenze.

La realizzazione di un moderno sistema di *streaming* di contenuti audiovisivi, basato su una piattaforma *standard de facto*, ha consentito di andare incontro alle esigenze di fruizione dell'Ufficio in corrispondenza di eventi che hanno visto la presenza o la partecipazione attiva dell'Autorità. Tra questi, la *Spring Conference* 2008, organizzata dal Garante, nel cui ambito il Dipartimento ha realizzato e gestito gli aspetti tecnici informatici e la connettività.

Impegno per la sicurezza informatica dell'Ufficio

Anche nel corso del 2008 nessun incidente informatico 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 attraverso canali di rete o trasferimento da supporti, né si sono verificate perdite di dati cui non sia stato possibile porre rimedio con le ordinarie procedure di *backup* e *recovery*.

Nell'ambito della formalizzazione di procedure esistenti e dell'individuazione di ulteriori margini di miglioramento è stata avviata un'attività di analisi propedeutica alla certificazione ISO 27001 delle procedure di gestione della sicurezza delle informazioni nel perimetro dell'Ufficio, unitamente a un'attività di *gap analysis* secondo i *Common Criteria* delle applicazioni informatiche esposte su rete pubblica.

Attività di consulenza e cooperazione interne ed esterne

Il Dipartimento ha fornito quotidiano supporto di consulenza alle unità dell'area giuridica dell'Ufficio, provvedendo all'analisi tecnica necessaria nella fase istruttoria dei procedimenti e dei provvedimenti dell'Autorità, curando con relazioni, note informative l'approfondimento di argomenti a contenuto informatico-tecnologico, partecipando a incontri e riunioni di lavoro in cui sono stati affrontati profili tecnologici di diversi casi affrontati dall'Autorità, tra i quali si evidenziano: la protezione dei dati e la sicurezza dei *social network*s; i servizi di posta elettronica e il fenomeno dello *spamming*; il rapporto tra dati anonimi e dati personali e i rischi di reidentificazione; le tecniche di *data mining*, di *data-warehousing*, di profilazione.

Per quanto riguarda la partecipazione all'azione amministrativa dell'Autorità, si citano, in particolare, i contributi dati nel corso dell'elaborazione dei provvedimenti in tema di *data retention* adottati anche ai sensi dell'art. 132 del Codice nel gennaio 2008 e successivamente aggiornati in seguito all'introduzione di modifiche legislative; dei provvedimenti di divieto di conservazione dei dati di traffico di navigazione *web* rivolti nel gennaio 2008 ad alcuni fornitori di servizi di accesso a Internet in seguito all'accertamento, a seguito di ispezioni, della presenza di cospicue raccolte di dati di traffico telematico presso alcuni operatori.

Sempre in tema di *data retention*, il Dipartimento ha contribuito all'elaborazione legislativa del d.lg. 109/2008 presso il Ministro per le politiche comunitarie, con la proposta di introduzione di numerazioni univoche per gli accessi alla rete Internet, partecipando

successivamente al gruppo di lavoro presso il Dipartimento della pubblica sicurezza del Ministero dell'interno sull'applicazione della disciplina tecnica introdotta e sul suo impatto sull'attività giudiziaria e di pubblica sicurezza.

Tra gli altri lavori più significativi del Dipartimento nel corso del 2008 si segnalano i contributi forniti all'elaborazione dei provvedimenti del Garante in tema di: divieto di trattamento dei dati relativi agli indirizzi Ip e ad altre informazioni riguardanti le connessioni a reti *peer-to-peer* nell'ambito di azioni giudiziarie di tutela del diritto d'autore (*Provv.* 28 febbraio 2008 [doc. *web* n. 1495246]); prescrizioni all'Agenzia delle entrate relative all'adeguamento dei sistemi di sicurezza dell'anagrafe tributaria rispetto all'acceso alle informazioni da parte di enti esterni (*Provv.* 18 settembre 2008 [doc. *web* n. 1549548]); semplificazione di taluni adempimenti in ambito pubblico e privato rispetto a trattamenti per finalità amministrative e contabili (*Provv.* 19 giugno 2008 [doc. *web* n. 1526724]); semplificazione delle misure minime di sicurezza, individuando tra le misure previste dal *"Disciplinare tecnico"*, Allegato B. al Codice quelle suscettibili di applicazione semplificata (*Provv.* 27 novembre 2008 [doc. *web* n. 1571218]); rifiuti di apparecchiature elettriche ed elettroniche (Raee), nel cui ambito sono state individuate modalità sicure di cancellazione *software* dei dati e procedure di demagnetizzazione (*Provv.* 13 ottobre 2008 [doc. *web* n. 1571514]); linee-guida per i trattamenti di dati personali nell'ambito delle sperimentazioni cliniche di medicinali (*Provv.* 24 luglio 2008 [doc. *web* n. 1544575]); verifica preliminare *ex* art. 17 del Codice in tema di riconoscimento vocale e gestione di sistemi informatici (*Provv.* 28 febbraio 2008 [doc. *web* n. 1501094]); pareri resi dal Garante su provvedimenti del Governo e di pubbliche amministrazioni riguardanti l'attuazione del codice dell'amministrazione digitale.

Il Dipartimento ha inoltre curato direttamente l'elaborazione delle prescrizioni relative agli amministratori di sistema (*Provv.* 27 novembre 2008 [doc. *web* n. 1577499]) e ha offerto continuo supporto, in collaborazione con l'Urp, nelle risposte a quesiti e richieste di chiarimento, provvedendo all'elaborazione delle *Frequently asked questions* (*Faq*) pubblicate sul sito ufficiale dell'Autorità e contribuendo all'analisi delle richieste pervenute a seguito della consultazione pubblica avviata nell'aprile 2009.

Contributi all'attività ispettiva

Nel corso del 2008, nonostante l'accresciuta mole di lavoro sul fronte della consulenza interna, il Dipartimento ha continuato in modo proficuo la collaborazione con le altre unità organizzative dell'Ufficio e, in particolare, con dipartimenti giuridici e il Dipartimento attività ispettive e sanzioni.

Il Dipartimento ha contribuito significativamente allo svolgimento di ispezioni e accertamenti in collaborazione con il Dipartimento attività ispettive e sanzioni, partecipando, tra le altre, alle verifiche ispettive sul sistema informativo della fiscalità gestito dall'Agenzia delle entrate, contribuendo all'individuazione delle criticità e delle conseguenti misure di sicurezza e di adeguamento da mettere in atto relativamente agli accessi da parte degli enti esterni alla *cd. "anagrafe tributaria"* (poi oggetto di prescrizioni nell'ambito dei *provvedimenti* adottati dal Garante il 18 settembre 2008 [doc. *web* n. 1549548] e il 26 marzo 2009 [doc. *web* n. 1605576].

Ha inoltre partecipato agli accertamenti ispettivi sugli istituti di credito, verificando nello specifico la struttura degli archivi, le tipologie di informazioni trattate, le procedure riguardanti gli accessi ai sistemi e alle applicazioni, i sistemi di autenticazione, le abilitazioni e le autorizzazioni degli utenti, le applicazioni utilizzate, le misure di sicurezza; ad accertamenti sugli operatori telefonici; alle attività ispettive in materia di riscossione.

Contributi all'attività internazionale

Ha partecipato all'attività internazionale nell'ambito dell'Ue *Working Party* 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 del *Technology Subgroup* nel WP Art. 29. Ha contribuito alla stesura della *checklist* per le attività di verifica concordate a livello comunitario relativamente al recepimento, da parte degli Stati membri, della direttiva europea 24/2006/Ce sulla *data retention* di dati di traffico telefonico e telematico, nonché alle attività connesse alla revisione del quadro normativo e *privacy*.

22.5. IL MONITORAGGIO DELL'EFFICACIA E DELL'EFFICIENZA E IL SUPPORTO AL CONTROLLO INTERNO

Nel corso del 2008 è proseguito, a cura della "Unità *raccolta dati, flussi informativi e supporto al controllo interno*", il monitoraggio dell'attività svolta dalle unità organizzative dell'area giuridica dell'Ufficio.

La rilevazione, con cadenza mensile, fornisce dati analitici sul volume di affari assegnato a ciascuna unità organizzativa e sulle trattazioni effettuate, correlate alla concreta disponibilità delle risorse umane, utilizzate nei diversi processi di lavoro.

Nella logica della *"gestione per obiettivi"*, i *report* prodotti sono volti alla programmazione dei dirigenti, prevenendo eventuali *"picchi"* di domanda, consentendo all'Autorità, ad ogni livello di responsabilità, di adottare con tempestività le misure organizzative più opportune.

Nel periodo considerato, è stata avviata una riflessione per migliorare l'attività di rilevazione, in considerazione dell'esigenza di assicurare un monitoraggio costante dei procedimenti amministrativi aventi rilevanza esterna (disciplinati dai regolamenti interni 1 e 2/2007) e, in sintonia con le indicazioni fornite dal Servizio di controllo interno, di avviare una rilevazione dei prodotti e dei processi di lavoro – distinti per tipologie di procedimenti – estesa a tutte le unità organizzative dell'Ufficio.

23. Dati statistici (*)

1. Sintesi delle principali attività dell'Autorità

SINTESI DELLE PRINCIPALI ATTIVITÀ DELL'AUTORITÀ	
Numero complessivo dei provvedimenti collegiali adottati	524
Ricorsi decisi (art. 145 del Codice)	321
Pareri a Presidenza del Consiglio dei ministri e ministeri (art. 154 del Codice)	32
Altri provvedimenti collegiali sul trattamento dei dati personali	171
Notificazioni pervenute nell'anno 2008	1246
Notificazioni pervenute dal 2004 al 31 dicembre 2008	16512
Violazioni amministrative contestate	338
Sanzioni applicate con ordinanza di ingiunzione	52
Violazioni penali segnalate all'autorità giudiziaria	12
Riscontri a segnalazioni e reclami	5252
Risposte a quesiti	1058
Ricorsi (definiti) ex art. 152 del Codice	198
Opposizioni (definite) a provvedimenti del Garante	69
Accertamenti e controlli efffettuati direttamente presso i titolari del trattamento	500
Altre richieste ai sensi dell'art. 157 del Codice	277
Prescrizioni sulle misure minime di sicurezza (a fini di estinzione del reato)	26
Provvedimenti su verifiche preliminari per trattamenti che presentano rischi specifici	2
Comunicazioni al Garante su flussi di dati tra p.a. o in temi di ricerca	19
Pareri a soggetti pubblici sul trattamento dei dati sensibili e giudiziari	14
Risposte ad atti di sindacato ispettivo e di controllo	0

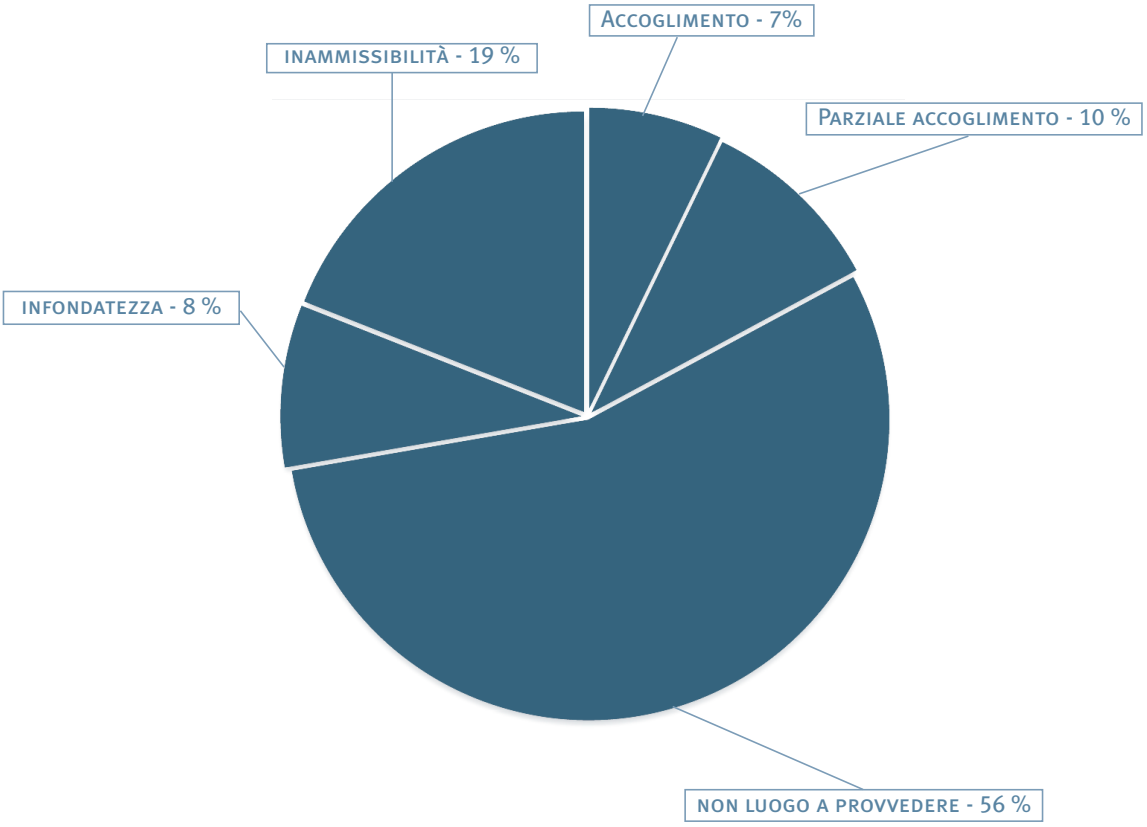
2. Altre attività

ALTRE ATTIVITÀ DELL'AUTORITÀ	
Comunicati stampa	54
Newsletter	19
Cd-rom (edizioni pubblicate)	1
Notiziario bimestrale	6
Dépliant	1
Conferenze internazionali	4

(*) Tutti i dati statistici riportati nella presente sezione sono riferiti all'anno solare 2008. Singole note indicano altri periodi o situazioni e casi specifici. I dati delle tabelle 8, 9, 10 si riferiscono ai fascicoli istituiti presso l'Ufficio

3. Tipologia delle decisioni sui ricorsi (tabella e grafico)

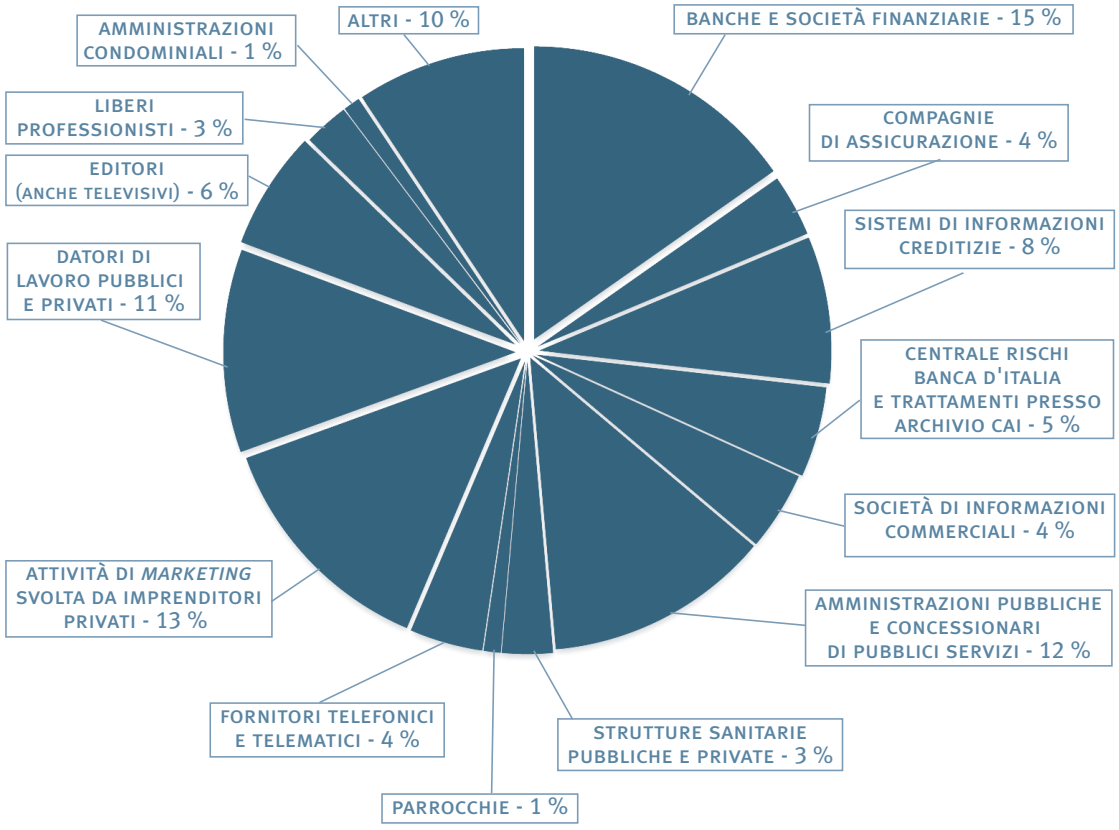
DECISIONI SU RICORSI	
TIPI DI DECISIONE (1)	NUMERO RICORSI
Accoglimento	23
Parziale accoglimento	32
Non luogo a provvedere (2)	177
Infondatezza	28
Inammissibilità	61
Totale	**321**



(1) Le decisioni sui ricorsi possono contenere più statuizioni in base alle diverse richieste presentate: la statistica prende in esame, in tali casi, la statuizione più "favorevole"
(2) Casi nei quali le richieste del ricorrente sono state soddisfatte nel corso del procedimento

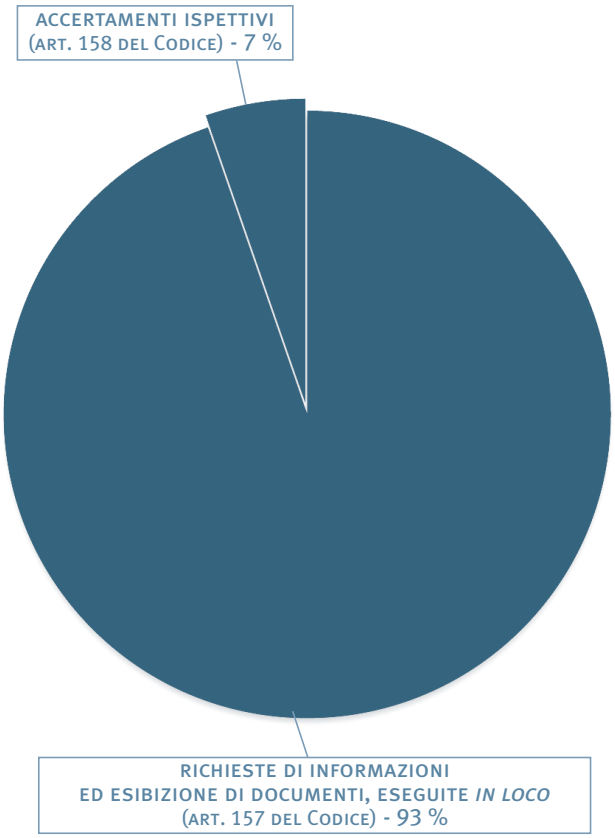
CATEGORIA DI TITOLARI	NUMERO RICORSI
Banche e società finanziarie	49
Compagnie di assicurazione	11
Sistemi di informazioni creditizie	26
Centrale rischi Banca d'Italia e trattamenti presso archivio Cai	16
Società di informazioni commerciali	14
Amministrazioni pubbliche e concessionari di pubblici servizi	40
Strutture sanitarie pubbliche e private	9
Parrocchie	3
Fornitori telefonici e telematici	13
Attività di *marketing* svolta da imprenditori privati	42
Datori di lavoro pubblici e privati	36
Editori (anche televisivi)	21
Liberi professionisti	8
Amministrazioni condominiali	3
Altri	30
Totale	**321**

4. Suddivisione dei ricorsi in relazione alla categoria di titolari del trattamento (tabella e grafico)



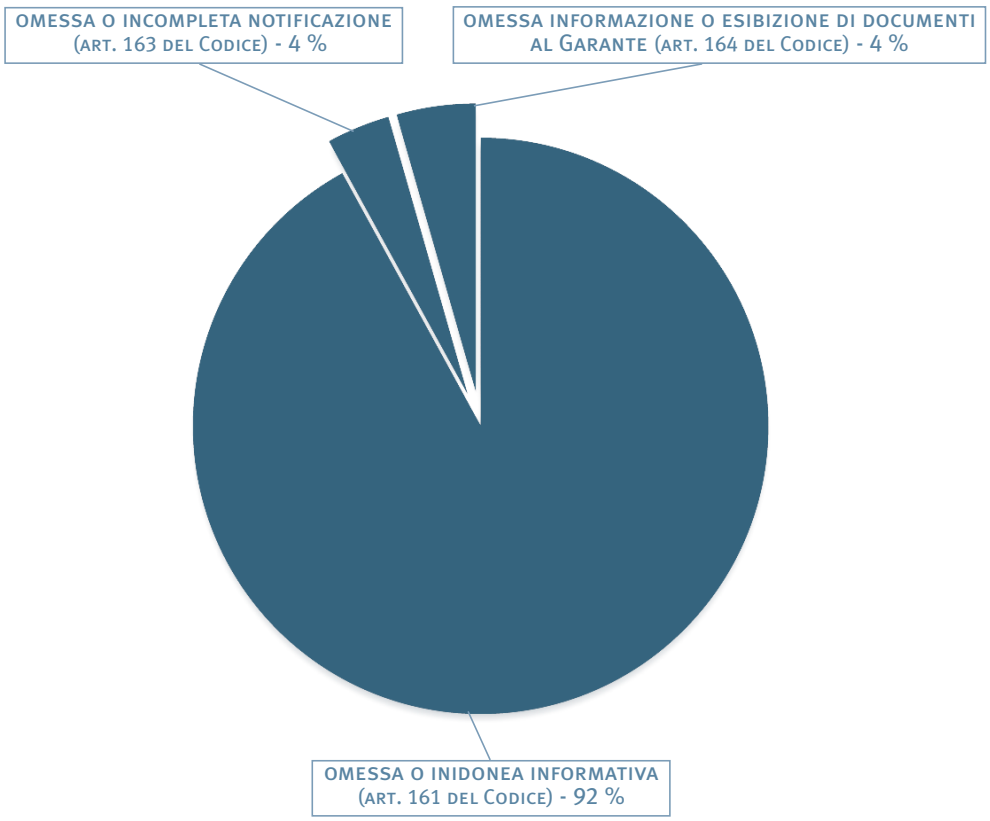
5. Accertamenti e controlli eseguiti (tabella e grafico)

ACCERTAMENTI E CONTROLLI ESEGUITI DIRETTAMENTE PRESSO TITOLARI DEL TRATTAMENTO	
Richieste di informazioni ed esibizione di documenti, eseguite *in loco* (art. 157 del Codice)	466
Accertamenti ispettivi (art. 158 del Codice)	34
Totale	**500**



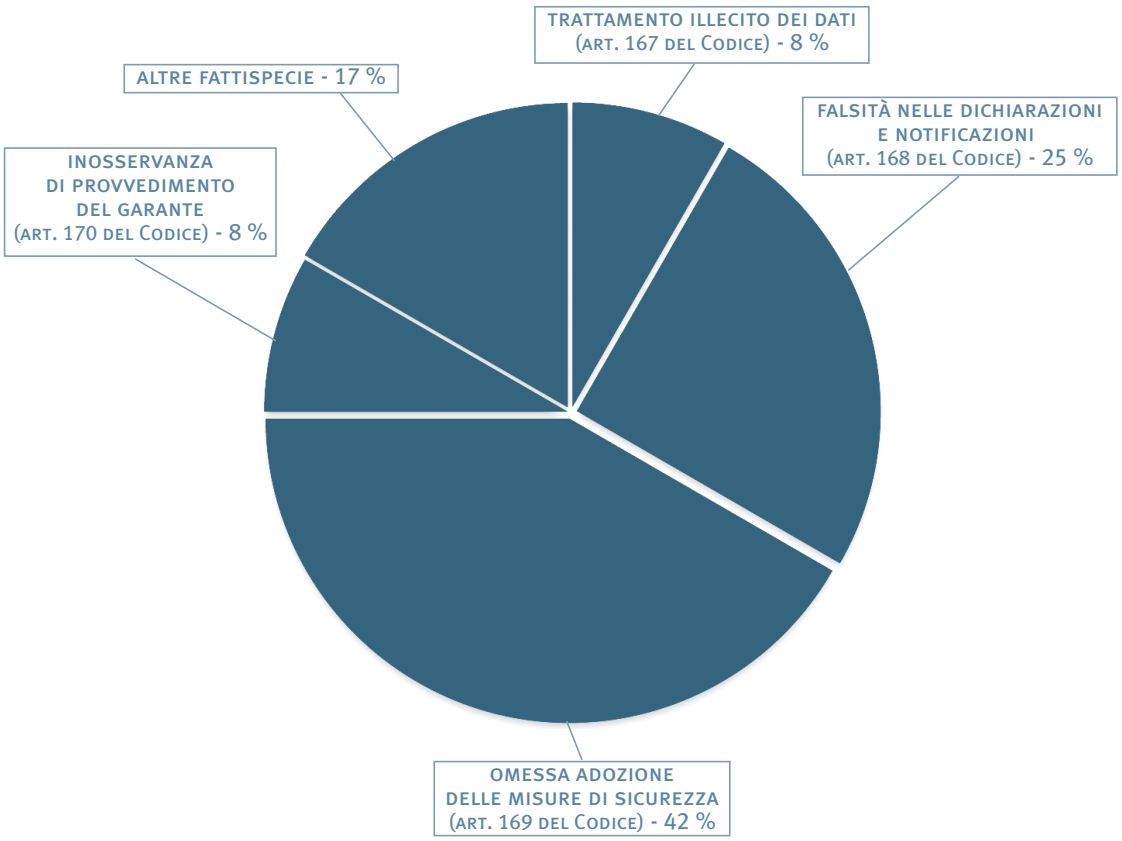
VIOLAZIONI AMMINISTRATIVE CONTESTATE	
Omessa o inidonea informativa (art. 161 del Codice)	311
Omessa o incompleta notificazione (art. 163 del Codice)	12
Omessa informazione o esibizione di documenti al Garante (art. 164 del Codice)	15
Totale	**338**
Somme versate a titolo di pagamento ridotto	**1.061.843**

6. Violazioni amministrative contestate (tabella e grafico)



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)	1	1
Falsità nelle dichiarazioni e notificazioni (art. 168 del Codice)	3	3
Omessa adozione delle misure di sicurezza (art. 169 del Codice)	5	7
Inosservanza di provvedimento del Garante (art. 170 del Codice)	1	1
Altre fattispecie	2	2
Totale	**12**	**14**
Ammontare complessivo delle somme pagate in sede di "ravvedimento operoso" (art. 169 del Codice)		**335.329**



8. Pareri (art. 154, comma 4, del Codice)

PARERI (ART. 154, COMMA 4, DEL CODICE)	
TEMI	RISCONTRI RESI NELL'ANNO (1)
Attività di polizia, sicurezza nazionale e governo del territorio	3
Giustizia	2
Informatizzazione e banche dati della p.a.	2
Formazione	2
Dipendenti pubblici	2
Solidarietà sociale	3
Banche ed altre imprese	7
Totale	**21**

(1) Inerenti anche ad affari pervenuti anteriormente al 2008

9. Tavola di comparazione delle voci di classificazione statistica relativamente ai quesiti ricevuti

TAVOLA DI COMPARAZIONE DELLE VOCI DI CLASSIFICAZIONE STATISTICA RELATIVAMENTE AI QUESITI RICEVUTI	
RELAZIONE ANNO 2007	RELAZIONE ANNO 2008
Albi ed elenchi pubblici	Albi, elenchi pubblici, anagrafe e stato civile
Anagrafe e stato civile	
Carte identificative, codice fiscale e numeri di identificazione personale	
Liste elettorali	
Registro dei protesti	
Dati (e fascicoli) personali di dipendenti	Dati dei dipendenti e fascicoli personali
Giornalismo (cronache giudiziarie; minori; pubblicazioni occasionali; trasmissioni radiofoniche e televisive; altre questioni)	Giornalismo
Giustizia (accertamenti di polizia; casellario giudiziario e carichi pendenti; modalità per notifiche e comunicazioni; prove nel processo; pubblicità dei provvedimenti; raccolta di dati per finalità di difesa; altre questioni)	Giustizia e accertamenti di polizia
Informatizzazione della p.a.	Internet e informatizzazione
Internet (foto in Internet; altre questioni; *newsgroup*; *spamming*)	
Rilevazioni biometriche	Rilevazioni biometriche
Sanità (cartelle cliniche; certificazioni di invalidità; certificazioni mediche; Hiv; monitoraggi sanitari; altre questioni)	Sanità e servizi di assistenza sociale
Servizi di assistenza sociale	
Telefonia (chiamate di disturbo; elenchi telefonici; fatturazione dettagliata; localizzazione; *Sms* istituzionali; altre questioni)	Telefonia
Trasparenza (attività organi collegiali; legge n. 241/1990; altre questioni)	Trasparenza
Tributi (banche dati fiscali; canone Rai; contenuto dichiarazione dei redditi; altre questioni)	Tributi
Uffici tributi locali	
Videosorveglianza (finalità di monitoraggio e controllo del traffico; finalità di prevenzione e repressione illeciti; finalità di rispetto disposizioni smaltimento rifiuti; finalità di sicurezza pubblica; da parte di privati; altre questioni)	Videosorveglianza
Indicatori di condizioni economiche	Altro
Lavoro (controlli difensivi del datore di lavoro)	
Lavoro (controlli sul lavoro)	
Notificazioni in busta aperta	
Polizia municipale	
Pubblicità esiti scolastici	
Raccolta dati in ambito assicurativo e banca dati Isvap	
Ricerca genetica e genealogica	
Riservatezza della corrispondenza	
Sistemi informativi creditizi	
Test di maternità e paternità	
Trasporti pubblici	
Zone a traffico limitato e parcheggi riservati	
Altro	

10. Quesiti

QUESITI		
	PERVENUTI NELL'ANNO	RISCONTRI RESI NELL'ANNO (1)
TOTALE	**348**	**1.058**
TEMI PRINCIPALI		
Albi, elenchi pubblici, anagrafe e stato civile	15	100
Dati dei dipendenti e fascicoli personali	21	55
Giornalismo	1	12
Giustizia e accertamenti di polizia	4	29
Internet e informatizzazione	10	39
Rilevazioni biometriche	2	11
Sanità e servizi di assistenza sociale	18	102
Telefonia	10	21
Trasparenza	11	107
Tributi	8	17
Videosorveglianza	30	87

11. Tavola di comparazione delle voci di classificazione statistica relativamente a segnalazioni e reclami ricevuti

TAVOLA DI COMPARAZIONE DELLE VOCI DI CLASSIFICAZIONE STATISTICA RELATIVAMENTE A SEGNALAZIONI E RECLAMI RICEVUTI	
RELAZIONE ANNO 2007	RELAZIONE ANNO 2008
Albi ed elenchi pubblici	Albi, elenchi pubblici, anagrafe e stato civile
Anagrafe e stato civile	
Carte identificative, codice fiscale e numeri di identificazione personale	
Liste elettorali	
Registro dei protesti	
Altro (assicurazioni)	Assicurazioni
Altro (associazioni)	Associazioni
Altro (centrali rischi)	Centrali rischi
Altro (condominio)	Condominio
Riservatezza della corrispondenza	Corrispondenza
Altro (credito)	Credito
Dati (e fascicoli) personali di dipendenti	Dati dei dipendenti e fascicoli personali
Giornalismo (cronache giudiziarie; dati contenuti in sentenze; foto segnaletiche e di persone arrestate; minori; pubblicazioni occasionali; trasmissioni radiofoniche e televisive; vittime di reato; altre questioni)	Giornalismo
Giustizia (accertamenti di polizia; archivi di polizia; indagini del pubblico ministero; modalità per notifiche e comunicazioni; prove nel processo; pubblicità dei provvedimenti; raccolta di dati per finalità di difesa; altre questioni)	Giustizia e accertamenti di polizia
Altro (imprese)	Imprese
Altro (informazioni commerciali)	Informazioni commerciali
Internet (*Enum*; foto in Internet; *newsgroup*; *software* spia, *cookies*; *spamming*; altre questioni)	Internet e informatizzazione
Lavoro (controlli difensivi del datore di lavoro; controlli sul lavoro)	Lavoro
Altro (lavoro)	
Altro (*marketing*)	*Marketing*

segue

(1) Inerenti anche ad affari pervenuti anteriormente al 2008

segue

Recapito pubblicità non gradita	Pubblicità non gradita
Altro (recupero crediti)	Recupero crediti
Rilevazioni biometriche	Rilevazioni biometriche
Altro (biometria)	
Sanità (cartelle cliniche; certificazioni di invalidità; certificazioni mediche; Hiv; monitoraggi sanitari; servizi di assistenza sociale; altre questioni)	Sanità e servizi di assistenza sociale
Telefonia (chiamate di disturbo; collegamenti a numerazioni con prefisso 709; elenchi telefonici; errata ricarica schede telefoniche; fatturazione dettagliata; *fax* indesiderati; localizzazione geografica; numeri riservati; servizi non richiesti; *Sms* anonimi; S*ms* istituzionali; *Sms* pubblicitari; altre questioni)	Telefonia
Trasparenza (attività organi collegiali; legge n. 241/1990; altre questioni)	Trasparenza
Tributi (banche dati fiscali; canone Rai; contenuti delle dichiarazioni dei redditi; altre questioni)	Tributi
Uffici (tributi locali)	
Videosorveglianza (finalità di monitoraggio e controllo del traffico; finalità di prevenzione e repressione illeciti; finalità di sicurezza pubblica; da parte di privati; altre questioni)	Videosorveglianza
Altro (videosorveglianza)	
Gas	Altro
Indicatori di condizioni economiche	
Licenze e autorizzazioni	
Mense e trasporti	
Notificazioni in busta aperta	
Polizia municipale	
Pubblicità esiti scolastici	
Smaltimento rifiuti	
Test di maternità e paternità	
Trasporti pubblici	
Altro	

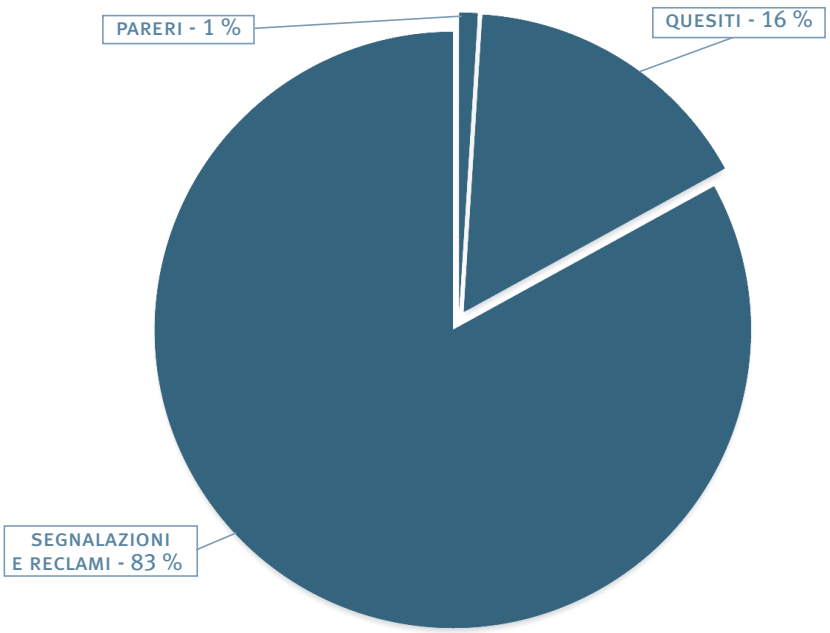
12. Segnalazioni e Reclami

SEGNALAZIONI E RECLAMI		
	PERVENUTI NELL'ANNO	RISCONTRI RESI NELL'ANNO (1)
TOTALE	3.272	5.252
TEMI PRINCIPALI		
Albi, elenchi pubblici, anagrafe e stato civile	24	79
Assicurazioni	90	73
Associazioni	31	15
Centrali rischi	198	154
Condominio	37	38
Corrispondenza	15	43
Credito	272	234
Dati dei dipendenti e fascicoli personali	71	171
Giornalismo	100	218
Giustizia e accertamenti di polizia	59	110
Imprese	154	124
Informazioni commerciali	23	31
Internet e informatizzazione	126	208
Lavoro	109	93
Marketing	15	17
Pubblicità non gradita	56	130
Recupero crediti	65	24
Rilevazioni biometriche	23	38
Sanità e servizi di assistenza sociale	76	235
Telefonia	806	1.103
Trasparenza	13	55
Tributi	40	67
Videosorveglianza	149	172

13. Atti di sindacato ispettivo e controllo

ATTI DI SINDACATO ISPETTIVO E CONTROLLO		
TEMI	PERVENUTI	DEFINITI
Giornalismo	1	0

14. Tipologie dei riscontri resi a interessati e richiedenti



(1) Inerenti anche ad affari pervenuti anteriormente al 2008

NOTIFICAZIONI - TIPOLOGIE			
	DA SOGGETTI PUBBLICI	DA SOGGETTI PRIVATI	TOTALE PERVENUTE (1)
Prima notificazione al Garante	29	592	621
Modifica di una precedente notificazione	14	521	535
Notificazione della cessazione del trattamento	6	84	90
Totale	**49**	**1.197**	**1.246**

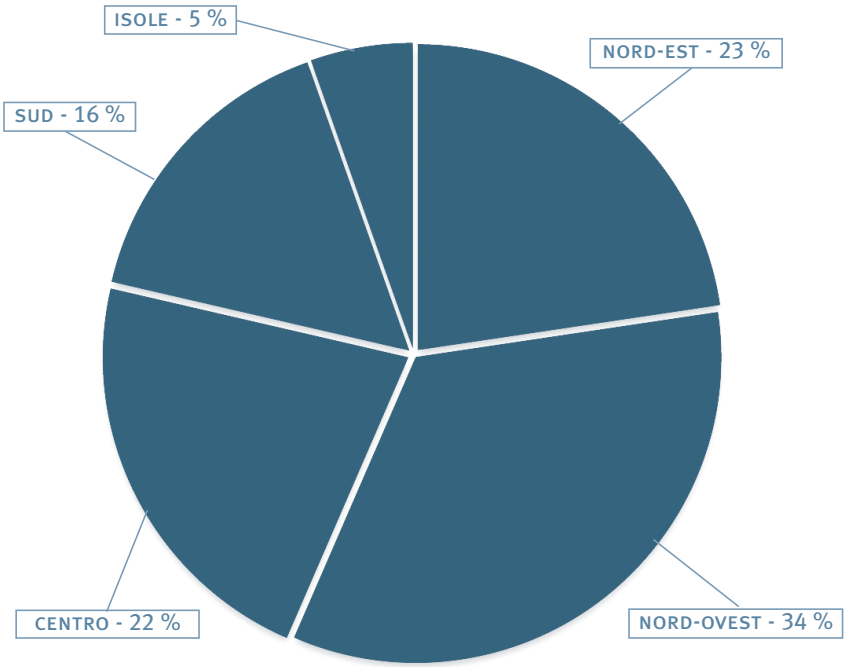
15. Tipologie di notificazioni pervenute nel 2008

TIPOLOGIE DI NOTIFICAZIONI PERVENUTE NEL PERIODO 2004-2008			
	DA SOGGETTI PUBBLICI	DA SOGGETTI PRIVATI	TOTALE PERVENUTE (2)
Prima notificazione al Garante	1.006	13.470	14.476
Modifica di una precedente notificazione	57	1614	1671
Notificazione della cessazione del trattamento	32	333	365
Totale	**1.095**	**15.417**	**16.512**

16. Tipologie di notificazioni pervenute nel periodo 2004-2008

PROVENIENZA GEOGRAFICA DELLE NOTIFICAZIONI: 2004-2008	
ITALIA	
ZONE GEOGRAFICHE	PERVENUTE
Nord- Est	3.728
Nord- Ovest	5.575
Centro	3.638
Sud	2.629
Isole	891
Totale	**16.461**
Da altri Paesi	51

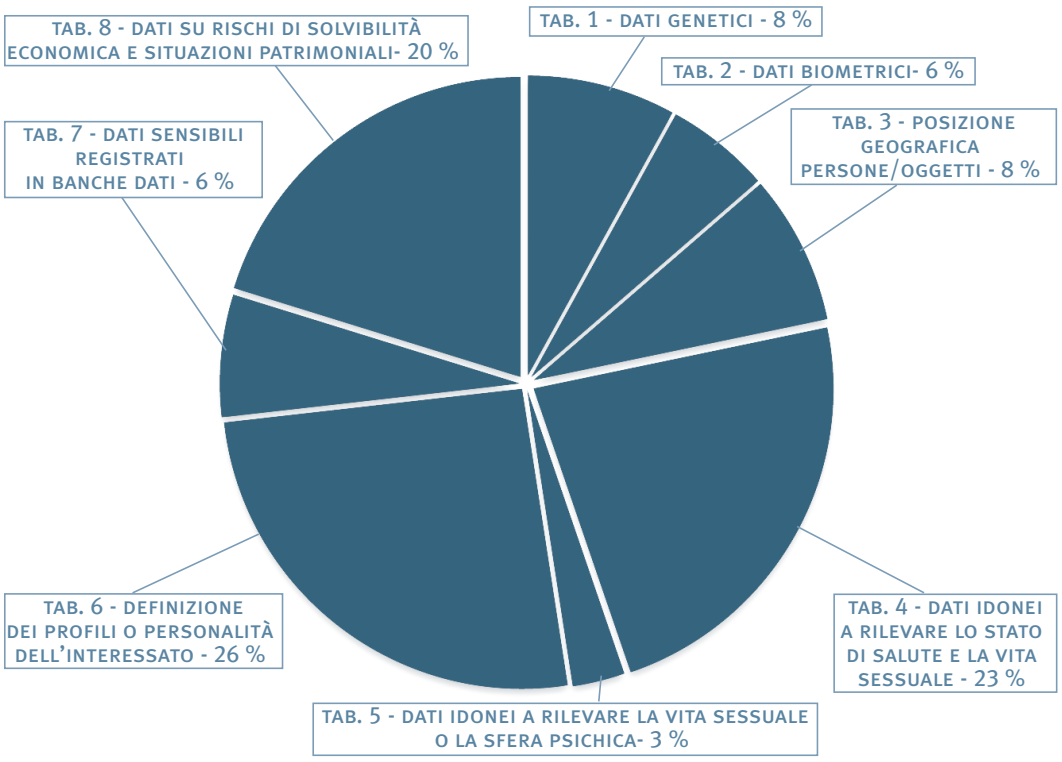
17. Provenienza geografica delle notificazioni: 2004-2008 (tabella e grafico)



(1) (2) Situazione alla data del 31 dicembre 2008

18. Suddivisione delle notificazioni per tipologia di trattamento periodo 2004 - 2008 (tabella e grafico)

SUDDIVISIONE DELLE NOTIFICAZIONI PER TIPOLOGIA DI TRATTAMENTO PERIODO 2004-2008	
TABELLE DI NOTIFICAZIONE COMPILATE (1)	NUMERO
Tabella 1 - Trattamento di dati genetici	1.952
Tabella 2 - Trattamento di dati biometrici	1.376
Tabella 3 - Trattamento di dati che indicano la posizione geografica di persone od oggetti mediante una rete di comunicazione elettronica	1.972
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	5.613
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	688
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	6.253
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	1.606
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	4.929
Totale	**24.389**



(1) Situazione alla data del 31 dicembre 2008

MODALITÀ DI INOLTRO DELLE NOTIFICAZIONI PERIODO 2004 - 2008	
Attraverso intermediari	8.733
Direttamente a cura dei titolari	7.779
Totale	16.512

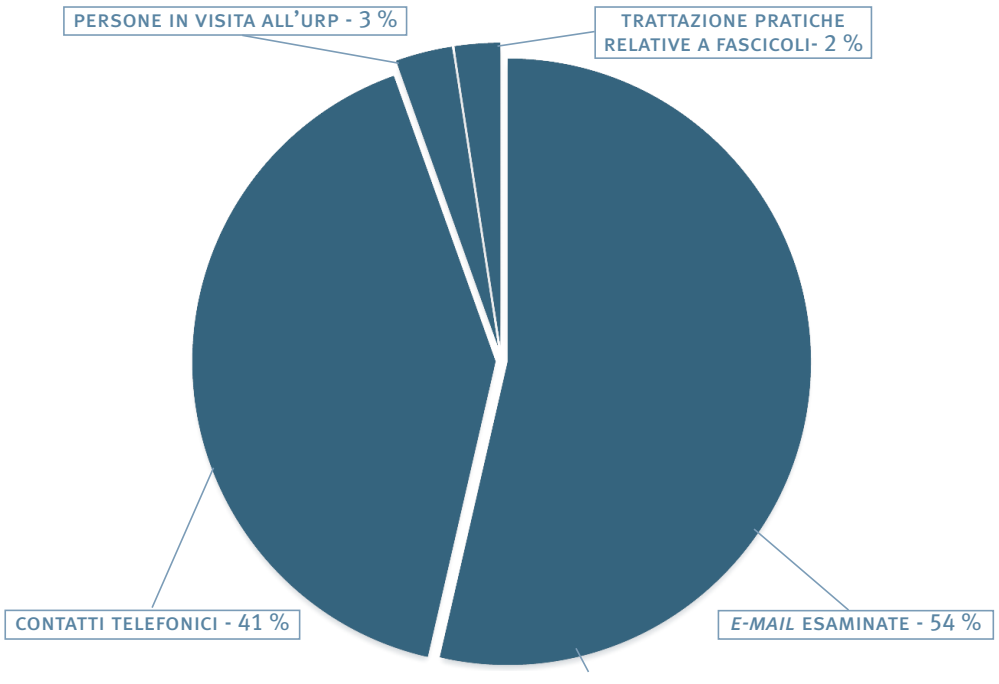
19 . Modalità di inoltro delle notificazioni periodo 2004 - 2008

MODALITÀ DI VERSAMENTO UTILIZZATE		
TIPO MOVIMENTO	NUMERO	TOTALE EURO
Versamento mediante bollettino postale	373	55.950
Versamento mediante bonifico bancario	542	81.300
Versamento mediante carta di credito	331	49.650
Totale	1.246	186.900

20 . Modalità di versamento utilizzate

UFFICIO RELAZIONI CON IL PUBBLICO		
	2007	2008
E-mail esaminate	24.419	19.497
Contatti telefonici	15.600	14.900
Persone in visita all'Urp	1.550	1.100
Trattazione pratiche relative a fascicoli	689	883
Totale	42.258	36.380

21. Ufficio relazioni con il pubblico (tabella e grafico)



22 . Posti previsti in organico

POSTI PREVISTI IN ORGANICO	
Segretario generale	1
Dirigenti	28
Funzionari	65
Operativi	30
Esecutivi	1
Totale	**125**
Personale a contratto	20

23. Personale in servizio

PERSONALE IN SERVIZIO (1)				
AREA	IN RUOLO (A)	IN POSIZIONE DI FUORI RUOLO (B)	COMANDATO PRESSO ALTRE AMMINISTRAZIONI O IN ASPETTATIVA [C]	IMPIEGATO DALL'UFFICIO (A+B-C)
Segretario generale		1		1
Dirigenti	15	3	1	17
Funzionari	52	4	3	53
Operativi	18	1		19
Esecutivi				0
Totale	**85**	**9**	**4**	**90**
Personale a contratto				13

24. Risorse finanziarie

RISORSE FINANZIARIE						
ENTRATE ACCERTATE	ANNO 2008		ANNO 2007		DIFFERENZA	
Correnti		20.895.487,96		20.616.159,72		279.328,24
di cui trasferimento dallo Stato	18.162.911,45		18.777.293,72		- 614.382,27	
Totale entrate		**20.895.487,96**		**20.616.159,72**		**279.328,24**
SPESE IMPEGNATE	ANNO 2008		ANNO 2007		DIFFERENZA	
Funzionamento		19.094.234,86	17.235.513,16			1.858.721,70
Capitale		570.985,77	1.081.688,86			- 510.703,09
Totale spese		**19.665.220,63**	**18.317.202,02**			**1.348.018,61**

(1) Alla data del 31 dicembre 2008

Documentazione

Provvedimenti del Garante

24. Codice di deontologia e di buona condotta per i trattamenti di dati personali effettuati per svolgere investigazioni difensive (*)

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Nella riunione odierna, in presenza del prof. Francesco Pizzetti, presidente, del dott. Mauro Paissan e del dott. Giuseppe Fortunato, componenti e del dott. Giovanni Buttarelli, segretario generale;

Visto l'art. 27 della direttiva n. 95/46/Ce del Parlamento europeo e del Consiglio del 24 ottobre 1995, secondo cui gli Stati membri e la Commissione incoraggiano l'elaborazione di codici di condotta destinati a contribuire, in funzione delle specificità settoriali, alla corretta applicazione delle disposizioni nazionali di attuazione della direttiva adottate dagli Stati membri;

Visti gli artt. 12 e 154, comma 1, lett. e) del Codice in materia di protezione dei dati personali (d.lg. 30 giugno 2003, n. 196), i quali attribuiscono al Garante il compito di promuovere nell'ambito delle categorie interessate, nell'osservanza del principio di rappresentatività e tenendo conto dei criteri direttivi delle raccomandazioni del Consiglio d'Europa sul trattamento dei dati personali, la sottoscrizione di codici di deontologia e di buona condotta per determinati settori, verificarne la conformità alle leggi e ai regolamenti anche attraverso l'esame di osservazioni di soggetti interessati e contribuire a garantirne la diffusione e il rispetto;

Visto l'art. 135 del Codice con il quale è stato demandato al Garante il compito di promuovere la sottoscrizione di un codice di deontologia e di buona condotta per il trattamento dei dati personali effettuati per svolgere le 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;

Vista la deliberazione n. 31-*bis* del 20 luglio 2006 con la quale il Garante ha adottato in base all'articolo 156, comma 3, lett. a) del Codice il regolamento n. 2/2006 concernente la proce-

(*) Provvedimento del Garante n. 60 del 6 novembre 2008, Gazzetta Ufficiale 24 novembre 2008, n. 275 [doc. *web* n. 1565171]

dura per la sottoscrizione dei codici di deontologia e di buona condotta;

Vista la deliberazione n. 3 del 16 febbraio 2006, pubblicata nella Gazzetta Ufficiale della Repubblica italiana del 1° marzo 2006, con la quale il Garante ha promosso la sottoscrizione del predetto codice di deontologia e di buona condotta;

Viste le comunicazioni pervenute al Garante in risposta al citato provvedimento con le quali soggetti pubblici e privati hanno manifestato la volontà di partecipare all'adozione di tale codice e rilevato che si è anche formato un apposito gruppo di lavoro composto da rappresentanti dei predetti soggetti, ai sensi dell'art. 4 del predetto regolamento n. 2/2006;

Considerato che il testo del codice di deontologia e di buona condotta è stato oggetto di ampia diffusione anche attraverso la sua pubblicazione sul sito Internet di questa Autorità, resa nota tramite avviso sulla Gazzetta Ufficiale della Repubblica italiana dell'8 aprile 2008, n. 83, al fine di favorire il più ampio dibattito e di permettere la raccolta di eventuali osservazioni e integrazioni al testo medesimo da parte di tutti i soggetti interessati;

Viste le osservazioni pervenute a seguito di tale avviso e le modifiche apportate allo schema del codice, poi sottoscritto il 27 ottobre 2008;

Constatata la conformità del codice di deontologia e di buona condotta alle leggi e ai regolamenti anche in relazione a quanto previsto dall'art. 12 del Codice;

Visto il verbale della riunione collegiale del 2 ottobre 2008 e il successivo verbale di sottoscrizione del predetto codice del 27 ottobre 2008;

Rilevato che il rispetto delle disposizioni contenute nel codice di deontologia e di buona condotta costituisce condizione essenziale per la liceità e la correttezza del trattamento dei dati personali effettuato da soggetti privati e pubblici (art. 12, comma 3, del Codice);

Considerato che, ai sensi dell'art. 12, comma 2, del Codice e dell'art. 9 del menzionato regolamento n. 2/2006, il codice di deontologia e di buona condotta deve essere pubblicato a cura del Garante nella Gazzetta Ufficiale della Repubblica italiana e, con decreto del Ministro della giustizia, riportato nell'Allegato A. al medesimo Codice;

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;

TUTTO CIÒ PREMESSO IL GARANTE

dispone la trasmissione del codice di deontologia e di buona condotta per il trattamento dei dati personali effettuato per svolgere le 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, sottoscritto il 27 ottobre 2008 e che figura in allegato, quale parte integrante della presente deliberazione, all'Ufficio pubblicazione leggi e decreti del Ministero della giustizia per la sua pubblicazione nella Gazzetta Ufficiale della Repubblica italiana, nonché al Ministro della giustizia per essere riportato nell'Allegato A. al Codice.

Roma, 6 novembre 2008

IL PRESIDENTE
Pizzetti

IL RELATORE
Pizzetti

IL SEGRETARIO GENERALE
Buttarelli

Codice di deontologia e di buona condotta per i trattamenti di dati personali effettuati per svolgere investigazioni difensive

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, soprattutto quando non sia tale da 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 con-

ciliazione, 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. del Garante del 9 luglio 2003);

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; del. 31 marzo 2004, n. 1 e nota di chiarimenti n. 9654/33365 del 23 aprile 2004);

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 ai sensi degli artt. 51 e 52 del Codice, per la quale apposite disposizioni di legge hanno individuato opportune cautele per tutelare gli interessati senza pregiudicare l'informazione scientifico-giuridica;

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 assistenza o 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 trattamento 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 e, se ne dispone, pubblicazione sul proprio sito Internet, 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. Restano ferme le prescrizioni relative al trattamento dei dati sensibili contenute in atti autorizzativi del Garante.

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 dei soggetti che hanno curato l'attività svolta, a i 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 1° gennaio 2009.

25. Linee-guida in materia di trattamento di dati personali da parte dei consulenti tecnici e dei periti ausiliari del giudice e del pubblico ministero (*)

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);

Ritenuta la necessità di provvedere in relazione ai rischi connessi al trattamento di dati personali effettuato da consulenti tecnici e periti ausiliari del giudice e del pubblico ministero nell'ambito di procedimenti in sede civile, penale e amministrativa;

Rilevata l'esigenza di individuare un quadro unitario di misure e di accorgimenti necessari e opportuni, volti a fornire orientamenti utili per i professionisti interessati;

Viste le pertinenti disposizioni del codice di procedura civile (in particolare gli articoli da 61 a 64 e da 191 a 200) e del codice di procedura penale (in particolare gli articoli da 220 a 232, 359 e 360);

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:

1. di adottare le "Linee-guida" contenute nel documento allegato quale parte integrante della presente deliberazione;
2. di inviare copia del presente provvedimento al Ministero della giustizia e al Consiglio superiore della magistratura, per opportuna conoscenza nonché –per quanto di rispettiva competenza– per l'adozione di ogni iniziativa ritenuta idonea alla massima diffusione presso gli uffici giudiziari interessati;

(*) Deliberazione n. 46 del 26 giugno 2008, Gazzetta Ufficiale 31 luglio 2008, n. 178 [doc. *web* n. 1534086]

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, unitamente alle menzionate "Linee-guida", per la loro pubblicazione sulla Gazzetta Ufficiale della Repubblica italiana.

Roma, 26 giugno 2008

IL PRESIDENTE
Pizzetti

IL RELATORE
Chiaravalloti

IL SEGRETARIO GENERALE
Buttarelli

LINEE-GUIDA IN MATERIA DI TRATTAMENTO DI DATI PERSONALI DA PARTE DEI CONSULENTI TECNICI E DEI PERITI AUSILIARI DEL GIUDICE E DEL PUBBLICO MINISTERO

1. PREMESSA

1.1. *Scopo delle linee guida*

I consulenti tecnici e i periti ausiliari del giudice e del pubblico ministero coadiuvano e assistono l'autorità giudiziaria nello svolgimento delle proprie funzioni, quando ciò si rende necessario per compiere atti o esprimere valutazioni che richiedono particolari e specifiche competenze tecniche (art. 61 c.p.c.; artt. 220 e 359 c.p.p.).

L'attività svolta dai consulenti tecnici e dai periti è strettamente connessa e integrata con l'attività giurisdizionale, di cui mutua i compiti e le finalità istituzionali.

Nell'espletamento delle relative incombenze, il consulente e il perito di regola vengono a conoscenza e devono custodire, contenuti nella documentazione consegnata dall'ufficio giudiziario, anche dati personali di soggetti coinvolti a diverso titolo nelle vicende giudiziarie (quali le parti di un giudizio civile o le persone sottoposte a procedimento penale), e possono acquisire altre informazioni di natura personale nel corso delle operazioni (cfr. ad esempio, art. 194 c.p.c., richiesta di chiarimenti alle parti e assunzione di informazioni presso terzi; art. 228, comma 3, c.p.p., richiesta di notizie all'imputato, alla persona offesa o ad altre persone). L'attività dell'ausiliario comporta quindi il trattamento di diversi dati personali, talvolta di natura sensibile o di carattere giudiziario (art. 4, comma 1, lettere d) ed e) del Codice), di uno o più soggetti, persone fisiche o giuridiche.

A tali trattamenti, in quanto direttamente correlati alla trattazione giudiziaria di affari e di controversie, si applicano le norme del Codice relative ai trattamenti effettuati presso uffici giudiziari di ogni ordine e grado "per ragioni di giustizia" (art. 47, comma 2, del Codice; *cfr.* Provv. del Garante 31 dicembre 1998, [doc. *web* n. 39608]; Provv. 27 marzo 2002, [doc. *web* n. 1063421]).

Le presenti linee guida mirano a fornire indicazioni di natura generale ai professionisti nominati consulenti tecnici e periti dall'autorità giudiziaria nell'ambito di procedimenti civili, penali e ammi-

nistrativi al fine esclusivo di garantire il rispetto dei princìpi in materia di protezione dei dati personali ai sensi del Codice in materia protezione dei dati personali (d.lg. 30 giugno 2003, n. 196).

1.2. *Ambito considerato*

Le predette indicazioni non incidono sulle forme processuali che gli ausiliari devono rispettare nello svolgimento delle attività e nell'adempimento degli obblighi derivanti dall'incarico e dalle istruzioni ricevuti dall'autorità giudiziaria, come disciplinati dalle pertinenti disposizioni codicistiche.

All'interno del paragrafo 6. sono poi formulate alcune indicazioni applicabili anche ai trattamenti di dati personali effettuati dai soggetti nominati consulenti tecnici dalle parti private con riferimento a procedimenti giudiziari (artt. 87, 194, 195 e 201 c.p.c.; artt. 225 e ss., 233 e 360 c.p.p.).

2. IL RISPETTO DEI PRINCÌPI DI PROTEZIONE DEI DATI PERSONALI

2.1. *Considerazioni generali*

La peculiare disciplina posta dal Codice con riguardo ai trattamenti svolti per ragioni di giustizia (art. 47) rende non applicabili alcune disposizioni del medesimo Codice relative alle modalità di esercizio dei diritti da parte dell'interessato (art. 9), al riscontro da fornire al medesimo (art. 10), ai codici di deontologia e di buona condotta (art. 12), all'informativa agli interessati (art. 13), alla cessazione del trattamento (art. 16), al trattamento svolto da soggetti pubblici (artt. da 18 a 22), alla notificazione al Garante (artt. 37 e 38, commi da 1 a 5), a determinati obblighi di comunicazione all'Autorità, alle autorizzazioni e al trasferimento dei dati all'estero (artt. da 39 a 45), nonché ai ricorsi al Garante (artt. da 145 a 151).

Sono invece pienamente applicabili le altre pertinenti disposizioni del Codice. In particolare, il trattamento dei dati effettuato a cura di consulenti tecnici e periti deve avvenire:

- nel rispetto dei princìpi di liceità e che riguardano la qualità dei dati (art. 11);
- adottando le misure di sicurezza idonee a preservare i dati da alcuni eventi, tra i quali accessi e utilizzazioni indebite (artt. 31 e ss. e disciplinare tecnico Allegato B. al Codice).

2.2. *Liceità, finalità, esattezza, pertinenza*

Il consulente e il perito possono trattare lecitamente dati personali, nei limiti in cui ciò è necessario per il corretto adempimento dell'incarico ricevuto e solo nell'ambito dell'accertamento deman-

dato dall'autorità giudiziaria; devono rispettare, altresì, le disposizioni sulle funzioni istituzionali della medesima autorità giudiziaria contenute in leggi e regolamenti, avvalendosi in particolare di informazioni personali e di modalità di trattamento proporzionate allo scopo perseguito (art. 11, comma 1, lett. a) e b)), nel rigoroso rispetto delle istruzioni impartite dall'autorità giudiziaria.

In tale quadro, l'eventuale utilizzo incrociato di dati può ritenersi consentito se è chiaramente collegato alle indagini delegate ed è stato autorizzato dalle singole autorità giudiziarie dinanzi alle quali pendono i procedimenti o, se questi si sono conclusi, che ebbero a conferire l'incarico o da altra autorità giudiziaria competente.

Nel pieno rispetto dell'ambito e della natura dell'incarico ricevuto, il consulente e il perito sono tenuti ad acquisire, utilizzare e porre a fondamento delle proprie operazioni e valutazioni informazioni personali che, con riguardo all'oggetto dell'indagine da svolgere, siano idonee a fornire una rappresentazione (finanziaria, sanitaria, patrimoniale, relazionale, ecc.) corretta, completa e corrispondente ai dati di fatto anche quando vengono espresse valutazioni soggettive di ciascun interessato, persona fisica o giuridica. Ciò, non solo allo scopo di fornire un riscontro esauriente in relazione al compito assegnato, ma anche al fine di evitare che, da un quadro inesatto o comunque inidoneo di informazioni possa derivare nocumento all'interessato, anche nell'ottica di una non fedele rappresentazione della sua identità (art. 11, comma 1, lett. c)).

Particolare attenzione deve essere inoltre posta dal consulente e dal perito nell'acquisire e utilizzare solo le informazioni che risultino effettivamente necessarie in riferimento alle specifiche finalità di accertamento perseguite. In ossequio al principio di pertinenza nel trattamento dei dati, le relazioni e le informative fornite al magistrato ed eventualmente alle parti non devono né riportare dati, specie se di natura sensibile o di carattere giudiziario o comunque di particolare delicatezza, chiaramente non pertinenti all'oggetto dell'accertamento peritale, né contenere ingiustificatamente informazioni personali relative a soggetti estranei al procedimento (art. 11, comma 1, lett. d)).

3. COMUNICAZIONE DEI DATI

Le informazioni personali acquisite nel corso dell'accertamento possono essere comunicate alle parti, come rappresentate nel procedimento (ad esempio, attraverso propri consulenti tecnici),

con le modalità e nel rispetto dei limiti fissati dalla pertinente normativa posta a tutela della segretezza e riservatezza degli atti processuali. Fermo l'obbligo per l'ausiliare di mantenere il segreto sulle operazioni compiute (art. 226 c.p.p.; cfr. anche art. 379-*bis* c.p.), eventuali comunicazioni di dati a terzi, ove ritenute indispensabili in funzione del perseguimento delle finalità dell'indagine, restano subordinate a quanto eventualmente direttamente stabilito per legge o, comunque, a preventive e specifiche autorizzazioni rilasciate dalla competente autorità giudiziaria.

4. CONSERVAZIONE E CANCELLAZIONE DEI DATI

In riferimento ai trattamenti di dati svolti per ragioni di giustizia non è applicabile la disposizione del Codice (art. 16) relativa alla cessazione del trattamento di dati personali, evenienza che, nel caso del trattamento effettuato dal consulente e dal perito, di regola coincide con l'esaurimento dell'incarico.

Trova, peraltro, applicazione anche ai trattamenti di dati personali effettuati per ragioni di giustizia il dettato dell'art. 11, comma 1, lett. e), del Codice il quale prevede che i dati non possono essere conservati per un periodo di tempo superiore a quello necessario al perseguimento degli scopi per i quali essi sono stati raccolti e trattati.

Ne consegue che, espletato l'incarico e terminato quindi il connesso trattamento delle informazioni personali, l'ausiliario deve consegnare per il deposito agli atti del procedimento non solo la propria relazione, ma anche la documentazione consegnatagli dal magistrato e quella ulteriore acquisita nel corso dell'attività svolta, salvo quanto eventualmente stabilito da puntuali disposizioni normative o da specifiche autorizzazioni dell'autorità giudiziaria che dispongano legittimamente ed espressamente in senso contrario.

Ove non ricorrano tali ultime due ipotesi, il consulente e il perito non possono quindi conservare, in originale o in copia, in formato elettronico o su supporto cartaceo, informazioni personali acquisite nel corso dell'incarico concernenti i soggetti, persone fisiche o giuridiche, nei cui confronti hanno svolto accertamenti.

Analogamente, la documentazione acquisita nel corso delle operazioni peritali deve essere restituita integralmente al magistrato in caso di revoca o di rinuncia all'incarico da parte dell'ausiliario.

Qualora sia prevista una conservazione per adempiere a uno specifico obbligo normativo (ad

esempio, in materia fiscale o contabile), possono essere custoditi i soli dati personali effettivamente necessari per adempiere tale obbligo.

Eventuali, ulteriori informazioni devono essere quindi cancellate, oppure trasformate in forma anonima anche per finalità scientifiche o statistiche, tale da non poter essere comunque riferita a soggetti identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione (art. 4, comma 1, lett. b), del Codice).

Tutto ciò non pregiudica l'espletamento di eventuali ulteriori attività dell'ausiliare, conseguenti a richieste di chiarimenti o di supplementi di indagine, che il consulente e il perito possono soddisfare acquisendo dal fascicolo processuale, in conformità alle regole poste dai codici di rito, la documentazione necessaria per fornire i nuovi riscontri.

5. MISURE DI SICUREZZA

5.1. *Misure idonee e misure minime*

Limitatamente all'espletamento degli accertamenti, l'attività dell'ausiliare è connotata da peculiari caratteri di autonomia, in relazione alla natura squisitamente tecnica delle indagini che si svolgono, di regola, senza l'intervento del magistrato.

Ricevuto l'incarico e sino al momento della consegna al giudice o al pubblico ministero delle risultanze dell'attività svolta, incombono concretamente al consulente tecnico e al perito, riguardo ai dati personali acquisiti all'atto dell'incarico e alle ulteriori informazioni raccolte nel corso delle operazioni, le responsabilità e gli obblighi relativi al profilo della sicurezza prescritti dal Codice.

L'ausiliare è tenuto quindi a impiegare tutti gli accorgimenti idonei a evitare un'indebita divulgazione delle informazioni e, al contempo, la loro perdita o distruzione, adottando, a tal fine, le misure atte a garantire la sicurezza dei dati e dei sistemi eventualmente utilizzati. Egli deve curare personalmente, con il grado di autonomia riconosciuto per legge o con l'incarico ricevuto, sia le "misure idonee e preventive" cui fa riferimento l'art. 31 del Codice, sia le "misure minime" specificamente indicate negli articoli da 33 a 35 e nel disciplinare tecnico Allegato B. al Codice, la cui mancata adozione costituisce fattispecie penalmente sanzionata (art. 169 del Codice). Ove reso necessario dal trattamento di dati sensibili o giudiziari effettuato con l'ausi-

lio di strumenti elettronici, nell'ambito delle misure minime (art. 33, comma 1, lett. g) del Codice) deve essere redatto il documento programmatico sulla sicurezza, con le modalità e i contenuti previsti al punto 19. del citato disciplinare tecnico.

5.2. *Incaricati*

L'obbligo di preporre alla custodia e al trattamento dei dati personali raccolti nel corso dell'accertamento solo il personale specificamente incaricato per iscritto resta fermo anche nel caso in cui il consulente e il perito si avvalgano dell'opera di collaboratori, anche se addetti a compiti di collaborazione amministrativa (art. 30 del Codice). L'attività di tali incaricati deve essere oggetto di precise istruzioni oltre che sulle modalità e sull'ambito del trattamento consentito, anche in ordine alla scrupolosa osservanza della riservatezza relativamente ai dati di cui vengono a conoscenza.

6. I CONSULENTI TECNICI DI PARTE NEI PROCEDIMENTI GIUDIZIARI

Ferma restando ogni altra disposizione contenuta nel Codice, nei provvedimenti generali adottati dal Garante e in un codice deontologico concernente le condizioni e i limiti applicabili ai trattamenti di dati personali effettuati dai consulenti tecnici di parte nei procedimenti giudiziari, anche a tali trattamenti trovano applicazione i princìpi di liceità e che riguardano la qualità dei dati (art. 11 del Codice) e le disposizioni in materia di misure di sicurezza volte alla protezione dei dati stessi (artt. 31 e ss. e disciplinare tecnico Allegato B. al Codice).

In particolare, il consulente di parte:

- può trattare lecitamente i dati personali nei limiti in cui ciò è necessario per il corretto adempimento dell'incarico ricevuto dalla parte o dal suo difensore ai fini dello svolgimento delle indagini difensive di cui alla legge n. 397/2000 o, comunque, per far valere o difendere un diritto in sede giudiziaria (art. 11, comma 1, lett. a) e b)); dati sensibili o giudiziari possono essere utilizzati solo se ciò è indispensabile;
- può acquisire e utilizzare solo i dati personali comunque pertinenti e non eccedenti rispetto alle finalità perseguite con l'incarico ricevuto, avvalendosi di informazioni personali e di modalità di trattamento proporzionate allo scopo perseguito (art. 11, comma 1, lett. d));
- salvi i divieti di legge posti a tutela della segretezza e riservatezza delle informazioni acqui-

site nel corso di un procedimento giudiziario (cfr., ad esempio, l'art. 379-*bis* c.p.p.) e i limiti e i doveri derivanti dal segreto professionale e dal fedele espletamento dell'incarico ricevuto (cfr. artt. 380 e 381 c.p.), può comunicare a terzi dati personali solo ove ciò risulti necessario per finalità di tutela dell'assistito, limitatamente ai dati strettamente funzionali all'esercizio del diritto di difesa della parte e nel rispetto dei diritti e della dignità dell'interessato e di terzi;

- relativamente ai dati personali acquisiti e trattati nell'espletamento dell'incarico ricevuto da una parte, assume personalmente le responsabilità e gli obblighi relativi al profilo della sicurezza prescritti dal Codice, relativamente sia alle "misure idonee e preventive" (art. 31) sia alle "misure minime" (artt. da 33 a 35 e disciplinare tecnico Allegato B. al Codice; art. 169 del Codice); ove l'incarico comporti il trattamento con strumenti elettronici di dati sensibili o giudiziari, è tenuto a redigere il documento programmatico sulla sicurezza (art. 33, comma 1, lett. g) e punto 19. del disciplinare tecnico Allegato B.);
- deve incaricare per iscritto gli eventuali collaboratori, anche se adibiti a mansioni di carattere amministrativo, che siano addetti alla custodia e al trattamento, in qualsiasi forma, dei dati personali (art. 30 del Codice), impartendo loro precise istruzioni sulle modalità e l'ambito del trattamento loro consentito e sulla scrupolosa osservanza della riservatezza dei dati di cui vengono a conoscenza.

26. Il sistema Eurodac (*)

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 regolamento (Ce) n. 2725/2000 del Consiglio dell'11 dicembre 2000 che istituisce l'Eurodac per il confronto delle impronte digitali ai fini dell'efficace applicazione della Convenzione di Dublino (Convenzione sulla determinazione dello Stato competente per l'esame di una domanda di asilo presentata in uno degli Stati membri delle Comunità europee);

Visto il Codice in materia di protezione dei dati personali (d. lg. 30 giugno 2003, n. 196);

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 Fortunato;

PREMESSO

Il Garante per la protezione dei dati personali è l'autorità indipendente incaricata di esercitare il controllo sul trattamento dei dati a carattere personale effettuato sul territorio nazionale ai sensi del regolamento comunitario n. 2725/2000 e di verificare che la trasmissione dei dati alla banca dati centrale informatizzata, gestita dall'unità centrale istituita presso la Commissione europea, avvenga lecitamente (art. 154, comma 2, lett. d), del Codice; art. 19 reg. n. 2725/2000).

Il Garante europeo della protezione dei dati, cui sono state conferite funzioni di supervisione dell'Eurodac già svolte dall'autorità comune di controllo prevista all'articolo 20 del citato regolamento, ha individuato, in accordo con le autorità nazionali di protezione dei dati, linee di azione utili per svolgere in parallelo indagini in ciascuno Stato, concentrate su alcuni aspetti considerati prioritari che concernono: a) le cd. "ricerche speciali", ovvero le richieste che gli Stati membri inviano alla predetta unità centrale in relazione all'art. 18 del menzionato regolamento

(*) [doc. *web* n. 1537606]

(in tema di accesso dell'interessato) e che risultano variare da paese a paese; b) le possibilità di uso dei dati a fini diversi da quelli consentiti dal regolamento; c) la qualità –sotto il profilo tecnico– dei dati.

Sulla base di tali indicazioni, in una prima fase il Garante ha inoltrato al Ministero dell'interno una richiesta preliminare di informazioni in relazione agli aspetti sopra evidenziati.

Al fine di completare l'azione richiesta, in una seconda fase il Garante ha deliberato di procedere ai sensi dell'art. 160 del Codice, anche con visita in loco presso i competenti uffici del Ministero dell'interno, centrali e periferici, a una verifica delle informazioni ottenute e riscontrare, in particolare, la sussistenza della base giuridica necessaria per l'inserimento dei dati dattiloscopici nella banca dati centrale e per l'interrogazione del sistema, nonché l'adeguatezza delle misure di sicurezza adottate nel trattamento. Con la medesima deliberazione l'Autorità ha, inoltre, ritenuto necessario svolgere accertamenti più ampi sulla liceità e correttezza dei trattamenti comunque effettuati in attuazione della Convenzione di Dublino.

Gli uffici interessati hanno prestato la propria collaborazione fornendo anche gli elementi e la documentazione richiesti.

Concluse le verifiche, il presente provvedimento viene adottato anche con riguardo alle raccomandazioni formulate dal Garante europeo a seguito del riscontro fornito dall'Autorità al termine della prima fase di accertamenti.

OSSERVA

1. IL SISTEMA EURODAC

Il regolamento n. 2725/2000 istituisce il sistema Eurodac, che si compone dell'unità centrale, di una banca dati centrale informatizzata e dei mezzi di trasmissione dei dati tra gli Stati membri e tale banca dati centrale. Gli Stati membri, direttamente o attraverso l'unità centrale, inseriscono nella banca dati centrale i dati personali (impronte digitali e sesso) appartenenti a tre tipologie di soggetti di età non inferiore a quattordici anni: a) richiedenti asilo; b) stranieri fermati in relazione all'attraversamento irregolare di una frontiera esterna; c) stranieri presenti irregolarmente in uno Stato membro.

I dati vengono inseriti affinché siano confrontati con i dati dei richiedenti l'asilo registrati già presso l'unità centrale, al fine di concorrere alla determinazione dello Stato membro compe-

tente, ai sensi della Convenzione (oggi regolamento) di Dublino, per l'esame di una domanda di asilo presentata in uno Stato membro.

Il regolamento n. 2725/2000 prevede che le norme cui è soggetto il sistema Eurodac si applicano anche alle operazioni effettuate dagli Stati membri, dal momento della trasmissione dei dati all'unità centrale fino all'utilizzazione dei risultati del confronto; specifica inoltre che, fatta salva l'utilizzazione delle informazioni destinate all'Eurodac da parte dello Stato membro d'origine nell'ambito di banche dati istituite ai sensi della propria legislazione nazionale, i dati sulle impronte digitali e le altre informazioni personali possono essere trattati nell'Eurodac solo per gli scopi previsti dall'articolo 15, paragrafo 1, della Convenzione di Dublino (art. 1 reg. n. 2725/2000).

Con riferimento al trattamento dei dati effettuato in Italia, la procedura si articola in due fasi distinte.

La prima si svolge interamente nell'ambito del Dipartimento della pubblica sicurezza del Ministero dell'interno, in particolare attraverso le questure e il Servizio di polizia scientifica, ed è rivolta alla presentazione e ricezione della domanda di asilo, alla raccolta delle informazioni necessarie (tra cui il fotosegnalamento e le verifiche sugli archivi nazionali), alla valutazione dell'ammissibilità della domanda e al suo invio alla Commissione per il riconoscimento dello status di rifugiato, alla trasmissione dei dati alla banca dati centrali Eurodac e, in caso di riscontro positivo, all'Unità Dublino.

Le direttive di carattere tecnico-operativo e di rilievo giuridico vengono impartite dalla Direzione centrale dell'immigrazione e della polizia delle frontiere del Dipartimento della pubblica sicurezza, che cura, su richiesta dell'Unità Dublino, gli approfondimenti necessari ai fini della verifica di eventuali reati a carico dello straniero, nonché ogni altra informazione circa la presenza regolare o meno dello stesso sul territorio nazionale.

La seconda fase fa capo al Dipartimento delle libertà civili e l'immigrazione del Ministero dell'interno, che espleta la procedura di accettazione/rinvio della richiesta prevista dalla Convenzione di Dublino.

In particolare, all'esito degli accertamenti svolti risulta accertata la seguente procedura.

1.1. *Invio dei dati alla banca dati centrale*

Su richiesta dell'ufficio immigrazione presso le questure il Gabinetto provinciale di polizia scientifica della Polizia di Stato effettua il fotosegnalamento dell'interessato al fine dell'inserimento in A.f.i.s. (Automated fingerprint identification system) e in Eurodac, qualora ricorra una delle fattispecie previste dal regolamento n. 2725/2000 sopra precisate alle lett. a), b) e c). Il cartellino fotosegnaletico viene quindi inviato presso il Gabinetto regionale di polizia scientifica, che provvede al controllo della sua qualità tecnica e lo inserisce effettivamente in A.f.i.s. e, se richiesto dal Gabinetto provinciale, nell'Eurodac. L'invio avviene mediante il Servizio di polizia scientifica sito presso il Dipartimento della pubblica sicurezza, designato dall'Italia quale unico punto di accesso nazionale per l'interscambio dei dati con l'unità centrale sita a Bruxelles.

1.2. *Riscontro dell'unità centrale*

In caso di confronto positivo ("risposta pertinente" secondo l'art. 4 reg. n. 2725/2000) l'unità centrale invia i rilievi dattiloscopici al competente gabinetto di polizia scientifica per la conferma della corrispondenza con i rilievi già presenti nella banca dati. A seguito di tale conferma la questura interessata invia la richiesta di asilo, corredata dalla pertinente documentazione, sia alla Commissione per il riconoscimento dello status di rifugiato territorialmente competente a decidere nel merito, sia all'Unità Dublino, ufficio del Dipartimento per le libertà civili e l'immigrazione del Ministero dell'interno che ha il compito di intrattenere i rapporti e curare lo scambio di informazioni con altri omologhi uffici nazionali al fine di individuare lo Stato membro competente a decidere sulla richiesta di asilo. L'Unità Dublino tratta anche i casi in cui la richiesta di asilo è presentata in un altro Stato membro e nel sistema risultano le impronte digitali della persona inserite dall'Italia.

2. PROFILI CRITICI E PRESCRIZIONI DEL GARANTE

Il regolamento n. 2725/2000 e il Codice pongono precisi obblighi in relazione ai trattamenti di dati personali effettuati in funzione dell'applicazione della Convenzione di Dublino.

Le informazioni acquisite, anche attraverso gli accertamenti in loco, hanno permesso di verificare che alcuni di questi obblighi non sono stati attuati correttamente.

In relazione a tali aspetti il Garante rileva pertanto la necessità di impartire ai sensi degli

artt. 154 e 160 del Codice le necessarie modificazioni e integrazioni da apportare al trattamento, di cui, in relazione agli obblighi di controllo ad essa affidati, questa Autorità si riserva di verificare periodicamente l'attuazione ai sensi del medesimo art. 160.

2.1. *Titolare ed eventuali responsabili del trattamento*

Profili critici

La complessità della procedura descritta, con l'intervento di molteplici organi facenti capo a diverse articolazioni del Ministero dell'interno, non consente una chiara individuazione delle diverse responsabilità nel trattamento dei dati per le finalità proprie del sistema Eurodac.

L'imputabilità a più soggetti delle operazioni da svolgere, con la conseguente, mancata individuazione di un unico interlocutore, ha determinato anche ritardi e difficoltà nello stesso svolgimento degli accertamenti deliberati dal Garante.

Prescrizioni

L'art. 13 del regolamento n. 2725/2000 pone precisi obblighi a carico di ciascuno Stato membro, il quale è tenuto a garantire "la legalità del rilevamento delle impronte digitali" e della loro trasmissione all'unità centrale, l'esattezza e l'attualità delle informazioni al momento della trasmissione, "la legalità della registrazione, conservazione, rettifica e cancellazione dei dati nella banca dati centrale", "la legalità dell'uso dei risultati del confronto dei dati sulle impronte trasmessi dall'unità centrale" (paragrafo 1), nonché la sicurezza dei dati in ogni fase del trattamento (paragrafo 2).

Tali obblighi impongono la necessità di identificare chiaramente le responsabilità dei diversi servizi che utilizzano il sistema Eurodac nell'ambito del Ministero dell'interno, ivi compreso il servizio competente per l'accertamento dell'età del soggetto ai fini dell'inserimento delle impronte digitali nel sistema. In particolare, devono essere individuati il titolare (o i co-titolari) del trattamento dei dati, nonché eventuali responsabili; i relativi estremi identificativi devono essere comunicati al Garante, al fine di consentire a questa Autorità di svolgere efficacemente il ruolo di controllo attribuitole (art. 19 reg. cit.).

A questo fine, va posta particolare attenzione al fatto che la descritta attività è "servente" rispetto alla procedura di asilo; pertanto, è richiesto il rigoroso rispetto del principio di finalità del trattamento per tutte le operazioni compiute, dalla raccolta all'utilizzo, alla conservazione e alla comunicazione dei dati.

2.2. *Soggetti che hanno accesso ai dati registrati nell'Eurodac*

Profili critici

L'articolo 15, paragrafo 2, del regolamento Eurodac prevede che ciascuno Stato membro designi "le autorità" che possono accedere ai dati dallo stesso trasmessi e registrati nella banca dati centrale, e comunichi l'elenco di tali autorità alla Commissione europea. Solo tali autorità possono modificare, rettificare, integrare o cancellare i dati da esse inseriti (paragrafo 3).

L'Italia risulta avere designato il Servizio di polizia scientifica che, per sua stessa precisazione, fornisce solo il supporto tecnico alle attività di competenza degli uffici titolari della gestione delle pratiche di asilo e di quelle relative agli accertamenti Eurodac e non è, pertanto, in grado di assumere le responsabilità per le operazioni di trattamento indicate nell'art. 15, nonché per le attività, precisate al punto 2.1, che l'art. 13 del regolamento prevede a carico degli Stati membri e delle autorità da questi designate.

Prescrizioni

Ferme restando le attribuzioni di carattere tecnico del Servizio di polizia scientifica, devono essere individuati dal titolare (o dai co-titolari) del trattamento i soggetti ("le autorità") che assicurino il giusto livello di responsabilità richiesto dagli artt. 13 e 15 del regolamento nelle decisioni di modifica, rettifica, integrazione e cancellazione dei dati inseriti nell'Eurodac.

Sempre al fine dell'espletamento delle necessarie attività di controllo, gli estremi identificativi dei soggetti investiti di tale responsabilità devono essere anch'essi comunicati al Garante, come pure i soggetti che hanno accesso ai risultati delle ricerche in Eurodac, in particolare a quelle relative ai confronti con le categorie b) e c) indicate al punto 1. del presente provvedimento.

2.3. *Finalità dell'accesso al sistema Eurodac*

Profili critici

I rilievi esposti ai punti che precedono evidenziano la mancanza di una chiara definizione dei livelli di responsabilità delle diverse autorità che partecipano al sistema e di una procedura definita e formalizzata che consenta di monitorare il grado di corretta applicazione delle regole che disciplinano il trattamento dei dati da parte dei diversi uffici abilitati, sul territorio nazionale, ad assumere decisioni rilevanti riguardo ai diritti delle persone e a inserire, correggere, richiamare, utilizzare i dati personali conservati nella base di dati gestita dall'unità centrale.

In particolare, per quanto riguarda l'Italia, la Commissione europea e il Garante europeo hanno segnalato l'alto numero di accessi nella base dati centrale giustificati ai sensi dell'art. 18 del regolamento (le cd. "ricerche speciali"), il quale prevede che in ciascuno Stato membro l'interessato può esercitare i diritti di accesso, comunicazione, rettifica e cancellazione dei dati personali che lo riguardano. Nel corso degli accertamenti è risultato che in nessuno dei casi segnalati l'accesso ai dati era stato effettuato su richiesta dell'interessato; né, sono state presentate a questa Autorità istanze di interessati volte a esercitare i diritti conferiti dall'art. 18. In risposta alla richiesta dell'Autorità di verificare la legittimità degli accessi, il Servizio di polizia scientifica presso il Dipartimento della pubblica sicurezza è intervenuto assicurando di avere disattivato per gli uffici periferici tale possibilità di accesso ai dati, che attualmente potrebbe essere effettuato solo presso il Servizio stesso. Nonostante tale assicurazione, e benché il numero di tali casi sia diminuito fortemente, la Commissione europea, nei suoi report trimestrali, ha continuato a segnalare richieste di accesso ai sensi dell'art. 18 non basate su istanze degli interessati.

Prescrizioni

Il titolare e gli eventuali responsabili del trattamento, che vanno individuati ai sensi della prescrizione di cui al punto 2.1, devono adottare un'idonea regolamentazione volta a garantire che l'accesso ai dati gestiti dall'unità centrale sia limitato alle sole finalità previste dal regolamento Eurodac. In particolare, va garantita la conoscibilità di ogni accesso per le *cd.* "ricerche speciali" previste dall'art. 18 del regolamento; deve essere altresì assicurato che solo le autorità competenti per la procedura di asilo possano accedere ai risultati del confronto tra i dati dei soggetti appartenenti alle categorie c) e b) e quelli dei soggetti appartenenti alla categoria a) di cui al punto 1 del presente provvedimento.

2.4. *Formazione del personale e diritti degli interessati*

Profili critici

Con circolare del gennaio 2003 il Dipartimento della pubblica sicurezza ha informato gli uffici di polizia sul territorio dell'imminente entrata in vigore del regolamento Eurodac e ha impartito le relative istruzioni. La circolare fa riferimento alla necessità di garantire i diritti delle persone e reca in allegato un modulo per l'informativa da rendere agli interessati, redatto in più lingue, che viene consegnato alla persona e da questa sottoscritto all'atto del fotosegna-

lamento. Nel corso dell'accertamento del Garante le suddette istruzioni sono state reiterate. Dalle informazioni acquisite non risulta peraltro che finora alcun interessato –direttamente o attraverso il proprio legale o organizzazioni umanitarie– abbia esercitato i diritti conferiti dall'art. 18.

Mancano inoltre informazioni certe sull'effettivo utilizzo del modulo da parte di tutte le questure.

Prescrizioni

Il titolare e gli eventuali responsabili del trattamento devono garantire un'adeguata formazione del personale, in particolare in merito all'uso legittimo delle cd. "ricerche speciali", e assicurare che l'intera procedura, dall'identificazione della persona alla decisione sulla richiesta di asilo avvenga nel rispetto della dignità dell'interessato.

In coerenza con quanto previsto dal regolamento Eurodac, il titolare e gli eventuali responsabili del trattamento devono assicurare il puntuale rispetto di quanto previsto nell'articolo 18, fornendo le informazioni previste e precisando le relative procedure al fine di mettere l'interessato nella condizione di esercitare i diritti riconosciutigli. Al riguardo, l'informativa non risulta del tutto adeguata rispetto a quanto prescritto dall'art. 18, con particolare riferimento all'indicazione del titolare (o co-titolari) del trattamento dai dati (l'informativa attualmente fornita indica come responsabile del trattamento dei dati il Gabinetto di polizia scientifica che procede all'operazione di fotosegnalamento), degli specifici diritti che possono essere esercitati dagli interessati e delle autorità (Garante e autorità giudiziaria) a cui presentare un eventuale ricorso.

Si rende quindi necessario aggiornare il testo dell'informativa attualmente fornita con l'inserimento di tali ulteriori informazioni.

2.5. *Misure di sicurezza*

In relazione agli elementi acquisiti, la particolare natura dei dati induce a evidenziare la necessità che, ferme restando le cautele attualmente previste dagli artt. 31 e ss. e dall'Allegato B. al Codice, vengano adottate, da parte degli organi interessati dalla procedura, ulteriori misure e accorgimenti, di seguito indicati, volti a rafforzare il livello di protezione delle informazioni oggetto di trattamento, anche in attuazione dell'obbligo di garantire la sicurezza dei dati prima, durante e dopo la trasmissione all'unità centrale, nonché dei dati ricevuti dall'unità centrale che l'art. 13, paragrafo 2, del regolamento n. 2725/2000 pone a carico di ogni Stato membro.

2.5.1. *Credenziali di autenticazione presso il Servizio di polizia scientifica*

Profili critici

Presso il Servizio di polizia scientifica del Dipartimento della pubblica sicurezza vengono conservati i log file relativi al tracciamento delle operazioni effettuate sulle impronte digitali destinate a confluire in Eurodac (e in A.f.i.s) dai gabinetti provinciali e regionali della polizia scientifica. Nei log vengono memorizzate le attività svolte, il nome dell'utente, il codice della postazione client di provenienza della richiesta, il numero originario identificativo dell'operazione effettuata dal client e il codice A.f.i.s..

L'accesso alla sala macchine che ospita il server centrale è consentito mediante badge profilato.

L'accesso degli amministratori al database dei log Eurodac (e A.f.i.s.) avviene mediante credenziali di autenticazione (username e password) condivise tra il personale dell'area Gruppo sistemistico sezione A.f.i.s..

Prescrizioni

Per l'accesso al database Eurodac (e A.f.i.s.), a ogni incaricato deve essere assegnata o associata individualmente almeno una credenziale di autenticazione costituita da un codice utente e da una parola chiave composta da non meno di otto caratteri, che deve essere modificata dall'incaricato al primo utilizzo e, successivamente, almeno ogni tre mesi.

2.5.2. *Conservazione dei fascicoli cartacei presso l'Unità Dublino*

Profili critici

Presso l'Unità Dublino del Dipartimento per le libertà civili e l'immigrazione vengono conservati, in numero di oltre 90.000, i fascicoli cartacei relativi ai soggetti i cui dati personali vengono trattati dall'Unità in relazione ai compiti da questa svolti nell'ambito della procedura che disciplina Eurodac. Si tratta di dati anche biometrici (le impronte digitali contenute nei cartellini dattiloscopici) e di carattere giudiziario, tra i quali le informazioni relative agli interessati acquisite dal Centro elaborazioni dati del Dipartimento della pubblica sicurezza.

Allo stato, i fascicoli sono sistemati in armadi privi di chiusura collocati in stanze non chiuse a chiave. Sono in corso attività volte a dotare di serrature gli armadi e le stanze.

É installato un impianto di rilevazione incendi e un sistema di videosorveglianza, che entra in funzione al di fuori dell'orario di lavoro del personale.

Prescrizioni

I dati personali contenuti nei fascicoli cartacei devono essere custoditi e controllati con modalità che riducano al minimo i rischi di distruzione o perdita o di accesso non autorizzato.

L'accesso ai locali ove sono custoditi i fascicoli va consentito previa adozione di un sistema di controllo basato sull'utilizzo di una tessera individuale (ad esempio, un badge profilato) a disposizione dei soli soggetti incaricati del trattamento delle informazioni.

I fascicoli devono essere collocati in armadi ignifughi dotati di idonee serrature di sicurezza.

I varchi di accesso ai locali devono essere anch'essi dotati di idonee serrature di sicurezza.

2.5.3 *Trattamento dei dati con strumenti elettronici presso l'Unità Dublino*

Profili critici

Lo scambio di informazioni e documentazione con uffici esterni all'Unità (omologhi uffici di Stati membri e questure) avviene mediante posta elettronica certificata e non, posta tradizionale e fax, con esclusione, quanto al fax, della trasmissione dei cartellini dattiloscopici, causa la cattiva risoluzione dell'immagine.

L'accesso alle postazioni informatiche da parte del personale avviene mediante credenziali di autenticazione personale di dominio Windows.

L'accesso all'applicazione web DubliNET, attraverso cui l'Unità gestisce i dati e le comunicazioni con gli Stati membri, avviene attraverso un sito non Ssl (Secure Socket Layer) e, quindi, senza certificato di sicurezza.

Le credenziali di autenticazione (username e password) per l'accesso all'applicazione DubliNET sono condivise fra i vari operatori.

La documentazione scaricabile dal sistema DubliNET (ad esempio, in formato Pdf), ivi compresi i cartellini dattiloscopici, viene firmata digitalmente dal mittente, ma le postazioni informatiche in uso al personale dell'Unità non sono dotate del sistema di verifica della firma digitale (all'interno del file nell'area dedicata alla firma digitale risulta presente un punto interrogativo).

Gli accessi all'applicazione DubliNET e le operazioni compiute sui dati vengono tracciate.

Prescrizioni

Lo scambio di informazioni e documentazione da e verso l'Unità Dublino deve avvenire con modalità che assicurino la provenienza della comunicazione e l'integrità del suo contenuto.

Le comunicazioni devono quindi avvenire esclusivamente attraverso posta elettronica certificata e i documenti trasmessi devono essere cifrati.

Per l'accesso all'applicazione web DubliNET, a ogni incaricato deve essere assegnata o associata individualmente almeno una credenziale di autenticazione costituita da un codice utente e da una parola chiave composta da non meno di otto caratteri, che deve essere modificata dall'incaricato al primo utilizzo e, successivamente, almeno ogni tre mesi.

3. TERMINE PER ATTUARE LE PRESCRIZIONI DEL GARANTE

Attesa la particolare delicatezza dei dati in questione, il Garante constata la necessità che le prescritte modificazioni e integrazioni da apportare al trattamento siano adottate entro termini brevi, decorrenti dalla data di ricezione del presente provvedimento, che risulta congruo fissare:

a) in trenta giorni, relativamente alle misure di sicurezza concernenti l'adozione delle credenziali individuali di autenticazione da parte del personale dell'area Gruppo sistemistico sezione A.f.i.s. del Servizio di Polizia scientifica del Dipartimento della pubblica sicurezza e degli operatori dell'Unità Dublino del Dipartimento per le libertà civili e l'immigrazione;

b) in sei mesi, relativamente alle altre modificazioni e integrazioni, ivi comprese le ulteriori misure di sicurezza prescritte (punto 2.5).

Il Ministero, che allo stato risulta titolare del trattamento, è invitato a fornire riscontro al decorso di ciascuno di tali termini circa l'attuazione delle presenti prescrizioni.

TUTTO CIÒ PREMESSO IL GARANTE

1) ai sensi degli artt. 154, comma 1, lett. c) e 160 del Codice dispone che il Ministero dell'interno adotti le prescritte modificazioni e integrazioni al trattamento dei dati personali effettuati in attuazione del regolamento n. 2725/2000 istitutivo del sistema Eurodac e della Convenzione di Dublino relativamente a:

   a) individuazione e comunicazione al Garante degli estremi identificativi del titolare (o co-titolari) e eventuali responsabili del trattamento, con indicazione dei compiti e delle responsabilità dei vari soggetti che effettuano il trattamento dei dati nell'ambito della procedura, al fine di assicurare la liceità del trattamento, la correttezza e sicurezza dei dati e il rigoroso rispetto del principio di finalità del trattamento per tutte

le operazioni compiute, dalla raccolta all'utilizzo, alla conservazione e alla comunicazione dei dati (punto 2.1);

b) individuazione e comunicazione al Garante degli estremi identificativi dei soggetti "le autorità") che assicurino il livello di responsabilità richiesto dagli artt. 13 e 15 del regolamento n. 2725/2000 nelle decisioni di modifica, rettifica, integrazione e cancellazione dei dati registrati presso la banca dati centrale e che possono accedere ai risultati delle ricerche nel sistema, in particolare a quelle relative ai confronti con le categorie b) e c) indicate al punto 1 del presente provvedimento (punto 2.2);

c) adozione di una idonea regolamentazione volta a garantire che l'accesso ai dati gestiti dall'unità centrale sia limitato alle sole finalità previste dal regolamento n. 2725/2000 e alle sole autorità competenti per la procedura di asilo, con particolare riferimento alle cd. "ricerche speciali" di cui all'art. 18 del regolamento (punto 2.3);

d) formazione del personale in relazione al trattamento dei dati effettuato nel corso della procedura, con particolare riferimento all'uso legittimo delle cd. "ricerche speciali"; aggiornamento del testo dell'informativa da rendere all'interessato con particolare riferimento all'inserimento dell'indicazione del titolare (o co-titolari) del trattamento dei dati e degli specifici diritti che possono essere esercitati dagli interessati e delle autorità (Garante e autorità giudiziaria) a cui presentare un eventuale ricorso (punto 2.4);

2) ai sensi degli artt. 154, comma 1, lett. c) e 160 del Codice dispone che il Ministero dell'interno adotti adeguate misure di sicurezza nel trattamento dei dati, volte a rafforzare il livello di protezione delle informazioni trattate nell'ambito del sistema Eurodac, con particolare riferimento a (punto 2.5):

a) assegnazione al personale dell'area Gruppo sistemistico sezione A.f.i.s. del Servizio di Polizia scientifica del Dipartimento della pubblica sicurezza e del personale dell'Unità Dublino del Dipartimento per le libertà civili e l'immigrazione di credenziali individuali di autenticazione costituite da un codice utente e da una parola chiave composta da non meno di otto caratteri, che deve essere modificata dall'incaricato al primo utilizzo e, successivamente, almeno ogni tre mesi;

b) conservazione dei fascicoli cartacei presso l'Unità Dublino del Dipartimento per le

libertà civili e l'immigrazione in armadi ignifughi dotati di serrature di sicurezza collocati in locali con accesso consentito previa adozione di un sistema di controllo basato sull'utilizzo di una tessera individuale (ad esempio, un badge profilato) a disposizione dei soli soggetti incaricati del trattamento delle informazioni e con varchi dotati di idonee serrature di sicurezza;

c) trattamento dei dati con strumenti elettronici presso la medesima Unità mediante comunicazioni basate sull'uso esclusivo di posta elettronica certificata e sulla trasmissione di documenti cifrati;

3) ai sensi delle medesime disposizioni prescrive che le suesposte modificazioni e integrazioni da apportare al trattamento siano adottate entro il termine, decorrente dalla data di ricezione del presente provvedimento, di trenta giorni relativamente alle misure di sicurezza concernenti l'adozione delle credenziali individuali di autenticazione da parte del personale dell'area Gruppo sistemistico sezione A.f.i.s. del Servizio di Polizia scientifica del Dipartimento della pubblica sicurezza e del personale dell'Unità Dublino del Dipartimento per le libertà civili e l'immigrazione, e di sei mesi relativamente alle altre modificazioni e integrazioni, ivi comprese le ulteriori misure di sicurezza prescritte, fornendo riscontro a questa Autorità circa la loro attuazione al decorso dei medesimi termini.

Roma, 29 maggio 2008

IL PRESIDENTE
Pizzetti

IL RELATORE
Fortunato

IL SEGRETARIO GENERALE
Buttarelli

27. Recepimento normativo in tema di dati di traffico telefonico e telematico (*)

ALLEGATO A

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Nella riunione odierna, in presenza 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 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.

(*) Gazzetta Ufficiale 13 agosto 2008, n. 189 [doc. *web* n. 1538237], in inglese [doc. *web* n. 1542849]

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.

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 con-

servazione 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 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 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 l., con modificazioni, dall'art. 1 l. 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 limi-

tino 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 prevedeva temporaneamente la conservazione (lett. d) sopra citata), la normativa di riferimento prescriveva 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 prescriveva 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, introduceva la prescrizione, tutt'ora vigente, che la conservazione dei predetti dati fosse 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.

La direttiva è stata recepita con il d.lg. 30 maggio 2008, n. 109, che ha previsto un periodo unico di conservazione pari a 24 mesi per i dati di traffico telefonico, a 12 mesi per i dati di traffico telematico e a 30 giorni per i dati relativi alle chiamate senza risposta, senza ulteriori distinzioni in base al tipo di reato.

La legge 18 marzo 2008, n. 48, di ratifica della Convenzione del Consiglio d'Europa sulla criminalità informatica fatta a Budapest il 23 novembre 2001 ha poi previsto una specifica ipotesi di conservazione temporanea dei dati relativi al traffico telematico a fini di svolgimento di investigazioni preventive o di accertamento e repressione di reati.

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 nelle 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;
- 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 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 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).

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. parere n. 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; parere n. 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; parere n. 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.

Tali misure e accorgimenti devono essere adottati dai fornitori di comunicazione elettronica anche in caso di conservazione temporanea dei dati relativi al traffico telematico a fini di svolgimento di investigazioni preventive o di accertamento e repressione di reati, ai sensi del menzionato art. 132, comma 4 ter, del Codice.

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.

Tale fase di autenticazione può essere realizzata con procedure strettamente integrate alle applicazioni informatiche con cui il fornitore tratta i dati di traffico, oppure con procedure per la protezione delle singole postazioni di lavoro che si integrino alle funzioni di autenticazione proprie dei sistemi operativi utilizzati. Nel secondo caso, il fornitore deve assicurare che non esistano modalità di accesso alle applicazioni informatiche da parte dei propri incaricati di trattamento che consentano di eludere le procedure di strong authentication predisposte per l'accesso alla postazione di lavoro.

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 data base) 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 e, infine, dalle funzioni di trattamento dei dati in caso di esercizio dei diritti dell'interessato (art. 7 del Codice).

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.

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 con-

cernente 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'esercizio delle relative procedure informatiche, nei data base 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, data base administrator e manuten-

tori 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 30 aprile 2009, ovvero per quanto riguarda la strong authentication riferita agli incaricati che accedono ai dati di traffico nell'ambito dell'attività di call center, al 30 giugno 2009. 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 data base) 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 tec-

nologie 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 data base) 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, 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 utiliz-

zati 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. 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 data base 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 prov-

vedimento 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 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;

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 data base 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 30 aprile 2009, 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 30 aprile 2009, ovvero per quanto riguarda la strong authentication riferita agli incaricati che accedono ai dati di traffico nell'ambito dell'attività di call center, 30 giugno 2009, 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 data base) 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 data base 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

28. Anagrafe tributaria: sicurezza e accessi (*)

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);

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 prof. Francesco Pizzetti;

PREMESSO

Sulla base di un'analisi preliminare del sistema informativo della fiscalità, il 14 dicembre 2007 il Garante ha deliberato l'avvio di accertamenti volti a verificare, in più fasi, i trattamenti di dati personali effettuati presso l'anagrafe tributaria, rilevando che elementi di maggior criticità e urgenza erano da ravvisarsi nelle misure di sicurezza adottate per gli accessi da parte di enti esterni, pubblici e privati, all'amministrazione finanziaria.

La prima fase di accertamenti attinente a tali accessi è stata completata. Il Garante svolgerà nel prosieguo le altre verifiche programmate sul trattamento dei dati effettuato dalle articolazioni dell'amministrazione finanziaria, con particolare riguardo alla struttura degli archivi, alle modalità di accesso, alle applicazioni utilizzate, alle tipologie di informazioni, alle misure di sicurezza, alle abilitazioni e alle autorizzazioni degli utenti.

Le attività ispettive completate hanno invece riguardato, in particolare:

1) il controllo degli applicativi che consentono l'accesso all'anagrafe tributaria a soggetti esterni all'amministrazione finanziaria (loro funzionalità; tipologie di dati visualizzabili con i differenti profili di autorizzazione previsti);
2) la designazione di responsabili e di incaricati, i sistemi di autenticazione (ad es., modalità di formazione e gestione delle password; controlli degli accessi ai sistemi applicativi)

(*) [doc. *web* n. 1549548]

e i sistemi di autorizzazione;

3) le procedure di audit interno ed esterno sull'accesso alle informazioni contenute nell'anagrafe tributaria (ad es., controlli sulle abilitazioni e sulle autorizzazioni degli utenti abilitati all'utilizzo degli applicativi, modalità di raccolta dei logfile e loro analisi automatizzata).

Gli accertamenti ispettivi hanno avuto luogo presso l'Agenzia delle entrate, Sogei S.p.A. (Società generale d'informatica, responsabile del trattamento dei dati contenuti nell'anagrafe tributaria), regioni, province, comuni e altri enti che accedono a tale anagrafe, con la piena collaborazione degli enti coinvolti. Le verifiche hanno consentito di evidenziare criticità, in ambito sia informatico, sia organizzativo, documentate nei verbali in atti.

Dalle risultanze emerge che i sistemi di collegamento all'anagrafe tributaria utilizzati dai soggetti esterni all'amministrazione finanziaria sono i seguenti:

- "Siatel", applicazione web utilizzata principalmente da comuni, province, regioni, università, asl e consorzi di bonifica, per un totale di circa 9.400 enti e 60.000 utenze, che consente di visualizzare dati anagrafici completi, dati fiscali e atti del registro relativi alla totalità dei contribuenti;
- "Puntofisco", applicazione web di recente realizzazione e attualmente in dotazione a enti previdenziali, tribunali, camere di commercio e società varie, per un totale di circa 180 enti e 18.000 utenze. Puntofisco consente di visualizzare dati anagrafici, fiscali e atti del registro relativi alla totalità dei contribuenti, più aggiornati e con maggiore segmentazione delle informazioni rispetto a Siatel (ad es., differenziando tra dati anagrafici attuali o completi dello storico), ma permette anche di accedere a dati sensibili (presenti nel dettaglio degli oneri deducibili);
- "3270 enti esterni", collegamento diretto, tramite terminali fisici o emulatori di terminale, ai sistemi centrali dell'anagrafe tributaria, in corso di dismissione per esigenze di aggiornamento tecnologico, che tuttora consente a soggetti anche privati (Telecom Italia S.p.A., Enel, Inail, Inps, camere di commercio, Ministero delle politiche agricole, "interforze") di collegarsi a informazioni anagrafiche e fiscali relative alla totalità dei contribuenti; la struttura dell'applicativo non consente all'Agenzia delle entrate di conoscere il numero di utenti;
- "Entratel", applicativo utilizzato dagli enti principalmente ai fini della trasmissione delle

dichiarazioni, con flussi di dati solo in entrata verso l'Agenzia delle entrate; le credenziali di autenticazione fornite dall'Agenzia permettono altresì all'operatore di visualizzare la posizione fiscale dell'ente attraverso l'apposita web application ("Fisconline"/"Cassetto fiscale");

- "web services", strumenti realizzati sulla base di specifiche tecniche definite caso per caso dall'Agenzia delle entrate, che consentono di accedere a dati anagrafici anche completi relativi alla totalità dei contribuenti. Tali collegamenti sono utilizzati da 21 enti, ma la configurazione del collegamento non consente all'Agenzia di conoscere il numero di utenti;
- "file transfer", collegamenti per la gestione di flussi di dati per la gran parte in entrata (principalmente provenienti da banche), ma alcuni anche in uscita (ad es., verso concessionari della riscossione), utilizzati da circa 200 enti.

OSSERVA

Nel corso dei menzionati accertamenti ispettivi, sulla base della documentazione in atti, sono state riscontrate alcune criticità di seguito descritte, già in parte riconosciute dall'Agenzia, relative agli accessi all'anagrafe tributaria da parte degli enti esterni all'amministrazione finanziaria, riferibili in particolare alle autenticazioni e alle autorizzazioni degli utenti, ai controlli da parte dell'Agenzia e alle estese possibilità di accesso alle banche dati. Accanto a diverse problematiche attinenti alla sicurezza, sono emersi e vengono affrontati connessi profili concernenti aspetti sostanziali del trattamento.

Il Garante, ai sensi dell'art. 154, comma 1, lett. c) del Codice, ritiene necessario prescrivere una serie di misure e accorgimenti che devono essere adottati dall'Agenzia delle entrate, anche in riferimento ai soggetti esterni che accedono all'anagrafe tributaria, di seguito indicati. Tali misure e accorgimenti, principalmente di carattere tecnico e organizzativo, sono necessari al fine di porre rimedio alle carenze riscontrate e a incrementare, in particolare, i livelli di sicurezza degli accessi all'anagrafe tributaria, rendendo il trattamento conforme alle disposizioni vigenti.

1. ACCESSI ALL'ANAGRAFE TRIBUTARIA DA PARTE DI SOGGETTI ESTERNI ALL'AMMINISTRAZIONE FINANZIARIA: PROFILI GENERALI

Criticità

Alcuni accertamenti in proposito sono risultati meno agevoli in considerazione del fatto che l'Agenzia non aveva immediatamente disponibile, come richiesto dall'Autorità, una completa documentazione relativa sia ai soggetti esterni collegati, sia ai sistemi di accesso utilizzati da questi ultimi (numero e categorie di soggetti, finalità degli accessi e tipologie di collegamenti e di dati comunicati).

Dagli atti emerge ora che l'Agenzia autorizza gli accessi all'anagrafe tributaria solo in seguito alla stipula di apposite convenzioni, anche standard, a livello centrale e regionale. Tuttavia, l'assenza di una documentazione di insieme sui collegamenti in essere non agevola un monitoraggio costante sulla sussistenza dei presupposti che hanno consentito l'attivazione del canale informativo, nonché i dovuti controlli sulla correttezza della gestione degli accessi e della consultazione delle informazioni. La periodica ricognizione degli enti che accedono all'anagrafe tributaria, e dei rispettivi utenti, costituisce infatti la premessa per prevenire usi impropri e illeciti delle informazioni in essa contenute.

È stato inoltre riscontrato in atti che in alcune convenzioni stipulate per l'accesso all'anagrafe tributaria non risultano delimitate chiaramente le finalità per cui gli accessi vengono autorizzati; sotto tale aspetto, è stato rilevato che alcuni enti, attraverso gli amministratori locali (soggetti deputati all'abilitazione degli utenti), hanno abilitato di propria iniziativa alcuni utenti al fine di attivare nuovi flussi di dati per finalità ulteriori rispetto a quelle consentite.

Non risulta altresì dagli atti che gli operatori che effettuano gli accessi abbiano l'onere (o la possibilità) di registrare, anche al fine di successivi controlli, le ragioni a supporto delle interrogazioni eseguite.

È stato inoltre verificato che i dati visualizzabili attraverso gli applicativi non sono segmentabili in relazione al bacino di utenza dell'ente che chiede il collegamento (ad es., territorio comunale), e sono relativi a tutto il territorio nazionale.

Infine, le informazioni consultabili non risultano, talvolta, sufficientemente aggiornate per lo svolgimento delle funzioni istituzionali cui gli accessi sono finalizzati (ad es., in Siatel, ai fini

della verifica dell'Isee non sono visualizzabili i dati dell'ultima dichiarazione presentata e vengono invece visualizzati dati reddituali riferiti ad annualità pregresse, eccedenti e non pertinenti rispetto alle finalità perseguite, che non consentono di effettuare i puntuali controlli sulle autocertificazioni reddituali ai sensi del d.P.R. n. 445/2000).

Da ultimo, sulla base delle risultanze in atti, è stato rilevato che gli accessi all'anagrafe tributaria vengono effettuati talvolta per conoscere informazioni (ad es., la residenza) che, ai sensi della normativa vigente, dovrebbero essere invece controllate presso altri soggetti (ad es., amministrazioni certificanti ai sensi dell'art. 71 del d.P.R. n. 445/2000).

Prescrizioni

L'Agenzia deve disporre di informazioni complete e strutturate sulla molteplicità di soggetti che, a vario titolo, accedono alla banca dati dell'anagrafe tributaria. Occorre pertanto che la stessa rediga un documento, con formalità descrittive standard, che riporti tutti i flussi di trasferimento di dati da e verso l'anagrafe tributaria e tutti gli accessi di tipo interattivo, batch o di altro genere, specificando per ciascun flusso o accesso l'identità dei soggetti legittimati a realizzarlo, la base normativa (anche ai sensi dell'art. 19, comma 2 del Codice, previa comunicazione al Garante), la finalità istituzionale, la natura e la qualità dei dati trasferiti o a cui si è avuto accesso, la frequenza e il volume dei trasferimenti o degli accessi e il numero di soggetti che utilizzano la procedura. Tale documento dovrà essere mantenuto costantemente aggiornato, nonché reso disponibile nel caso di controlli.

L'Agenzia deve altresì verificare, con cadenza periodica annuale, l'attualità delle finalità per cui ha concesso l'accesso agli enti esterni, anche con riferimento al numero di utenze attive, inibendo gli accessi (autorizzazioni o singole utenze) effettuati al di fuori dei presupposti riconducibili all'art. 19 del Codice (norme di legge o regolamento, nonché eventuali comunicazioni al Garante ai sensi dell'art. 19 del Codice) e quelli non conformi a quanto stabilito nelle convenzioni. All'esito di tali verifiche, in particolare, devono essere eliminati gli accessi effettuati per conoscere informazioni che, ai sensi della normativa vigente, dovrebbero essere invece controllate presso altri soggetti.

Per vincolare effettivamente gli accessi alle finalità consentite, l'Agenzia deve introdurre nelle applicazioni volte all'uso interattivo da parte di incaricati un campo per l'indicazione obbliga-

toria del numero di riferimento della pratica (ad es. numero del protocollo o del verbale) nell'ambito della quale viene effettuata la consultazione.

L'Agenzia deve poi far sì che gli applicativi consentano, per quanto più possibile, la segmentazione dei dati visualizzabili -in particolare in modo cronologico (attuale o storico, per periodi di imposta), geografico (comune, provincia, regione) e per tipologia di dati (ad es. di sintesi)- al fine di rendere consultabili dall'utente, anche in base al proprio profilo e in relazione al bacino di utenza dell'ente che chiede il collegamento, esclusivamente i dati necessari rispetto alle finalità perseguite (ad es. l'ultimo domicilio fiscale o l'ultimo periodo di imposta).

2. I SISTEMI UTILIZZATI PER IL COLLEGAMENTO ALL'ANAGRAFE TRIBUTARIA

2.1. *Profili comuni*

Le principali criticità di carattere generale relative all'utilizzo degli applicativi riscontrate nel corso degli accertamenti ispettivi sugli accessi da parte dei soggetti esterni sono di seguito individuate.

2.1.1. Sicurezza dei sistemi di autenticazione

Criticità

Per le web application è stato utilizzato un certificato Ssl di tipo self signed (non firmato da una Ca, Certification authority, ufficiale) non attendibile che, in mancanza di una Ca affidabile, non offre le garanzie di certezza dell'identità dell'erogatore del servizio tipiche della certificazione digitale tramite Pki (public key infrastructure): risultano pertanto facilitate azioni di phishing in danno di utenti del sistema e la possibile acquisizione indebita di credenziali di autenticazione, idonea a consentire utilizzi impropri dell'applicazione.

Dalle risultanze agli atti emerge inoltre che, rispetto a taluni collegamenti, l'identificazione dell'utente finale dell'applicazione è in molti casi in capo all'ente esterno. L'Agenzia non ha pertanto alcuna conoscenza dell'effettiva identità e del numero degli utenti che accedono, con tali modalità di connessione, da sistemi informativi esterni collegati direttamente all'anagrafe tributaria (ad es., 3270 enti esterni e web services).

È risultato, poi, possibile accedere alle web application Siatel e Puntofisco attraverso l'utilizzo delle medesime credenziali contemporaneamente da postazioni diverse, anche con indirizzo Ip

diverso (perfino da rete esterna all'ente), nonostante, per quanto riguarda il Siatel, all'atto dell'accesso tale possibilità venga esclusa da un apposito avviso.

Prescrizioni

L'Agenzia deve prevedere che tutte le applicazioni accessibili da rete pubblica in forma di web application siano implementate con protocolli https/ssl provvedendo ad asseverare l'identità digitale dei server erogatori dei servizi tramite l'utilizzo di certificati digitali emessi da una Certification Authority ufficiale, evitando il ricorso a certificati di tipo self-signed.

Allo scopo di identificare le postazioni da cui vengono effettuati gli accessi, occorre inoltre che l'Agenzia implementi un sistema di certificazione digitale e di censimento delle postazioni terminali, in modo da realizzare procedure di autenticazione che, basandosi sul mutuo riconoscimento tra i server che erogano il servizio e le postazioni che accedono a esso, consentano di definire condizioni di accesso più complesse e sicure per determinate classi di incaricati o profili di autorizzazione.

A fronte dell'accertata possibilità per taluni applicativi di effettuare più accessi contemporanei con le medesime credenziali, al fine di consentire a ciascun utente di controllare l'utilizzo del proprio account, l'Agenzia deve poi prevedere -in considerazione della specificità dell'anagrafe tributaria- la visualizzazione, nella prima schermata successiva al collegamento, di informazioni relative all'ultima sessione effettuata con le stesse credenziali (almeno con l'indicazione di data, ora e indirizzo di rete da cui è stata effettuata la precedente connessione). Per accrescere la consapevolezza del controllo, le stesse informazioni devono essere riportate anche relativamente alla sessione corrente.

Infine, l'Agenzia deve disciplinare la possibilità di effettuare accessi contemporanei con le medesime credenziali (sessioni multiple), limitandone l'utilizzo ai soli casi necessari per esigenze di servizio (ad es., per le connessioni originate da una stessa postazione di lavoro). In ogni caso, tale possibilità deve essere consentita esclusivamente laddove il certificato digitale o l'indirizzo Ip siano sufficienti a discriminare l'identità digitale delle postazioni accedenti, come sopra descritto. Nel caso in cui non sia possibile individuare la postazione di lavoro, nelle more dell'attuazione delle prescrizioni sopra individuate, deve essere inibita la possibilità di accessi contemporanei.

2.1.2. Amministratori locali, abilitazioni e autorizzazioni

Criticità

È stato verificato negli accertamenti ispettivi che gli enti esterni hanno spesso affidato il compito di amministratore locale (il soggetto deputato alla gestione delle utenze) a personale non in grado né di valutare la pertinenza delle richieste di abilitazione delle utenze, né di monitorarne gli eventuali utilizzi impropri. In taluni enti è stata riscontrata la presenza di più amministratori locali con funzionalità che non consentivano di gestire gli utenti in modo tra loro coordinato.

Dalle risultanze agli atti è emerso, inoltre, che non è stato predeterminato un adeguato flusso informativo tra l'amministratore locale e l'unità organizzativa deputata alla gestione del personale al fine di consentire l'immediata disabilitazione o revisione del profilo di autorizzazione dei soggetti indirizzati ad altre mansioni o il cui rapporto con l'ente sia cessato.

Sono stati riscontrati poi casi di cessioni e condivisioni di credenziali di accesso, profili di autorizzazione inadeguati e/o eccessivi rispetto alle finalità perseguite, nonché mancate designazioni di incaricati al trattamento.

É stato verificato altresì che alcuni enti hanno utilizzato strumenti automatizzati di interrogazione che hanno consentito la duplicazione anche massiva di dati contenuti nell'anagrafe tributaria, con la creazione di autonome basi di dati, non conforme alle finalità per le quali è stato autorizzato l'accesso all'anagrafe tributaria.

Dalla documentazione in atti emerge che l'Agenzia, anche a seguito delle prime risultanze dell'attività ispettiva sopra illustrate, ha manifestato l'intenzione di voler gestire direttamente l'abilitazione di tutte le utenze, eliminando gli amministratori di sistema degli enti esterni.

Al riguardo, nonostante le predette criticità concernenti l'attività svolta dagli amministratori esterni, il modello decentrato di gestione delle utenze incentrato su tali figure, opportunamente integrato con le misure di seguito descritte, costituisce comunque il perno per un corretto sistema di accesso all'anagrafe tributaria. L'amministratore locale, infatti, è il soggetto più idoneo a controllare l'attività quotidiana dei propri utenti senza limitarne l'operatività, anche a fronte dell'ingente numero di enti, e quindi di utenti, abilitati ad accedere all'anagrafe tributaria, ognuno per il proprio specifico fabbisogno informativo.

Prescrizioni

L'Agenzia, nelle convenzioni che disciplinano l'accesso all'anagrafe tributaria, deve prevedere che gli "amministratori locali" (soggetti deputati alla gestione delle utenze) scelti dagli enti esterni siano individuati sulla base di elevati requisiti di idoneità soggettiva, preferibilmente tra soggetti che abbiano un rapporto stabile con essi. Questi soggetti, prima di intraprendere la loro attività, devono essere formati dall'Agenzia delle entrate in ordine alle funzionalità dell'applicativo e all'attività di autorizzazione degli utenti. L'amministratore locale dell'ente esterno che accede all'anagrafe tributaria deve rimanere il punto di riferimento per le richieste di abilitazione e autorizzazione con la possibilità di gestire direttamente le utenze; deve essere altresì dotato degli adeguati strumenti di controllo sugli accessi (cfr. punto 3).

Nelle convenzioni deve essere poi previsto che gli enti esterni, anche per mezzo degli amministratori locali, debbano istruire adeguatamente il personale addetto all'utilizzo dei vari applicativi in ordine al corretto utilizzo delle funzionalità dei software. Le convenzioni, entro i medesimi termini, devono inoltre imporre periodici controlli sugli accessi agli enti esterni -anche attraverso gli appositi strumenti di monitoraggio e alert in dotazione all'amministratore locale che saranno attivati dall'Agenzia (cfr. punto 3)- i cui esiti devono essere documentati secondo le modalità definite nelle convenzioni stesse.

Le convenzioni devono anche predefinire una procedura per le autenticazioni e le autorizzazioni che coinvolga attivamente le figure apicali degli uffici interessati e un unico supervisore (soggetto giuridicamente preposto all'individuazione degli utenti e dei profili). Il supervisore può anche non coincidere con l'amministratore tecnicamente deputato alla materiale gestione delle abilitazioni (e del relativo profilo), ma deve rispondere del controllo sullo stesso. Occorre inoltre che venga assicurato un flusso di comunicazione tra l'amministratore locale e l'articolazione che si occupa della gestione delle risorse umane, al fine di procedere alla tempestiva revisione del profilo di abilitazione o alla disabilitazione dei soggetti preposti ad altre mansioni o che abbiano cessato il rapporto con l'ente (soprattutto con riguardo ad enti di rilevanti dimensioni), anche con apposite verifiche a cadenza almeno trimestrale.

Per quanto riguarda la possibilità di individuare più amministratori locali per ciascun ente, l'Agenzia deve valutare e coordinare attentamente i profili di autorizzazione da attribuire, garan-

tendo in capo a un'unica figura la possibilità, ove occorra, di intervenire su tutti gli utenti anche amministratori, monitorandone l'operato (amministratore con ruolo di supervisore).

É necessario che l'Agenzia predefinisca anche soglie relative al numero di utenti abilitabili da ciascun ente in relazione alle sue dimensioni e alle finalità per le quale viene richiesto il collegamento. Le richieste di superamento di tali soglie devono essere valutate caso per caso dall'Agenzia stessa.

Le web application predisposte dall'Agenzia per l'utilizzo da parte di enti esterni vanno integrate con procedure di "autenticazione forte" (strong authentication) per ridurre la possibilità di usi impropri delle credenziali, la loro cessione o la loro sottrazione ai legittimi assegnatari. Tali procedure devono essere prefigurate nei confronti delle classi di utenti cui corrispondono profili di autorizzazione più critici in relazione alle funzioni o ai dati accessibili e, comunque, almeno per tutti i profili di autorizzazione corrispondenti alle funzioni di amministrazione locale delle applicazioni. Tali procedure potranno essere basate sull'utilizzo di dispositivi standard quali smart card o token per la generazione di one-time-password.

L'Agenzia deve infine prevedere limitazioni orarie per gli accessi, mantenendo la possibilità di specifiche deroghe adeguatamente motivate.

Le convenzioni stipulate con ciascun ente devono prevedere espressamente i vincoli necessari ad assicurare un corretto trattamento dei dati e devono stabilire le condizioni per escludere il rischio di duplicazione delle basi dati realizzata anche attraverso l'utilizzo di strumenti automatizzati di interrogazione.

2.2. *I singoli sistemi*

2.2.1. Siatel

Criticità

Con particolare riferimento all'applicativo Siatel, nel corso degli accertamenti sono state rilevate le seguenti criticità:

- l'area di gestione dei file da scaricare nella funzione "fornitura dati" disponibile per i comuni e le regioni riporta soltanto la data di primo download del file, che rimane da quel momento disponibile per ulteriori e illimitati download non censiti e, pertanto, non controllabili;

- le funzionalità di file transfer, predisposte per i comuni ai fini dell'allineamento dell'anagrafe tributaria con le anagrafi della popolazione, sono state talvolta utilizzate per finalità diverse, potendo determinare l'introduzione di informazioni errate nei sistemi;
- i dati anagrafici visualizzabili sono completi (ad es., forniscono sempre lo "storico" delle residenze) e non è possibile limitare la consultazione alle sole informazioni anagrafiche attuali.

Prescrizioni

L'Agenzia deve introdurre misure di controllo per la funzionalità di "fornitura dati" visualizzabile nell'apposita schermata dell'applicativo (ad es., rimuovendo il file messo a disposizione in rete dopo un certo tempo dalla richiesta, ovvero indicando il numero di operazioni di download già effettuate per ciascun file, l'utenza, la data e l'orario del download, nonché limitandoli alla sola utenza richiedente).

Con riferimento alle funzionalità di Siatel utilizzabili da parte degli operatori comunali a soli fini anagrafici, devono essere inserite nell'applicativo da parte dell'Agenzia specifiche indicazioni all'amministratore locale affinché vengano autorizzati solo utenti che agiscono presso l'ufficio anagrafe del comune.

2.2.2. Puntofisco

Criticità

In relazione al sistema Puntofisco è stato verificato dalle risultanze in atti che l'applicativo permette di visualizzare i dati sensibili relativi agli oneri deducibili contenuti nelle dichiarazioni dei redditi. L'amministratore locale ("gestore") non è in grado di visualizzare lo stato delle utenze (attiva/disattiva) e la lista utenti a lui disponibile comprende anche gli utenti già disabilitati. Il sistema di gestione delle utenze, inoltre, non permette regolarmente al gestore (amministratore), visualizzando il profilo dell'utente, di conoscere l'effettiva possibilità di accesso dello stesso al sistema.

Prescrizioni

Occorre aggiornare il profilo di autorizzazione assegnato agli enti esterni abilitati, escludendo a priori la consultabilità di dati sensibili laddove non sussista un'idonea base normativa che consenta la comunicazione di tale categoria di dati.

L'Agenzia deve inserire all'interno della procedura informatica di gestione degli utenti in uso

all'amministratore locale indicazioni che gli consentano di visualizzare lo status di tutte le utenze con i profili abilitativi correnti, comprese quelle già cancellate. Deve essere corretta altresì l'anomalia, relativa al sistema di gestione, che non permette regolarmente all'amministratore locale, visualizzando il profilo del singolo utente, di conoscerne l'effettiva possibilità di accesso dello stesso al sistema.

2.2.3. 3270 enti esterni, web services e file transfer

Criticità

Con riferimento alle risultanze ispettive, è stato rilevato che il collegamento denominato 3270 enti esterni, l'accesso tramite web service e lo scambio dati mediante file transfer non consentono attualmente di limitare e controllare gli accessi in relazione alla loro provenienza, e non garantiscono misure idonee a verificare il rispetto delle regole di sicurezza di cui all'Allegato B del Codice. In particolare, è risultato che:

- l'Agenzia non è in grado di quantificare i soggetti che accedono ai dati, di attribuire agli stessi le operazioni tracciate dal sistema e di verificare il rispetto delle misure di sicurezza poiché l'identificazione degli end-user degli applicativi è affidata all'ente esterno che chiede il collegamento, come anche l'attribuzione certa a ogni incaricato di una o più credenziali per l'autenticazione, nonché la periodica scadenza della parola chiave;
- è impossibile per l'Agenzia individuare la postazione che effettua gli accessi, risultando assenti idonei sistemi che la consentirebbero quali, ad esempio, la certificazione digitale sulle postazioni e sugli emulatori di terminale utilizzati.

Prescrizioni

Devono essere garantite condizioni adeguate di protezione dei dati personali, di controllo e di verifica delle attività compiute (funzioni di audit) sugli applicativi utilizzati per accedere all'anagrafe tributaria, nonché strumenti che permettano all'Agenzia di verificare il rispetto delle misure di sicurezza.

Per quanto riguarda gli accessi all'anagrafe tributaria effettuati mediante l'applicativo 3270 enti esterni gli enti ad oggi abilitati devono migrare verso applicativi che offrono maggiori garanzie (ad es., Puntofisco o Siatel).

Con riferimento ai web service, l'Agenzia deve effettuare una ricognizione dei servizi al

momento esposti e sospenderne l'attività in attesa della revisione delle attuali modalità di implementazione con le adeguate misure e gli accorgimenti di seguito descritti.

Laddove, infatti, l'Agenzia intenda impiegare web service esposti anche in una rete pubblica per l'utilizzo da parte di enti esterni, questi, in considerazione della delicatezza delle informazioni contenute nell'anagrafe tributaria, anche al fine di evitare duplicazioni delle banche dati e rischi di disallineamento, devono essere configurati offrendo un livello minimo di accesso ai dati e limitando i risultati delle interrogazioni a valori di tipo booleano (ad es., web service che forniscono un risultato di tipo vero/falso nel caso di controlli sull'esistenza o sulla correttezza di un determinato codice fiscale). Le convenzioni per l'utilizzo di tali servizi, inoltre, devono prevedere stringenti condizioni d'uso tali da consentire anche un'effettiva capacità di controllo da parte dell'Agenzia. Dal punto di vista tecnico, tali condizioni d'uso dei web service devono essere trasposte in appositi "accordi di servizio", redatti secondo il modello della cooperazione applicativa impiegata all'interno del sistema pubblico di connettività istituito dal Codice dell'amministrazione digitale. Gli "accordi di servizio" devono individuare idonee garanzie per il trattamento dei dati personali, prevedendo, in particolare, il tracciamento delle operazioni compiute in cooperazione applicativa, con possibilità di identificazione dell'utente che accede ai dati, il timestamp, l'indirizzo Ip di provenienza dell'utente e del server interconnesso, l'operazione effettuata e i dati trattati.

I collegamenti per la gestione di flussi di dati mediante file transfer devono essere realizzati su canali di connessione sicuri e l'Agenzia deve garantire, anche attraverso la configurazione dei sistemi, che le credenziali di abilitazione utilizzate dagli operatori dell'ente esterno rispettino le prescrizioni indicate nell'Allegato B al Codice, in particolare identificando il soggetto che effettua lo scambio dei dati e prevedendo che la parola chiave prevista sia soggetta a scadenza periodica secondo i termini ivi indicati.

2.2.4. Entratel

Criticità

Dagli accertamenti ispettivi è emerso che le caratteristiche tecniche di Entratel, in uso dal 1998, sono state realizzate al fine di consentire al tempo la massima fruibilità dell'applicativo anche a soggetti con limitate risorse tecnologiche. Allo stato degli atti, le credenziali attribuite

dall'Agenzia (anche le chiavi asimmetriche) identificano però solo l'ente richiedente, anziché l'operatore finale. Per quanto riguarda l'accesso all'applicativo Fisconline/Cassetto fiscale, le password non sono soggette a scadenza periodica.

Prescrizioni

L'Agenzia deve configurare Entratel e Fisconline/Cassetto fiscale in modo da poter verificare il rispetto delle prescrizioni indicate nell'Allegato B al Codice relative, in particolare, al sistema di scadenza delle password e all'attribuzione di credenziali idonee ad identificare direttamente, oltre all'ente abilitato, anche il singolo incaricato che fisicamente effettua l'accesso, autentica e trasmette i file.

3. LE PROCEDURE DI *AUDIT* SULL'ACCESSO ALLE INFORMAZIONI CONTENUTE NELL'ANAGRAFE TRIBUTARIA DA PARTE DI SOGGETTI ESTERNI

Criticità

Gli accertamenti hanno permesso di verificare che tutti i file di log relativi alle transazioni effettuate nell'anagrafe tributaria sono conservati a tempo indeterminato da Sogei S.p.a., quelli relativi agli ultimi sette giorni sono mantenuti in linea, mentre quelli precedenti sono conservati su nastri magnetici. Talvolta Sogei S.p.a., di propria iniziativa, al fine di monitorare anomalie e funzionalità del sistema, ha eseguito alcuni rilievi quantitativi sulle transazioni effettuate provvedendo a segnalare all'Agenzia le attività difformi riscontrate.

Secondo quanto si evince dalla documentazione in atti, l'Agenzia dispone di uno strumento di business intelligence denominato Vermont che, per quanto riguarda gli enti esterni, consente di controllare gli accessi effettuati dagli utenti con Siatel (e non quindi, in particolare, con Puntofisco e web services) dal 1° gennaio 2005 alle informazioni loro disponibili. Tale strumento permette poi monitoraggi statistici degli accessi e la predisposizione di sistemi di alert. Vermont utilizza database multidimensionali e consente di visualizzare i log relativi a un'interrogazione delle cd. "informazioni generalizzate at" (principalmente, dati anagrafici e fiscali contenuti in anagrafe tributaria), mentre quelli relativi alle variazioni delle utenze o agli accessi a dati diversi, pur essendo registrati, non vengono rilevati da tale sistema. Analogo strumento è in dotazione anche a Sogei S.p.a.

Sulla base delle risultanze ispettive, è possibile rilevare tuttavia che l'Agenzia delle entrate non ha predisposto idonee procedure di audit anche periodiche sugli enti esterni.

Con particolare riferimento alle web application (Siatel e Puntofisco), non risultano monitorati l'attività degli amministratori locali, il numero di utenze abilitate da questi ultimi, i profili di autorizzazione e gli accessi; ciò, sebbene, per quanto riguarda Siatel, siano disponibili gli strumenti applicativi di gestione delle utenze (in uso alla Direzione centrale e alle direzioni regionali competenti) e il predetto sistema Vermont.

L'applicativo di business intelligence Vermont utilizzato dall'Agenzia non registra, in particolare, le interrogazioni effettuate dagli utenti attraverso Puntofisco e i web service.

Non risultano allo stato strumenti di controllo idonei a monitorare gli accessi effettuati attraverso l'applicativo 3270 enti esterni, web service e file transfer.

Dagli atti emerge che gli amministratori locali degli enti esterni che accedono all'anagrafe tributaria non hanno effettuato i necessari controlli, anche periodici, sugli accessi e sulla sussistenza dei requisiti per le abilitazioni e le autorizzazioni degli utenti, anche per l'assenza di idonei strumenti a ciò finalizzati; tali soggetti, oltre alle anomalie relative alla gestione degli utenti riscontrate nei punti precedenti, non sono dotati di un sistema di alert o di un "cruscotto" che consenta loro di monitorare a livello statistico gli accessi all'anagrafe tributaria da parte degli utenti dell'ente. Peraltro, in taluni enti sono presenti più amministratori la cui attività non è risultata essere coordinata.

Prescrizioni

L'Agenzia deve predisporre idonee e concrete procedure di audit anche periodiche sugli enti esterni e anche sull'attività svolta da Sogei S.p.a. in qualità di responsabile del trattamento. In particolare, per quanto riguarda gli enti esterni, oltre ad attività di audit basate sul monitoraggio delle transazioni e su sistemi di alert, tali procedure devono prevedere la verifica periodica, anche a campione, del rispetto dei presupposti stabiliti nelle convenzioni che autorizzano l'accesso.

Negli strumenti di business intelligence (applicativo Vermont o altri analoghi) utilizzati dall'Agenzia per monitorare gli accessi all'anagrafe tributaria dovranno confluire i log relativi a tutti gli attuali e futuri applicativi utilizzati per gli accessi da parte degli enti esterni.

Deve essere prefigurata da parte dell'Agenzia l'attivazione di specifici alert che individuino com-

portamenti anomali o a rischio, anche attraverso il monitoraggio e l'analisi periodica, a livello statistico, dei dati relativi alle transazioni eseguite dagli enti esterni.

Gli amministratori locali presso gli enti esterni devono essere dotati di strumenti di gestione delle utenze più efficaci e intuitivi che prevedano anche la possibilità di monitoraggi statistici degli accessi con l'attivazione di sistemi di alert. Gli strumenti in dotazione agli amministratori locali devono essere idonei a supportare i controlli che gli enti sono tenuti ad effettuare ai sensi delle convenzioni che autorizzano l'accesso all'anagrafe tributaria. Tali controlli devono riguardare in particolare, anche a campione, la rispondenza delle interrogazioni a una precisa finalità amministrativa (cfr. l'inserimento del numero di pratica nell'applicativo), e essere effettuati con cadenze periodiche e documentati con le modalità stabilite con l'Agenzia.

***

Le prescrizioni sopra illustrate devono essere predisposte al più presto. Anche sulla base del confronto con l'Agenzia -curato da ultimo dall'Ufficio- rispetto all'impiego delle risorse necessarie per la loro idonea attuazione e tenuto conto del rispetto dei diritti degli interessati, si ritiene necessario che le misure e gli accorgimenti sopra indicati, valutati singolarmente e nel loro complesso, siano accorpati in due distinti gruppi di adempimenti che dovranno essere posti in essere dall'Agenzia entro i termini, rispettivamente, di tre e di sei mesi. Limitatamente a taluni specifici e limitati profili, considerata la particolare complessità organizzativa richiesta, alcune delle misure e degli accorgimenti indicati devono essere invece completati entro il temine di dodici mesi. L'adempimento di tutte le prescrizioni del Garante dovrà essere, di volta in volta, puntualmente documentato a questa Autorità nei termini indicati decorrenti dalla data di ricezione del presente provvedimento.

TUTTO CIÒ PREMESSO IL GARANTE

ai sensi dell'art. 154, comma 1, lett. c) del Codice prescrive all'Agenzia delle entrate, con particolare riferimento alle attività dei soggetti esterni che accedono all'anagrafe tributaria, di adottare al più presto le misure e gli accorgimenti seguenti al fine di porre rimedio alle carenze indicate in motivazione, riferibili in particolare alle autenticazioni e alle autorizzazioni degli utenti, ai controlli da parte dell'Agenzia e alle estese possibilità di accesso alle banche dati, rendendo il trattamento conforme alle disposizioni vigenti e provve-

dendo comunque entro, e non oltre, i distinti termini di volta in volta indicati. L'adempimento delle prescrizioni dovrà essere, di volta in volta, documentato puntualmente a questa Autorità nei medesimi termini indicati decorrenti dalla data di ricezione del presente provvedimento.

a) Con riferimento ai profili generali relativi agli accessi all'anagrafe tributaria da parte di soggetti esterni all'amministrazione finanziaria:

I) entro 6 mesi:

- l'Agenzia deve redigere con formalità descrittive standard un documento, costantemente aggiornato, che riporti tutti i flussi di trasferimento di dati da e verso l'anagrafe tributaria e tutti gli accessi di tipo interattivo, batch o di altro genere, specificando per ciascun flusso o accesso l'identità dei soggetti legittimati a realizzarlo, la base normativa, la finalità istituzionale, la natura e la qualità dei dati trasferiti o a cui si è avuto accesso, la frequenza e il volume dei trasferimenti o degli accessi e il numero di soggetti che utilizzano la procedura. Tale documento deve essere mantenuto costantemente aggiornato, e reso disponibile nel caso di controlli;
- con cadenza periodica annuale, l'Agenzia deve verificare l'attualità delle finalità per cui ha concesso l'accesso agli enti esterni, anche con riferimento al numero di utenze attive, inibendo gli accessi effettuati al di fuori dei presupposti riconducibili all'art. 19 del Codice e quelli non conformi a quanto stabilito nelle convenzioni. All'esito di tali verifiche, in particolare, devono essere eliminati gli accessi effettuati per conoscere informazioni che, ai sensi della normativa vigente, dovrebbero essere invece controllate presso altri soggetti;

II) entro 12 mesi:

- l'Agenzia deve introdurre nelle applicazioni volte all'uso interattivo da parte di incaricati un campo per l'indicazione obbligatoria del numero di riferimento della pratica nell'ambito della quale viene effettuata la consultazione;
- devono essere segmentati per quanto più possibile i dati visualizzabili attraverso gli applicativi (in modo cronologico, geografico e per tipologia di dati).

b) In relazione alla sicurezza dei sistemi di autenticazione degli applicativi utilizzati, l'Agenzia delle entrate deve:

I) entro 3 mesi:

- prevedere che tutte le applicazioni accessibili da rete pubblica in forma di web application siano implementate con protocolli https/ssl provvedendo ad asseverare l'identità digitale dei server erogatori dei servizi tramite l'utilizzo di certificati digitali emessi da una Certification Authority ufficiale;
- permettere la visualizzazione, nella prima schermata successiva al collegamento, di informazioni relative all'ultima sessione effettuata con le stesse credenziali (almeno con l'indicazione di data, ora e indirizzo di rete da cui è stata effettuata la precedente connessione). Le stesse informazioni devono essere riportate anche relativamente alla sessione corrente;
- disciplinare la possibilità di effettuare accessi contemporanei con le medesime credenziali, limitandone l'utilizzo ai soli casi necessari per esigenze di servizio. In ogni caso, tale possibilità deve essere consentita esclusivamente laddove il certificato digitale o l'indirizzo Ip siano sufficienti a discriminare l'identità digitale delle postazioni accedenti. Nel caso in cui non sia possibile individuare la postazione di lavoro, la possibilità di accessi contemporanei deve essere inibita;

II) entro 6 mesi:

- provvedere all'implementazione di un sistema di certificazione digitale e di censimento delle postazioni terminali, in modo da realizzare procedure di autenticazione che consentano di definire condizioni di accesso più complesse e sicure per determinate classi di incaricati o profili di autorizzazione.

c) Per quanto riguarda gli amministratori locali, le abilitazioni e le autorizzazioni degli utenti occorre che:

I) entro 3 mesi:

- nelle convenzioni che disciplinano l'accesso all'anagrafe tributaria sia previsto che gli enti esterni individuino gli "amministratori locali" sulla base di ele-

vati requisiti di idoneità soggettiva, preferibilmente tra soggetti che abbiano un rapporto stabile con essi. Questi soggetti, prima di intraprendere la loro attività, devono essere formati dall'Agenzia delle entrate in ordine alle funzionalità dell'applicativo e all'attività di autorizzazione degli utenti. L'amministratore locale dell'ente esterno che accede all'anagrafe tributaria deve rimanere il punto di riferimento per le richieste di abilitazione e autorizzazione con la possibilità di gestire direttamente le utenze;

- l'Agenzia stabilisca nelle convenzioni che gli enti esterni debbano istruire adeguatamente il personale addetto all'utilizzo dei vari applicativi in ordine al corretto utilizzo delle funzionalità dei software. Le convenzioni, entro i medesimi termini, devono imporre agli enti, anche attraverso gli strumenti di audit in uso all'amministratore locale, controlli periodici i cui esiti devono essere documentati secondo le modalità definite nella stessa convenzione;
- le convenzioni stipulate dall'Agenzia predefiniscano una procedura per le autenticazioni e le autorizzazioni che coinvolga attivamente le figure apicali degli uffici interessati e un supervisore unico (soggetto giuridicamente preposto all'individuazione degli utenti e dei profili). Il supervisore può anche non coincidere con l'amministratore tecnicamente deputato alla materiale gestione delle abilitazioni (e del relativo profilo), ma deve rispondere del controllo sullo stesso. Occorre inoltre che venga assicurato un flusso di comunicazione tra l'amministratore locale e l'articolazione che si occupa della gestione delle risorse umane al fine di procedere alla tempestiva revisione del profilo di abilitazione o alla disabilitazione dei soggetti preposti ad altre mansioni o che abbiano cessato il rapporto con l'ente, anche con apposite verifiche a cadenza almeno trimestrale;
- in presenza di più amministratori locali per ciascun ente, l'Agenzia valuti e coordini i profili di autorizzazione da attribuire, garantendo in capo a un'unica figura la possibilità di intervenire su tutti gli utenti anche amministratori, monitorandone l'operato;

- l'Agenzia predefinisca, soglie relative al numero di utenti abilitabili da ciascun ente. Le richieste di superamento di tali soglie devono essere valutate caso per caso dall'Agenzia;
- siano previste limitazioni orarie per gli accessi, mantenendo comunque la possibilità di specifiche deroghe adeguatamente motivate;

II) entro 6 mesi:

- le web application predisposte dall'Agenzia per l'utilizzo da parte di enti esterni siano integrate, con procedure di "autenticazione forte" per ridurre la possibilità di usi impropri delle credenziali. Tali procedure devono essere prefigurate nei confronti di quelle classi di utenti cui corrispondano profili di autorizzazione che risultano più critici e, comunque, almeno per tutti i profili di autorizzazione corrispondenti alle funzioni di amministrazione locale;
- le convenzioni stipulate con ciascun ente prevedano espressamente i vincoli necessari ad assicurare un corretto trattamento dei dati e stabiliscano anche le condizioni per escludere il rischio di duplicazione delle basi dati realizzata anche attraverso l'utilizzo di strumenti automatizzati di interrogazione.

d) Con riguardo ai singoli sistemi l'Agenzia deve:

I) entro 3 mesi:

- rispetto all'applicativo Siatel, introdurre misure di controllo per la funzionalità di "fornitura dati" visualizzabile nell'apposita schermata dell'applicativo e, con riferimento alle funzionalità utilizzabili da parte degli operatori comunali a soli fini anagrafici, inserire nell'applicativo medesimo specifiche indicazioni all'amministratore locale affinché vengano autorizzati solo utenti che agiscono presso l'ufficio anagrafe del comune;
- per quanto riguarda l'applicativo Puntofisco, aggiornare il profilo di autorizzazione assegnato agli enti esterni abilitati, escludendo a priori la consultabilità di dati sensibili laddove non sussista un'idonea base normativa. All'interno della procedura informatica di gestione degli utenti in uso all'amministratore locale devono essere inserite indicazioni che consentano

all'Agenzia di visualizzare lo status di tutte le utenze con i profili abilitativi correnti, comprese quelle già cancellate. Entro il medesimo termine, deve essere corretta l'anomalia, relativa al sistema di gestione, che non permette regolarmente all'amministratore locale, visualizzando il profilo del singolo utente, di conoscerne l'effettiva possibilità di accesso dello stesso al sistema;

- per quanto riguarda gli applicativi Entratel e Fisconline/Cassetto fiscale, configurare i sistemi in modo da poter verificare il rispetto delle prescrizioni indicate nell'Allegato B al Codice relative, con particolare riferimento al sistema di scadenza delle password e all'attribuzione di credenziali idonee a identificare direttamente, oltre all'ente abilitato, anche il singolo incaricato che fisicamente effettua l'accesso, autentica e trasmette i file;

II) entro 6 mesi:

- realizzare la migrazione degli enti a oggi abilitati ad accedere all'anagrafe tributaria mediante 3270 enti esterni verso applicativi che offrono maggiori garanzie;
- con riferimento ai web service, effettuare una ricognizione dei servizi attualmente esposti e sospenderne l'attività in attesa della revisione delle attuali modalità di implementazione con le misure e gli accorgimenti di seguito descritti. Laddove l'Agenzia intenda impiegare web service esposti anche in rete pubblica per l'utilizzo da parte di enti esterni, questi devono essere configurati offrendo un livello minimo di accesso ai dati e limitando i risultati delle interrogazioni a valori di tipo booleano. Le convenzioni per l'utilizzo di tali servizi, inoltre, devono prevedere stringenti condizioni d'uso tali da consentire anche un'effettiva capacità di controllo da parte dell'Agenzia. Dal punto di vista tecnico, tali condizioni d'uso dei web service devono essere trasposte in appositi "accordi di servizio", redatti secondo il modello della cooperazione applicativa impiegata all'interno del sistema pubblico di connettività istituito dal Codice dell'amministrazione digitale. Gli "accordi di servizio" devono individuare idonee garanzie per il trattamento dei dati per-

sonali, prevedendo, in particolare, il tracciamento delle operazioni compiute in cooperazione applicativa, con possibilità di identificazione dell'utente che accede ai dati, il timestamp, l'indirizzo Ip di provenienza dell'utente e del server interconnesso, l'operazione effettuata e i dati trattati;

III) entro 12 mesi:

- realizzare i collegamenti per la gestione di flussi di dati mediante file transfer su canali di connessione sicuri e garantire, anche attraverso la configurazione dei sistemi, che le credenziali di abilitazione utilizzate dagli operatori dell'ente esterno rispettino le prescrizioni indicate nell'Allegato B al Codice, in particolare identificando il soggetto che effettua lo scambio dei dati e prevedendo che la parola chiave prevista sia soggetta a scadenza periodica secondo i termini ivi indicati.

e) In relazione alle procedure di audit sull'accesso alle informazioni contenute nell'anagrafe tributaria da parte di soggetti esterni:

I) entro 3 mesi:

- l'Agenzia deve predisporre idonee e concrete procedure di audit anche periodiche sugli enti esterni e anche sull'attività svolta da Sogei S.p.a. In particolare, per quanto riguarda gli enti esterni, oltre ad attività di audit basate sul monitoraggio delle transazioni e su sistemi di alert, tali procedure devono prevedere la verifica periodica, anche a campione, del rispetto dei presupposti stabiliti nelle convenzioni che autorizzano l'accesso;

II) entro 6 mesi:

- negli strumenti di business intelligence utilizzati dall'Agenzia per monitorare gli accessi all'anagrafe tributaria devono confluire i log relativi a tutti gli attuali e futuri applicativi utilizzati per gli accessi da parte degli enti esterni;
- deve essere prefigurata da parte dell'Agenzia l'attivazione di specifici alert che individuino comportamenti anomali o a rischio, anche attraverso il monitoraggio e l'analisi periodica, a livello statistico, dei dati relativi alle transazioni eseguite dagli enti esterni;

- gli amministratori locali presso gli enti esterni devono essere dotati di strumenti di gestione delle utenze più efficaci e intuitivi che prevedano anche la possibilità di monitoraggi statistici degli accessi con l'attivazione di sistemi di alert. Gli strumenti in dotazione agli amministratori locali devono essere idonei a supportare i controlli che gli enti sono tenuti ad effettuare ai sensi delle convenzioni che autorizzano l'accesso all'anagrafe tributaria. Tali controlli devono riguardare, in particolare, anche a campione la rispondenza delle interrogazioni ad una precisa finalità amministrativa e essere effettuati con cadenze periodiche e documentati con le modalità stabilite con l'Agenzia.

Roma, 18 settembre 2008

IL PRESIDENTE
Pizzetti

IL RELATORE
Pizzetti

IL SEGRETARIO GENERALE
Buttarelli

29. Archivi storici *on-line* dei quotidiani: accoglimento dell'opposizione dell'interessato alla reperibilità delle proprie generalità attraverso i motori di ricerca (*)

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Nella riunione odierna, in presenza 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;

Visti gli interpelli preventivi ex artt. 7 e 8 del Codice in materia di protezione dei dati personali (d.lg. 30 giugno 2003, 196) inviati a Google Inc. e Rcs Quotidiani S.p.A. con i quali XY, in relazione alla pubblicazione nella sezione del sito Internet dedicata all'archivio storico del quotidiano "Il Corriere della Sera" di un articolo del KW dal titolo "WZ", che contiene dati personali che lo riguardano e che è attualmente reperibile anche mediante il motore di ricerca "www.google.it", ha chiesto "di mettere in atto ogni più opportuno accorgimento (cancellazione della notizia oppure trasformazione della stessa in forma anonima oppure blocco elettronico della stessa) affinché chiunque, via internet, faccia una ricerca nominativa" relativa alla sua persona, attraverso il motore di ricerca, non acceda direttamente ai dati personali che lo riguardano contenuti nel citato articolo;

Visto il ricorso presentato il 21 luglio 2008 nei confronti di Google Inc. e di Rcs Quotidiani S.p.A., in qualità di editore del sito Internet "www.corriere.it", con il quale XY, non avendo ricevuto un idoneo riscontro, ha ribadito le precedenti richieste rilevando che, a suo avviso, la riproposizione on-line, a QJ anni di distanza, dell'articolo in questione –nel quale si narra del suo arresto nell'ambito di un'ampia inchiesta giudiziaria relativa a episodi di concussione e corruzione in ambito militare– sarebbe illecita, non rispondendo più "ai requisiti di attualità, essenzialità ed interesse pubblico" e sarebbe "in contrasto con il cd. diritto all'oblìo"; tale riproposizione sarebbe inoltre lesiva della sua reputazione e dignità, non tenendosi conto del fatto che "dalla vicenda de qua ad oggi sono trascorsi ben QJ anni durante i quali il ricorrente si è ricostruito una nuova vita" e che l'articolo "riflette un'immagine del ricorrente non più corrispon-

(*) [doc. *web* n. 1583162]

dente con il suo attuale modo di essere e ne mette a rischio la presente e rinnovata dimensione sociale"; rilevato che, con il ricorso, il ricorrente ha chiesto anche di porre a carico delle controparti le spese sostenute per il procedimento;

Visti gli ulteriori atti d'ufficio e, in particolare, la nota del 28 luglio 2008 con la quale questa Autorità, ai sensi dell'art. 149 del Codice, ha invitato il titolare del trattamento a fornire riscontro alle richieste dell'interessato, nonché la nota del 3 novembre 2008 con la quale questa Autorità ha disposto la proroga del termine per la decisione sul ricorso ai sensi dell'art. 149, comma 7, del Codice;

Vista la memoria datata 16 settembre 2008 con la quale Google Inc. (rappresentata e difesa dagli avv.ti Marco Berliri e Massimiliano Masnada), nel richiamare un riscontro fornito al ricorrente prima della presentazione del ricorso e dopo aver eccepito la sua inammissibilità poiché "al trattamento di dati personali per mezzo di copie cache con cui Google mette a disposizione degli utenti le pagine web indicizzate contenenti parole chiave utilizzate nella ricerca, non si applica la legge italiana", avendo il titolare del trattamento sede negli Usa, ha comunque illustrato le modalità di funzionamento del sistema di scansione utilizzato da Google; rilevato che la società ha precisato che è possibile escludere pagine web di siti sorgente ancora disponibili in rete dall'indicizzazione automaticamente operata dai propri crawler esclusivamente con la collaborazione dei webmaster dei medesimi siti sorgente e che, quindi, "nel caso specifico, solo rimuovendo dall'archivio storico del sito www.corriere.it la pagina web cui" il ricorrente "fa riferimento o inserendo un codice (robot.txt) che impedisca al crawler di Google di selezionare automaticamente la pagina, potrà essere definitivamente impedita l'indicizzazione della stessa da parte di Google";

Viste le memorie del 17 e del 22 settembre 2008 con le quali Rcs Quotidiani S.p.A. ha negato di poter dar corso alle richieste del ricorrente, sostenendo che il trattamento effettuato è lecito; secondo la resistente, la richiesta di cancellazione dei dati non può essere accolta facendo riferimento a un articolo (che peraltro "riferiva di fatti veri") contenuto nell'archivio storico del quotidiano che, "per assolvere alla sua funzione, deve contenere tutti gli articoli pubblicati su tutte le edizioni" e non potrebbe subire alcuna "amputazione" a pena di perdere tale carattere di storicità e di completezza; il trattamento sarebbe lecito anche perché è effet-

tuato, allo stato, non per finalità giornalistiche (come all'atto della sua pubblicazione o nel caso di una "nuova pubblicazione" nell'ambito di una "nuova iniziativa giornalistica"), ma "a fini documentaristici, nell'ambito di un archivio reso liberamente consultabile con lo strumento più rapido ed agevole, la rete internet, e attraverso i meccanismi di recupero del dato più diffusi, i motori di ricerca" e nel rispetto peraltro delle specifiche disposizioni poste con riferimento al trattamento di dati effettuato per scopi storici; sempre ad avviso della resistente, il trattamento non sarebbe altresì lesivo tenuto conto che "la particolarità della fonte, cioè la collezione dei numeri del periodico già pubblicati, rende immediatamente evidente a chiunque giunga alla notizia, la data della sua pubblicazione sul quotidiano, fugando ogni dubbio sul fatto che si tratta di vicenda passata, più o meno remota. L'utente, inoltre, può autonomamente comprenderne la eventuale inattualità, apprezzandone invece il valore di documento storico, con le sue potenzialità, ma anche i suoi limiti, in termini di informazione"; rilevato che, con riferimento al caso di specie, la resistente ha altresì considerato che l'articolo oggetto del ricorso fa riferimento a un fatto "dotato di rilevante interesse pubblico; interesse che non è affatto detto che sia oggi del tutto scemato" e contiene comunque dati che non "appartengono esclusivamente alla vita privata dell'interessato", quale la circostanza del suo arresto;

Vista la nota datata 17 settembre 2008 con la quale il ricorrente ha ribadito le proprie richieste rilevando che se è vero che "l'archivio storico della R.c.s. deve conservare memoria delle notizie accadute nel tempo", sarebbe altresì necessario che "dopo un congruo periodo di tempo (…) la pagina, al limite" possa essere "accessibile solo dall'indirizzo principale (appunto www.corriere.it) e non dai singoli motori di ricerca";

Vista la nota fatta pervenire via fax il 17 novembre 2008 con la quale R.c.s. Quotidiani S.p.A. ha richiamato le precedenti argomentazioni e, in ordine alle considerazioni del ricorrente relative all'accessibilità dell'articolo per il tramite del motore di ricerca, ha rilevato che "la legittimità della conservazione del dato e della sua libera fruizione (…) non può che implicare necessariamente la possibilità di porre al servizio della ricerca tutti i mezzi che la tecnica informatica permette di utilizzare"; ciò, a maggior ragione quando il dato in questione è contenuto nell'"archivio storico documentaristico del Corriere della Sera";

Vista la memoria del 17 novembre 2008 con la quale Google Inc. ha ribadito di ritenere inammissibile il ricorso proposto nei propri confronti, precisando che l'attività di trattamento posta in essere dalla società è "interamente gestita attraverso i suoi server che (…) sono localizzati presso la sede del titolare in Usa", e ha ulteriormente illustrato le modalità di funzionamento del proprio motore di ricerca;

Ritenuta di dover dichiarare inammissibile il ricorso proposto nei confronti di Google Inc. dal momento che la società resistente non risulta stabilita nel territorio di un paese appartenente all'Unione europea e che la stessa ha dichiarato di effettuare il trattamento dei dati esclusivamente attraverso i server localizzati in tale paese terzo (cfr. art. 5, commi 1 e 2, del Codice);

Rilevato, in ordine al merito del ricorso proposto nei confronti di Rcs Quotidiani S.p.A., che, al fine di contemperare i diritti della persona (in particolare il diritto alla riservatezza) con la libertà di manifestazione del pensiero –e con essa anche l'esercizio della libera ricerca storica e del diritto allo studio e all'informazione–, la disciplina in materia di protezione dei dati personali prevede specifiche garanzie e cautele nel caso di trattamenti effettuati per tali finalità, confermando la loro liceità, anche laddove si svolgano senza il consenso degli interessati, purché avvengano nel rispetto dei diritti, delle libertà fondamentali e della dignità delle persone alle quali si riferiscono i dati trattati (cfr. artt. 136 e s. e art. 102, comma 2, lett. a), del Codice, nonché artt. 1, comma 1, e 3, comma 1, codice di deontologia e di buona condotta per i trattamenti di dati personali per scopi storici, pubblicato in G. U. 5 aprile 2001, n. 80);

Rilevato che il trattamento dei dati personali del ricorrente cui fa riferimento l'odierno ricorso, a suo tempo effettuato in modo lecito per finalità giornalistiche nel rispetto del principio dell'essenzialità dell'informazione riguardo a fatti di interesse pubblico, rientra ora, attraverso la riproposizione dei medesimi dati nell'articolo pubblicato quale parte integrante dell'archivio storico del quotidiano reso disponibile on-line sul sito Internet dell'editore resistente, tra i trattamenti effettuati al fine di concretizzare e favorire la libera manifestazione del pensiero e, in particolare, la libertà di ricerca, cronaca e critica storica; rilevato che, alla luce di ciò, l'attuale trattamento può essere effettuato senza il consenso degli interessati (cfr. art. 136 e s. del Codice), è compatibile con i diversi scopi per i quali i dati sono stati in precedenza raccolti o trattati e può essere effettuato in termini generali anche oltre il periodo di tempo necessario per conse-

guire tali diversi scopi (cfr. art. 99 del Codice);

Rilevato che, ai sensi dell'art. 7, comma 3, lett. b), del Codice, ogni interessato ha diritto di chiedere la cancellazione o la trasformazione in forma anonima o il blocco dei dati personali che lo riguardano qualora gli stessi siano trattati in violazione di legge, ovvero nel caso in cui la loro conservazione non sia necessaria in relazione agli scopi per i quali sono stati raccolti o successivamente trattati;

Rilevato che, nel caso in esame, alla luce delle citate disposizioni normative, il trattamento di dati personali relativi all'interessato effettuato mediante la riproposizione on-line, sul sito Internet dell'editore resistente, dell'articolo che li contiene quale parte integrante dell'archivio storico del quotidiano non risulta in termini generali illecito, essendo riferito ad una notizia relativa a un fatto vero, non contestato dalle parti e di interesse pubblico e ciò, tanto al tempo della sua iniziale pubblicazione sull'edizione cartacea del quotidiano, quanto attualmente, soprattuto per chi opera una ricerca relativa alle vicende giudiziarie in questione; ritenuto pertanto di dover dichiarare, nel caso di specie, stante anche la liceità dell'originaria pubblicazione, infondata la richiesta del ricorrente volta a ottenere la cancellazione o la trasformazione in forma anonima o il blocco dei dati personali che lo riguardano contenuti nel citato articolo;

Rilevato tuttavia che vanno separatamente considerati i motivi legittimi di opposizione sostanzialmente argomentati dall'interessato, il quale ha rappresentato legittimamente la propria aspirazione affinché sulla rete Internet, per mezzo delle "scansioni" operate automaticamente dai motori di ricerca esterni al sito dell'editore resistente, non resti associata perennemente al proprio nominativo la notizia oggetto dell'articolo pubblicato sul Corriere della sera nel KW; ciò pur nell'ipotesi che la stessa permanga nell'archivio storico conservato e diffuso dall'editore resistente mediante il proprio sito Internet e quindi possa essere rinvenuta da coloro che la cerchino direttamente nell'archivio del giornale mediante il motore di ricerca interno a tale sito, avendone magari una pur vaga conoscenza;

Ritenuto che tali motivi di opposizione appaiono meritevoli di tutela, tenuto conto delle peculiarità del funzionamento della rete Internet che può comportare la diffusione di un gran numero di dati personali riferiti a un medesimo interessato e relativi a vicende anche risalenti

nel tempo –e dalle quali gli interessati stessi hanno cercato di allontanarsi, intraprendendo nuovi percorsi di vita personale e sociale– che però, per mezzo della rappresentazione istantanea e comulativa derivante dai risultati delle ricerche operate mediante i motori di ricerca, rischiano di riverberare comunque per un tempo indeterminato i propri effetti sugli interessati come se tali vicende fossero sempre attuali; ciò, tanto più considerando che il successivo utilizzo degli esiti delle ricerche effettuate sulla rete Internet mediante i motori di ricerca può avvenire per le finalità più diverse e non sempre per finalità di ricerca storica in senso proprio;

Ritenuto che, tenuto anche conto del tempo trascorso dalla vicenda oggetto dell'articolo cui si riferisce l'odierno ricorso, una perenne associazione al ricorrente della stessa, nei termini predetti, comporta un sacrificio sproporzionato dei suoi diritti (cfr. art. 2, comma 1, del Codice); ritenuto pertanto di dover dichiarare, nel caso di specie, parzialmente fondato il ricorso e di dover indicare, quale misura a tutela dei diritti dell'interessato, che la pagina web che contiene i dati personali del ricorrente oggetto del ricorso sia tecnicamente sottratta, all'atto della ricerca del nominativo del ricorrente, alla diretta individuabilità tramite i più diffusi motori di ricerca esterni, pur restando inalterata nel contesto dell'archivio consultabile telematicamente accedendo all'indirizzo web dell'editore resistente;

Rilevato che, alla luce dell'attuale meccanismo di funzionamento dei motori di ricerca standard, intendendo con ciò quelli a maggiore diffusione, la raccolta delle informazioni sulle pagine disponibili nel world wide web (fase di grabbing) è influenzabile dal solo amministratore di un sito web sorgente per il tramite della compilazione del file robots.txt, previsto dal "Robots Exclusion Protocol", o tramite l'uso dei "Robots Meta tag", secondo convenzioni concordate nella comunità Internet (avendo presente comunque come tali accorgimenti non siano immediatamente efficaci rispetto a contenuti già indicizzati da parte dei motori di ricerca Internet, la cui rimozione potrà avvenire secondo le modalità da ciascuno di questi previste);

Rilevato comunque che l'Autorità si riserva di avviare sul tema un eventuale autonomo procedimento nell'ambito del quale, anche attraverso il coinvolgimento delle istituzioni e dei soggetti allo stesso interessati (ordine dei giornalisti, associazioni rappresentative degli editori, gestori di motori di ricerca, ecc.), potranno essere valutate le molteplici implicazioni che la diffusione mediante la rete Internet di vasti archivi contenenti dati personali, seppur lecita e

di indiscusso interesse e valore, comporta per i soggetti cui gli stessi si riferiscono e per i loro diritti;

Ritenuto allo stato di dover ordinare, ai sensi dell'art. 150, comma 2, del Codice, a R.c.s. quotidiani S.p.A. di adottare, entro il termine di sessanta giorni dalla data di ricezione del presente provvedimento, ogni misura tecnicamente idonea ad evitare che le generalità del ricorrente contenute nell'articolo oggetto del ricorso siano rinvenibili direttamente attraverso l'utilizzo dei comuni motori di ricerca esterni al proprio sito Internet (anche, ad esempio, mediante predisposizione di distinte versioni o di differenti modalità di presentazione delle pagine web interessate a seconda dello strumento di ricerca utilizzato dagli utenti –motori di ricerca Internet o funzioni di ricerca interne al sito– o con modalità che l'Autorità si riserva, ove del caso, di valutare ai sensi dell'art. 150, comma 5, del Codice) e di dare conferma dell'avvenuto adempimento al ricorrente e a questa Autorità entro il medesimo termine;

Ritenuto che sussistono giusti motivi per compensare le spese tra le parti;

Visti gli artt. 145 e s. del 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;

TUTTO CIÒ PREMESSO IL GARANTE

a) dichiara inammissibile il ricorso proposto nei confronti di Google Inc.;

b) dichiara infondate le richieste del ricorrente volte a ottenere la cancellazione o la trasformazione in forma anonima o il blocco dei dati personali che lo riguardano contenuti nell'articolo oggetto del ricorso;

c) dichiara parzialmente fondato il ricorso in ordine all'opposizione manifestata dal ricorrente e ordina, quale misura a tutela dell'interessato ai sensi dell'art. 150, comma 2, del Codice, a R.c.s. quotidiani S.p.A. di adottare, entro il termine di sessanta giorni dalla data di ricezione del presente provvedimento, ogni misura tecnicamente idonea ad evitare che i dati personali del ricorrente contenuti nell'articolo oggetto del ricorso siano rinvenibili direttamente attraverso l'utilizzo dei comuni motori di ricerca esterni al proprio sito

Internet e di dare conferma dell'avvenuto adempimento al ricorrente e a questa Autorità entro il medesimo termine;

d) dichiara compensate le spese tra le parti.

Roma, 11 dicembre 2008

IL PRESIDENTE
Pizzetti

IL RELATORE
Chiaravalloti

IL SEGRETARIO GENERALE
Buttarelli

30. Prescrizioni ai titolari di banche dati costituite sulla base di elenchi telefonici formati prima del 1° agosto 2005 a seguito della deroga introdotta dall'art. 44 d.l. n. 207/2008 (*)

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 cons. Filippo Patroni Griffi, segretario generale;

Visto il Codice in materia di protezione dei dati personali (d.lg. 30 giugno 2003, n. 196, di seguito "Codice");

Visto l'art. 129, comma 2, del Codice che, in attuazione della disciplina comunitaria e, in particolare, della direttiva 2002/58/Ce, ha individuato nella "mera ricerca dell'abbonato per comunicazioni interpersonali" la finalità primaria degli elenchi telefonici realizzati in qualunque forma;

Considerato che tale disposizione ribadisce che il trattamento dei dati inseriti negli elenchi, se realizzato per fini ulteriori tra cui rientrano quelli pubblicitari, promozionali o commerciali, è lecito solo se è effettuato con il consenso espresso liberamente e specificamente dagli interessati, documentato per iscritto e previa informativa;

Visto il provvedimento del 15 luglio 2004 (in www.garanteprivacy.it, doc. web n. 1032381) con il quale l'Autorità ha individuato le modalità di inserimento e di successivo utilizzo dei dati personali relativi agli abbonati e agli acquirenti del traffico prepagato negli elenchi telefonici "alfabetici" del servizio universale, realizzati in qualsiasi forma, in rapporto alle diverse finalità sopraindicate, anche in rapporto all'informativa;

Visto il provvedimento del 14 luglio 2005 (in www.garanteprivacy.it, doc. web n. 1151640) con il quale l'Autorità ha individuato procedure semplificate per la redazione e l'utilizzo degli elenchi organizzati per categorie merceologiche/professionali (cd. elenchi "categorici");

Rilevato che la disciplina in materia di protezione dei dati personali prevede la possibilità di utilizzare, per attività di carattere promozionale, pubblicitario o commerciale, alcune categorie di dati e, in particolare: a) quelli presenti negli elenchi cd. "alfabetici" per i quali l'interessato ha

(*) Gazzetta Ufficiale 20 marzo 2009, n. 66 [doc. *web* n. 1598808], in inglese [doc. *web* n. 1613568]

manifestato il proprio consenso (Provv. 15 luglio 2004 cit.); b) quelli presenti negli elenchi cd. "categorici" (Provv. 14 luglio 2005 cit.); c) quelli presenti nelle banche dati costituite utilizzando anche dati estratti da elenchi telefonici formati precedentemente al 1° agosto 2005, sempre che il titolare del trattamento sia in grado di dimostrare di aver fornito effettivamente, prima di tale data, l'informativa agli interessati ai sensi dell'art. 13 del Codice;

Rilevato che resta impregiudicato quanto previsto dall'art. 130 del Codice riguardo alle attività promozionali effettuate attraverso sistemi automatizzati di chiamata senza l'intervento di un operatore, per le quali è sempre necessario il consenso espresso dell'interessato;

Visto l'art. 44, comma 1-*bis* del decreto legge 30 dicembre 2008, n. 207, convertito, con modificazioni, nella legge 27 febbraio 2009, n. 14 (in G.U. n. 28L del 28 febbraio 2009), che ha stabilito che i dati personali presenti nelle banche dati costituite sulla base di elenchi telefonici pubblici formati prima del 1° agosto 2005 sono lecitamente utilizzabili per fini promozionali sino al 31 dicembre 2009, anche in deroga agli articoli 13 e 23 del Codice, dai soli titolari del trattamento che hanno provveduto a costituire dette banche dati prima del 1° agosto 2005;

Considerato che la predetta previsione ha introdotto una deroga temporanea ai principi generali della vigente disciplina sopra richiamata che, in quanto tale, cessa alla scadenza del 31 dicembre 2009 e non istituisce, invece, un regime speciale applicabile anche successivamente a tale data;

Considerato che la deroga in questione è subordinata al contemporaneo verificarsi di due condizioni, ossia che le banche dati siano state costituite prima del 1° agosto 2005 e che i dati in esse presenti vengano utilizzati per finalità promozionali esclusivamente dagli stessi titolari che le hanno a suo tempo costituite;

Considerato che la stessa deroga ha posto quindi un vincolo di finalità e un vincolo di carattere temporale nell'utilizzo delle predette banche dati, rappresentato dallo svolgimento di attività di carattere promozionale sino al 31 dicembre 2009 e che, quindi, i dati personali presenti nelle predette banche dati non possono essere utilizzati, in vigenza del regime derogatorio, per finalità ulteriori e al di fuori dell'ambito temporale di operatività della deroga;

Ritenuto, pertanto, che rendere una informativa e acquisire un consenso, nel predetto periodo, finalizzati alla costituzione di una banca dati da utilizzare per attività promozionali anche in data

successiva al 31 dicembre 2009, costituisce una attività ulteriore rispetto ai vincoli di finalità e di ordine temporale indicati nella norma derogatoria e transitoria;

Considerato, inoltre, che l'informativa, ove resa agli interessati nel corso del predetto periodo, non renderebbe lecita la costituzione di una banca dati utilizzabile per attività di carattere promozionale, come avveniva anteriormente al 1° agosto 2005;

Considerato, poi, in ragione del predetto vincolo di finalità introdotto per il periodo transitorio, che il consenso, anche laddove fosse acquisito in vigenza della deroga, non rileverebbe in alcun modo per lo svolgimento di attività promozionali o per lo svolgimento di altre attività per le quali è necessario acquisirlo, anche in data successiva al 31 dicembre 2009;

Considerato, dunque, che una banca dati potrebbe essere utilizzata per attività promozionali, successivamente al 31 dicembre 2009, solo se formata nel rispetto della disciplina ordinaria, atteso che la disciplina derogatoria e transitoria cessa alla predetta data e, come già rilevato, costituisce una deroga di carattere temporaneo alla disciplina generale e non istituisce un regime speciale applicabile anche successivamente alla scadenza indicata;

Considerato inoltre che, in ragione di quanto detto, i dati personali presenti nelle banche dati considerate dalla norma derogatoria e transitoria, non possono essere ceduti, a qualunque titolo, a terzi;

Considerato che, in relazione all'attuale utilizzo delle predette banche dati per finalità promozionali, resta comunque impregiudicata la disciplina generale prevista dal Codice e, in particolare, quella relativa ai diritti degli interessati; e che, pertanto, le predette banche dati non possono contenere i dati degli interessati che, nel corso del tempo, abbiano esercitato il diritto di opposizione ai sensi dell'art. 7 del Codice;

Ritenuta la necessità di prescrivere ai titolari del trattamento, ai sensi dell'art. 143, comma 1, lett. b) e art. 154, comma 1, lett. c) del Codice, le misure necessarie per rendere il trattamento conforme alle disposizioni vigenti, anche in considerazione delle recenti modifiche normative;

Tenuto conto che, ai sensi dell'art. 162, comma 2-*ter* del Codice, in caso di inosservanza del presente provvedimento prescrittivo, è applicata in sede amministrativa, in ogni caso, la sanzione del pagamento di una somma da trentamila euro a centottantamila euro;

Tenuto conto, inoltre, che, ai sensi dell'art. 164-bis, comma 2, del Codice, in caso di più viola-

zioni di un'unica o di più disposizioni relative a violazioni amministrative, commesse anche in tempi diversi in relazione a banche di dati di particolare rilevanza o dimensioni, si applica la sanzione amministrativa del pagamento di una somma da cinquantamila euro a trecentomila euro;

Tenuto conto, infine, che ai sensi dell'art. 168 del Codice, chiunque, in comunicazioni, atti, documenti o dichiarazioni resi o esibiti in un procedimento dinanzi al Garante o nel corso di accertamenti, dichiara o attesta falsamente notizie o circostanze o produce atti o documenti falsi, è punito, salvo che il fatto costituisca più grave reato, con la reclusione da sei mesi a tre anni;

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

ai sensi degli artt. 143, comma 1, lett. b) e 154, comma 1, lett. c) del Codice, prescrive a tutti i titolari del trattamento che siano in possesso di banche dati costituite sulla base di elenchi telefonici pubblici formati prima del 1° agosto 2005 e che intendano utilizzarle per fini promozionali avvalendosi della deroga introdotta dalla legge 27 febbraio 2009, n. 14, le seguenti misure necessarie per rendere il trattamento conforme alle disposizioni vigenti:

a) documentare in modo adeguato l'avvenuta costituzione della banca dati prima del 1° agosto 2005 e conservare la relativa documentazione presso la sede legale del titolare;

b) trattare direttamente i dati personali presenti nelle banche dati oggetto del presente provvedimento, senza possibilità di cederli, a qualunque titolo, a terzi;

c) specificare, in occasione di ogni contatto con gli interessati, chi rivesta la qualifica di titolare del trattamento dei dati, anche nel caso in cui questi operi per conto di terzi e fare presente agli interessati stessi che hanno il diritto di opporsi ai sensi dell'art. 7 del Codice;

d) registrare in via immediata l'eventuale opposizione dell'interessato al trattamento dei suoi dati personali effettuato dal titolare (art. 7, comma 4, del Codice), con effetto anche nei confronti dei terzi per conto dei quali questo operi, anche qualora ciò

avvenga telefonicamente, e fornire altresì all'interessato l'identificativo dell'operatore o dell'operazione compiuta;

e) utilizzare i dati personali presenti nelle banche dati di cui alla lett. a) esclusivamente per finalità promozionali e sino al 31 dicembre 2009, non potendo i titolari rendere un'informativa agli interessati e richiedere agli stessi un consenso per l'uso dei loro dati per attività di carattere promozionale da effettuare in data successiva al 31 dicembre 2009;

f) comunicare al Garante, entro quindici giorni dalla pubblicazione in Gazzetta Ufficiale del presente provvedimento, di essere in possesso di banche dati costituite anteriormente al 1° agosto 2005 che si intendono utilizzare per attività promozionali fino al 31 dicembre 2009, chiarendo se il trattamento dei dati personali venga effettuato anche per conto di terzi.

Si dispone la trasmissione di copia del presente provvedimento al Ministero della giustizia-Ufficio pubblicazione leggi e decreti, per la sua pubblicazione sulla Gazzetta Ufficiale della Repubblica italiana.

Roma, 12 marzo 2009

Il Presidente
Pizzetti

Il Relatore
Pizzetti

Il Segretario generale
Patroni Griffi

31. Trasporto pubblico: geolocalizzazione e sicurezza dei passeggeri (*)

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;

Esaminata la richiesta di verifica preliminare presentata da Air Pullman S.p.A. ai sensi dell'art. 17 del Codice in materia di protezione dei dati personali (d.lg. 30 giugno 2003, n. 196);

Visti gli atti d'ufficio;

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. TRATTAMENTO DI DATI MEDIANTE SISTEMI DI LOCALIZZAZIONE SATELLITARE E DI SISTEMI DI REGISTRAZIONE DI EVENTI DI GUIDA

1.1. Air Pullman S.p.A., società che gestisce linee di trasporto pubblico, ha presentato una richiesta di verifica preliminare ai sensi dell'art. 17 del Codice, relativa al trattamento di dati personali dei conducenti dei veicoli in dotazione –nonché di quelli a disposizione delle società controllate "Air Pullman Noleggi s.r.l." e "Saco s.r.l."– conseguente all'utilizzo di un sistema satellitare di localizzazione basato su tecnologia Gps (Global Positioning System). Tale sistema, comprensivo della gestione di una banca dati e del portale messi a disposizione della società di trasporto, verrebbe fornito da Digigroup s.r.l. (di seguito, denominata "fornitore del servizio").

Unitamente ai trattamenti effettuati mediante il sistema, la cui installazione è presupposto per partecipare a gare relative all'affidamento di servizi di trasporto pubblico locale, verrebbero trattate, con l'ausilio del fornitore del servizio, ulteriori informazioni relative allo "stile di guida" del conducente e ad alcuni parametri (quali la pressione nei serbatoi freni a inizio e fine frenata e la velocità del veicolo, anche durante la frenata) rilevati in occasione di eventuali sinistri mediante

(*) [doc. *web* n. 1531604]

un dispositivo di registrazione e trasmissione dei dati ("event data recorder", denominato dalla società "black box").

Nel complesso, la società sarebbe in grado di:

a) localizzare geograficamente i propri veicoli su una mappa cartografica e di conoscerne velocità e direzione;

b) verificare l'osservanza, da parte dei conducenti, della normativa in tema di circolazione stradale e delle prescrizioni aziendali;

c) valutare la sicurezza e il "comfort" della condotta di guida degli autisti;

d) analizzare il consumo di carburante (e l'efficienza energetica) nella fase di marcia;

e) ricostruire la dinamica di eventuali sinistri;

f) riscontrare anomalie tecnico-meccaniche dei veicoli.

1.2. Secondo quanto prospettato dalla società, il trattamento di dati personali riferiti ai conducenti per mezzo di un codice identificativo appositamente cifrato, associati a quelli necessari per la localizzazione del veicolo (posizione in tempo reale del veicolo, data e ora di transito, velocità sostenuta e direzione percorsa), servirebbe a "garantire la sicurezza dei passeggeri e del mezzo rintracciandone sul percorso la posizione, per ogni necessità di intervento che assicuri l'espletamento del servizio a favore dei passeggeri e la possibilità di assistenza ai medesimi" (cfr. richiesta di verifica preliminare, p. 4).

Le predette informazioni, acquisite automaticamente dal sistema di bordo secondo criteri concordati previamente con il fornitore del servizio (all'accensione e allo spegnimento del veicolo; ogni cinque minuti con veicolo fermo o in movimento; ogni cinque km con veicolo in movimento; all'inizio e al termine di ogni fermata: cfr. allegato A alla menzionata richiesta), confluirebbero in una banca dati gestita dal fornitore medesimo.

Gli stessi dati, unitamente al servizio per la loro elaborazione (come, ad esempio, il tracciato del percorso effettuato), sarebbero resi fruibili all'azienda dal fornitore attraverso un portale ad accesso riservato, denominato "i-Nets" (cfr. richiesta di verifica preliminare, cit., p. 6); non verrebbero trattati, comunque, dati personali relativi ai passeggeri trasportati (cfr. richiesta di verifica preliminare, cit., p. 3).

1.3. Con riferimento alle funzionalità correlate alla sicurezza stradale e al consumo energetico,

la società intende acquisire i dati identificativi dei conducenti associati a informazioni relative alle loro "condotte di guida". Le informazioni (riferite, in particolare, ai tempi di permanenza oltre il numero massimo di giri motore consentito, al superamento delle velocità massime, al "comfort di guida" durante la marcia e in sede di frenata e al consumo energetico connesso all'utilizzo dell'acceleratore) sarebbero trattate solo in forma di indici medi e non sulla base di dati analitici.

Le medesime informazioni sarebbero utilizzate esclusivamente per finalità connesse al "rispetto delle prescrizioni normative di marcia su strada pubblica" (cfr. richiesta di verifica preliminare cit., p. 4) e alla corresponsione di trattamenti economici premianti a beneficio dei lavoratori che conformino il proprio stile di guida agli standard della società (in coerenza con la politica di incentivazione da essa portata avanti, che "formerebbe oggetto di negoziazione a livello aziendale": cfr. verbale di incontro del 31 marzo 2008). Anche le informazioni in questione confluirebbero all'interno di una banca dati fruibile dall'azienda per mezzo del portale "i-Nets".

1.4. La sicurezza dei dati personali sarebbe monitorata e implementata costantemente mediante accorgimenti tecnici atti a garantire la loro protezione (cfr. richiesta di verifica preliminare, cit., p. 9). In particolare, l'accesso al portale "i-Nets" –e, conseguentemente, a tutte le informazioni ivi contenute– verrebbe consentito esclusivamente previo inserimento di una password associata a un identificativo utente ("UserId"), in funzione del profilo di autorizzazione predefinito con il fornitore.

2. PROTEZIONE DEI DATI PERSONALI, LOCALIZZAZIONE E REGISTRAZIONE DELLA CONDOTTA DI GUIDA

Con esclusione delle funzionalità del sistema utilizzato dalla società per la telediagnostica del veicolo (punto 1.1. lett. f), in relazione al quale la società ha dichiarato che verranno trattate informazioni riconducibili non agli autisti, ma al solo veicolo: cfr. verbale di riunione, cit.), il caso sottoposto a verifica preliminare riguarda un trattamento di dati personali riferiti ai conducenti, con particolare riferimento alla localizzazione.

I dati relativi all'ubicazione dei veicoli, infatti, se associati a codici identificativi dei conducenti, costituiscono anche informazioni personali riconducibili agli interessati (art. 4, comma 1,

lett. b), del Codice). Ciò, anche nel caso in cui i dati di localizzazione del veicolo non siano associati immediatamente dal sistema informativo al nominativo dei conducenti (o a codici ad essi attribuiti), atteso che la società sarebbe comunque in condizione di risalire in ogni momento al conducente assegnatario di ciascun veicolo (cfr., in proposito, Parere n. 5/2005 sull'uso di dati relativi all'ubicazione al fine di fornire servizi a valore aggiunto del Gruppo di lavoro ex art. 29, direttiva n. 95/46/Ce, WP115, p. 10; v. altresì Parere n. 4/2007 sul concetto di dati personali del Gruppo di lavoro ex art. 29, direttiva n. 95/46/Ce, WP136, p. 11).

Anche gli ulteriori dati trattati per il tramite del fornitore del servizio, quali quelli relativi allo "stile di guida" o registrati mediante la "black box", devono ritenersi dati personali, essendo riconducibili (anche in un secondo momento, ad esempio in occasione di sinistro) ad azioni poste in essere dai conducenti.

A tali trattamenti trova pertanto applicazione la disciplina contenuta nel Codice.

Per tutte le finalità indicate nel presente provvedimento, il trattamento dovrà quindi avvenire con modalità comunque rispettose, in concreto, dei diritti e delle libertà fondamentali, nonché della dignità degli interessati (art. 2, primo comma, del Codice) e dovrà essere svolto, in ogni caso, in conformità all'art. 11, comma 1, lett. a) del medesimo Codice, con le garanzie e procedure espressamente previste a tutela dei lavoratori dall'art. 4 della legge n. 300/1970.

3. Rapporto tra società di trasporto pubblico locale (titolare del trattamento) e fornitore del servizio

L'esternalizzazione delle attività finalizzate all'esecuzione del servizio sopra descritto, grazie a un apposito contratto di collaborazione, asseconda legittime esigenze organizzative in base alle quali la società di trasporto, "titolare del trattamento", si avvale del fornitore del servizio che viene a rivestire, ai sensi dell'art. 29 del Codice, il ruolo di "responsabile del trattamento" (in tal senso cfr. i pareri resi il 19 dicembre 1998, in www.garanteprivacy.it, doc. web n. 41941 e l'8 giugno 1999, doc. web n. 1092666).

Il fornitore del servizio, chiamato a operare in base a un apposito incarico, non gode di spazi di autonomia in ordine alle finalità perseguibili (salva la necessaria autonomia dal punto di vista tecnico per fornire il servizio richiesto), atteso che il potere decisionale in relazione alle mede-

sime finalità rimane in capo alla società di trasporto (cfr. in tal senso già il parere del 9 dicembre 1997, doc. web n. 30915; Provv. 16 febbraio 2006, doc. web n. 1242592).

Pertanto, l'accordo con la società di trasporto deve permettere di delimitare gli obiettivi da raggiungere, di orientare al loro esclusivo perseguimento le operazioni di trattamento dei dati effettuate dal fornitore del servizio e di individuare analiticamente i dati pertinenti e non eccedenti da trattare (artt. 4, comma 1, lett. g) e 29 del Codice). L'attività del fornitore del servizio deve essere vincolata dalle istruzioni impartite dal titolare, che devono a loro volta tener conto delle prescrizioni stabilite dal Garante con il presente provvedimento.

4. LICEITÀ, FINALITÀ E PERTINENZA DEL TRATTAMENTO RISPETTO ALLA LOCALIZZAZIONE

La finalità del trattamento dichiarata dalla società in relazione al funzionamento del sistema Gps risulta lecita. Il sistema di localizzazione del veicolo (e indirettamente del conducente) è preordinato a rendere più efficiente il servizio di trasporto pubblico locale (con una migliore allocazione dei mezzi in dotazione, specie in caso di sopravvenienze), consentendo di fornire un'informazione tempestiva a vantaggio della società che gestisce il servizio di trasporto (oltre che, eventualmente, dell'utenza), anche per l'eventuale attività di reportistica nei confronti dell'ente pubblico affidante e per il monitoraggio del servizio (cfr. artt. 14, comma 3, lett. f), 18, comma 3-quater, lett. a) e 19, comma 3, lett. c) d.lg. 19 novembre 1997, n. 422, Conferimento alle regioni ed agli enti locali di funzioni e compiti in materia di trasporto pubblico locale). Le informazioni verranno utilizzate anche per incrementare le condizioni di sicurezza del conducente e delle persone trasportate (cfr. nota della società del 12 marzo 2008).

Per tali finalità verranno trattati i dati relativi alla localizzazione dei veicoli, ivi compresa la loro direzione e velocità media tenuta negli intervalli spazio-temporali sopra indicati (punto 1.2.).

Risulta conforme al principio di necessità (art. 3 del Codice) l'adozione di opportuni accorgimenti al fine di non rendere conoscibile al fornitore del servizio i dati identificativi dei conducenti, attribuendo a questi ultimi, come dichiarato dalla società, codici cifrati (v. punto 1.2.).

Per quanto riguarda le predette finalità, funzionali al perseguimento di esigenze organizzative e produttive e a un incremento della sicurezza del lavoro, la società, assolti gli obblighi previsti dall'art. 4 della legge 20 maggio 1970, n. 300, potrà avvalersi del sistema di localizzazione e trat-

tare i dati personali necessari al suo funzionamento (nello stesso senso v. il decreto del Ministero del lavoro e delle politiche sociali, Direzione generale della tutela delle condizioni di lavoro, Divisione IV, 24 giugno 2004, in tema di installazione di impianti di controllo satellitare su autovetture di pronto intervento di un'impresa erogatrice di gas, nonché la risposta a una istanza di interpello del medesimo Ministero, Direzione generale per l'attività ispettiva, prot. n. 25/I/0006585 del 28 novembre 2006, in materia di localizzazione mediante computer palmari assegnati in dotazione a informatori scientifici del farmaco).

5. Liceità e finalità rispetto all'osservanza delle prescrizioni normative in materia di circolazione e alla definizione dello "stile di guida"

5.1. In termini generali, del pari lecito risulta il trattamento di dati personali riferiti agli autisti in relazione alla "condotta di guida" osservata (sintetizzata in forma di indici medi) per finalità connesse al "rispetto delle prescrizioni normative di marcia su strada pubblica" (cfr. richiesta di verifica preliminare cit., p. 4). Al riguardo, deve infatti rilevarsi che la sicurezza stradale, specie nell'ambito del trasporto professionale, costituisce per l'ordinamento un obiettivo di primaria rilevanza, come confermato dalla stessa disciplina comunitaria (ad esempio, in tema di cronotachigrafo digitale: cfr. regg. Ce nn. 3821/85, 2135/98 e 561/2006) e nazionale (si pensi alla "Carta di qualificazione del conducente", che obbliga gli esercenti a conseguire una qualificazione iniziale e a sottostare a periodici corsi di formazione: cfr. artt. 14 ss. e 20 d.lg. 21 novembre 2005, n. 286, recante Disposizioni per il riassetto normativo in materia di liberalizzazione regolata dell'esercizio dell'attività di autotrasportatore).

Nel rispetto delle specifiche disposizioni di legge in materia (in particolare, il d.lg. n. 285/1992 "Nuovo codice della strada" e successive modifiche e integrazioni), la società potrà quindi trattare le informazioni relative alle "condotte di guida" dei conducenti.

5.2. Con riguardo al trattamento delle informazioni relative alla "condotta di guida" al fine di riconoscere trattamenti economici premiali "ai lavoratori che conformino il proprio stile di guida agli standard fissati dalla società" (cfr. verbale di riunione cit.), sebbene tali dati siano ricavati mediante l'impiego di "apparecchiature per finalità di controllo a distanza dell'attività dei lavoratori", non può escludersi che il controllo posto in essere sia giustificato da esigenze orga-

nizzative e produttive della società di trasporto (art. 4, secondo comma, legge n. 300/1970). Tali sono da ritenersi il risparmio derivante dal monitoraggio delle "condotte di guida" e l'eventuale utilizzo degli indici medi per riconoscere premi ai dipendenti, eventualmente in aggiunta agli elementi attualmente in uso; alla luce dell'accordo aziendale in atti, infatti, il premio di risultato è correlato alla "diminuzione di danni per sinistri interni e passivi" e "all'andamento del parametro fatturato dell'attività di linea su dipendenti medi".

La società dovrà selezionare attentamente i dati pertinenti e non eccedenti ai fini del calcolo degli indici medi che intende utilizzare per riconoscere trattamenti economici premiali ai dipendenti (v. sopra punto 1.3.), tenendo presenti nel trattamento dei dati i limiti di legge in materia (in particolare, per quanto riguarda il divieto operante per le imprese di trasporto di "retribuire i conducenti salariati o concedere loro premi o maggiorazioni di salario in base alle distanze percorse [...], se queste retribuzioni siano di natura tale da mettere in pericolo la sicurezza stradale": art. 10 reg. Ce n. 561/2006 del 15 marzo 2006).

Il trattamento, previo espletamento, da parte della società di trasporto, degli adempimenti richiesti dal menzionato art. 4, dovrà essere altresì svolto nel rispetto degli ulteriori adempimenti formulati al successivo punto 7.

6. LICEITÀ DEL TRATTAMENTO RISPETTO ALLA TRACCIABILITÀ DEI SINISTRI MEDIANTE LA *CD. BLACK BOX*

Ancorché la società non abbia chiarito del tutto in atti la finalità che intende perseguire mediante la cd. black box (e debba meglio esplicitarla negli atti attuativi del presente provvedimento), con riguardo ai dati dei conducenti dai quali sia possibile ritrarne la condotta in occasione di un sinistro, il trattamento che si intende porre in essere risulta anch'esso, allo stato degli atti, lecito.

Infatti, l'acquisizione di elementi volti alla ricostruzione di un sinistro, oltre che a incrementare, in prospettiva, gli standard di sicurezza dei soggetti trasportati (e, in primo luogo, dello stesso conducente), può rivelarsi utile ai fini dell'accertamento di condotte non conformi alla disciplina in materia di sicurezza stradale e per l'accertamento di eventuali responsabilità in capo ai conducenti medesimi.

La società, anche alla luce delle specifiche previsioni contrattuali in materia (cfr., in particolare,

artt. 73 e 74 del vigente Ccnl degli autoferrotranvieri, che pongono in capo all'autista specifiche responsabilità in ordine al rispetto della circolazione stradale e l'eventuale risarcimento dei danni imputabili), potrà trattare le informazioni relative ai conducenti inerenti alla tracciabilità degli eventuali sinistri; la stessa società, al fine di garantire la liceità e correttezza del trattamento (art. 11, comma 1, lett. a), del Codice), dovrà tuttavia provvedere al preventivo espletamento delle procedure richieste dall'art. 4, secondo comma, della legge n. 300/1970; dovrà essere inoltre garantito il rispetto degli ulteriori adempimenti formulati al successivo punto 7.

7. ADEMPIMENTI ULTERIORI

Resta fermo che per tutte le finalità indicate nel presente provvedimento (punti 4-6):

a) ai lavoratori dovranno essere forniti gli elementi prescritti dall'art. 13 del Codice unitamente a compiuti ragguagli sulla natura dei dati trattati e sulle caratteristiche del sistema, tenuto conto delle diverse finalità perseguite (in proposito, cfr. già Provv. 1° marzo 2007, Linee-guida del Garante per posta elettronica e internet, doc. web n. 1387522);

b) l'accesso ai dati riferiti ai conducenti, concernenti la localizzazione o inerenti alle "condotte di guida", dovrà essere consentito ai soli incaricati della società che possono prenderne legittimamente conoscenza in ragione delle mansioni svolte (ad esempio, in relazione alla circolazione dei veicoli, il personale incaricato di coordinare il servizio di trasporto pubblico nei diversi turni di lavoro; nel caso degli indici medi utili a misurare la "condotta di guida", agli incaricati operanti nella gestione delle risorse umane);

c) i dati personali non potranno essere conservati per un tempo superiore a quello necessario al conseguimento delle finalità indicate (art. 11, comma 1. lett. e), del Codice). In particolare, le informazioni relative alla localizzazione, opportunamente anonimizzate, potranno essere trattate per le attività di monitoraggio e pianificazione del servizio di trasporto pubblico solo se in forma aggregata (artt. 3 e 11, comma 1, lett. e), del Codice);

d) la società dovrà designare il fornitore del servizio oggetto della verifica preliminare quale responsabile del trattamento ai sensi dell'art. 29 del Codice (v. sopra, punto 3);

e) infine, con specifico riferimento ai dati relativi alla localizzazione, la società dovrà notificare il trattamento nel rispetto di quanto previsto dagli artt. 37 e ss. del Codice.

TUTTO CIÒ PREMESSO IL GARANTE

a conclusione della verifica preliminare relativa all'utilizzo di un sistema di localizzazione satellitare che Air Pullman S.p.A. e le società controllate "Air Pullman Noleggi s.r.l." e "Saco s.r.l." intendono installare per finalità connesse alla gestione di linee di trasporto, prende atto del trattamento di dati personali oggetto di dichiarazioni della società che potrà essere svolto, fermo restando che:

1. agli interessati, unitamente agli elementi da fornire ai sensi dell'art. 13 del Codice, dovranno essere forniti compiuti ragguagli sulla natura dei dati trattati e sulle caratteristiche del sistema, tenuto conto delle diverse finalità perseguite (punto 7);
2. l'accesso ai dati trattati dovrà essere consentito ai soli incaricati della società che, in ragione delle mansioni svolte, possono prenderne legittimamente conoscenza (punto 7);
3. i dati dovranno essere conservati per il tempo necessario al conseguimento delle finalità perseguite. In particolare, le informazioni relative alla localizzazione, opportunamente anonimizzate, dovranno essere trattate per le attività di monitoraggio e pianificazione del servizio di trasporto pubblico solo in forma aggregata (punto 7);
4. per la finalità richiamata al punto 5.2, il trattamento dei dati dovrà avvenire tenuto conto dei limiti di legge in materia, in particolare dell'art. 10 reg. Ce n. 561/2006 del 15 marzo 2006;
5. siano previamente espletate le procedure previste dall'art. 4, secondo comma, della legge n. 300/1970;
6. la società dovrà notificare al Garante il trattamento, con specifico riferimento ai dati relativi alla localizzazione, e designare il fornitore del servizio quale responsabile del trattamento ai sensi dell'art. 29 del Codice.

Roma, 5 giugno 2008

IL PRESIDENTE
Pizzetti

IL RELATORE
Paissan

IL SEGRETARIO GENERALE
Buttarelli

32. Semplificazioni di taluni adempimenti in ambito pubblico e privato rispetto a trattamenti per finalità amministrative e contabili (*)

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) e ritenuta l'opportunità di promuovere alcune misure di semplificazione per l'intero settore pubblico e privato in relazione alle correnti attività amministrative e contabili, in particolare nei riguardi di piccole e medie imprese, liberi professionisti e artigiani;

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. Esigenze alla base di nuove misure di semplificazione

Presso vari operatori si avverte l'esigenza di alcune semplificazioni nell'applicazione della disciplina sulla protezione dei dati personali.

La riflessione in ambito pubblico e privato è avvertita in modo particolare presso piccole e medie imprese, liberi professionisti e artigiani, per quanto riguarda la gestione di informazioni attinenti ad altre imprese, amministrazioni, clienti, fornitori e dipendenti utilizzate, anche in relazione a obblighi contrattuali e normativi, per correnti finalità amministrative e contabili.

(*) Gazzetta Ufficiale 1° luglio 2008, n. 152 [doc. *web* n. 1526724]
Congiuntamente al presente provvedimento sulla semplificazione, in fase di pubblicazione sulla Gazzetta ufficiale, il Garante ha segnalato alle competenti autorità di Governo l'opportunità di apportare una modifica al Codice con riferimento alla disciplina delle misure minime di sicurezza e al documento programmatico, per contemperare meglio l'applicazione delle necessarie cautele di sicurezza dei dati e dei sistemi con l'esigenza di adattarle alle attività che, specie presso piccole e medie imprese, liberi professionisti e artigiani, vengono svolte in relazione ad attività di corrente gestione amministrativa e contabile.
In tale prospettiva, il Garante ha ipotizzato una modifica normativa dell'art. 33 del Codice, del seguente tenore:

"Art.
All'articolo 33 del decreto legislativo 30 giugno 2003 n. 196, dopo il comma 1, è aggiunto il seguente:
"1-bis. Il Garante può individuare con proprio provvedimento modalità semplificate in ordine all'adozione delle misure minime di cui al comma 1, con riferimento ai trattamenti effettuati per correnti finalità amministrative e contabili, in particolare presso piccole e medie imprese, liberi professionisti e artigiani"."

Sulla base dell'esperienza acquisita in materia vengono prospettate alcune criticità rispetto a determinate modalità per adempiere a obblighi di legge o derivanti da un contratto, avvertite come troppo onerose in rapporto alle garanzie per gli interessati.

Il Garante ha completato un'analisi approfondita della problematica. In aggiunta alle misure di semplificazione disposte con decisioni per casi specifici, l'Autorità ha intrapreso varie iniziative, anche sulla base di un dialogo con le categorie interessate, che ha già comportato l'approvazione di un provvedimento di carattere generale ("Guida pratica e misure di semplificazione per le piccole e medie imprese", Provv. 24 maggio 2007, n. 21, in G.U. 21 giugno 2007, n. 142 e doc. web n. 1412271).

Dall'istruttoria sono emerse tre valutazioni di fondo:

a) alcune modalità applicative, seguite soprattutto presso piccole imprese, liberi professionisti e artigiani, sono ancora basate su approcci prettamente burocratici e di ordine puramente formale. Istituti posti a garanzia degli interessati vengono banalizzati in contrasto con lo spirito del Codice che intende assicurare una protezione elevata dei diritti e delle libertà fondamentali "nel rispetto dei princìpi di semplificazione, armonizzazione ed efficacia" (art. 2, comma 2). Da tali prassi conseguono adempimenti superflui o ripetuti inutilmente, talvolta anche per effetto di erronee valutazioni fornite in sede di consulenza, con oneri organizzativi da cui non deriva un reale valore aggiunto ai fini della correttezza e della trasparenza del trattamento e che gli interessati avvertono con disinteresse o fastidio;

b) è possibile apportare ulteriori semplificazioni (in particolare per agevolare la corrente attività gestionale di organismi pubblici e privati di ridotte dimensioni), in aggiunta a quelle già introdotte per legge o da questa Autorità e in armonia con la disciplina complessiva, anche comunitaria, della materia, salvaguardando i diritti e le libertà fondamentali dei cittadini;

c) la protezione dei dati personali può rappresentare una risorsa, anche per piccole e medie imprese, rendere più efficiente l'attività gestionale e incrementare la fiducia degli interessati.

L'Autorità intende fornire un suo nuovo contributo in materia esercitando le attribuzioni che le sono conferite per legge.

Con il presente provvedimento sono pertanto individuate soluzioni concrete volte ad agevolare

ulteriormente l'ordinaria attività di gestione amministrativa e contabile, in modo particolare rispetto ai casi in cui non sono trattati dati di carattere sensibile o giudiziario. Di seguito, vengono quindi enunciate nuove linee guida-interpretative della normativa vigente e sono individuate alcune modalità innovative per semplificare taluni adempimenti, in modo particolare per l'informativa agli interessati e il consenso.

2. L'INFORMATIVA AGLI INTERESSATI

Diverse realtà, specie imprenditoriali di piccole e medie dimensioni, trattano dati, anche in relazione a obblighi contrattuali, precontrattuali o di legge, esclusivamente per finalità di ordine amministrativo e contabile (gestione di ordinativi, buste paga e di ordinaria corrispondenza con clienti, fornitori, realtà esterne di supporto anche in outsourcing, dipendenti); spesso, ciò accade in relazione a informazioni che non hanno carattere sensibile o giudiziario.

Alcune tra le criticità menzionate riguardano le modalità con cui l'informativa è fornita per iscritto, anziché oralmente (art. 13). Sono stati formati spesso moduli lunghi e burocratici, privi di comunicatività e basati sull'eccessivo uso di espressioni prettamente giuridiche, inidonee a far comprendere le caratteristiche principali del trattamento. Alla mancanza di chiarezza si è sommata l'inutile ripetizione dell'informativa in occasione di ciascun contatto con gli interessati, frazionando le spiegazioni che andrebbero invece fornite in modo organico e possibilmente unitario.

Il Garante intende prescrivere a tutti i titolari in ambito privato e pubblico alcune misure opportune e formulare indicazioni per semplificare l'informativa nei termini di cui al seguente dispositivo (artt. 2, comma 2, 13, commi 3 e 5 e 154, comma 1, lett. c)).

3. IL CONSENSO

Il Garante, con riferimento al consenso (art. 23), considerati i princìpi di efficacia e proporzionalità e in relazione agli artt. 2, 18, 24 comma 1 e 154, comma 1, lett. c), del Codice, intende anche prescrivere a tutti i titolari del trattamento pubblici e privati alcune misure opportune affinché non richiedano il consenso nei vari casi in cui esso non deve essere richiesto (dai soggetti pubblici) o è superfluo (per i soggetti privati). Ciò, in particolare, quando:

a) il trattamento dei dati in ambito privato è svolto per adempiere a obblighi contrattuali o

normativi o, comunque, per ordinarie finalità amministrative e contabili;

b) i dati trattati provengono da pubblici registri ed elenchi pubblici conoscibili da chiunque o sono relativi allo svolgimento di attività economiche dell'interessato (v., per i presupposti relativi a ciascuno dei predetti casi, l'art. 24, comma 1; v. anche l'art. 18, comma 4).

Il Garante, in applicazione dell'istituto del bilanciamento degli interessi (art. 24, comma 1, lett. g)) intende anche individuare un'ulteriore ipotesi nella quale il consenso non va richiesto.

Il titolare del trattamento che abbia già venduto un prodotto o prestato un servizio a un interessato, nel quadro dello svolgimento di ordinarie finalità amministrative e contabili, potrà utilizzare nei termini di cui al seguente dispositivo i recapiti (oltre che di posta elettronica, come già previsto per legge: art. 130, comma 4) di posta cartacea forniti dall'interessato medesimo, per inviare ulteriore suo materiale pubblicitario o promuovere una sua vendita diretta o per compiere sue ricerche di mercato o di comunicazione commerciale.

Tale bilanciamento degli interessi considera le difficoltà rappresentate da alcuni operatori economici nel conservare un proprio diretto "canale comunicativo" con i soggetti con i quali abbiano già instaurato un rapporto contrattuale; tiene al tempo stesso conto del diritto dell'interessato a non essere disturbato mediante comunicazioni promozionali, in base a garanzie analoghe a quelle previste, per la situazione appena indicata, per l'uso della posta elettronica (art. 130, comma 4; v. anche, con riguardo alle comunicazioni postali, l' art. 58, comma 2, d.lg. n. 206/2005).

Non è necessario rivolgere un'istanza al Garante per avvalersi delle opportunità previste dal presente punto 3.

Viene infine dato atto nel seguente dispositivo di alcune altre risultanze dell'istruttoria relative alla designazione degli incaricati del trattamento e alla notificazione dei trattamenti.

TUTTO CIÒ PREMESSO IL GARANTE

1) ai sensi degli artt. 2, comma 2, 13, commi 3 e 5 e 154, comma 1, lett. c), del Codice formula a tutti i titolari del trattamento in ambito privato e pubblico, in particolare a piccole e medie imprese, liberi professionisti, artigiani, le seguenti indicazioni per semplificare l'informativa rispetto allo svolgimento di correnti finalità amministrative e contabili, anche in relazione all'adempimento di obblighi contrattuali, precontrattuali o normativi.

Detti soggetti possono:

a) fornire un'unica informativa per il complesso dei trattamenti, anziché per singoli aspetti del rapporto con gli interessati;

b) fornire a questi ultimi una ricostruzione organica dei trattamenti e con linguaggio semplice, senza frammentarla o reiterarla inutilmente;

c) indicare le informazioni essenziali in un quadro adeguato di lealtà e correttezza;

d) redigere, per quanto possibile, una prima informativa breve. All'interessato, anche oralmente, andrebbero indicate sinteticamente alcune prime notizie chiarendo subito, con immediatezza, le principali caratteristiche del trattamento. In linea di massima l'informativa breve, quando è scritta, può avere la seguente formulazione:

"I SUOI DATI PERSONALI

Utilizziamo –anche tramite collaboratori esterni– i dati che la riguardano esclusivamente per nostre finalità amministrative e contabili, anche quando li comunichiamo a terzi. Informazioni dettagliate, anche in ordine al suo diritto di accesso e agli altri suoi diritti, sono riportate su ...";

e) per l'informativa, specie per quella breve, si possono utilizzare gli spazi utili nel materiale cartaceo e nella corrispondenza che si impiegano già, ordinariamente, per finalità amministrative e contabili;

f) l'informativa breve può rinviare a un testo più articolato, disponibile agevolmente senza oneri per gli interessati, in luoghi e con modalità facilmente accessibili anche con strumenti informatici e telematici (in particolare, tramite reti Intranet o siti Internet, affissioni in bacheche o locali, avvisi e cartelli agli sportelli per la clientela, messaggi preregistrati disponibili digitando un numero telefonico gratuito).

Anche questa più ampia informativa deve essere improntata a correttezza, tenendo conto di possibili modifiche del trattamento, ed essere basata su espressioni sintetiche, chiare e comprensibili. Le notizie da indicare per legge (art. 13, comma 1) devono essere aggiornate, specificando la data dell'ultimo aggiornamento;

g) è possibile non inserire nell'informativa più articolata gli elementi noti all'interessato (art. 13, commi 2 e 4). È opportuno omettere riferimenti meramente burocratici o

circostanze ovvie, per esempio quando alcune informazioni, compresi gli estremi identificativi del titolare, risultano da altre parti del documento in cui è presente l'informativa. Vanno utilizzate espressioni efficaci, anche se sintetiche, anche per quanto riguarda i diritti degli interessati e l'organismo o soggetto al quale rivolgersi per esercitarli. Se è prevista la raccolta di dati presso terzi è possibile formulare una sola informativa per i dati forniti direttamente dall'interessato e per quelli che saranno acquisiti presso terzi. Per questi ultimi dati, l'informativa può non essere fornita quando vi è un obbligo normativo di trattarli (art. 13, comma 5);

h) è opportuno che l'informativa più articolata sia basata su uno schema tendenzialmente uniforme per il settore di attività del titolare del trattamento;

i) è invece necessario fornire un'informativa specifica o ad hoc quando il trattamento ha caratteristiche del tutto particolari perché coinvolge, ad esempio, peculiari informazioni (es. dati genetici) o prevede forme inusuali di utilizzazione di dati, specie sensibili, rispetto alle ordinarie esigenze amministrative e contabili, o può comportare rischi specifici per gli interessati (ad esempio, rispetto a determinate forme di uso di dati biometrici o di controllo delle attività dei lavoratori). Se il titolare del trattamento è un soggetto pubblico devono essere inserite le indicazioni che la legge prevede per i dati sensibili e giudiziari;

2) invita le associazioni di categoria a predisporre informative-tipo per determinati settori o categorie di trattamento, anche in collaborazione con questa Autorità. Il Garante si riserva in questo quadro di porre a disposizione gratuita (chiedendo anche la collaborazione delle camere di commercio), un kit contenente concrete istruzioni e fac-simile per semplificare tutti gli adempimenti in materia;

3) richiama l'attenzione dei titolari del trattamento sulla circostanza che la designazione degli incaricati del trattamento può avvenire in modo semplificato evitando singoli atti circostanziati relativi distintamente a ciascun incaricato, individuando i trattamenti di dati e le relative modalità che sono consentiti all'unità cui sono addetti gli incaricati stessi (art. 30);

4) richiama l'attenzione dei titolari del trattamento sulla circostanza che, per effetto delle previsioni del Codice e delle determinazioni già adottate da questa Autorità, la notifica-

zione telematica al Garante non è necessaria per perseguire finalità amministrative e contabili, salvo che per eventuali casi eccezionali indicati per legge (art. 37);

5) ai sensi degli artt. 2, comma 2, 24 e 154, comma 1, lett. c), del Codice invita tutti i titolari del trattamento pubblici e privati a non chiedere il consenso degli interessati quando il trattamento dei dati è svolto, anche in relazione all'adempimento di obblighi contrattuali, precontrattuali o normativi, esclusivamente per correnti finalità amministrative e contabili, nonché quando i dati provengono da pubblici registri ed elenchi pubblici conoscibili da chiunque, o sono relativi allo svolgimento di attività economiche o sono trattati da un soggetto pubblico;

6) in applicazione del principio del bilanciamento degli interessi (art. 24, comma 1, lett. g)), dispone che i titolari del trattamento in ambito privato che hanno venduto un prodotto o prestato un servizio, nel quadro del perseguimento di ordinarie finalità amministrative e contabili, possono utilizzare senza il consenso i recapiti (oltre che di posta elettronica come già previsto per legge) di posta cartacea forniti dall'interessato, ai fini dell'invio diretto di proprio materiale pubblicitario o di propria vendita diretta o per il compimento di proprie ricerche di mercato o di comunicazione commerciale. Ciò, rispettando anche le garanzie previste per le attività di profilazione degli interessati (Provv. 24 febbraio 2005, doc. web n. 1103045), a condizione che:

   a) tale attività promozionale riguardi beni e servizi del medesimo titolare e analoghi a quelli oggetto della vendita;

   b) l'interessato, al momento della raccolta e in occasione dell'invio di ogni comunicazione effettuata per le menzionate finalità, sia informato della possibilità di opporsi in ogni momento al trattamento, in maniera agevole e gratuitamente, anche mediante l'utilizzo della posta elettronica o del fax o del telefono e di ottenere un immediato riscontro che confermi l'interruzione di tale trattamento (art. 7, comma 4);

   c) l'interessato medesimo, così adeguatamente informato già prima dell'instaurazione del rapporto, non si opponga a tale uso, inizialmente o in occasione di successive comunicazioni;

7) 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, nonché alle associazioni di categoria, ai ministeri interessati e alle camere di commercio.

Roma, 19 giugno 2008

IL PRESIDENTE
Pizzetti

IL RELATORE
Pizzetti

IL SEGRETARIO GENERALE
Buttarelli

33. Semplificazione delle misure di sicurezza contenute nel disciplinare tecnico di cui all'Allegato B. al Codice in materia di protezione dei dati personali (*)

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) e, in particolare gli articoli 33 ss., nonché il relativo Allegato B. contenente il disciplinare tecnico in materia di misure minime di sicurezza;

Visto l'art. 29 del decreto-legge 25 giugno 2008, n. 112, come modificato dalla legge di conversione 6 agosto 2008, n. 133, con il quale è stato, fra l'altro, modificato l'art. 34 del Codice;

Ritenuta l'esigenza di individuare alcune modalità semplificate di applicazione del predetto disciplinare tecnico da parte dei "soggetti che trattano soltanto dati personali non sensibili e che trattano come unici dati sensibili quelli costituiti dallo stato di salute o malattia dei propri dipendenti e collaboratori anche a progetto, senza indicazione della relativa diagnosi, ovvero dall'adesione ad organizzazioni sindacali o a carattere sindacale", nonché rispetto a "trattamenti comunque effettuati per correnti finalità amministrative e contabili, in particolare presso piccole e medie imprese, liberi professionisti e artigiani", nel rispetto dei diritti degli interessati (comma 1-*bis* art. 34 cit.);

Rilevata l'ulteriore esigenza che di tali modalità semplificate, da aggiornare periodicamente, sia data la più ampia pubblicità anche attraverso il sito Internet dell'Autorità (www.garanteprivacy.it);

Visto il parere del Ministro per la semplificazione normativa formulato con nota del 21 novembre 2008, sullo schema preliminare del presente provvedimento trasmesso con nota del 3 novembre 2008;

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;

(*) Gazzetta Ufficiale 9 dicembre 2008, n. 287 [doc. *web* n. 1571218], in inglese [doc. *web* n. 1619241]

PREMESSO

Il presente provvedimento individua modalità semplificate di applicazione delle misure minime di sicurezza contenute nel disciplinare tecnico di cui all'Allegato B. al Codice in materia di protezione dei dati personali, di seguito indicato come Allegato B.

LA DISCIPLINA SULLE MISURE MINIME DI SICUREZZA

I soggetti che trattano dati personali sono tenuti a proteggerli attraverso adeguate misure di sicurezza.

Alcune di esse sono individuate puntualmente dal Codice e delineano il livello minimo di protezione dei dati: si tratta delle misure indicate dagli articoli 33 ss. del Codice, da adottare nei modi previsti dall'Allegato B.

Di recente sono state introdotte con disposizione di legge alcune semplificazioni relative ai trattamenti effettuati con strumenti elettronici da parte dei soggetti che utilizzano soltanto dati personali non sensibili e che trattano, come unici dati sensibili, quelli inerenti allo stato di salute o alla malattia dei propri dipendenti e collaboratori anche a progetto, senza indicazione della relativa diagnosi, ovvero all'adesione a organizzazioni sindacali o a carattere sindacale.

Per questi casi, la tenuta di un aggiornato documento programmatico sulla sicurezza (art. 34, comma 1, lett. g) del Codice) è stata sostituita da un obbligo di autocertificazione (resa dal titolare del trattamento ai sensi dell'articolo 47 del testo unico di cui al decreto del Presidente della Repubblica 28 dicembre 2000, n. 445) di trattare soltanto tali dati in osservanza delle altre misure di sicurezza prescritte (art. 29 d.l. 25 giugno 2008, n. 112, come modificato dalla legge di conversione 6 agosto 2008, n. 133).

In relazione ai trattamenti sopra menzionati, nonché a quelli effettuati da chiunque per correnti finalità amministrative e contabili in particolare presso piccole e medie imprese, liberi professionisti e artigiani, il Garante deve individuare modalità semplificate di applicazione dell'Allegato B) sentito il Ministro per la semplificazione normativa.

Tale individuazione avviene mediante il presente provvedimento, che sarà aggiornato con cadenza periodica.

SEMPLIFICAZIONE PER TALUNI TRATTAMENTI

Come il Garante ha già evidenziato nel provvedimento del 19 giugno 2008 (in Gazzetta Ufficiale 1° luglio 2008, n. 152 e in www.garanteprivacy.it, doc. web n. 1526724), nonché mediante la segnalazione al Parlamento e al Governo in materia di misure minime di sicurezza del 19 giugno 2008, da parte di taluni titolari del trattamento le medesime misure di sicurezza possono essere attuate in modo semplificato, alla luce dell'esperienza applicativa e senza diminuire dal punto di vista sostanziale le cautele volte a prevenire determinati rischi (art. 34, comma 1 bis, del Codice, come introdotto dall'art. 29 cit.).

Sono state pertanto individuate alcune nuove modalità volte a semplificare incisivamente l'applicazione di varie regole contenute nell'Allegato B.

L'obiettivo è garantire egualmente un idoneo livello di sicurezza tenendo conto delle ridotte dimensioni di alcune realtà organizzative, nonché della particolare natura di alcuni trattamenti a fini esclusivamente amministrativo-contabili. Ciò, sulla base di una dettagliata ricognizione delle singole questioni e di approfondimenti svolti in ordine alle questioni applicative che sono state poste a vario titolo all'attenzione di questa Autorità, in particolare attraverso quesiti e segnalazioni.

Le modalità semplificate elencate nell'unito prospetto potranno essere applicate immediatamente dai soggetti interessati.

TUTTO CIÒ PREMESSO IL GARANTE

a) ai sensi dell'art. 34, comma 1-bis, del Codice individua nell'unito prospetto che costituisce parte integrante del presente provvedimento le modalità semplificate per applicare le misure minime di sicurezza per il trattamento dei dati personali;

b) 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.

Roma, 27 novembre 2008

IL PRESIDENTE
Pizzetti

IL RELATORE
Pizzetti

IL SEGRETARIO GENERALE
Buttarelli

Misure semplificate per applicare le misure minime di sicurezza nel trattamento dei dati personali

1. Soggetti che possono avvalersi della semplificazione

Le seguenti modalità semplificate sono applicabili dai soggetti pubblici o privati che:

a) utilizzano dati personali non sensibili o che trattano come unici dati sensibili riferiti ai propri dipendenti e collaboratori anche a progetto quelli costituiti dallo stato di salute o malattia senza indicazione della relativa diagnosi, ovvero dall'adesione a organizzazioni sindacali o a carattere sindacale;

b) trattano dati personali unicamente per correnti finalità amministrative e contabili, in particolare presso liberi professionisti, artigiani e piccole e medie imprese (cfr. art. 2083 cod. civ. e d.m. 18 aprile 2005, recante adeguamento alla disciplina comunitaria dei criteri di individuazione di piccole e medie imprese, pubblicato nella Gazzetta Ufficiale 12 ottobre 2005, n. 238).

2. Trattamenti effettuati con strumenti elettronici

I soggetti di cui al paragrafo 1 possono applicare le misure minime di sicurezza prescritte dalla disciplina in materia di trattamenti realizzati con l'ausilio di strumenti elettronici (art. 34 del Codice e regole da 1 a 26 dell'Allegato B.) osservando le modalità semplificate di seguito individuate.

2.1. *Istruzioni agli incaricati del trattamento (modalità applicative delle regole di cui ai punti 4, 9, 18 e 21 dell'Allegato B.)*

Le istruzioni in materia di misure minime di sicurezza previste dall'Allegato B. possono essere impartite agli incaricati del trattamento anche oralmente, con indicazioni di semplice e chiara formulazione.

2.2. *Sistema di autenticazione informatica (modalità applicative delle regole di cui ai punti 1, 2, 3, 5, 6, 7, 8, 10 e 11 dell'Allegato B.)*

Per l'accesso ai sistemi informatici si può utilizzare un qualsiasi sistema di autenticazione basato su un codice per identificare chi accede ai dati (di seguito, "username"), associato

a una parola chiave (di seguito: "password"), in modo che:

a) l'username individui in modo univoco una sola persona, evitando che soggetti diversi utilizzino codici identici;

b) la password sia conosciuta solo dalla persona che accede ai dati.

L'username deve essere disattivato quando l'incaricato non ha più la qualità che rende legittimo l'utilizzo dei dati (ad esempio, in quanto non opera più all'interno dell'organizzazione).

Può essere adottata, quale procedura di autenticazione anche la procedura di login disponibile sul sistema operativo delle postazioni di lavoro connesse a una rete.

In caso di prolungata assenza o impedimento dell'incaricato che renda indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema, se l'accesso ai dati e agli strumenti elettronici è consentito esclusivamente mediante uso della password, il titolare può assicurare la disponibilità di dati o strumenti elettronici con procedure o modalità predefinite. Riguardo a tali modalità, sono fornite preventive istruzioni agli incaricati e gli stessi sono informati degli interventi effettuati (ad esempio, prescrivendo ai lavoratori che si assentino dall'ufficio per ferie l'attivazione di modalità che consentano di inviare automaticamente messaggi di posta elettronica ad un altro recapito accessibile: si vedano le Linee-guida in materia di lavoro per posta elettronica e Internet approvate dal Garante e pubblicate nella Gazzetta ufficiale 10 marzo 2007 , n. 58 [doc. web n. 1387522]).

2.3. *Sistema di autorizzazione (modalità applicative delle regole di cui ai punti 12, 13 e 14 dell'Allegato B.)*

Qualora sia necessario diversificare l'ambito del trattamento consentito, possono essere assegnati agli incaricati –singolarmente o per categorie omogenee corrispondenti profili di autorizzazione, tramite un sistema di autorizzazione o funzioni di autorizzazione incorporate nelle applicazioni software o nei sistemi operativi, così da limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento.

2.4. *Altre misure di sicurezza (modalità applicative delle regole di cui ai punti 15, 16, 17 e 18 dell'Allegato B.)*

I soggetti di cui al paragrafo 1 assicurano che l'ambito di trattamento assegnato ai singoli incaricati, nonché agli addetti alla gestione o alla manutenzione degli strumenti elettronici, sia coe-

rente con i princìpi di adeguatezza, proporzionalità e necessità, anche attraverso verifiche periodiche, provvedendo, quando è necessario, ad aggiornare i profili di autorizzazione eventualmente accordati.

Gli aggiornamenti periodici dei programmi per elaboratore volti a prevenire la vulnerabilità di strumenti elettronici (ad esempio, antivirus), anche con riferimento ai programmi di cui all'art. 615-quinquies del codice penale, nonché a correggerne difetti, sono effettuati almeno annualmente. Se il computer non è connesso a reti di comunicazione elettronica accessibili al pubblico (linee Adsl, accesso a Internet tramite rete aziendale, posta elettronica), l'aggiornamento deve essere almeno biennale.

I dati possono essere salvaguardati anche attraverso il loro salvataggio con frequenza almeno mensile. Il salvataggio periodico può non riguardare i dati non modificati dal momento dell'ultimo salvataggio effettuato (dati statici), purché ne esista una copia di sicurezza da cui effettuare eventualmente il ripristino.

2.5. *Documento programmatico sulla sicurezza (modalità applicative delle regole di cui ai punti da 19.1 a 19.8 dell'Allegato B.)*

2.5.1. Fermo restando che per alcuni casi è già previsto per disposizione di legge che si possa redigere un'autocertificazione in luogo del documento programmatico sulla sicurezza (vedi il precedente par. 1, lett. a); art. 29 d.l. n. 112/2008 cit.), i soggetti pubblici e privati che trattano dati personali unicamente per correnti finalità amministrative e contabili, in particolare presso liberi professionisti, artigiani e piccole e medie imprese, possono redigere un documento programmatico sulla sicurezza semplificato sulla base delle indicazioni di seguito riportate.

Il documento deve essere redatto prima dell'inizio del trattamento e deve essere aggiornato entro il 31 marzo di ogni anno nel caso in cui, nel corso dell'anno solare precedente, siano intervenute modifiche rispetto a quanto dichiarato nel precedente documento.

Il documento deve avere i seguenti contenuti:

a) le coordinate identificative del titolare del trattamento, nonché, se designati, gli eventuali responsabili. Nel caso in cui l'organizzazione preveda una frequente modifica dei responsabili designati, potranno essere indicate le modalità attraverso le quali è possibile individuare l'elenco aggiornato dei responsabili del trattamento;

b) una descrizione generale del trattamento o dei trattamenti realizzati, che permetta di valutare l'adeguatezza delle misure adottate per garantire la sicurezza del trattamento. In tale descrizione vanno precisate le finalità del trattamento, le categorie di persone interessate e dei dati o delle categorie di dati relativi alle medesime, nonché i destinatari o le categorie di destinatari a cui i dati possono essere comunicati;

c) l'elenco, anche per categorie, degli incaricati del trattamento e delle relative responsabilità. Nel caso in cui l'organizzazione preveda una frequente modifica dei responsabili designati, potranno essere indicate le modalità attraverso le quali è possibile individuare l'elenco aggiornato dei responsabili del trattamento con le relative responsabilità;

d) una descrizione delle altre misure di sicurezza adottate per prevenire i rischi di distruzione o perdita, anche accidentale, dei dati, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.

3. Modalità applicative per i trattamenti realizzati senza l'ausilio di strumenti elettronici (modalità applicative delle regole di cui ai punti 27, 28 e 29 dell'allegato B.)

I soggetti di cui al paragrafo 1 possono adempiere all'obbligo di adottare le misure minime di sicurezza di cui all'art. 35 del Codice applicando le misure contenute nell'Allegato B. relativamente ai trattamenti realizzati senza l'ausilio di strumenti elettronici (regole da 27 a 29 dello stesso Allegato B.), con le modalità semplificate di seguito individuate.

3.1. Agli incaricati sono impartite, anche oralmente, istruzioni finalizzate al controllo e alla custodia, per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento, degli atti e dei documenti contenenti dati personali.

3.2. Quando gli atti e i documenti contenenti dati personali sensibili o giudiziari sono affidati agli incaricati del trattamento per lo svolgimento dei relativi compiti, i medesimi atti e documenti sono controllati e custoditi dai medesimi incaricati fino alla restituzione in modo che a essi non accedano persone prive di autorizzazione, e sono restituiti al termine delle operazioni affidate.

34. Proroga delle misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema (*)

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Nella riunione odierna, in presenza del prof. Francesco Pizzetti, presidente, del dott. Giuseppe Chiaravalloti, vicepresidente, del dott. Mauro Paissan e del dott. Giuseppe Fortunato, componenti e del dott. Daniele De Paoli, segretario generale reggente;

Visto il Codice in materia di protezione dei dati personali (d.lg. 30 giugno 2003, n. 196) e, in particolare, gli artt. 31 ss. e 154, comma 1, lett. c) e h), nonché il disciplinare tecnico in materia di misure minime di sicurezza di cui all'allegato B del medesimo Codice;

Visto il provvedimento del Garante del 27 novembre 2008 relativo a "misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema", pubblicato sulla G.U. n. 300 del 24 dicembre 2008;

Visto il punto 3 del dispositivo del predetto provvedimento, il quale prescrive che le misure e gli accorgimenti di cui al punto 2 del medesimo dispositivo siano introdotti, per i trattamenti già iniziati o che avranno inizio entro trenta giorni dalla data di pubblicazione nella Gazzetta Ufficiale del provvedimento stesso, al più presto e comunque entro e non oltre il termine di centoventi giorni dalla medesima data, mentre, per i trattamenti che avranno inizio dopo il termine di trenta giorni dalla pubblicazione, tali accorgimenti e misure siano introdotti anteriormente all'inizio del trattamento dei dati;

Tenuto conto dei quesiti pervenuti sia da singoli titolari del trattamento sia da alcune associazioni rappresentative di categoria, relativi all'esatta interpretazione degli adempimenti prescritti dal citato provvedimento del 27 novembre 2008;

Considerata l'ampia platea di soggetti interessati all'adempimento del suddetto provvedimento e la conseguente necessità di assicurare la massima diffusione e la più completa e precisa conoscenza delle prescrizioni in esso contenute;

Riservata la possibilità, all'esito di un attento esame dei quesiti già pervenuti e di quelli che

(*) Gazzetta Ufficiale 24 febbraio 2009, n. 45 [doc. *web* n. 1591970]

potranno essere sottoposti all'attenzione del Garante, anche a seguito dell'attività di consultazione attualmente in corso all'interno di alcune associazioni professionali e di categoria, di fornire chiarimenti in merito attraverso risposte ai quesiti più frequenti da diffondere anche tramite il sito Internet dell'Autorità;

Ritenuta l'opportunità di unificare i termini previsti per l'adempimento delle prescrizioni di cui al citato provvedimento del 27 novembre 2008 e ravvisata altresì la necessità di prorogare tali termini, disponendo che tutti i titolari del trattamento (qualunque sia la data di inizio dei trattamenti che li riguardano) adottino le misure e gli accorgimenti di cui al punto 2 del dispositivo di tale provvedimento entro il 30 giugno 2009;

Viste le osservazioni formulate dal segretario generale ai sensi dell'art. 15 del regolamento del Garante n. 1/2000;

Relatore il prof. Francesco Pizzetti;

DISPONE:

a) di unificare e contestualmente prorogare i termini per l'adempimento delle prescrizioni di cui al citato provvedimento del 27 novembre 2008, prescrivendo che tutti i titolari del trattamento interessati (qualunque sia la data di inizio dei trattamenti che li riguardano) adottino le misure e gli accorgimenti di cui al punto 2 del dispositivo del provvedimento medesimo entro il 30 giugno 2009;

b) di trasmettere copia del presente provvedimento al Ministero della giustizia-Ufficio pubblicazione leggi e decreti per la sua pubblicazione sulla Gazzetta Ufficiale della Repubblica italiana.

Roma, 12 febbraio 2009

IL PRESIDENTE
Pizzetti

IL RELATORE
Pizzetti

IL SEGRETARIO GENERALE REGGENTE
De Paoli

35. Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema (*)

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) e, in particolare, gli artt. 31 ss. e 154, comma 1, lett. c) e h), nonché il disciplinare tecnico in materia di misure minime di sicurezza di cui all'allegato B al medesimo Codice;

Visti gli atti d'ufficio relativi alla protezione dei dati trattati con sistemi informatici e alla sicurezza dei medesimi dati e sistemi;

Rilevata l'esigenza di intraprendere una specifica attività rispetto ai soggetti preposti ad attività riconducibili alle mansioni tipiche dei cd. "amministratori di sistema", nonché di coloro che svolgono mansioni analoghe in rapporto a sistemi di elaborazione e banche di dati, evidenziandone la rilevanza rispetto ai trattamenti di dati personali anche allo scopo di promuovere presso i relativi titolari e nel pubblico la consapevolezza della delicatezza di tali peculiari mansioni nella "Società dell'informazione" e dei rischi a esse associati;

Considerata l'esigenza di consentire più agevolmente, nei dovuti casi, la conoscibilità dell'esistenza di tali figure o di ruoli analoghi svolti in relazione a talune fasi del trattamento all'interno di enti e organizzazioni;

Ritenuta la necessità di promuovere l'adozione di specifiche cautele nello svolgimento delle mansioni svolte dagli amministratori di sistema, unitamente ad accorgimenti e misure, tecniche e organizzative, volti ad agevolare l'esercizio dei doveri di controllo da parte del titolare (due diligence);

Constatato che lo svolgimento delle mansioni di un amministratore di sistema, anche a seguito di una sua formale designazione quale responsabile o incaricato del trattamento, comporta di

(*) Gazzetta Ufficiale 24 dicembre 2008, n. 300 [doc. *web* n. 1577499], in inglese [doc. *web* n. 1583535]

regola la concreta capacità, per atto intenzionale, ma anche per caso fortuito, di accedere in modo privilegiato a risorse del sistema informativo e a dati personali cui non si è legittimati ad accedere rispetto ai profili di autorizzazione attribuiti;

Rilevata la necessità di richiamare l'attenzione su tale rischio del pubblico, nonché di persone giuridiche, pubbliche amministrazioni e di altri enti (di seguito sinteticamente individuati con l'espressione "titolari del trattamento": art. 4, comma 1, lett. f) del Codice) che impiegano, in riferimento alla gestione di banche dati o reti informatiche, sistemi di elaborazione utilizzati da una molteplicità di incaricati con diverse funzioni, applicative o sistemistiche;

Rilevato che i titolari sono tenuti, ai sensi dell'art. 31 del Codice, ad adottare misure di sicurezza "idonee e preventive" in relazione ai trattamenti svolti, dalla cui mancata o non idonea predisposizione possono derivare responsabilità anche di ordine penale e civile (artt. 15 e 169 del Codice);

Constatato che l'individuazione dei soggetti idonei a svolgere le mansioni di amministratore di sistema riveste una notevole importanza, costituendo una delle scelte fondamentali che, unitamente a quelle relative alle tecnologie, contribuiscono a incrementare la complessiva sicurezza dei trattamenti svolti, e va perciò curata in modo particolare evitando incauti affidamenti;

Considerato inoltre che, qualora ritenga facoltativamente di designare uno o più responsabili del trattamento, il titolare è tenuto a individuare solo 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);

Ritenuto che i titolari di alcuni trattamenti effettuati in ambito pubblico e privato a fini amministrativo-contabili, i quali pongono minori rischi per gli interessati e sono stati pertanto oggetto di recenti misure di semplificazione (art. 29 d.l. 25 giugno 2008, n. 112, conv., con mod., con l. 6 agosto 2008, n. 133; art. 34 del Codice; Provv. Garante 6 novembre 2008), debbano essere allo stato esclusi dall'ambito applicativo del presente provvedimento;

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;

PREMESSO:

1. CONSIDERAZIONI PRELIMINARI

Con la definizione di "amministratore di sistema" si individuano generalmente, in ambito informatico, figure professionali finalizzate alla gestione e alla manutenzione di un impianto di elaborazione o di sue componenti. Ai fini del presente provvedimento vengono però considerate tali anche altre figure equiparabili dal punto di vista dei rischi relativi alla protezione dei dati, quali gli amministratori di basi di dati, gli amministratori di reti e di apparati di sicurezza e gli amministratori di sistemi software complessi.

Gli amministratori di sistema così ampiamente individuati, pur non essendo preposti ordinariamente a operazioni che implicano una comprensione del dominio applicativo (significato dei dati, formato delle rappresentazioni e semantica delle funzioni), nelle loro consuete attività sono, in molti casi, concretamente "responsabili" di specifiche fasi lavorative che possono comportare elevate criticità rispetto alla protezione dei dati.

Attività tecniche quali il salvataggio dei dati (backup/recovery), l'organizzazione dei flussi di rete, la gestione dei supporti di memorizzazione e la manutenzione hardware comportano infatti, in molti casi, un'effettiva capacità di azione su informazioni che va considerata a tutti gli effetti alla stregua di un trattamento di dati personali; ciò, anche quando l'amministratore non consulti "in chiaro" le informazioni medesime.

La rilevanza, la specificità e la particolare criticità del ruolo dell'amministratore di sistema sono state considerate anche dal legislatore il quale ha individuato, con diversa denominazione, particolari funzioni tecniche che, se svolte da chi commette un determinato reato, integrano ad esempio una circostanza aggravante. Ci si riferisce, in particolare, all'abuso della qualità di operatore di sistema prevista dal codice penale per le fattispecie di accesso abusivo a sistema informatico o telematico (art. 615-*ter*) e di frode informatica (art. 640-*ter*), nonché per le fattispecie di danneggiamento di informazioni, dati e programmi informatici (artt. 635-*bis* e *ter*) e di danneggiamento di sistemi informatici e telematici (artt. 635-*quater* e *quinques*) di recente modifica (1).

La disciplina di protezione dei dati previgente al Codice del 2003 definiva l'amministratore di

(1) V., ad es., l'art. 5 l. 18 marzo 2008, n. 48 che prevede, oltre a una maggiore pena, la procedibilità d'ufficio nel caso in cui il reato sia commesso con "abuso della qualità di operatore del sistema"

sistema, individuandolo quale "soggetto al quale è conferito il compito di sovrintendere alle risorse del sistema operativo di un elaboratore o di un sistema di banca dati e di consentirne l'utilizzazione" (art. 1, comma 1, lett. c) d.P.R. 318/1999).

Il Codice non ha invece incluso questa figura tra le proprie definizioni normative. Tuttavia le funzioni tipiche dell'amministrazione di un sistema sono richiamate nel menzionato Allegato B, nella parte in cui prevede l'obbligo per i titolari di assicurare la custodia delle componenti riservate delle credenziali di autenticazione. Gran parte dei compiti previsti nel medesimo Allegato B spettano tipicamente all'amministratore di sistema: dalla realizzazione di copie di sicurezza (operazioni di backup e recovery dei dati) alla custodia delle credenziali alla gestione dei sistemi di autenticazione e di autorizzazione.

Nel loro complesso, le norme predette mettono in rilievo la particolare capacità di azione propria degli amministratori di sistema e la natura fiduciaria delle relative mansioni, analoga a quella che, in un contesto del tutto differente, caratterizza determinati incarichi di custodia e altre attività per il cui svolgimento è previsto il possesso di particolari requisiti tecnico-organizzativi, di onorabilità, professionali, morali o di condotta, a oggi non contemplati per lo svolgimento di uno dei ruoli più delicati della "Società dell'informazione" (2).

Nel corso delle attività ispettive disposte negli ultimi anni dal Garante è stato possibile rilevare quale importanza annettano ai ruoli di system administrator (e di network administrator o database administrator) la gran parte di aziende e di grandi organizzazioni pubbliche e private, al di là delle definizioni giuridiche, individuando tali figure nell'ambito di piani di sicurezza o di documenti programmatici e designandoli a volte quali responsabili.

In altri casi, non soltanto in organizzazioni di piccole dimensioni, si è invece riscontrata, anche a elevati livelli di responsabilità, una carente consapevolezza delle criticità insite nello svolgimento delle predette mansioni, con preoccupante sottovalutazione dei rischi derivanti dall'azione incontrollata di chi dovrebbe essere preposto anche a compiti di vigilanza e controllo del corretto utilizzo di un sistema informatico.

(2) Per altro verso il legislatore, nell'intervenire in tema di "Società dell'informazione", ha previsto che i certificatori di firma elettronica, i quali sono preposti al trattamento dei dati connessi al rilascio del certificato di firma, debbano possedere i requisiti di onorabilità richiesti ai soggetti che svolgono funzioni di amministrazione, direzione e controllo presso banche, oltre ai requisiti tecnici necessari per lo svolgimento della loro attività (artt. 26, 27 e 29 del d.lg. 7 marzo 2005 n. 82)

Con il presente provvedimento il Garante intende pertanto richiamare tutti i titolari di trattamenti effettuati, anche in parte, mediante strumenti elettronici alla necessità di prestare massima attenzione ai rischi e alle criticità implicite nell'affidamento degli incarichi di amministratore di sistema. L'Autorità ravvisa inoltre l'esigenza di individuare in questa sede alcune prime misure di carattere organizzativo che favoriscano una più agevole conoscenza, nell'ambito di organizzazioni ed enti pubblici e privati, dell'esistenza di determinati ruoli tecnici, delle responsabilità connesse a tali mansioni e, in taluni casi, dell'identità dei soggetti che operano quali amministratori di sistema in relazione ai diversi servizi e banche di dati.

2. QUADRO DI RIFERIMENTO NORMATIVO

Nell'ambito del Codice il presente provvedimento si richiama, in particolare, all'art. 154, comma 1, lett. h), rientrando tra i compiti dell'Autorità quello di promuovere la "conoscenza tra il pubblico della disciplina rilevante in materia di trattamento dei dati personali e delle relative finalità, nonché delle misure di sicurezza dei dati".

La lett. c) del medesimo comma 1 prevede poi la possibilità, da parte del Garante, di prescrivere misure e accorgimenti, specifici o di carattere generale, che i titolari di trattamento sono tenuti ad adottare.

3. SEGNALAZIONE AI TITOLARI DI TRATTAMENTI RELATIVA ALLE FUNZIONI DI AMMINISTRATORE DI SISTEMA

Ai sensi del menzionato art. 154, comma 1, lett. h) il Garante, nel segnalare a tutti i titolari di trattamenti di dati personali soggetti all'ambito applicativo del Codice ed effettuati con strumenti elettronici la particolare criticità del ruolo degli amministratori di sistema, richiama l'attenzione dei medesimi titolari sulla necessità di adottare idonee cautele volte a prevenire e ad accertare eventuali accessi non consentiti ai dati personali, in specie quelli realizzati con abuso della qualità di amministratore di sistema; richiama inoltre l'attenzione sull'esigenza di valutare con particolare cura l'attribuzione di funzioni tecniche propriamente corrispondenti o assimilabili a quelle di amministratore di sistema, laddove queste siano esercitate in un contesto che renda ad essi tecnicamente possibile l'accesso, anche fortuito, a dati personali. Ciò, tenendo in considerazione

l'opportunità o meno di tale attribuzione e le concrete modalità sulla base delle quali si svolge l'incarico, unitamente alle qualità tecniche, professionali e di condotta del soggetto individuato, da vagliare anche in considerazione delle responsabilità, specie di ordine penale e civile (artt. 15 e 169 del Codice), che possono derivare in caso di incauta o inidonea designazione.

4. Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici

Di seguito sono indicati gli accorgimenti e le misure che vengono prescritti ai sensi dell'art. 154, comma 1, lett. c) del Codice, a tutti i titolari dei trattamenti di dati personali effettuati con strumenti elettronici, esclusi, allo stato, quelli effettuati in ambito pubblico e privato a fini amministrativo-contabili che, ponendo minori rischi per gli interessati, sono stati oggetto delle recenti misure di semplificazione (art. 29 d.l. 25 giugno 2008, n. 112, conv., con mod., con l. 6 agosto 2008, n. 133; art. 34 del Codice; Provv. Garante 6 novembre 2008).

I seguenti accorgimenti e misure lasciano impregiudicata l'adozione di altre specifiche cautele imposte da discipline di settore per particolari trattamenti o che verranno eventualmente prescritte dal Garante ai sensi dell'art. 17 del Codice.

Per effetto del presente provvedimento:

4.1. *Valutazione delle caratteristiche soggettive*

L'attribuzione delle funzioni di amministratore di sistema deve avvenire previa valutazione dell'esperienza, della capacità e dell'affidabilità del soggetto designato, il quale deve fornire idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento ivi compreso il profilo relativo alla sicurezza.

Anche quando le funzioni di amministratore di sistema o assimilate sono attribuite solo nel quadro di una designazione quale incaricato del trattamento ai sensi dell'art. 30 del Codice, il titolare e il responsabile devono attenersi comunque a criteri di valutazione equipollenti a quelli richiesti per la designazione dei responsabili ai sensi dell'art. 29.

4.2. *Designazioni individuali*

La designazione quale amministratore di sistema deve essere in ogni caso individuale e recare l'elencazione analitica degli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato.

4.3. *Elenco degli amministratori di sistema*

Gli estremi identificativi delle persone fisiche amministratori di sistema, con l'elenco delle funzioni ad essi attribuite, devono essere riportati nel documento programmatico sulla sicurezza, oppure, nei casi in cui il titolare non è tenuto a redigerlo, annotati comunque in un documento interno da mantenere aggiornato e disponibile in caso di accertamenti anche da parte del Garante.

Qualora l'attività degli amministratori di sistema riguardi anche indirettamente servizi o sistemi che trattano o che permettono il trattamento di informazioni di carattere personale di lavoratori, i titolari pubblici e privati nella qualità di datori di lavoro sono tenuti a rendere nota o conoscibile l'identità degli amministratori di sistema nell'ambito delle proprie organizzazioni, secondo le caratteristiche dell'azienda o del servizio, in relazione ai diversi servizi informatici cui questi sono preposti. Ciò, avvalendosi dell'informativa resa agli interessati ai sensi dell'art. 13 del Codice nell'ambito del rapporto di lavoro che li lega al titolare, oppure tramite il disciplinare tecnico la cui adozione è prevista dal provvedimento del Garante n. 13 del 1° marzo 2007 (in G.U. 10 marzo 2007, n. 58); in alternativa si possono anche utilizzare strumenti di comunicazione interna (a es., intranet aziendale, ordini di servizio a circolazione interna o bollettini). Ciò, salvi i casi in cui tale forma di pubblicità o di conoscibilità non sia esclusa in forza di un'eventuale disposizione di legge che disciplini in modo difforme uno specifico settore.

Nel caso di servizi di amministrazione di sistema affidati in outsourcing il titolare deve conservare direttamente e specificamente, per ogni eventuale evenienza, gli estremi identificativi delle persone fisiche preposte quali amministratori di sistema.

4.4. *Verifica delle attività*

L'operato degli amministratori di sistema deve essere oggetto, con cadenza almeno annuale, di un'attività di verifica da parte dei titolari del trattamento, in modo da controllare la sua rispondenza alle misure organizzative, tecniche e di sicurezza rispetto ai trattamenti dei dati personali previste dalle norme vigenti.

4.5. *Registrazione degli accessi*

Devono essere adottati sistemi idonei alla registrazione degli accessi logici (autenticazione informatica) ai sistemi di elaborazione e agli archivi elettronici da parte degli amministratori di

sistema. Le registrazioni (access log) devono avere caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo di verifica per cui sono richieste.

Le registrazioni devono comprendere i riferimenti temporali e la descrizione dell'evento che le ha generate e devono essere conservate per un congruo periodo, non inferiore a sei mesi.

5. TEMPI DI ADOZIONE DELLE MISURE E DEGLI ACCORGIMENTI

Per tutti i titolari dei trattamenti già iniziati o che avranno inizio entro trenta giorni dalla data di pubblicazione nella Gazzetta Ufficiale del presente provvedimento, le misure e gli accorgimenti di cui al punto 4 dovranno essere introdotti al più presto e comunque entro, e non oltre, il termine che è congruo stabilire, in centoventi giorni dalla medesima data.

Per tutti gli altri trattamenti che avranno inizio dopo il predetto termine di trenta giorni dalla pubblicazione, gli accorgimenti e le misure dovranno essere introdotti anteriormente all'inizio del trattamento dei dati.

TUTTO CIÒ PREMESSO IL GARANTE:

1. ai sensi dell'art. 154, comma 1, lett. h) del Codice, nel segnalare a tutti i titolari di trattamenti di dati personali soggetti all'ambito applicativo del Codice ed effettuati con strumenti elettronici la particolare criticità del ruolo degli amministratori di sistema, richiama l'attenzione dei medesimi titolari sull'esigenza di valutare con particolare attenzione l'attribuzione di funzioni tecniche propriamente corrispondenti o assimilabili a quelle di amministratore di sistema (system administrator), amministratore di base di dati (database administrator) o amministratore di rete (network administrator), laddove tali funzioni siano esercitate in un contesto che renda ad essi tecnicamente possibile l'accesso, anche fortuito, a dati personali. Ciò, tenendo in considerazione l'opportunità o meno di tale attribuzione e le concrete modalità sulla base delle quali si svolge l'incarico, unitamente alle qualità tecniche, professionali e di condotta del soggetto individuato;
2. ai sensi dell'art. 154, comma 1, lett. c) del Codice prescrive l'adozione delle seguenti misure ai titolari dei trattamenti di dati personali soggetti all'ambito applicativo del Codice ed effettuati con strumenti elettronici, anche in ambito giudiziario e di forze di

polizia (artt. 46 e 53 del Codice), salvo per quelli effettuati in ambito pubblico e privato a fini amministrativo-contabili che pongono minori rischi per gli interessati e sono stati oggetto delle misure di semplificazione introdotte di recente per legge (art. 29 d.l. 25 giugno 2008, n. 112, conv., con mod., con l. 6 agosto 2008, n. 133; art. 34 del Codice; Provv. Garante 6 novembre 2008):

a. Valutazione delle caratteristiche soggettive

L'attribuzione delle funzioni di amministratore di sistema deve avvenire previa valutazione delle caratteristiche di esperienza, capacità e affidabilità del soggetto designato, il quale deve fornire idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza.

Anche quando le funzioni di amministratore di sistema o assimilate sono attribuite solo nel quadro di una designazione quale incaricato del trattamento ai sensi dell'art. 30 del Codice, il titolare e il responsabile devono attenersi comunque a criteri di valutazione equipollenti a quelli richiesti per la designazione dei responsabili ai sensi dell'art. 29.

b. Designazioni individuali

La designazione quale amministratore di sistema deve essere individuale e recare l'elencazione analitica degli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato.

c. Elenco degli amministratori di sistema

Gli estremi identificativi delle persone fisiche amministratori di sistema, con l'elenco delle funzioni ad essi attribuite, devono essere riportati nel documento programmatico sulla sicurezza oppure, nei casi in cui il titolare non è tenuto a redigerlo, annotati comunque in un documento interno da mantenere aggiornato e disponibile in caso di accertamenti da parte del Garante.

Qualora l'attività degli amministratori di sistema riguardi anche indirettamente servizi o sistemi che trattano o che permettono il trattamento di informazioni di carattere personale dei lavoratori, i titolari pubblici e privati sono tenuti a rendere nota o conoscibile l'identità degli amministratori di sistema nell'ambito delle proprie orga-

nizzazioni, secondo le caratteristiche dell'azienda o del servizio, in relazione ai diversi servizi informatici cui questi sono preposti. Ciò, avvalendosi dell'informativa resa agli interessati ai sensi dell'art. 13 del Codice nell'ambito del rapporto di lavoro che li lega al titolare, oppure tramite il disciplinare tecnico di cui al provvedimento del Garante n. 13 del 1° marzo 2007 (in G.U. 10 marzo 2007, n. 58) o, in alternativa, mediante altri strumenti di comunicazione interna (ad es., intranet aziendale, ordini di servizio a circolazione interna o bollettini). Ciò, salvi i casi in cui tali forme di pubblicità o di conoscibilità siano incompatibili con diverse previsioni dell'ordinamento che disciplinino uno specifico settore.

d. Servizi in outsourcing

Nel caso di servizi di amministrazione di sistema affidati in outsourcing il titolare deve conservare direttamente e specificamente, per ogni eventuale evenienza, gli estremi identificativi delle persone fisiche preposte quali amministratori di sistema.

e. Verifica delle attività

L'operato degli amministratori di sistema deve essere oggetto, con cadenza almeno annuale, di un'attività di verifica da parte dei titolari del trattamento, in modo da controllare la sua rispondenza alle misure organizzative, tecniche e di sicurezza riguardanti i trattamenti dei dati personali previste dalle norme vigenti.

f. Registrazione degli accessi

Devono essere adottati sistemi idonei alla registrazione degli accessi logici (autenticazione informatica) ai sistemi di elaborazione e agli archivi elettronici da parte degli amministratori di sistema. Le registrazioni (access log) devono avere caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo per cui sono richieste. Le registrazioni devono comprendere i riferimenti temporali e la descrizione dell'evento che le ha generate e devono essere conservate per un congruo periodo, non inferiore a sei mesi;

3. dispone che le misure e gli accorgimenti di cui al punto 2 del presente dispositivo siano introdotti, per tutti i trattamenti già iniziati o che avranno inizio entro trenta giorni dalla data di pubblicazione nella Gazzetta Ufficiale del presente provvedimento, al più presto e

comunque entro, e non oltre, il termine che è congruo stabilire in centoventi giorni dalla medesima data; per tutti gli altri trattamenti che avranno inizio dopo il predetto termine di trenta giorni dalla pubblicazione, gli accorgimenti e le misure dovranno essere introdotti anteriormente all'inizio del trattamento dei dati;

4. dispone che copia del presente provvedimento sia trasmesso al Ministero della giustizia–Ufficio pubblicazione leggi e decreti per la sua pubblicazione sulla Gazzetta Ufficiale della Repubblica Italiana.

Roma, 27 novembre 2008

IL PRESIDENTE
Pizzetti

IL RELATORE
Pizzetti

IL SEGRETARIO GENERALE
Buttarelli

Provvedimento "Amministratori di sistema" del 27 novembre 2008 (*)

Risposte alle domande più frequenti (FAQ) (1)

1) Cosa deve intendersi per "amministratore di sistema"?

In assenza di definizioni normative e tecniche condivise, nell'ambito del provvedimento del Garante l'amministratore di sistema è assunto quale figura professionale dedicata alla gestione e alla manutenzione di impianti di elaborazione con cui vengano effettuati trattamenti di dati personali, compresi i sistemi di gestione delle basi di dati, i sistemi software complessi quali i sistemi ERP (Enterprise resource planning) utilizzati in grandi aziende e organizzazioni, le reti locali e gli apparati di sicurezza, nella misura in cui consentano di intervenire sui dati personali.

Il Garante non ha inteso equiparare gli "operatori di sistema" di cui agli articoli del Codice penale relativi ai delitti informatici, con gli "amministratori di sistema": questi ultimi sono dei particolari operatori di sistema, dotati di specifici privilegi.

Anche il riferimento al d.P.R. 318/1999 nella premessa del provvedimento è puramente descrittivo poiché la figura definita in quell'atto normativo (ormai abrogato) è di minore portata rispetto a quella cui si fa riferimento nel provvedimento.

Non rientrano invece nella definizione quei soggetti che solo occasionalmente intervengono (p.es., per scopi di manutenzione a seguito di guasti o malfunzioni) sui sistemi di elaborazione e sui sistemi software.

2) Cosa vuol dire la locuzione "Qualora l'attività degli ADS riguardi anche indirettamente servizi o sistemi che …"

I titolari sono tenuti a instaurare un regime di conoscibilità dell'identità degli amministratori di sistema, quale forma di trasparenza interna all'organizzazione a tutela dei lavoratori, nel caso in cui un amministratore di sistema, oltre a intervenire sotto il profilo tecnico in generici trattamenti di dati personali in un'organizzazione, tratti anche dati personali riferiti ai lavoratori operanti nell'am-

(*) Gazzetta Ufficiale del 24 dicembre 2008, n. 300
(1) Così richiamate dal provvedimento "Amministratori di sistema: avvio di una consultazione pubblica" del 21 aprile 2009 [doc. *web* n. 1611986]

bito dell'organizzazione medesima o sia nelle condizioni di acquisire conoscenza di dati a essi riferiti (in questo senso il riferimento nel testo del provvedimento all'"anche indirettamente …").

3) Il caso di uso esclusivo di un personal computer da parte di un solo amministratore di sistema rientra nell'ambito applicativo del provvedimento?

Non è possibile rispondere in generale. In diversi casi, anche con un personal computer possono essere effettuati delicati trattamenti rispetto ai quali il titolare ha il dovere di prevedere e mettere in atto anche le misure e gli accorgimenti previsti nel provvedimento. Nel caso-limite di un titolare che svolga funzioni di unico amministratore di sistema, come può accadere in piccolissime realtà d'impresa, non si applicheranno le previsioni relative alla verifica delle attività dell'amministratore né la tenuta del log degli accessi informatici.

4) Relativamente all'obbligo di registrazione degli accessi logici degli AdS, sono compresi anche i sistemi client oltre che quelli server?

Si, anche i client, intesi come "postazioni di lavoro informatizzate", sono compresi tra i sistemi per cui devono essere registrati gli accessi degli AdS.

Nei casi più semplici tale requisito può essere soddisfatto tramite funzionalità già disponibili nei più diffusi sistemi operativi, senza richiedere necessariamente l'uso di strumenti software o hardware aggiuntivi. Per esempio, la registrazione locale dei dati di accesso su una postazione, in determinati contesti, può essere ritenuta idonea al corretto adempimento qualora goda di sufficienti garanzie di integrità.

Sarà comunque con valutazione del titolare che dovrà essere considerata l'idoneità degli strumenti disponibili oppure l'adozione di strumenti più sofisticati, quali la raccolta dei log centralizzata e l'utilizzo di dispositivi non riscrivibili o di tecniche crittografiche per la verifica dell'integrità delle registrazioni.

5) Cosa si intende per operato dell'amministratore di sistema soggetto a controllo almeno annuale?

È da sottoporre a verifica l'attività svolta dall'amministratore di sistema nell'esercizio delle sue

funzioni. Va verificato che le attività svolte dall'amministratore di sistema siano conformi alle mansioni attribuite, ivi compreso il profilo relativo alla sicurezza.

6) Chiarire i casi di esclusione dall'obbligo di adempiere al provvedimento.

Sono esclusi i trattamenti effettuati in ambito pubblico e privato a fini amministrativo-contabili che, ponendo minori rischi per gli interessati, sono stati oggetto delle misure di semplificazione introdotte nel corso del 2008 per legge (art. 29 d.l. 25 giugno 2008, n. 112, conv., con mod., con l. 6 agosto 2008, n. 133; art. 34 del Codice; Provv. Garante 27 novembre 2008).

7) Cosa si intende per descrizione analitica degli ambiti di operatività consentiti all'ADS? [Rif. comma 2, lettera d]

Il provvedimento prevede che all'atto della designazione di un amministratore di sistema, venga fatta "elencazione analitica" degli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato, ovvero la descrizione puntuale degli stessi, evitando l'attribuzione di ambiti insufficientemente definiti, analogamente a quanto previsto al comma 4 dell'art. 29 del Codice riguardante i responsabili del trattamento.

8) Oltre alla job description si deve andare più in dettaglio? Si devono indicare i singoli sistemi e le singole operazioni affidate?

No, è sufficiente specificare l'ambito di operatività in termini più generali, per settori o per aree applicative, senza obbligo di specificarlo rispetto a singoli sistemi, a meno che non sia ritenuto necessario in casi specifici.

9) Cosa si intende per access log (log-in, log-out, tentativi falliti di accesso, altro?...) [Rif. comma 2, lettera f]

Per access log si intende la registrazione degli eventi generati dal sistema di autenticazione informatica all'atto dell'accesso o tentativo di accesso da parte di un amministratore di sistema o all'atto della sua disconnessione nell'ambito di collegamenti interattivi a sistemi di elaborazione o a sistemi software.

Gli event records generati dai sistemi di autenticazione contengono usualmente i riferimenti allo "username" utilizzato, alla data e all'ora dell'evento (timestamp), una descrizione dell'evento (sistema di elaborazione o software utilizzato, se si tratti di un evento di log-in, di log-out, o di una condizione di errore, quale linea di comunicazione o dispositivo terminale sia stato utilizzato …).

10) Laddove il file di log contenga informazioni più ampie, va preso tutto il log o solo la riga relativa all'access log? [Rif. comma 2, lettera f]

Qualora il sistema di log adottato generi una raccolta dati più ampia, comunque non in contrasto con le disposizioni del Codice e con i principi della protezione dei dati personali, il requisito del provvedimento è certamente soddisfatto. Comunque è sempre possibile effettuare un'estrazione o un filtraggio dei logfiles al fine di selezionare i soli dati pertinenti agli AdS.

11) Come va interpretata la caratteristica di completezza del log? Si intende che ci devono essere tutte le righe? L'adeguatezza rispetto allo scopo della verifica deve prevedere un'analisi dei rischi?

La caratteristica di completezza è riferita all'insieme degli eventi censiti nel sistema di log, che deve comprendere tutti gli eventi di accesso interattivo che interessino gli amministratori di sistema su tutti i sistemi di elaborazione con cui vengono trattati, anche indirettamente, dati personali. L'analisi dei rischi aiuta a valutare l'adeguatezza delle misure di sicurezza in genere, e anche delle misure tecniche per garantire attendibilità ai log qui richiesti.

12) Come va interpretata la caratteristica di inalterabilità dei log?

Caratteristiche di mantenimento dell'integrità dei dati raccolti dai sistemi di log sono in genere disponibili nei più diffusi sistemi operativi, o possono esservi agevolmente integrate con apposito software. Il requisito può essere ragionevolmente soddisfatto con la strumentazione software in dotazione, nei casi più semplici, e con l'eventuale esportazione periodica dei dati di log su supporti di memorizzazione non riscrivibili. In casi più complessi i titolari potranno ritenere di

adottare sistemi più sofisticati, quali i log server centralizzati e "certificati".

È ben noto che il problema dell'attendibilità dei dati di audit, in genere, riguarda in primo luogo la effettiva generazione degli auditable events e, successivamente, la loro corretta registrazione e manutenzione. Tuttavia il provvedimento del Garante non affronta questi aspetti, prevedendo soltanto, come forma minima di documentazione dell'uso di un sistema informativo, la generazione del log degli "accessi" (login) e la loro archiviazione per almeno sei mesi in condizioni di ragionevole sicurezza e con strumenti adatti, in base al contesto in cui avviene il trattamento, senza alcuna pretesa di instaurare in modo generalizzato, e solo con le prescrizioni del provvedimento, un regime rigoroso di registrazione degli usage data dei sistemi informativi.

13) Si individuano livelli di robustezza specifici per la garanzia della integrità?

No. La valutazione è lasciata al titolare, in base al contesto operativo (cfr. faq n. 14).

14) Quali potrebbero essere gli scopi di verifica rispetto ai quali valutare l'adeguatezza?

Quelli descritti al paragrafo 4.4 del provvedimento e ribaditi al punto 2, lettera e), del dispositivo. L'adeguatezza è da valutare in rapporto alle condizioni organizzative e operative dell'organizzazione.

15) Cosa dobbiamo intendere per evento che deve essere registrato nel log? Solo l'accesso o anche le attività eseguite?

Il provvedimento non chiede in alcun modo che vengano registrati dati sull'attività interattiva (comandi impartiti, transazioni effettuate) degli amministratori di sistema. Si veda la risposta alla faq n. 11.

16) Quali sono le finalità di audit che ci dobbiamo porre con la registrazione e raccolta di questi log?

La raccolta dei log serve per verificare anomalie nella frequenza degli accessi e nelle loro modalità (orari, durata, sistemi cui si è fatto accesso…). L'analisi dei log può essere compresa tra i criteri di valutazione dell'operato degli amministratori di sistema.

17) Cosa si intende per "consultazione in chiaro"?

Il riferimento in premessa (par. 1 "Considerazioni preliminari") è alla criticità di mansioni che comportino la potenzialità di violazione del dato personale anche in condizioni in cui ne sia esclusa la conoscibilità, come può avvenire, per esempio, nel caso della cifratura dei dati.

18) Il regime di conoscibilità degli amministratori di sistema è da intendersi per i soli trattamenti inerenti i dati del personale e dei lavoratori?

Si.

19) La registrazione degli accessi è relativa al sistema operativo o anche ai DBMS?

Tra gli accessi logici a sistemi e archivi elettronici sono comprese le autenticazioni nei confronti dei data base management systems (DBMS), che vanno registrate.

20) Nella designazione degli amministratori di sistema occorre valutare i requisiti morali? [Rif. comma 2, lettera a]

No. Il riferimento alle caratteristiche da prendere in considerazione, al comma 2, lettera a), del dispositivo, è all'esperienza, alla capacità e all'affidabilità del soggetto designato. Si tratta quindi di qualità tecniche, professionali e di condotta, non di requisiti morali.

21) Cosa si intende per "estremi identificativi" degli amministratori di sistema?

Si tratta del minimo insieme di dati identificativi utili a individuare il soggetto nell'ambito dell'organizzazione di appartenenza. In molti casi possono coincidere con nome, cognome, funzione o area organizzativa di appartenenza.

22) È corretto affermare che l'accesso a livello applicativo non rientri nel perimetro degli adeguamenti, in quanto l'accesso a una applicazione informatica è regolato tramite profili autorizzativi che disciplinano per tutti gli utenti i trattamenti consentiti sui dati?

Si. L'accesso applicativo non è compreso tra le caratteristiche tipiche dell'amministratore di sistema e quindi non è necessario, in forza del provvedimento del Garante, sottoporlo a registrazione.

23) Si chiede se sia necessario conformarsi al provvedimento nel caso della fornitura di servizi di gestione sistemistica a clienti esteri (housing, hosting, gestione applicativa, archiviazione remota...) da parte di una società italiana non titolare dei dati gestiti.

Il provvedimento si rivolge solo ai titolari di trattamento. I casi esemplificati prefigurano al più una responsabilità di trattamento (secondo il Codice italiano), e sono quindi esclusi dall'ambito applicativo del provvedimento.

24) Si possono ritenere esclusi i trattamenti relativi all'ordinaria attività di supporto delle aziende, che non riguardino dati sensibili, giudiziari o di traffico telefonico/telematico? Ci si riferisce ai trattamenti con strumenti elettronici finalizzati, ad esempio, alla gestione dell'autoparco, alle procedure di acquisto dei materiali di consumo, alla manutenzione degli immobili sociali ecc. ...).

Tali trattamenti possono considerarsi compresi tra quelli svolti per ordinarie finalità amministrativo-contabili e, come tali, esclusi dall'ambito applicativo del provvedimento.

36. Rifiuti di apparecchiature elettriche ed elettroniche (Raae) e misure di sicurezza dei dati personali (*)

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;

Visti gli atti d'ufficio relativi alla problematica del rinvenimento di dati personali all'interno di apparecchiature elettriche ed elettroniche cedute a un rivenditore per la dismissione o la vendita o a seguito di riparazioni e sostituzioni; viste, altresì, le recenti notizie di stampa in ordine al rinvenimento da parte dell'acquirente di un disco rigido usato, commercializzato attraverso un sito Internet, di dati bancari relativi a oltre un milione di individui contenuti nel disco medesimo;

Visto il d.lg. 30 giugno 2003, n. 196 (Codice in materia di protezione dei dati personali), con particolare riferimento agli artt. 31 e ss. e 154, comma 1, lett. h), nonché alle regole 21 e 22 del disciplinare tecnico in materia di misure minime di sicurezza allegato "B" al Codice;

Visto il d.lg. 25 luglio 2005, n. 151 (Attuazione delle direttive 2002/95/Ce, 2002/96/Ce e 2003/108/Ce, relative alla riduzione dell'uso di sostanze pericolose nelle apparecchiature elettriche ed elettroniche, nonché allo smaltimento dei rifiuti), che prevede misure e procedure finalizzate a prevenire la produzione di rifiuti di apparecchiature elettriche e elettroniche, nonché a promuovere il reimpiego, il riciclaggio e altre forme di recupero di tali rifiuti in modo da ridurne la quantità da avviare allo smaltimento (cfr. art. 1, comma 1, lett. a) e b));

Considerato che l'applicazione della disciplina contenuta nel menzionato d.lg. n. 151/2005, mirando (tra l'altro) a privilegiare il recupero di componenti provenienti da rifiuti di apparecchiature elettriche ed elettroniche (Raee), anche nella forma del loro reimpiego o del riciclaggio in beni oggetto di (nuova) commercializzazione (cfr. in particolare artt. 1 e 3, comma 1, lett. e) ed f), d.lg. n. 151/2005), comporta un rischio elevato di "circolazione" di componenti elettroniche "usate" contenenti dati personali, anche sensibili, che non siano stati cancellati in modo idoneo, e di conseguente accesso ad essi da parte di terzi non autorizzati (quali, ad esempio,

(*) Gazzetta Ufficiale 9 dicembre 2008, n. 287 [doc. *web* n. 1571514], in inglese [doc. *web* n. 1583482]

coloro che provvedono alle predette operazioni propedeutiche al riutilizzo o che acquistano le apparecchiature sopra indicate);

Considerato che il "reimpiego" consiste nelle operazioni che consentono l'utilizzo dei rifiuti elettrici ed elettronici o di loro componenti "allo stesso scopo per il quale le apparecchiature erano state originariamente concepite, compresa l'utilizzazione di dette apparecchiature o di loro componenti successivamente alla loro consegna presso i centri di raccolta, ai distributori, ai riciclatori o ai fabbricanti" (art. 3, comma 1, lett. e), d.lg. n. 151/2005) e il "riciclaggio" consiste nel "ritrattamento in un processo produttivo dei materiali di rifiuto per la loro funzione originaria o per altri fini" (art. 3, comma 1, lett. e), d.lg. n. 151/2005);

Considerato che rischi di accessi non autorizzati ai dati memorizzati sussistono anche in relazione a rifiuti di apparecchiature elettriche ed elettroniche avviati allo smaltimento (art. 3, comma 1, lett. i), d.lg. n. 151/2005);

Rilevata la necessità di richiamare l'attenzione su tali rischi di persone giuridiche, pubbliche amministrazioni, altri enti e persone fisiche che, avendone fatto uso nello svolgimento delle proprie attività, in particolare quelle industriali, commerciali, professionali o istituzionali (di seguito sinteticamente individuati con la locuzione "titolari del trattamento": art. 4, comma 1, lett. f) del Codice), dismettono sistemi informatici o, più in generale, apparecchiature elettriche ed elettroniche contenenti dati personali (come pure dei soggetti che, su base individuale o collettiva, provvedono al reimpiego, al riciclaggio o allo smaltimento dei rifiuti di dette apparecchiature);

Rilevato che la disciplina di cui al citato d.lg. n. 151/2005 e alla normativa secondaria che ne è derivata (allo stato contenuta nel d.m. 25 settembre 2007, n. 185, recante "Istituzione e modalità di funzionamento del registro nazionale dei soggetti obbligati al finanziamento dei sistemi di gestione dei rifiuti di apparecchiature elettriche ed elettroniche (Raee)", nell'ulteriore d.m. del 25 settembre 2007, recante "Istituzione del Comitato di vigilanza e di controllo sulla gestione dei Raee", nonché nel d.m. 8 aprile 2008, recante "Disciplina dei centri di raccolta dei rifiuti urbani raccolti in modo differenziato come previsto dall'art. 183, comma 1, lettera cc) del decreto legislativo 3 aprile 2006, n. 152 e successive modifiche") lascia impregiudicati gli obblighi che gravano sui titolari del trattamento relativamente alle misure di sicurezza nel trattamento dei dati personali (e la conseguente responsabilità);

Rilevato che ogni titolare del trattamento deve quindi adottare appropriate misure organizzative e tecniche volte a garantire la sicurezza dei dati personali trattati e la loro protezione anche nei confronti di accessi non autorizzati che possono verificarsi in occasione della dismissione dei menzionati apparati elettrici ed elettronici (artt. 31 ss. del Codice); ciò, considerato anche che, impregiudicati eventuali accordi che prevedano diversamente, produttori, distributori e centri di assistenza di apparecchiature elettriche ed elettroniche non risultano essere soggetti, in base alla particolare disciplina di settore, a specifici obblighi di distruzione dei dati personali eventualmente memorizzati nelle apparecchiature elettriche ed elettroniche a essi consegnate;

Rilevato che dall'inosservanza delle misure di sicurezza può derivare in capo al titolare del trattamento una responsabilità penale (art. 169 del Codice) e, in caso di danni cagionati a terzi, civile (artt. 15 del Codice e 2050 cod. civ.);

Rilevato che analoghi obblighi relativi alla destinazione dei dati gravano sul titolare del trattamento nel caso in cui la dismissione delle apparecchiature coincida con la cessazione del trattamento (art. 16 del Codice);

Rilevato che le misure da adottare in occasione della dismissione di componenti elettrici ed elettronici suscettibili di memorizzare dati personali devono consistere nell'effettiva cancellazione o trasformazione in forma non intelligibile dei dati personali negli stessi contenute, sì da impedire a soggetti non autorizzati che abbiano a vario titolo la disponibilità materiale dei supporti di venirne a conoscenza non avendone diritto (si pensi, ad esempio, ai dati personali memorizzati sul disco rigido dei personal computer o nelle cartelle di posta elettronica, oppure custoditi nelle rubriche dei terminali di comunicazione elettronica);

Considerato che tali misure risultano allo stato già previste quali misure minime di sicurezza per i trattamenti di dati sensibili o giudiziari, sulla base delle regole 21 e 22 del disciplinare tecnico in materia di misure minime di sicurezza che disciplinano la custodia e l'uso dei supporti rimovibili sui quali sono memorizzati i dati, che vincolano il riutilizzo dei supporti alla cancellazione effettiva dei dati o alla loro trasformazione in forma non intelligibile;

Ritenuto che i titolari del trattamento, in occasione della dismissione delle menzionate apparecchiature elettriche ed elettroniche, qualora siano sprovvisti delle necessarie competenze e strumentazioni tecniche per la cancellazione dei dati personali, possono ricorrere all'ausilio o con-

ferendo incarico a soggetti tecnicamente qualificati in grado di porre in essere le misure idonee a cancellare effettivamente o rendere non intelligibili i dati, quali centri di assistenza, produttori e distributori di apparecchiature che attestino l'esecuzione di tali operazioni o si impegnino ad effettuarle;

Ritenuto che chi procede al reimpiego o al riciclaggio di rifiuti di apparecchiature elettriche ed elettroniche o di loro componenti debba comunque assicurarsi dell'inesistenza o della non intelligibilità di dati personali sui supporti, acquisendo, ove possibile, l'autorizzazione a cancellarli o a renderli non intelligibili;

Considerato che, ferma restando l'adozione di ulteriori opportune cautele volte a prevenire l'indebita acquisizione di informazioni personali, anche fortuita, da parte di terzi, le predette misure, suscettibili di aggiornamento alla luce dell'evoluzione tecnologica, possono in particolare consistere, a seconda dei casi, anche nelle procedure di cui agli allegati documenti, che costituiscono parte integrante del presente provvedimento;

Ritenuta la necessità di curare la conoscenza tra il pubblico della disciplina rilevante in materia di trattamento dei dati personali e delle relative finalità, nonché delle misure di sicurezza dei dati (art. 154, comma 1, lett. h), del Codice), con riferimento alla dismissione di apparecchiature elettriche ed elettroniche, anche attraverso la pubblicazione del presente provvedimento sulla Gazzetta Ufficiale della Repubblica Italiana;

Vistele osservazioni formulate dal segretario generale ai sensi dell'art. 15 del regolamento del Garante n. 1/2000;

Relatore il dott. Giuseppe Fortunato;

TUTTO CIÒ PREMESSO IL GARANTE:

1. ai sensi dell'art. 154, comma 1, lett. h) del Codice, richiama l'attenzione di persone giuridiche, pubbliche amministrazioni, altri enti e persone fisiche che, avendone fatto uso nello svolgimento delle proprie attività, in particolare quelle industriali, commerciali, professionali o istituzionali, non distruggono, ma dismettono supporti che contengono dati personali, sulla necessità di adottare idonei accorgimenti e misure, anche con l'ausilio di terzi tecnicamente qualificati, volti a prevenire accessi non consentiti ai dati personali memorizzati nelle apparecchiature elettriche ed elettroniche destinate a essere:

a. reimpiegate o riciclate, anche seguendo le procedure di cui all'allegato A);

b. smaltite, anche seguendo le procedure di cui all'allegato B).

Tali misure e accorgimenti possono essere attuate anche con l'ausilio o conferendo incarico a terzi tecnicamente qualificati, quali centri di assistenza, produttori e distributori di apparecchiature che attestino l'esecuzione delle operazioni effettuate o che si impegnino ad effettuarle.

Chi procede al reimpiego o al riciclaggio di rifiuti di apparecchiature elettriche ed elettroniche o di loro componenti è comunque tenuto ad assicurarsi dell'inesistenza o della non intelligibilità di dati personali sui supporti, acquisendo, ove possibile, l'autorizzazione a cancellarli o a renderli non intelligibili;

2. dispone che copia del presente provvedimento sia trasmesso al Ministero della giustizia-Ufficio pubblicazione leggi e decreti, per la sua pubblicazione sulla Gazzetta Ufficiale della Repubblica Italiana.

Roma, 13 ottobre 2008

IL PRESIDENTE
Pizzetti

IL RELATORE
Fortunato

IL SEGRETARIO GENERALE
Buttarelli

Reimpiego e riciclaggio di rifiuti di apparecchiature elettriche ed elettroniche

In caso di reimpiego e riciclaggio di rifiuti di apparecchiature elettriche ed elettroniche le misure e gli accorgimenti volti a prevenire accessi non consentiti ai dati personali in esse contenuti, adottati nel rispetto delle normative di settore, devono consentire l'effettiva cancellazione dei dati o garantire la loro non intelligibilità. Tali misure, anche in combinazione tra loro, devono tenere conto degli standard tecnici esistenti e possono consistere, tra l'altro, in:

Misure tecniche preventive per la memorizzazione sicura dei dati, applicabili a dispositivi elettronici o informatici:

1. Cifratura di singoli file o gruppi di file, di volta in volta protetti con parole-chiave riservate, note al solo utente proprietario dei dati, che può con queste procedere alla successiva decifratura. Questa modalità richiede l'applicazione della procedura di cifratura ogni volta che sia necessario proteggere un dato o una porzione di dati (file o collezioni di file), e comporta la necessità per l'utente di tenere traccia separatamente delle parole-chiave utilizzate.
2. Memorizzazione dei dati sui dischi rigidi (hard-disk) dei personal computer o su altro genere di supporto magnetico od ottico (cd-rom, dvd-r) in forma automaticamente cifrata al momento della loro scrittura, tramite l'uso di parole-chiave riservate note al solo utente. Può effettuarsi su interi volumi di dati registrati su uno o più dispositivi di tipo disco rigido o su porzioni di essi (partizioni, drive logici, file-system) realizzando le funzionalità di un cd. file-system crittografico (disponibili sui principali sistemi operativi per elaboratori elettronici, anche di tipo personal computer, e dispositivi elettronici) in grado di proteggere, con un'unica parola-chiave riservata, contro i rischi di acquisizione indebita delle informazioni registrate. L'unica parola-chiave di volume verrà automaticamente utilizzata per le operazioni di cifratura e decifratura, senza modificare in alcun modo il comportamento e l'uso dei programmi software con cui i dati vengono trattati.

Misure tecniche per la cancellazione sicura dei dati, applicabili a dispositivi elettronici o informatici:

3. Cancellazione sicura delle informazioni, ottenibile con programmi informatici (quali wiping program o file shredder) che provvedono, una volta che l'utente abbia eliminato dei file da un'unità disco o da analoghi supporti di memorizzazione con i normali strumenti previsti dai diversi sistemi operativi, a scrivere ripetutamente nelle aree vuote del disco (precedentemente occupate dalle informazioni eliminate) sequenze casuali di cifre "binarie" (zero e uno) in modo da ridurre al minimo le probabilità di recupero di informazioni anche tramite strumenti elettronici di analisi e recupero di dati.

Il numero di ripetizioni del procedimento considerato sufficiente a raggiungere una ragionevole sicurezza (da rapportarsi alla delicatezza o all'importanza delle informazioni di cui si vuole impedire l'indebita acquisizione) varia da sette a trentacinque e incide proporzionalmente sui tempi di applicazione delle procedure, che su dischi rigidi ad alta capacità (oltre i 100 gigabyte) possono impiegare diverse ore o alcuni giorni), a secondo della velocità del computer utilizzato.

4. Formattazione "a basso livello" dei dispositivi di tipo hard disk (low-level formatting - LLF), laddove effettuabile, attenendosi alle istruzioni fornite dal produttore del dispositivo e tenendo conto delle possibili conseguenze tecniche su di esso, fino alla possibile sua successiva inutilizzabilità;
5. Demagnetizzazione (degaussing) dei dispositivi di memoria basati su supporti magnetici o magneto-ottici (dischi rigidi, floppy-disk, nastri magnetici su bobine aperte o in cassette), in grado di garantire la cancellazione rapida delle informazioni anche su dispositivi non più funzionanti ai quali potrebbero non essere applicabili le procedure di cancellazione software (che richiedono l'accessibilità del dispositivo da parte del sistema a cui è interconnesso).

ALLEGATO B) AL PROVVEDIMENTO DEL GARANTE DEL 13 OTTOBRE 2008

Smaltimento di rifiuti elettrici ed elettronici

In caso di smaltimento di rifiuti elettrici ed elettronici, l'effettiva cancellazione dei dati personali dai supporti contenuti nelle apparecchiature elettriche ed elettroniche può anche risultare da procedure che, nel rispetto delle normative di settore, comportino la distruzione dei supporti di memorizzazione di tipo ottico o magneto-ottico in modo da impedire l'acquisizione indebita di dati personali.

La distruzione dei supporti prevede il ricorso a procedure o strumenti diversi a secondo del loro tipo, quali:

- sistemi di punzonatura o deformazione meccanica;
- distruzione fisica o di disintegrazione (usata per i supporti ottici come i cd-rom e i dvd);
- demagnetizzazione ad alta intensità.

37. Linee-guida per i trattamenti di dati personali nell'ambito delle sperimentazioni cliniche di medicinali (*)

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. Giuseppe Fortunato, componente, e del dott. Giovanni Buttarelli, segretario generale;

Vista la deliberazione 29 novembre 2007, n. 62, con la quale l'Autorità ha avviato una procedura di consultazione pubblica su un documento, adottato in pari data, contenente "Linee-guida per i trattamenti di dati personali nell'ambito delle sperimentazioni cliniche di medicinali" 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 15 febbraio 2008;

Considerate le risultanze degli incontri intercorsi con i rappresentanti di categoria e con altri enti e organismi che hanno partecipato alla consultazione pubblica;

Ritenuto, in base agli approfondimenti svolti, di individuare un quadro unitario di misure e accorgimenti necessari e opportuni volti a fornire orientamenti utili per i promotori e gli altri operatori che, a vario titolo, intervengono nelle sperimentazioni cliniche riguardo al trattamento dei dati delle persone coinvolte;

Visto il Codice in materia di protezione dei dati personali (d.lg. 30 giugno 2003, n. 196);

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;

DELIBERA:

a) di adottare in via definitiva le "Linee-guida per i trattamenti di dati personali nell'ambito

(*) Deliberazione n. 52 del 24 luglio 2008, Gazzetta Ufficiale 14 agosto 2008, n. 190 [doc. *web* n. 1533155], in inglese [doc. *web* n. 1544272]

delle sperimentazioni cliniche di medicinali" unitamente ad un modello di riferimento per l'informativa e la manifestazione del consenso al trattamento dei dati personali, contenuti nei documenti allegati quali parti integranti della presente deliberazione (Allegati A e n. 1);

b) che copia della presente deliberazione, unitamente ai menzionati allegati, 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;

c) che copia dei predetti documenti sia, altresì, trasmessa per opportuna conoscenza, al Ministero della salute, all'Istituto superiore di sanità, all'Agenzia italiana del farmaco e alla Conferenza Stato-Regioni.

Roma, 24 luglio 2008

IL PRESIDENTE
Pizzetti

IL RELATORE
Chiravalloti

IL SEGRETARIO GENERALE
Buttarelli

ALLEGATO A. LINEE-GUIDA PER I TRATTAMENTI DI DATI PERSONALI NELL'AMBITO DELLE SPERIMENTAZIONI CLINICHE DI MEDICINALI

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 generalmente promossi da una società farmaceutica (committente o sponsor, di seguito individuata come "promotore") a livello nazionale e (specie a cura di società facenti parte di gruppi multinazionali) internazionale.

A tal fine detto soggetto, dopo aver predisposto un protocollo che descrive la progettazione, gli obiettivi e la metodologia della sperimentazione, cura 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 in base alla legge (centri di sperimentazione) e appositamente individuati dalle società committenti. Vengono raccolti, in conformità al protocollo e a più riprese nel corso dello studio, varie informazioni di carattere medico/clinico e i campioni biologici delle persone 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, nell'ambito della loro attività di monitoraggio, visitano i centri di sperimentazione e, se necessario, esaminano la documentazione medica originale degli individui partecipanti allo studio messa a loro disposizione dai medici (ad es. cartelle ospedaliere, registri clinici, note di laboratorio, referti ecc.).

Le informazioni medico/cliniche raccolte da medici sperimentatori presso ciascun centro vengono trasmesse al promotore 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 dal promotore, direttamente o tramite soggetti

esterni di cui si avvale, su un data-base 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 promotori che operano nell'ambito di gruppi multinazionali, il destinatario dei dati medico/clinici raccolti dai medici sperimentatori è solitamente la società capogruppo che può avere sede al di fuori del territorio nazionale. Inoltre, i promotori 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 che possono accedervi o averne la disponibilità e che possono essere situati anche in Paesi terzi che non offrono un livello di protezione adeguato dei dati personali (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 e, in alcuni casi, alla vita sessuale, delle persone coinvolte in 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.

Al fine di individuare tali cautele, l'Autorità ha svolto preliminarmente alcuni accertamenti ispettivi presso talune società farmaceutiche; ha indetto una specifica consultazione pubblica su un documento articolato indicante le misure e gli accorgimenti ritenuti allo stato idonei per il trattamento dei dati nell'ambito delle sperimentazioni cliniche di medicinali; ha, infine, effet-

tuato diversi altri approfondimenti, anche di carattere tecnico, con i principali organismi interessati alla consultazione, volti a verificare i profili critici evidenziati nelle osservazioni pervenute all'Autorità.

Le cautele ipotizzate in sede di consultazione pubblica hanno trovato conforto all'esito della stessa e degli specifici approfondimenti tecnici svolti successivamente.

Tutte le riflessioni e i commenti pervenuti sono stati comunque oggetto di specifica analisi e considerazione nell'elaborazione delle presenti "Linee-guida" che recano alcune circoscritte modifiche rispetto al precedente documento, giustificate dall'idoneità delle osservazioni formulate.

Le presenti "Linee-guida" sono pertanto rivolte a individuare gli accorgimenti e le misure necessari e opportuni riguardo al trattamento dei dati personali dei partecipanti a sperimentazioni cliniche da parte dei promotori degli studi. Gli accorgimenti e le misure indicati vanno, altresì, prese in considerazione da tutti gli altri titolari di trattamenti di dati personali effettuati a fini di sperimentazione clinica, quali promotori diversi dalle società farmaceutiche, organizzazioni di ricerca a contratto e centri di sperimentazione.

Prima di indicare quali cautele risultano idonee a seguito del complesso procedimento curato dal Garante, sono necessarie alcune premesse sulla natura dei dati trattati, sul ruolo dei promotori e degli altri soggetti coinvolti nelle sperimentazioni cliniche di medicinali rispetto al trattamento dei medesimi dati, nonché sul quadro normativo di base al quale occorre fare riferimento per un trattamento lecito e corretto dei dati.

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'ordinamento italiano, v. d.lg. 6 novembre 2007, n. 200; d.lg. 24 giugno 2003, n. 211; d.m. 15 luglio 1997 e, da ultimo, d.m. 21 dicembre 2007) 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 gli individui inclusi nella sperimentazione 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, inoltre, a notificare al promotore le reazioni e gli eventi avversi (Ae e Adr), correlabili alla somministrazione del medicinale in sperimentazione o comunque al suo svolgimento, insieme a 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 delle persone coinvolte nello studio la medesima normativa prevede che il centro partecipante alla sperimentazione debba assegnare un codice di identificazione a ciascun interessato, al momento del suo coinvolgimento, 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, 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 punti 1.21 e 1.23, all. 1/2 punto 2.11, 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

I promotori hanno sviluppato in genere specifiche procedure interne per consentire ai medici sperimentatori di codificare i dati medico/clinici delle persone coinvolte nello studio: solitamente, si utilizzano codici numerici che consentono di identificare univocamente i singoli interessati all'interno dello stesso studio, senza utilizzare il nominativo, l'indirizzo o numeri di identificazione personale.

Tuttavia, alcuni promotori stabiliscono nel protocollo dello studio che i medici sperimentatori debbano registrare sulle schede raccolta dati e sulle segnalazioni di reazioni e eventi avversi -da trasmettere ai primi- le iniziali del nome e cognome dei singoli individui partecipanti, oltre ai rispettivi codici identificativi. Inoltre, in base alle finalità della ricerca e alle caratteristiche dello studio, il protocollo può prevedere che i medici raccolgano informazioni ulteriori rispetto ai dati medico/clinici riferiti agli interessati, quali dati di carattere demografico (data di nascita e/o età, sesso, origine etnica, peso e statura) o relativi alla storia medica dei soggetti, agli stili di vita o alla vita sessuale. Queste informazioni, riportate sui documenti essenziali alla conduzione dello studio, sono conservate dai centri partecipanti e dal promotore per un periodo di tempo che, a seconda della disciplina applicabile, può essere collegato all'intera durata dell'autorizzazione all'impiego del medicinale nei diversi Paesi.

Sebbene sia previsto che soltanto ciascun centro abbia la disponibilità della lista che consente di associare il nominativo della persona al relativo codice identificativo e che il promotore non debba venire a conoscenza della sua identità, quest'ultimo, tramite propri collaboratori addetti al monitoraggio, nell'ambito delle visite effettuate presso il centro di sperimentazione volte a controllare che lo studio è effettuato in osservanza del protocollo, ha tuttavia accesso sotto il controllo dei medici alla documentazione sanitaria originale delle persone coinvolte nello studio (per verificare l'accuratezza e la completezza dei dati), nonché alla lista contenente i dati nominativi degli interessati (per controllare le procedure riguardanti l'acquisizione del consenso informato).

Va, inoltre, rilevato che tra le informazioni raccolte nel corso degli studi in esame compaiono, in genere, uno o più elementi specifici caratteristici dell'identità delle persone coinvolte (ivi compresa la statura o particolari patologie). Come confermato dalle indicazioni formulate dal Gruppo dei garanti europei nel Parere n. 4/2007 (Wp 136) sulla definizione di dato personale,

la combinazione di tali elementi è suscettibile di consentire il riconoscimento dell'interessato (ad esempio, mediante combinazione delle iniziali del nome e del cognome della persona 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 codifica previste dai promotori rappresentano una specifica cautela adottata in applicazione delle disposizioni normative vigenti a tutela della riservatezza degli individui partecipanti a uno studio clinico 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. 2/2008 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. 1529389). Le predette modalità di utilizzo del codice identificativo mirano, del resto, a consentire, in base alla specifica disciplina applicabile, l'identificazione della singola persona 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 controllare, per conto del promotore, l'accuratezza e la completezza delle informazioni raccolte verificandone la corrispondenza con quelle contenute nella documentazione medica originale degli individui partecipanti; o, ancora, per consentire al promotore di utilizzare le informazioni raccolte per difendere i propri diritti nell'ambito di eventuali azioni legali. Analogamente, ai fini delle valutazioni da operare 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 a utilizzare per mantenere riservata l'identità delle persone che si sottopongono alla sperimentazione (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 com-

portano, quindi, la possibilità di identificare gli interessati, sia pure indirettamente, mediante il riferimento ad altre informazioni detenute dal promotore medesimo 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 promotore, 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 idonei a rivelare lo stato salute e, in qualche caso, la vita sessuale del singolo interessato (artt. 2, al. 1, lett. a) e 8 direttiva 95/46/Ce; art. 4, comma 1, lett. b) e d), del Codice). La loro acquisizione da parte del promotore 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 sensibili (art. 26), nonché le ulteriori cautele poste a tutela dei diritti e della riservatezza degli interessati dall'autorizzazione del Garante n. 2/2008 al trattamento dei dati sulla salute e sulla vita sessuale (Provv. 19 giugno 2008, n. 33, doc. web n. 1529389) e, ove applicabile, dall'autorizzazione del Garante al trattamento dei dati genetici (Provv. 22 febbraio 2007, doc. web n. 1389918).

4. NOTIFICAZIONE

Alcuni trattamenti effettuati nell'ambito delle sperimentazioni cliniche di medicinali sono soggetti all'obbligo di notificazione al Garante. Si tratta, in particolare, dei trattamenti di dati che ricadono nelle ipotesi considerate dall'art. 37, comma 1, del Codice, vale a dire quelli relativi a dati genetici, oppure effettuati a fini di indagine epidemiologica (art. 37, comma 1, lett. a) e b)). Il Garante ha sottratto dall'obbligo di notificazione alcuni tra i trattamenti che rientrano in tali ipotesi, individuando i presupposti in base ai quali non devono essere notificati i trattamenti riguardanti dati genetici o finalizzati a indagini epidemiologiche effettuati da esercenti le professioni sanitarie anche in forma associata (Provv. 31 marzo 2004, doc. web n. 852561). A proposito di tali categorie di trattamenti, va nuovamente rilevato che l'esonero disposto da questa Autorità opera soltanto nei riguardi di quelli eventualmente effettuati da medici sperimentatori per attività di cura della salute associate alle sperimentazioni cliniche, sempre che si tratti di trat-

tamenti non sistematici e non organizzati in banche dati accessibili a terzi per via telematica. Si pensi, ad esempio, al caso del medico che, nell'ambito delle visite o degli accertamenti diagnostici previsti in uno studio clinico, venga a conoscenza e tratti saltuariamente, senza trasmetterle al committente dello studio, informazioni di tipo genetico riguardanti le malattie ereditarie dei pazienti coinvolti, a fini di cura della salute o di tutela dell'incolumità fisica degli interessati (cfr. Nota 26 aprile 2004, doc. web n. 996680).

5. TITOLARITÀ DEI TRATTAMENTI FINALIZZATI ALLA SPERIMENTAZIONE

Risulta essenziale verificare quale rapporto intercorre tra i promotori di 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 quanto 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 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 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 le persone partecipanti 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.

Il promotore non effettua, quindi, alcuna attività di raccolta diretta dei dati, né può interloquire con gli individui inclusi nella sperimentazione; compiti, questi, spettanti ai medici sperimentatori. Tuttavia, il promotore 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 docu-

mentazione medica originale e nella lista di identificazione delle persone coinvolte nello studio; 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 delle persone partecipanti 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 di collaboratori che ritiene idonei ed è responsabile del loro operato; fornisce l'informativa alle persone coinvolte nello studio e acquisisce il loro consenso anche per ciò che attiene al trattamento dei dati che le riguardano; permette che i collaboratori del promotore accedano alla documentazione medica originale dei soggetti coinvolti 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 i promotori hanno in genere responsabilità distinte nell'ambito degli studi clinici e si configurano, quindi, quali autonomi titolari o, a seconda dei casi, contitolari del trattamento (art. 28 del Codice). Per poter effettuare lecitamente il trattamento dei dati relativi alle sperimentazioni, tali soggetti sono pertanto tenuti 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 notificazione all'Autorità, alla designazione degli incaricati e di eventuali responsabili, nonché alla custodia e sicurezza delle medesime informazioni (artt. 11, 29, 30, 31-35, 37 e 38 del Codice; v. anche autorizzazione n. 2/2008 cit., specie punto 1.2). La trasmissione dei dati dello studio da parte dei centri di sperimentazione ai promotori configura 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).

6. 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.) per demandare loro 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 individui 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.

In tutte queste ipotesi è necessario che il promotore definisca chiaramente, nei contratti di affidamento o in altri atti idonei, il ruolo svolto nel trattamento dei dati personali da eventuali collaboratori esterni ai quali demanda attività o parti di attività inerenti agli studi clinici (artt. 28, 29 e 30 del Codice).

Nell'ambito delle sperimentazioni questi soggetti eseguono generalmente attività per conto e, in alcuni casi, in nome del promotore, nel rispetto delle modalità 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 collaborazione, consegnano di regola al promotore tutte le informazioni e la documentazione che ne è conseguita.

Con specifico riferimento alle attività di monitoraggio, i promotori 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 tenuti a osservare le procedure del promotore e le sue specifiche istruzioni; sono inoltre soggetti al controllo del promotore medesimo 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 i promotori, da un lato e, dall'altro, i soggetti esterni ai quali vengono affidate alcune, o tutte le mansioni riguardanti gli studi clinici (ivi compresi gli addetti al monitoraggio) vanno 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 soggetti che, in quanto collaboratori dei promotori, accedono ai dati personali delle persone incluse nello studio per le finalità della sperimentazione devono essere inoltre menzionati, anche per categorie, nell'informativa da fornire agli interessati; qualora vengano designati più responsabili, occorre indicare anche gli estremi identificativi di almeno uno di essi, nonché le modalità per reperire, anche on-line, il loro elenco aggiornato (art. 13 del Codice).

Diversamente, qualora i promotori ritengano, in base alla legge, di non poter designare i soggetti esterni di cui si avvalgono quali "incaricati" o "responsabili", in quanto i ruoli svolti da questi non possono essere ricondotti alle predette figure previste dal Codice, il flusso delle informazioni riferite agli individui partecipanti di cui siano eventualmente destinatari tali collaboratori costituirebbe una comunicazione di dati personali che potrebbe essere effettuata lecitamente in presenza del consenso specifico e informato degli interessati o di altro presupposto equipollente (artt. 11, comma 1, lett. a), 13, 23 e 26 del Codice).

Analoghe cautele devono essere adottate dai centri di sperimentazione nel caso in cui essi deman-

dino attività o parti di attività inerenti agli studi clinici a soggetti esterni quali, ad esempio, laboratori di analisi (artt. 13, 29 e 30 del Codice, autorizzazione del Garante al trattamento dei dati genetici del 22 febbraio 2007, doc. web n. 1389918, in particolare punti 4.3, 8 e 9).

I promotori devono prestare, comunque, particolare attenzione nella scelta dei soggetti, responsabili e incaricati, ai quali affidare, ai sensi degli artt. 29 e 30 del Codice, alcune o tutte le mansioni inerenti alle sperimentazioni di farmaci, specie con riferimento al monitoraggio dello studio, assicurandosi che essi possiedano requisiti di esperienza, capacità e affidabilità tali da fornire idonee garanzie del pieno rispetto delle istruzioni da impartire e delle regole di riservatezza e confidenzialità previste dalla disciplina in materia di protezione di dati personali e dalle disposizioni di settore. Gli addetti al monitoraggio devono essere sottoposti a regole di condotta analoghe al segreto professionale. Il loro processo di designazione deve 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; artt. 11, 29, 30, 31 e ss. d.lg. n. 196/2003) e le specifiche precauzioni da utilizzare per tutelare l'identità degli interessati anche nei riguardi dello stesso promotore (d.m. 15 luglio 1997, all. 1/1A punto 1.21 e all. 1/2, punto 2.11).

7. INFORMATIVA AI PAZIENTI

I promotori, di regola, individuano le informazioni da comunicare alle persone coinvolte nello studio e la procedura da seguire per raccogliere il loro consenso 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 alle informazioni riconducibili agli individui inclusi nella sperimentazione, alcuni promotori invitano i centri a informare i pazienti interessati che i dati che li riguardano saranno trasmessi dal medico dello studio a chi lo ha commissionato esclusivamente in forma anonima. Questa indicazione, oltre a essere erronea, non consente alle persone interessate di comprendere quali siano

i ruoli effettivamente svolti dal promotore e dagli altri soggetti, della cui collaborazione questo eventualmente si avvalga, riguardo al trattamento dei dati.

Così formulata, l'informativa agli individui partecipanti in sperimentazioni cliniche è, quindi, inidonea ai sensi del Codice (art. 13); non permette altresì agli interessati di esprimere una volontà consapevole riguardo al fatto che i trattamenti effettuati presso il promotore o i soggetti che con esso eventualmente collaborano (anche al di fuori del territorio nazionale) concernono informazioni che, seppure codificate, come sopra evidenziato, sono riconducibili ai medesimi interessati.

L'informativa da fornire agli interessati tramite i centri di sperimentazione deve invece comprendere, anche con formule sintetiche, ma pur sempre agevolmente comprensibili, 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).

Al fine di agevolare l'individuazione degli elementi essenziali da precisare nell'informativa, il Garante individua nel prospetto allegato (all. n. 1) un modello di riferimento che potrà essere utilizzato facoltativamente dai promotori per adempiere, tramite i centri di sperimentazione, all'obbligo dell'informativa, in armonia con i princìpi di semplificazione, armonizzazione ed efficacia previsti dal Codice nel quadro di un elevato livello di tutela dei diritti degli interessati (art. 2 del Codice). Nelle ipotesi in cui lo studio preveda il trattamento di informazioni genetiche (ad esempio, nelle indagini farmacogenetiche o farmacogenomiche) tali elementi devono essere integrati da indicazioni chiare in ordine a profili specifici dell'utilizzo di dati genetici e di campioni biologici individuati nella citata autorizzazione del Garante (punto 5 aut. 22 febbraio 2007, doc. web n. 1389918; cfr. anche d.m. 21 dicembre 2007, appendice 14).

Inoltre, deve essere cura dei centri di sperimentazione garantire che il personale coinvolto nelle sperimentazioni cliniche e, in particolare, nei colloqui preliminari volti all'acquisizione del consenso informato, sia formato adeguatamente anche sugli aspetti rilevanti della disciplina sulla protezione dei dati personali, in modo da essere in grado di spiegare accuratamente e con completezza agli interessati gli elementi essenziali riguardanti il trattamento dei dati. I promotori, nell'individuare i centri presso i quali condurre sperimentazioni cliniche, devono verificare l'adeguatezza del personale del centro a gestire tale procedura predisponendo, ove necessario, appositi interventi formativi. Il profilo della formazione andrebbe considerato anche dai comitati etici nelle valutazioni relative all'idoneità del medico sperimentatore e dei suoi collaboratori.

8. CONSENSO AL TRATTAMENTO DEI DATI

Anche il modello che i centri di sperimentazione devono sottoporre agli interessati per acquisire le dichiarazioni di consenso al trattamento dei dati che li riguardano viene di regola predisposto dai promotori 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 delle persone che si sottopongono alla sperimentazione da parte del personale del promotore 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 esso nell'ambito della sperimentazione.

Il promotore e i suoi eventuali collaboratori non possono utilizzare lecitamente i dati personali degli individui partecipanti allo studio clinico 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). Per facilitare anche tale adempimento da parte dei promotori, in armonia con i citati princìpi di semplificazione, armonizzazione ed efficacia, è individuata nell'allegato n. 1 anche una formula di riferimento

per l'acquisizione del consenso, da sottoporre agli interessati, unitamente al modello d'informativa, tramite i centri di sperimentazione.

Particolare attenzione deve essere prestata anche alle modalità con cui il consenso degli interessati viene acquisto, specie quando si tratta di persone che, per il loro particolare stato di vulnerabilità, sono suscettibili di essere sottoposti a forme di coercizione o influenza tali da ostacolare la libera espressione del loro consenso. Si pensi a pazienti affetti da malattie incurabili o in situazioni di emergenza, a persone indigenti o ospitate nelle case di riposo o, ancora, ad appartenenti a gruppi "strutturati gerarchicamente", come gli studenti di medicina, il personale subordinato di un ospedale o di un laboratorio, i dipendenti di una società farmaceutica, ecc. In tali casi, oltre ad adottare le specifiche cautele richieste dalla normativa di settore (d.m. 15 luglio 1997, all. 1/1B punto 1.61 e all. 1/4B punto 4.8), è opportuno utilizzare procedure per acquisire il consenso informato degli interessati che non si limitino ad approcci meramente formali e individualizzati con i singoli individui, organizzando, ad esempio, momenti di confronto con la generalità o con gruppi di partecipanti, o coinvolgendo le associazioni, anche locali, di pazienti interessati.

9. ESERCIZIO DEI DIRITTI DI CUI ALL'ART. 7 DEL CODICE

Le persone partecipanti a sperimentazioni cliniche di medicinali possono esercitare in ogni momento i diritti di cui all'art. 7 del Codice, tra i quali quello di accedere ai dati che li riguardano e di ottenerne la comunicazione in forma intelligibile, ovvero l'integrazione, l'aggiornamento o la rettifica, rivolgendosi direttamente al centro di sperimentazione o, per il tramite del medico sperimentatore (che è a conoscenza della loro identità e, mediante l'accesso alla lista di identificazione, può individuare il codice identificativo di ciascun interessato), al promotore.

Quest'ultimo, come pure il centro di sperimentazione, anche per il tramite dei rispettivi responsabili, eventualmente designati, qualora siano destinatari di simili istanze (per la presentazione delle quali non sono, peraltro, richieste particolari formalità) devono fornire senza ritardo all'interessato un riscontro compiuto e analitico (artt. 7, 8, 9, 10 e 146 del Codice). In particolare, va fornito riscontro alle richieste di accesso ai dati personali estrapolando dagli archivi le informazioni detenute e comunicandole all'interessato con modalità tali da renderne agevole la comprensione, nonché, se richiesto, trasponendole su supporto cartaceo o informatico, non potendo opporre rifiuto

se non nei casi espressamente previsti dal Codice (art. 8). In tema di ricerche in ambito medico, biomedico ed epidemiologico il principio alla base della disciplina in materia è che il riscontro a istanze di integrazione, aggiornamento e rettificazione dei dati può essere fornito annotando le modifiche richieste dall'interessato senza modificare questi ultimi, quando il risultato di tali operazioni non produce effetti significativi sul risultato della ricerca (art. 110, comma 2, del Codice; art. 16, comma 2, codice di deontologia e di buona condotta per i trattamenti di dati personali per scopi statistici e scientifici, allegato A.4. al Codice, doc. web n. 1038384)).

Dal momento che la partecipazione allo studio clinico è su base volontaria, gli interessati possono interrompere in ogni momento e senza fornire alcuna giustificazione la loro partecipazione allo studio (art. 3, comma 1, lett. b) e c) d.lg. n. 211/2003; d.m. 15 luglio 1997, all. 1/1B punto 1.28 e all. 1/4B punto 4.8; d.m. 21 dicembre 2007, all. 1 punto 6.1.2.5; art. 7, comma 4, lett. a), del Codice). In questo caso, non è più possibile raccogliere ulteriori dati che riguardano gli interessati e i campioni biologici eventualmente prelevati e conservati in una forma che consente di identificarli vanno distrutti (punto 6, aut. al trattamento dei dati genetici del 22 febbraio 2007, doc. web n. 1389918; v. anche d.m. 21 dicembre 2007, all. 2 punto 6.1.2.5). Resta impregiudicata la possibilità di utilizzare i dati eventualmente già raccolti per determinare, senza alterarli, i risultati della ricerca (v. al riguardo, par. 3.3 Raccomandazione del Consiglio d'Europa R(83)10 del 23 settembre del 1983 relativa alla protezione dei dati a carattere personale utilizzati a fini di ricerca scientifica e di statistiche; par. 6.1 Raccomandazione del Consiglio d'Europa (97)18 del 30 settembre 1997 relativa alla protezione dei dati personali raccolti e trattati per scopi statistici).

10. TRASFERIMENTO DI DATI ALL'ESTERO

Nelle sperimentazioni cliniche dei medicinali accade, frequentemente, che le informazioni e i campioni biologici degli individui partecipanti, 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 promotori 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 alle singole persone coinvolte nello studio, 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 Provv. del Garante 10 aprile 2002 n. 3, 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 Provv. del Garante del 10 ottobre 2001, doc. web n. 42156; decisione del 27 dicembre 2004, n. 2004/915/Ce e Provv. del Garante del 9 giugno 2005, doc. web n. 1151949). Ai fini dell'utilizzazione delle citate clausole è 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 risultare effettivamente "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'idonea 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 Provv. del Garante del 10 ottobre 2001, doc. web n. 30939).

11. PERIODO DI CONSERVAZIONE E TRATTAMENTO DI DATI PER ULTERIORI FINI DI RICERCA

I dati e i campioni biologici delle persone che si sottopongono alle sperimentazioni devono essere conservati per un arco di tempo non superiore a quello necessario per conseguire le fina-

lità per le quali sono stati raccolti e trattati (art. 11, comma 1, lett. e) del Codice, aut. cit. 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 individui) debbano essere conservati presso il promotore 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 il promotore medesimo 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).

In termini generali, in applicazione della disposizione del Codice sopra richiamata sulla durata di conservazione, i dati devono essere conservati presso i soggetti esterni che eventualmente collaborano con il promotore per la gestione e l'analisi statistica, per il solo periodo di tempo non superiore a quello necessario per definire il rapporto finale della sperimentazione o pubblicare i risultati dello studio.

La possibilità di fissare un periodo di tempo più lungo rispetto a quello previsto dalla normativa applicabile per la conservazione dei medesimi dati presso il promotore e i centri partecipanti può, invece, essere valutata anche alla luce della durata dell'autorizzazione d'immissione in commercio del medicinale in sperimentazione o di eventuali ulteriori esigenze di analisi dei dati, connesse ad esempio, a nuove domande d'immissione in commercio o di estensione dell'autorizzazione, ovvero al manifestarsi di evidenze significative per la sicurezza dei pazienti.

I promotori di uno studio clinico possono utilizzare lecitamente in future attività di studio e di ricerca i dati e i campioni biologici riconducibili a ciascuna delle persone coinvolte, anche avvalendosi dei soggetti esterni che hanno collaborato con essi per l'esecuzione della sperimentazione, a condizione che gli interessati ne siano stati previamente e adeguatamente informati e abbiano manifestato per iscritto un consenso specifico e distinto rispetto a quello manifestato per lo studio principale (artt. 11, comma 1, lett. e), 13, 23, 26 e 99 del Codice; aut. del 22 febbraio 2007, doc. web n. 1389918).

12. CUSTODIA E SICUREZZA DEI DATI

A seguito degli approfondimenti, anche tecnici, svolti nell'ambito degli accertamenti ispettivi effettuati presso alcuni promotori e altri soggetti coinvolti nelle sperimentazioni, nonché di quelli effettuati, nell'ambito della consultazione pubblica, con i principali organismi interessati, 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 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 delle persone coinvolte nello studio presso i centri di sperimentazione, al loro trasferimento in via telematica verso un unico database presso il promotore o gli altri soggetti che svolgono, per conto di quest'ultimo, la validazione e l'elaborazione statistica dei dati, nonché alla gestione della medesima banca dati.

In relazione a tali operazioni di trattamento, i promotori di sperimentazioni cliniche di medicinali, le organizzazioni di ricerca a contratto e i centri di sperimentazione, ciascuno per la parte di propria competenza in relazione al ruolo ricoperto nel trattamento dei dati e alle conseguenti responsabilità ai fini dell'adozione delle misure di sicurezza, devono adottare:

a. laddove siano utilizzati sistemi di memorizzazione o archiviazione dei dati, idonei accorgimenti per garantire la protezione dei dati registrati dai rischi di accesso abusivo, furto o smarrimento parziali o integrali dei supporti di memorizzazione o dei sistemi di elaborazione portatili o fissi (ad esempio, attraverso l'applicazione parziale o integrale di tecnologie crittografiche a file system o database, oppure tramite l'adozione di altre misure informatiche di protezione che rendano inintelligibili i dati ai soggetti non legittimati);

b. 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 il promotore o gli altri soggetti che effettuano la successiva validazione ed elaborazione statistica dei dati;

c. con specifico riferimento al menzionato database:

- idonei sistemi di autenticazione e di autorizzazione per gli incaricati in funzione dei ruoli e delle esigenze di accesso e trattamento;
- procedure per la verifica periodica della 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, in relazione alle sperimentazioni cliniche multinazionali, di promuovere a livello comunitario e internazionale standard di sicurezza per i trattamenti di dati personali che prevedano un livello di protezione ancora più elevato in un quadro di armonizzazione delle misure e degli accorgimenti da adottare in tali ambiti per la custodia e la sicurezza dei dati.

13. ALTRE TIPOLOGIE DI STUDI CLINICI

Le indicazioni fornite nelle presenti "Linee-guida" a garanzia dei soggetti interessati possono, in linea generale, essere prese in considerazione come quadro unitario di riferimento per un uso lecito e corretto dei dati personali anche nell'ambito di altre tipologie di sperimentazioni cliniche, vale a dire quelle riguardanti i dispositivi medici (art. 7 d.lg 14 dicembre 1992, n. 507; art. 14 d.lg 24 febbraio 1997, n. 46; d.m. 2 agosto 2005) e quelle non promosse da società farmaceutiche o da altre strutture private per lo sviluppo industriale di un farmaco (cd. sperimentazioni "non aventi fini di lucro", cfr. art. 1 d.lg. n. 200/2007 e d.m. 17 dicembre 2004). In queste ipotesi, occorre verificare, innanzitutto, il ruolo dei soggetti coinvolti nello studio rispetto al trattamento dei dati (promotore, centro di sperimentazione, centro coordinatore, organizzazione di ricerca a contratto, laboratorio di analisi, ecc.) in modo da poter individuare il soggetto o i soggetti, titolari del trattamento, tenuti agli adempimenti previsti dal Codice in materia di notificazione, designazione di incaricati e di eventuali responsabili, consenso informato al trattamento dei dati, predisposizione di adeguate misure per la custodia e sicurezza dei dati, esercizio dei diritti di accesso e degli altri diritti riguardanti i dati personali. Occorre, inoltre, accertare, in base alle previsioni dello studio, eventuali flussi di dati, anche attraverso la loro messa a disposizione o consultazione (ad esempio, a fini di monitoraggio), verso soggetti esterni situati anche al di fuori dell'Unione europea, in modo da verificare la necessità di acquisire il

consenso specifico e informato degli interessati e/o di adottare garanzie equipollenti e adeguate (artt. 11, comma 1, lett. a), 13, 23, 26, 43 e 44 del Codice).

Vanno poi formulate in questa sede alcune precisazioni con riferimento ad altri studi, nei quali i medicinali sono prescritti e somministrati ai soggetti che accettano di parteciparvi secondo la normale pratica clinica (sperimentazioni "non interventistiche", v. art. 1 d.lg. n. 200/2007). Questi studi, cd. "osservazionali", qualora non siano strettamente associati ad attività di tutela della salute svolte da medici o organismi sanitari, ovvero -a differenza delle sperimentazioni cliniche sui medicinali- non possano ritenersi comparabili a tali attività in termini di ricaduta personalizzata sull'interessato, rientrano nell'ambito di applicazione delle previsioni del codice di deontologia e di buona condotta per i trattamenti di dati personali per scopi statistici e scientifici (Allegato A.4. al Codice, doc. web n. 1038384) la cui osservanza, oltre a rappresentare un obbligo deontologico, costituisce condizione essenziale per la liceità e la correttezza del trattamento medesimo (art. 12, comma 3, del Codice). Anche nell'ambito di questi studi, il trattamento di informazioni medico/cliniche può essere effettuato, in linea generale, per gli scopi della ricerca con riferimento ai soli dati personali degli individui che vi acconsentono specificatamente dopo aver ricevuto un'idonea informativa sul trattamento dei dati (artt. 106, 107 e 110 del Codice; punto 1.2, lett. a) aut. n. 2/2008 cit.). Ciò, indipendentemente dal fatto che lo studio preveda di raccogliere queste informazioni direttamente presso gli interessati o presso terzi. In presenza di particolari e comprovate circostanze (di carattere etico, metodologico o di impossibilità organizzativa), dalle quali derivi l'impossibilità di informare gli interessati, il trattamento può essere effettuato, anche in assenza del loro consenso, a condizione che il programma di ricerca sia stato oggetto di motivato parere favorevole del competente comitato etico e venga ottenuta l'autorizzazione del Garante, che può essere rilasciata anche con provvedimenti di carattere generale, relativi a determinate categorie di titolari o di trattamenti (artt. 110 ult. parte e 40 del Codice). Si pensi, ad esempio, ad alcuni studi di tipo retrospettivo in cui il tempo trascorso dal momento in cui i dati da analizzare sono stati raccolti, l'entità del campione da selezionare e le caratteristiche sulla base delle quali viene effettuato il campionamento (ad esempio, un gruppo di persone affette da patologie ad alta incidenza di mortalità) possono rendere ragionevolmente impossibile raggiungere gli interessati e fornire loro un'adeguata informativa.

Il Garante si riserva di adottare provvedimenti più specifici di prescrizione e di divieto che potranno derivare dalle verifiche di eventuali violazioni riguardanti singoli soggetti promotori, nonché di apportare alle presenti "Linee-guida" eventuali integrazioni riguardanti le concrete modalità di trattamento dei dati, anche alla luce dell'esperienza maturata nell'applicazione delle stesse e delle nuove tecnologie eventualmente intervenute.

ALLEGATO N. 1. INFORMATIVA E MANIFESTAZIONE DEL CONSENSO AL TRATTAMENTO DEI DATI PERSONALI (1)

Titolari del trattamento e relative finalità

Il Centro di sperimentazione (indicare il nome del centro) e l'Azienda farmaceutica (indicare il nome del promotore), che ha commissionato lo studio che Le è stato descritto, ciascuno per gli ambiti di propria competenza e in accordo alle responsabilità previste dalle norme della buona pratica clinica (d.l. 211/2003), tratteranno i Suoi dati personali, in particolare quelli sulla salute e, soltanto nella misura in cui sono indispensabili in relazione all'obiettivo dello studio, altri dati relativi alla Sua origine, ai Suoi stili di vita e alla Sua vita sessuale (ecc.) (variabili da specificare a seconda delle caratteristiche dello studio), esclusivamente in funzione della realizzazione dello studio e a fini di farmacovigilanza.

A tal fine i dati indicati saranno raccolti dal Centro di sperimentazione e trasmessi all'Azienda farmaceutica e alle persone o società esterne che agiscono per loro conto, tra le quali ... (inserire gli estremi identificativi di almeno uno dei terzi cui i dati saranno trasmessi) anche in Paesi non appartenenti all'Unione europea che non garantiscono un adeguato livello di protezione dei dati personali (da inserire nel caso si preveda di trasferire i dati al di fuori dell'Ue specificando gli estremi identificativi dei destinatari). (2)

(1) Da sottoporre agli interessati unitamente al modulo di consenso informato che descrive le caratteristiche scientifiche dello studio, anche mediante integrazione dello stesso

(2) Quando non è possibile conoscere al momento della redazione dell'informativa l'elenco completo dei soggetti terzi a cui i dati saranno trasmessi anche in paesi extra-UE occorre specificare come e quando l'elenco completo verrà reso disponibile

Il trattamento dei dati personali relativi a ... (variabili da specificare a seconda delle caratteristiche dello studio) è indispensabile allo svolgimento dello studio: il rifiuto di conferirli non Le consentirà di parteciparvi (Indicare inoltre gli eventuali dati che possono invece essere forniti facoltativamente).

Natura dei dati

Il medico che La seguirà nello studio La identificherà con un codice: i dati che La riguardano raccolti nel corso dello studio, ad eccezione del Suo nominativo, saranno trasmessi all'Azienda farmaceutica, registrati, elaborati e conservati unitamente a tale codice, alla Sua data di nascita, al sesso, al Suo peso e alla Sua statura (tutte le variabili di cui sopra da precisare secondo le specifiche dello studio). Soltanto il medico e i soggetti autorizzati potranno collegare questo codice al Suo nominativo.

Modalità del trattamento

I dati, trattati mediante strumenti anche elettronici, saranno diffusi solo in forma rigorosamente anonima, ad esempio attraverso pubblicazioni scientifiche, statistiche e convegni scientifici. La Sua partecipazione allo studio implica che, in conformità alla normativa sulle sperimentazioni cliniche dei medicinali, il personale dell'Azienda farmaceutica o delle società esterne che eseguono per conto della prima il monitoraggio e la verifica dello studio, il Comitato etico e le autorità sanitarie italiane e straniere potranno conoscere i dati che La riguardano, contenuti anche nella Sua documentazione clinica originale, con modalità tali da garantire la riservatezza della Sua identità.

Esercizio dei diritti

Potrà esercitare i diritti di cui all'art. 7 del Codice (es. accedere ai Suoi dati personali, integrarli, aggiornarli, rettificarli, opporsi al loro trattamento per motivi legittimi, ecc.) rivolgendosi direttamente al centro di sperimentazione (indicare il nome di una persona fisica o di un ufficio responsabile e un recapito) o, per il suo tramite, all'azienda farmaceutica.

Potrà interrompere in ogni momento e senza fornire alcuna giustificazione la Sua partecipazione allo studio: in tal caso, i campioni biologici a Lei correlati verranno distrutti. Non saranno inoltre raccolti ulteriori dati che La riguardano, ferma restando l'utilizzazione di quelli eventualmente già raccolti per determinare, senza alterarli, i risultati della ricerca.

Consenso

Sottoscrivendo tale modulo acconsento al trattamento dei miei dati personali e al loro trasferimento al di fuori dell'Unione europea (da inserire se effettuato specificando gli estremi identificativi dei destinatari) per gli scopi della ricerca nei limiti e con le modalità indicate nell'informativa fornitami con il presente documento.

Nome e Cognome dell'interessato (in stampatello): _____

Firma dell'interessato: _____

Data: _____

38. Linee-guida in tema di fascicolo sanitario elettronico e di *dossier* sanitario (*)

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. Daniele De Paoli, segretario generale reggente;

Considerato che l'Autorità ha svolto alcuni approfondimenti istruttori su numerose iniziative –diversamente denominate– promosse da organismi sanitari pubblici e privati inerenti ai trattamenti di dati personali effettuati attraverso il Fascicolo sanitario elettronico (Fse);

Rilevata l'esigenza di individuare misure e accorgimenti necessari e opportuni da porre a garanzia dei cittadini interessati, in relazione ai trattamenti di dati che li riguardano;

Visto il provvedimento adottato dall'Autorità il 22 gennaio 2009 recante Linee-guida in tema di Fascicolo sanitario elettronico che è stato sottoposto alla preliminare consultazione del gruppo di lavoro, costituito presso il Ministero del lavoro, della salute e delle politiche sociali, per l'istituzione di un sistema nazionale di Fascicolo sanitario elettronico;

Viste le osservazioni formulate su tale provvedimento dal suddetto tavolo di lavoro con nota del 18 febbraio 2009 (prot. 0000603-P-18);

Rilevata l'opportunità che la prescrizione di tali misure e accorgimenti, allo stato individuati dal Garante nell'unito documento, sia preceduta da una consultazione pubblica dei soggetti e delle categorie interessate, in particolare degli organismi e professionisti sanitari pubblici e privati, dei medici di medicina generale e dei pediatri di libera scelta, degli organismi rappresentativi di operatori sanitari e delle associazioni di pazienti interessati, anche al fine di acquisire eventuali riscontri e osservazioni;

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 reggente ai sensi dell'art. 15 del regolamento del Garante n. 1/2000;

(*) Deliberazione n. 8 del 5 marzo 2009, Gazzetta Ufficiale 26 marzo 2009, n. 71 [doc. *web* n. 1598313], in inglese [doc. *web* n. 1608673]

Relatore il dott. Giuseppe Chiaravalloti;

DELIBERA:

a) di adottare l'unito documento che forma parte integrante della presente deliberazione ("Linee-guida in tema di Fascicolo sanitario elettronico e di dossier sanitario");

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 organismi e professionisti sanitari pubblici e privati, dei medici di medicina generale e dei pediatri di libera scelta, di organismi rappresentativi di operatori sanitari e di associazioni di pazienti interessati.

Osservazioni e commenti potranno pervenire entro il 31 maggio 2009 all'indirizzo dell'Autorità di Piazza di Monte Citorio n. 121, 00186 Roma, ovvero all'indirizzo di posta elettronica:

fse@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, 5 marzo 2009

IL PRESIDENTE
Pizzetti

IL RELATORE
Chiaravalloti

IL SEGRETARIO GENERALE REGGENTE
De Paoli

Linee-guida in tema di fascicolo sanitario elettronico e di *dossier* sanitario

1. La sanità elettronica: profili generali

Nel quadro del processo di ammodernamento della sanità pubblica e privata sono in atto numerose iniziative volte a migliorare l'efficienza del servizio sanitario attraverso un ulteriore sviluppo delle reti e una più ampia gestione informatica e telematica di atti, documenti e procedure.

In tale contesto si collocano alcune iniziative volte ad archiviare, mediante nuove tecniche, la svariata documentazione di cui gli organismi sanitari si avvalgono a diverso titolo nei processi di cura dei pazienti come, ad esempio, le più recenti esperienze di informatizzazione della cartella clinica, documento sanitario che pure è regolato da specifiche disposizioni normative. Il trattamento dei dati utilizzati nell'ambito di tali iniziative è regolato già dal Codice sulla protezione dei dati personali (cfr., in particolare, artt. 75 e ss. e art. 20 del Codice).

Accanto a tali iniziative più generali emerge di recente un'attività più specifica che rientra anch'essa nel complesso delle azioni per modernizzare la realtà sanitaria, ma ha caratteristiche peculiari che ne rendono opportuna una considerazione in forma specifica.

La novità che si intende esaminare in questa sede in chiave autonoma riguarda la condivisione informatica, da parte di distinti organismi o professionisti, di dati e documenti sanitari che vengono formati, integrati e aggiornati nel tempo da più soggetti, al fine di documentare in modo unitario e in termini il più possibile completi un'intera gamma di diversi eventi sanitari riguardanti un medesimo individuo e, in prospettiva, l'intera sua storia clinica.

Questi dati e documenti possono presentare caratteristiche o sfumature diverse e sono da tempo oggetto di specifica attenzione nell'ambito della problematica del cosiddetto Fascicolo sanitario elettronico (di seguito Fse) e del cd. dossier sanitario (di seguito dossier). Nelle presenti Linee-guida per tali strumenti si ha riguardo all'insieme dei diversi eventi clinici occorsi ad un individuo, messo in condivisione logica dai professionisti o organismi sanitari che assistono l'interessato, al fine di offrirgli un migliore processo di cura.

La peculiarità della condivisione da parte di distinti soggetti delle delicate informazioni sanitarie che documentano un insieme di eventi di rilevanza medica occorsi a uno stesso individuo giustifica la formulazione di particolari considerazioni rispetto alla gestione cartacea di analoghi

documenti e alla più generale tematica dell'informatizzazione sanitaria.

Nelle more di un possibile intervento normativo che regoli alcuni aspetti di fondo, il Garante ritiene pertanto opportuno individuare un primo quadro di cautele, al fine di delineare per tempo specifiche garanzie e responsabilità, nonché alcuni diritti.

2. AMBITO DI APPLICAZIONE DELLE LINEE GUIDA

Il Fse e i dossier non risultano essere definiti a livello nazionale da norme di carattere primario o secondario. Ciò, comporta la necessità di utilizzare una definizione convenzionale del fenomeno che trae spunto anche da quanto emerso in sede europea nel Gruppo che riunisce le autorità garanti di protezione dei dati (cd. Gruppo Art. 29) (1).

Le considerazioni sviluppate nelle presenti linee guida sono applicabili al Fse e al dossier intesi, come detto, quali insieme di dati sanitari relativi di regola ad un medesimo soggetto e riportati in più documenti elettronici tra loro collegati, condivisibili da soggetti sanitari diversi, pubblici e privati.

Il Fse e il dossier contengono diverse informazioni inerenti allo stato di salute di un individuo relative ad eventi clinici presenti e trascorsi (es.: referti, documentazione relativa a ricoveri, accessi al pronto soccorso), volte a documentarne la storia clinica. I dati personali sono collegati tra loro con modalità informatiche di vario tipo che ne rendono, comunque, possibile un'agevole consultazione unitaria da parte dei diversi professionisti o organismi sanitari che prendono nel tempo in cura l'interessato.

Alla luce di quanto emerso a livello nazionale ed, in particolare, dalle osservazioni del gruppo di lavoro costituito presso il Ministero del lavoro, della salute e delle politiche sociali, per l'istituzione di un sistema nazionale di Fascicolo sanitario elettronico, nelle presenti Linee-guida il suddetto insieme di dati sanitari risulta diversamente denominato in funzione del suo ambito di operatività. In particolare, si parla di dossier sanitario qualora tale strumento sia costituito presso un organismo sanitario in qualità di unico titolare del trattamento (es., ospedale o clinica privata) al cui interno operino più professionisti. Si intende invece per Fse il fascicolo formato

(1) Documento di lavoro sul trattamento dei dati personali relativi alla salute contenuti nelle cartelle cliniche elettroniche (Cce) adottato il 15 febbraio 2007 consultabile sul sito: http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp131_it.pdf

con riferimento a dati sanitari originati da diversi titolari del trattamento operanti più frequentemente, ma non esclusivamente, in un medesimo ambito territoriale (es., azienda sanitaria, laboratorio clinico privato operanti nella medesima regione o area vasta). I dossier sanitari possono anche costituire, ad esempio, l'insieme di informazioni sanitarie detenute dai singoli titolari coinvolti in una iniziativa di Fse regionale.

Il Fse dovrebbe essere costituito preferendo di regola soluzioni che non prevedano una duplicazione in una nuova banca dati delle informazioni sanitarie formate dai professionisti o organismi sanitari che hanno preso in cura l'interessato.

In secondo luogo, provenendo i dati sanitari e i documenti riuniti nel Fse da più soggetti, dovrebbero essere adottate idonee cautele per ricostruire, anche in termini di responsabilità, chi ha raccolto e generato i dati e li ha resi disponibili nell'ambito del Fse.

Nel caso di Fse, venendo poi in considerazione documenti sanitari del tutto distinti tra loro, dovrebbe essere assicurato che ciascun soggetto che li ha prodotti autonomamente ne rimanga di regola l'unico titolare, anche se le informazioni sono -come detto- disponibili agli altri soggetti abilitati all'accesso (ad esempio -come spesso accade-, attraverso la condivisione, da parte di tutti i soggetti che prendono in cura l'interessato, dell'elenco degli eventi sanitari occorsi, elenco strutturato anche sotto forma di indici o di puntatori logici dei singoli episodi clinici).

In assenza di una previsione legislativa che preveda l'istituzione di tali strumenti per il perseguimento di finalità amministrative proprie delle regioni o di organi centrali dello Stato, le finalità che possono essere perseguite attraverso la costituzione del Fse o del dossier possono essere ricondotte esclusivamente a finalità di cura dell'interessato, ovvero ad assicurare un migliore processo di cura dello stesso attraverso la ricostruzione di un insieme -di regola su base logica- il più possibile completo della cronistoria degli eventi di rilievo clinico occorsi a un interessato relativi a distinti interventi medici.

A garanzia dell'interessato, le finalità perseguite dovrebbero essere ricondotte quindi solo alla prevenzione, diagnosi, cura e riabilitazione dell'interessato medesimo, con esclusione di ogni altra finalità (in particolare, per le attività di programmazione, gestione, controllo e valutazione dell'assistenza sanitaria, che possono essere, peraltro, espletate in vari casi anche senza la disponibilità di dati personali), ferme restando eventuali esigenze in ambito penale.

Qualora attraverso il Fse o il dossier si intendano perseguire anche talune finalità amministrative strettamente connesse all'erogazione della prestazione sanitaria richiesta dall'interessato (es. prenotazione e pagamento di una prestazione), tali strumenti dovrebbero essere strutturati in modo tale che i dati amministrativi siano separati dalle informazioni sanitarie (2), prevedendo profili diversi di abilitazione degli aventi accesso agli stessi in funzione della differente tipologia di operazioni ad essi consentite.

Eventuali, future utilizzazioni anche parziali del Fse o del dossier per ulteriori fini di ricerca scientifica, epidemiologica o statistica dovrebbero avvenire in conformità alla normativa di settore ed essere oggetto di preventiva e specifica attenzione, anche nei casi in cui -come accade per taluni progetti di Fse esaminati- la tenuta dell'elenco degli eventi sanitari riguardante un determinato interessato sia demandata a un'infrastruttura regionale.

3. DIRITTO ALLA COSTITUZIONE DI UN FASCICOLO SANITARIO ELETTRONICO O DI UN DOSSIER SANITARIO

In base alle disposizioni contenute nel Codice dell'amministrazione digitale, deve essere assicurata la disponibilità, la gestione, l'accesso, la trasmissione, la conservazione e la fruibilità dell'informazione in modalità digitale utilizzando le tecnologie dell'informazione e della comunicazione nel rispetto della disciplina rilevante in materia di trattamento dei dati personali e, in particolare, delle disposizioni del Codice dell'amministrazione digitale (d.lg. 7 marzo 2005, n. 82).

A ciò deve aggiungersi che allo stato delle notizie al momento acquisite dall'Autorità, non consta l'esistenza di una norma che obblighi gli organismi sanitari a costituire un Fse o un dossier, la cui introduzione deve ritenersi, pertanto, facoltativa.

Le finalità perseguite attraverso il Fse o il dossier, come sopra ricordato, sono generalmente riconducibili alla documentazione di una "memoria storica" degli eventi di rilievo sanitario relativi a un medesimo individuo consultabile dal medico curante.

Il trattamento dei dati personali effettuato mediante il Fse o il dossier, perseguendo le menzionate finalità di prevenzione, diagnosi, cura e riabilitazione, deve uniformarsi al principio di auto-

(2) Cfr. art. 22, comma 6, del Codice; regola 24 del Disciplinare tecnico in materia di misure minime di sicurezza di cui all'Allegato B. al Codice

determinazione (artt. 75 e ss. del Codice). All'interessato dovrebbe essere consentito di scegliere, in piena libertà, se far costituire o meno un Fse/dossier con le informazioni sanitarie che lo riguardano, garantendogli anche la possibilità che i dati sanitari restino disponibili solo al professionista o organismo sanitario che li ha redatti, senza la loro necessaria inclusione in tali strumenti.

Il diritto alla costituzione o meno del Fse/dossier si dovrebbe quindi tradurre nella garanzia di decidere liberamente, sulla base del consenso, se acconsentire o meno alla costituzione di un documento che, come si è detto, raccoglie un'ampia storia sanitaria.

Affinché tale scelta sia effettivamente libera, l'interessato che non desideri che sia costituito un Fse/dossier dovrebbe poter accedere comunque alle prestazioni del Servizio sanitario nazionale e non avere conseguenze negative sulla possibilità di usufruire di prestazioni mediche.

Il consenso, anche se manifestato unitamente a quello previsto per il trattamento dei dati a fini di cura (cfr. art. 81 del Codice), deve essere autonomo e specifico.

In ragione delle finalità perseguite attraverso il Fse/dossier, dovrebbe essere illustrata all'interessato l'utilità di costituire e disporre di un quadro il più possibile completo delle informazioni sanitarie che lo riguardano, in modo da poter offrire un migliore supporto all'organismo sanitario, al medico e all'interessato stesso. Una conoscenza approfondita dei dati clinici, relativi anche al passato, può infatti contribuire ad una più efficace ricognizione degli elementi utili alle valutazioni del caso.

Tuttavia, dovrebbero essere previsti momenti distinti in cui l'interessato possa esprimere la propria volontà, attraverso un consenso di carattere generale per la costituzione del Fse e di consensi specifici ai fini della sua consultazione o meno da parte dei singoli titolari del trattamento (es. medico di medicina generale, pediatra di libera scelta, farmacista, medico ospedaliero).

Ferma restando l'indubbia utilità di un Fse/dossier completo, dovrebbe essere garantita la possibilità di non far confluire in esso alcune informazioni sanitarie relative a singoli eventi clinici (ad es., con riferimento a una specifica visita specialistica o alla prescrizione di un farmaco). Ciò, analogamente a quanto avviene nel rapporto paziente-medico curante, nel quale il primo può addivenire a una determinazione consapevole di non informare il secondo di certi eventi.

L'"oscuramento" dell'evento clinico (revocabile nel tempo) dovrebbe peraltro avvenire con modalità tali da garantire che, almeno in prima battuta, tutti (o alcuni) soggetti abilitati all'accesso non possano venire automaticamente (anche temporaneamente) a conoscenza del fatto

che l'interessato ha effettuato tale scelta ("oscuramento dell'oscuramento").

In tale quadro, alcuni progetti di Fse esaminati garantiscono l'esercizio della "facoltà di oscuramento" mediante una "busta elettronica sigillata" non visibile, apribile di volta in volta solo con la collaborazione dell'interessato, ovvero utilizzando codici casuali relativi a singoli eventi che non consentono di collegare tra loro alcune informazioni contrassegnate.

Il titolare del trattamento che intenda istituire il Fse/dossier anche con informazioni sanitarie relative a eventi clinici precedenti alla sua costituzione (es. referti relativi a prestazioni mediche pregresse) dovrebbe essere autorizzato preventivamente dall'interessato, lasciando libero quest'ultimo di esercitare la facoltà di "oscuramento".

In caso di incapacità di agire deve essere acquisito il consenso di chi esercita la potestà. Raggiunta la maggiore età, deve essere acquisito nuovamente il consenso informato dell'interessato divenuto maggiorenne (artt. 13 e 82, comma 4, del Codice).

In caso di revoca (liberamente manifestabile) del consenso, il Fse/dossier non dovrebbe essere ulteriormente implementato. I documenti sanitari presenti dovrebbero restare disponibili per l'organismo che li ha redatti (es. informazioni relative a un ricovero utilizzabili dalla struttura di degenza) e per eventuali conservazioni per obbligo di legge, ma non dovrebbero essere più condivisi da parte degli altri organismi o professionisti che curino l'interessato (art. 22, comma 5, del Codice).

Il trattamento di dati genetici eventualmente effettuato in relazione al Fse/dossier deve avvenire nel rispetto dell'apposita autorizzazione generale al trattamento dei dati genetici rilasciata dal Garante.

4. I SOGGETTI CHE TRATTANO I DATI

Il trattamento di dati personali effettuato attraverso il Fse/dossier, perseguendo esclusivamente fini di prevenzione, diagnosi e cura dell'interessato, dovrebbe essere posto in essere esclusivamente da parte di soggetti operanti in ambito sanitario, con esclusione di periti, compagnie di assicurazione, datori di lavoro, associazioni o organizzazioni scientifiche, organismi amministrativi anche operanti in ambito sanitario, nonché del personale medico nell'esercizio di attività medico-legale (es. visite per l'accertamento dell'idoneità lavorativa o alla guida).

La titolarità del trattamento dei dati personali effettuato tramite il Fse/dossier dovrebbe essere di regola riconosciuta alla struttura o organismo sanitario inteso nel suo complesso e presso cui

sono state redatte le informazioni sanitarie (es. azienda sanitaria o ospedale) (art. 4, comma 1, lett. f) del Codice).

I titolari hanno la facoltà di designare gli eventuali soggetti responsabili del trattamento, mentre devono preporre in ogni caso le persone fisiche eventualmente incaricate, le quali possono venire lecitamente a conoscenza dei dati personali trattati attraverso tali strumenti attenendosi alle funzioni svolte e sulla base di idonee istruzioni scritte (artt. 4, comma 1, lett. g) e h), 29 e 30 del Codice).

Le persone fisiche legittimate a consultare il Fse/dossier dovrebbero essere adeguatamente edotte delle particolari modalità di creazione e utilizzazione di tali strumenti.

Nell'individuare gli incaricati il titolare o il responsabile dovrebbero indicare con chiarezza l'ambito delle operazioni consentite (operando, in particolare, le opportune distinzioni tra il personale con compiti amministrativi e quello con funzioni sanitarie), avendo cura di specificare se gli stessi abbiano solo la possibilità di consultare il Fascicolo/dossier o anche di integrarlo o modificarlo (cfr. punto 5 del presente provvedimento).

5. DATI CHE POSSONO ESSERE TRATTATI E ACCESSO AL FASCICOLO SANITARIO ELETTRONICO E AL DOSSIER SANITARIO

Il titolare deve valutare attentamente quali dati pertinenti, non eccedenti e indispensabili inserire nel Fse/dossier in relazione alle necessità di prevenzione, diagnosi, cura e riabilitazione (artt. 11, comma 1, lett. d) e 22, comma 5 del Codice).

Dovrebbero essere pertanto preferite soluzioni che consentano un'organizzazione modulare di tali strumenti in modo da limitare l'accesso dei diversi soggetti abilitati alle sole informazioni (e, quindi, al modulo di dati) indispensabili.

In alcuni progetti di Fse esaminati tale organizzazione modulare permette, ad esempio, di selezionare le informazioni sanitarie accessibili ai diversi titolari abilitati in funzione del loro settore di specializzazione (es. rete oncologica composta da unità operative specializzate nella lotta ai tumori), garantendo così l'accesso alle sole informazioni correlate con la patologia in cura.

Analogamente, alcune categorie di soggetti quali i farmacisti, che svolgono la propria attività in uno specifico segmento del percorso di cura, possono accedere ai soli dati (o moduli di dati)

indispensabili all'erogazione di farmaci (es. accesso limitato all'elenco dei farmaci già prescritti, al fine di valutare eventuali incompatibilità tra il farmaco vendibile senza obbligo di prescrizione medica (SOP) e altri farmaci precedentemente assunti).

In alcuni progetti di dossier sanitario è affidato alla direzione sanitaria il compito di valutare l'indispensabilità delle informazioni mediche generate dai diversi reparti/strutture ai fini della loro consultabilità, nonché quello di decidere se autorizzare o meno l'accesso alle informazioni relative agli eventi clinici anche pregressi da parte del reparto/struttura che ha in cura l'interessato sulla base del tipo di intervento medico e delle argomentazioni poste alla base della richiesta.

I titolari del trattamento, nel costituire il Fse/dossier e individuare la tipologia di informazioni che possono esservi anche successivamente riportate, dovrebbero rispettare le disposizioni normative a tutela dell'anonimato della persona tra cui quelle a tutela delle vittime di atti di violenza sessuale o di pedofilia (l. 15 febbraio 1996, n. 66; l. 3 agosto 1998, n. 269 e l. 6 febbraio 2006, n. 38), delle persone sieropositive (l. 5 giugno 1990, n. 135), di chi fa uso di sostanze stupefacenti, di sostanze psicotrope e di alcool (d.P.R. 9 ottobre 1990, n. 309), delle donne che si sottopongono a un intervento di interruzione volontaria della gravidanza o che decidono di partorire in anonimato (l. 22 maggio 1978, n. 194; d.m. 16 luglio 2001, n. 349), nonché con riferimento ai servizi offerti dai consultori familiari (l. 29 luglio 1975, n. 405).

Nella maggior parte dei progetti di Fse/dossier esaminati il rispetto delle garanzie di anonimato e riservatezza previste dalle sopra richiamate disposizioni di legge è stato ad esempio assicurato prevedendo che le informazioni relative ai suddetti eventi clinici non siano documentabili all'interno di tali strumenti.

In alcuni progetti esaminati all'interno del Fse/dossier è stata poi individuata una sintesi di rilevanti dati clinici sul paziente, ovvero un insieme di informazioni la cui conoscenza può rivelarsi indispensabile per salvaguardare la vita dell'interessato (es., malattie croniche, reazioni allergiche, uso di dispositivi o farmaci salvavita, informazioni relative all'impiego di protesi o a trapianti). Tali informazioni –raccolte di regola in un modulo distinto– sono conoscibili da parte di tutti i soggetti che prendono in cura l'interessato; circostanza di cui l'interessato dovrebbe essere edotto nell'informativa di cui all'art. 13 del Codice.

A garanzia del diritto all'autodeterminazione dovrebbero essere poi individuate modalità tali da

favorire un accesso modulare al Fse/dossier con riferimento ai dati personali e ai soggetti abilitati a consultarli.

L'identificazione dei soggetti abilitati a consultare il Fse/dossier dovrebbe essere effettuata con chiarezza. In relazione alle finalità perseguite con la costituzione del Fascicolo/dossier, l'accesso dovrebbe essere consentito solamente per fini di prevenzione, diagnosi e cura dell'interessato e unicamente da parte di soggetti operanti in ambito sanitario, con conseguente esclusione di periti, compagnie di assicurazione, datori di lavoro, associazioni o organizzazioni scientifiche, organismi amministrativi anche operanti in ambito sanitario, nonché del personale medico che agisca nell'esercizio di attività medico-legali.

Il personale amministrativo operante all'interno della struttura sanitaria in cui venga utilizzato il Fse/dossier dovrebbe consultare solo le informazioni necessarie per assolvere alle funzioni amministrative cui è preposto e strettamente correlate all'erogazione della prestazione sanitaria (ad es., il personale addetto alla prenotazione di esami diagnostici o visite specialistiche dovrebbe consultare unicamente i soli dati indispensabili per la prenotazione stessa).

L'abilitazione all'accesso deve essere consentita all'interessato nel rispetto delle cautele previste dall'art. 84 del Codice, secondo cui gli esercenti le professioni sanitarie e gli organismi sanitari possono comunicare all'interessato informazioni inerenti al suo stato di salute (es. referti, esiti di consulti medici) per il tramite di un medico –individuato dallo stesso interessato o dal titolare– o di un esercente le professioni sanitarie, che nello svolgimento dei propri compiti intrattiene rapporti diretti con il paziente (3). Tale garanzia dovrebbe essere osservata anche quando l'accesso al Fascicolo avviene mediante l'utilizzo di una smart card.

L'accesso al Fse/dossier dovrebbe essere consentito al soggetto che ha redatto il documento con riferimento allo stesso e agli altri soggetti che abbiano in cura l'interessato, sempre che quest'ultimo ne abbia consentito l'accesso nei termini sopra indicati. In alcuni progetti di Fse esaminati, l'accesso da parte di alcune categorie di soggetti (es. medici specialisti) è ad esempio autorizzato di volta in volta dallo stesso interessato attraverso la consegna di una smart card.

Il professionista o organismo sanitario che ha in cura l'interessato dovrebbe poter accedere a tali

(3) Cfr. Provvedimento del 9 novembre 2005 "Strutture sanitarie: rispetto della dignità" [doc. *web* n. 1191411]

strumenti consultando i documenti sanitari dallo stesso redatti e quelli relativi ad altri eventi clinici eventualmente formati da ulteriori reparti o strutture del medesimo titolare –nel caso di dossier-o da altri organismi o professionisti sanitari nel caso di Fse (es. ricovero pregresso, analisi cliniche antecedenti).

In ogni caso, l'accesso al Fse/dossier dovrebbe essere circoscritto al periodo di tempo indispensabile per espletare le operazioni di cura per le quali è abilitato il soggetto che accede. Ciò, comporta che i soggetti abilitati all'accesso dovrebbero poter consultare esclusivamente i fascicoli/dossier riferiti ai soggetti che assistono per il periodo di tempo in cui si articola il percorso di cura per il quale l'interessato si è rivolto ad essi.

L'elencazione della tipologia di informazioni da ricondurre ai cd. dati di emergenza dovrebbe essere effettuata in modo esaustivo dal titolare del trattamento, il quale procede anche ad aggiornare tale elenco.

Resta ovviamente ferma la normativa in materia di diritti di accesso ai documenti amministrativi (l. 7 agosto 1990, n. 241 e successive modificazioni e integrazioni).

6. INFORMATIVA

Per consentire all'interessato di esprimere scelte consapevoli, il titolare del trattamento deve fornire previamente un'idonea informativa (artt. 13, 79 e 80 del Codice).

L'informativa, da formulare con linguaggio chiaro, dovrebbe indicare tutti gli elementi richiesti dall'art. 13 del Codice. In particolare, dovrebbe essere evidenziata l'intenzione di costituire un Fascicolo/dossier il più possibile completo che documenti la storia sanitaria dell'interessato per migliorare il suo processo di cura e, quindi, per fini di prevenzione, diagnosi, cura e riabilitazione (cfr. art. 76, comma 1, lett. a) del Codice), spiegando in modo semplice le opportunità che offrono tali strumenti, ma, al tempo stesso, l'ampia sfera conoscitiva che essi possono avere.

A garanzia del diritto alla costituzione o meno del Fse/dossier, l'interessato dovrebbe essere - come detto- informato che il mancato consenso totale o parziale non incide sulla possibilità di accedere alle cure mediche richieste.

L'informativa, anche con formule sintetiche, ma agevolmente comprensibili, dovrebbe indicare in modo chiaro –nel caso di dossier– i soggetti (ad es., medici che operano in un reparto in cui

è ricoverato l'interessato o che operano in strutture di pronto soccorso) e –nel caso di Fse- le categorie di soggetti diversi dal titolare (es., medico di medicina generale, farmacista) che, nel prendere in cura l'interessato, possono accedere a tali strumenti, nonché la connessa possibilità di acconsentire che solo alcuni di questi soggetti possano consultarlo.

Nel caso di Fse, l'informativa e la connessa manifestazione del consenso potrebbero essere formulate distintamente per ciascuno dei titolari o, più opportunamente, in modo cumulativo, avendo comunque cura di indicare con chiarezza l'ambito entro il quale i singoli soggetti trattano i dati rispetto al Fse.

L'interessato dovrebbe essere informato anche della circostanza che il Fascicolo/dossier potrebbe essere consultato, anche senza il suo consenso, ma nel rispetto dell'autorizzazione generale del Garante, qualora sia indispensabile per la salvaguardia della salute di un terzo o della collettività (art. 76 del Codice).

L'informativa dovrebbe anche mettere in luce la circostanza che il consenso alla consultazione del Fascicolo/dossier da parte di un determinato soggetto (ad es., del medico di medicina generale o del medico di reparto in cui è avvenuto il ricovero) potrebbe essere riferito anche al suo sostituto.

L'informativa dovrebbe rendere note all'interessato anche le modalità attraverso le quali rivolgersi al titolare per esercitare i diritti di cui agli artt. 7 e ss. del Codice (cfr. successivo punto 10), come pure per revocare il consenso all'implementazione del suo Fse/dossier o per esercitare la facoltà di oscurare alcuni eventi clinici (cfr. punto n. 3).

Al fine di assicurare una piena comprensione degli elementi indicati nell'informativa, il titolare dovrebbe formare adeguatamente il personale coinvolto sugli aspetti rilevanti della disciplina sulla protezione dei dati personali, anche ai fini di un più efficace rapporto con gli interessati.

7. MISURE DI SICUREZZA

La particolare delicatezza dei dati personali trattati mediante il Fse/dossier impone l'adozione di specifici accorgimenti tecnici per assicurare idonei livelli di sicurezza (art. 31 del Codice), ferme restando le misure minime che ciascun titolare del trattamento deve comunque adottare ai sensi del Codice (artt. 33 e ss.).

Nell'utilizzo di sistemi di memorizzazione o archiviazione dei dati dovrebbero essere utilizzati idonei accorgimenti per la protezione dei dati registrati rispetto ai rischi di accesso abusivo, furto o smarrimento parziali o integrali dei supporti di memorizzazione o dei sistemi di elaborazione portatili o fissi (ad esempio, attraverso l'applicazione anche parziale di tecnologie crittografiche a file system o database, oppure tramite l'adozione di altre misure di protezione che rendano i dati inintelligibili ai soggetti non legittimati).

Dovrebbero essere, inoltre, assicurati:

- idonei sistemi di autenticazione e di autorizzazione per gli incaricati in funzione dei ruoli e delle esigenze di accesso e trattamento (ad es., in relazione alla possibilità di consultazione, modifica e integrazione dei dati);
- procedure per la verifica periodica della qualità e coerenza delle credenziali di autenticazione e dei profili di autorizzazione assegnati agli incaricati;
- individuazione di criteri per la cifratura o per la separazione dei dati idonei a rivelare lo stato di salute e la vita sessuale dagli altri dati personali;
- tracciabilità degli accessi e delle operazioni effettuate;
- sistemi di audit log per il controllo degli accessi al database e per il rilevamento di eventuali anomalie.

Nel caso di Fse, dovrebbero essere, poi, garantiti protocolli di comunicazione sicuri basati sull'utilizzo di standard crittografici per la comunicazione elettronica dei dati tra i diversi titolari coinvolti.

8. NOTIFICAZIONE AL GARANTE

Il Fse, costituendo un insieme logico di informazioni e documenti sanitari volto a documentare la storia clinica di un individuo condiviso da più titolari del trattamento, dovrebbe essere improntato a criteri di massima trasparenza nella sua strutturazione e nel suo funzionamento. A garanzia di tale evidenza i trattamenti di dati personali effettuati attraverso il Fse dovrebbero essere resi noti al Garante mediante lo strumento della notificazione da parte degli organismi pubblici e privati coinvolti e non anche a cura di singoli medici di base o professionisti che consultano un Fse (art. 37 del Codice).

Il Codice ha, infatti, demandato all'Autorità il compito di individuare ulteriori trattamenti -in aggiunta a quelli elencati nell'art. 37- da notificare potendo recare pregiudizio ai diritti e alle libertà dell'interessato in ragione delle relative modalità o della natura dei dati personali (art. 37, comma 2, del Codice). La particolare delicatezza delle informazioni trattate attraverso il Fse, nonché la possibilità di utilizzazione delle stesse da parte di diversi titolari induce a considerare allo stato necessaria una notificazione preventiva al Garante di tali trattamenti. L'Autorità si riserva pertanto di disporre all'esito della consultazione pubblica che le attività di gestione del Fse siano oggetto di notificazione in tutto o in parte.

9. DIFFUSIONE E TRASFERIMENTO ALL'ESTERO DEI DATI

I dati sanitari documentati nel Fse/dossier non devono essere in alcun modo diffusi. La circolazione indiscriminata delle informazioni idonee a rivelare lo stato di salute è infatti vietata espressamente dal Codice (artt. 22, comma 8 e 23, comma 5, del Codice). La violazione di tale divieto configura un trattamento illecito di dati personali sanzionato penalmente (art. 167 del Codice). Anche il trasferimento all'estero dei dati sanitari documentati nel Fse/dossier per finalità di prevenzione, diagnosi e cura dell'interessato può avvenire esclusivamente con il suo consenso, salvo il caso in cui sia necessario per la salvaguardia della vita o della incolumità di un terzo (art. 43 del Codice). Non a caso, nell'ambito dei progetti esaminati, la necessità di comunicare all'estero informazioni sanitarie dell'interessato contenute in tali strumenti si verifica prevalentemente per consentire all'interessato di usufruire di cure mediche all'estero o per consultare un esperto straniero.

10. DIRITTI DELL'INTERESSATO

Rispetto ai dati personali trattati mediante il Fse/dossier dovrebbe essere garantita la possibilità di esercitare in ogni momento i diritti di cui all'art. 7 del Codice. Tali diritti, tra i quali quello di accedere ai dati e di ottenerne la comunicazione in forma intelligibile, ovvero l'integrazione, l'aggiornamento o la rettifica, andrebbero esercitati direttamente nei confronti di ciascun organismo o professionista sanitario.

All'interessato dovrebbe essere fornito senza ritardo un riscontro compiuto e analitico in merito alle sue eventuali istanze (artt. 7, 8, 9, 10 e 146 del Codice). In particolare, dovrebbe essere for-

nito riscontro alle richieste di accesso ai dati personali estrapolando le informazioni oggetto dell'accesso e comunicandole all'interessato con modalità tali da renderne agevole la comprensione, se del caso trasponendole su supporto cartaceo o informatico; a tali istanze può essere opposto un rifiuto nei soli casi previsti dal Codice (art. 8). Trattandosi di documentazione medica, in analogia a quanto disposto dall'Autorità in tema di ricerche in ambito medico, biomedico ed epidemiologico (4), il riscontro a istanze di integrazione, aggiornamento e rettificazione dei dati potrebbe essere fornito annotando le modifiche richieste senza alterare necessariamente la documentazione di riferimento.

(4) Provvedimento generale del 24 luglio 2008 "Linee-guida per i trattamenti di dati personali nell'ambito delle sperimentazioni cliniche di medicinali" pubblicato in Gazzetta Ufficiale 14 agosto 2008, n. 190, [doc. *web* n. 1533155]

39. Segnalazione al Parlamento e al Governo sulla videosorveglianza nei condomini (*)

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

SEGNALAZIONE AL PARLAMENTO E AL GOVERNO SULLA VIDEOSORVEGLIANZA NEI CONDOMINI

(art. 154, comma 1, lett. f), d.lg. 30 giugno 2003, n. 196)

1. La presente segnalazione individua le ragioni per le quali il Garante ritiene opportuno un intervento normativo volto a disciplinare alcuni profili relativi alla videosorveglianza all'interno di edifici condominiali e nelle relative pertinenze, tematica che forma oggetto di recenti quesiti e segnalazioni indirizzate all'Autorità. Più specificamente, oggetto della presente segnalazione è il caso in cui non i singoli condomini, ma l'intera compagine condominiale intenda effettuare tali trattamenti (previa installazione di sistemi di videosorveglianza per il tramite della relativa amministrazione condominiale, anche presso amministrazioni di residence o di multiproprietà) in aree comuni (quali portoni d'ingresso, androni, cortili, scale, aree di accesso a parcheggi o dedicate a servizi comuni).

2. Da tempo, il tema più generale della videosorveglianza specie in luoghi pubblici o aperti al pubblico è all'attenzione del Garante e ha formato oggetto, oltre che di numerose decisioni in singoli casi, di due provvedimenti di carattere generale: il primo, del 29 novembre 2000 (in www.garanteprivacy.it, doc. web n. 31019, nel quale si impartivano prime prescrizioni "nell'attesa di una specifica legislazione"), il secondo, più dettagliato perché volto a tener conto di variegate sollecitazioni provenienti da prassi applicative, del 29 aprile 2004 (doc. web n. 1003482). Con tali interventi, il Garante non si è soffermato specificamente sulle condizioni di liceità per il trattamento di dati personali all'interno dei condomìni: non sono stati di conseguenza identificati né i soggetti la cui manifestazione di volontà è necessaria nel contesto condominiale per svolgere tali trattamenti (i proprietari e i titolari di diritti reali parziari o anche soggetti diversi, primi fra tutti i conduttori), né le eventuali maggioranze da rispettare.

(*) [doc. *web* n. 1523997]

3. In tempi più recenti, si sono moltiplicati i quesiti e le segnalazioni relativi allo specifico profilo delle condizioni di impiego della videosorveglianza da parte di compagini condominiali all'interno di aree comuni.

Dal loro esame emerge l'esistenza di due non convergenti approcci alla tematica, da parte dei contrapposti interessi potenzialmente coinvolti dal funzionamento di questi sistemi di videosorveglianza: da un lato, l'esigenza volta a preservare la sicurezza di persone e la tutela di beni comuni (ad esempio, rispettivamente, contro aggressioni e danneggiamenti o furti); dall'altro, la preoccupazione che i trattamenti effettuati, nel rendere più agevolmente conoscibili a terzi informazioni relative alla vita privata di chi vive in edifici condominiali, come pure abitudini e stili di vita individuali e familiari, siano idonei a incidere sulla libertà degli interessati di muoversi, non controllati, nel proprio domicilio e all'interno delle aree comuni.

4. Il profilo in esame non è regolato da una puntuale disciplina. Esso non trova (né avrebbe potuto trovare) espressa regolamentazione nel Codice civile del 1942; né, è chiaro, pur applicando i princìpi generali, se l'installazione di sistemi di videosorveglianza possa essere effettuata in base alla sola volontà dei (com)proprietari (comunque, il quadro normativo esistente e l'interpretazione giurisprudenziale non consentono di comprendere con quale maggioranza) o se rilevi anche la volontà di coloro che rivestono la qualità di conduttori.

Deve essere anche tenuto in considerazione che l'art. 615 *bis* del codice penale sanziona "chiunque mediante l'uso di strumenti di ripresa visiva o sonora, si procura indebitamente notizie o immagini attinenti alla vita privata svolgentesi nei luoghi indicati nell'articolo 614", vale a dire nel domicilio (nozione che, secondo la giurisprudenza, è suscettibile di comprendere anche le aree comuni (1)): ciò comporterebbe, nel contesto condominiale, la necessaria acquisizione preventiva del consenso di un numero assai ampio di soggetti, non sempre peraltro di agevole identificazione, sì da rendere arduo il legittimo impiego dei sistemi di videosorveglianza nel peculiare contesto qui tenuto in considerazione.

Più in generale, gli orientamenti giurisprudenziali sull'uso delle aree comuni non appaiono utili a dissolvere i dubbi relativi ai profili in esame.

(1) Cfr. Cass. Pen., sez. V, 20 ottobre 1998, n. 12751; Cass., 15 maggio 1987; v. pure Cass. pen., 27 marzo 2006, n. 10444

5. Per tali ragioni il Garante auspica che gli aspetti segnalati del tema qui rappresentato, suscettibile di interessare larga parte della popolazione, possano trovare una più specifica regolamentazione, con l'individuazione di una disciplina che assicuri un equo contemperamento tra i diritti fondamentali delle persone coinvolte e le legittime esigenze di difesa e protezione di persone e cose. Ciò, peraltro, potrebbe avvenire anche nell'ambito di più generali iniziative normative relative all'amministrazione dei condomini, già oggetto di diversi disegni di legge sottoposti all'esame di entrambi i rami del Parlamento. (2)

PER QUESTE RAGIONI

il Garante segnala al Parlamento e al Governo l'opportunità che sia valutata anche l'eventuale adozione di una possibile regolamentazione dell'utilizzo di sistemi di videosorveglianza delle aree comuni identificando le condizioni per assumere idonee determinazioni, con particolare riferimento all'individuazione:

- dei partecipanti al processo decisionale (i soli condomini, ovvero anche i conduttori);
- del numero di voti necessari per l'approvazione della deliberazione (l'unanimità o una determinata maggioranza).

Roma, 13 maggio 2008

(2) A questo proposito può evidenziarsi che nel corso della XV Legislatura (ripercorrendo testi ampiamente discussi e condivisi nel corso della XIV) sono stati presentati i seguenti disegni di legge: C. 1199 On. Cosimo Giuseppe Sgobio, Modifiche al codice civile in materia di condominio negli edifici, presentato il 26 giugno 2006; S. 647 Sen. Giovanni Legnini e altri, Modifiche alla disciplina del condominio negli edifici, presentato il 14 giugno 2006; S. 310 Sen. Franco Mugnai e altri, Modifiche alla disciplina del condominio negli edifici, presentato il 10 maggio 2006; S. 6 Sen. Andrea Pastore e altri, Modifiche alla normativa in materia di condominio negli edifici, presentato il 28 aprile 2006

40. Provvedimenti di particolare rilievo

Autorizzazione n. 1/2008 al trattamento dei dati sensibili nei rapporti di lavoro
19 giugno 2008 [doc. *web* n. 1529374]

Autorizzazione n. 2/2008 al trattamento dei dati idonei a rivelare lo stato di salute e la vita sessuale
19 giugno 2008 [doc. *web* n. 1529389]

Autorizzazione n. 3/2008 al trattamento dei dati sensibili da parte degli organismi di tipo associativo e delle fondazioni
19 giugno 2008 [doc. *web* n. 1529399]

Autorizzazione n. 4/2008 al trattamento dei dati sensibili da parte dei liberi professionisti
19 giugno 2008 [doc. *web* n. 1529408]

Autorizzazione n. 5/2008 al trattamento dei dati sensibili da parte di diverse categorie di titolari
19 giugno 2008 [doc. *web* n. 1529420]

Autorizzazione n. 6/2008 al trattamento dei dati sensibili da parte degli investigatori privati
19 giugno 2008 [doc. *web* n. 1529549]

Autorizzazione n. 7/2008 al trattamento dei dati a carattere giudiziario da parte di privati, di enti pubblici economici e di soggetti pubblici
19 giugno 2008 [doc. *web* n. 1529557]

Differimento dell'efficacia dell'autorizzazione al trattamento dei dati genetici rilasciata il 22 febbraio 2007
19 dicembre 2008 [doc. *web* n. 1582871]

Semplificazione al modello per la notificazione al Garante

22 ottobre 2008 [doc. *web* n. 1571196]

Misure in materia di propaganda elettorale - Esonero dall'informativa

2 aprile 2009 [doc. *web* n. 1603863]

Redditi *on-line*: illegittima la diffusione dei dati sul sito Internet dell'Agenzia delle entrate

6 maggio 2008 [doc. *web* n. 1512255]

Riconoscimento vocale e gestione di sistemi informatici

28 febbraio 2008 [doc. *web* n. 1501094]

Dati biometrici: vietati per la rilevazione dell'orario di lavoro

2 ottobre 2008 [doc. *web* n. 1571502]

Controlli *anti-doping* e trattamento dei dati personali dei ciclisti

13 ottobre 2008 [doc. *web* n. 1563970]

41. Ulteriori provvedimenti citati

Dichiarazione di appartenenza o aggregazione al gruppo linguistico in provincia di Bolzano

10 gennaio 2008 [doc. *web* n. 1484669]

Sicurezza dei dati di traffico telefonico e telematico

17 gennaio 2008 [doc. *web* n. 1482111]

Preiscrizioni universitarie per l'anno accademico 2008/2009

31 gennaio 2008 [doc. *web* n. 489926]

Trattamento di dati personali in albergo per finalità di *marketing*

31 gennaio 2008 [doc. *web* n. 1490553]

Marketing: possibile inviare materiale pubblicitario e comunicazioni commerciali solo con il consenso preventivo dell'interessato

31 gennaio 2008 [doc. *web* n. 1488781]

31 gennaio 2008 [doc. *web* n. 1489843]

13 maggio 2008 [doc. *web* n. 1520217]

13 maggio 2008 [doc. *web* n. 1520243]

13 maggio 2008 [doc. *web* n. 1520263]

19 dicembre 2008 [doc. *web* n. 1584213]

Consenso e trattamento dei dati personali a fini di *marketing*

31 gennaio 2008 [doc. *web* n. 1500829]

Trattamento di dati giudiziari del personale di società di *rating*

31 gennaio 2008 [doc. *web* n. 1488729]

Trattamento dei dati sensibili e giudiziari presso la Scuola superiore della pubblica amministrazione locale
7 febbraio 2008 [doc. *web* n. 1491594]

Banche: configurazione dei sistemi di allerta rientranti nelle misure previste per il contrasto finanziario al terrorismo
7 febbraio 2008 [doc. *web* n. 1523046]

Pubblicità dei dati di debitori nelle esecuzioni immobiliari
7 febbraio 2008 [doc. *web* n. 1490838]

Movimenti politici: limiti e garanzie nel trattamento dei dati personali
15 febbraio 2008 [doc. *web* n. 1523069]

Trattamento dei dati biometrici di dipendenti per incrementare la sicurezza della rete idrica
15 febbraio 2008 [doc. *web* n. 1497675]

Modalità di inserimento negli elenchi dei beneficiari del 5 per mille Irpef delle associazioni sportive
21 febbraio 2008 [doc. *web* n. 1497596]

Sportello unico doganale delle operazioni di importazione ed esportazione
28 febbraio 2008 [doc. *web* n. 1523079]

Esonero dall'informativa per partiti e movimenti politici sino al 31 luglio 2008
28 febbraio 2008 [doc. *web* n. 1493909]

Diffusione di dati relativi a contributi per l'acquisto di testi scolastici
28 febbraio 2008 [doc. *web* n. 1501081]

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]

Modalità di richiesta di ammissione al beneficio del 5 per mille Irpef

13 marzo 2008 [doc. *web* n. 1500816]

Comunicazione unica per la nascita dell'impresa

13 marzo 2008 [doc. *web* n. 1500799]

Fondazioni bancarie: regolamento di bilancio

20 marzo 2008 [doc. *web* n.1502866]

Impresa: presentazione dei bilanci e altri atti al registro delle imprese

20 marzo 2008 [doc. *web* n. 1519563]

Tutela della salute e sicurezza nei luoghi di lavoro

31 marzo 2008 [doc. *web* n. 1504941]

Documenti caratteristici del personale dell'Esercito, della Marina, dell'Aeronautica e dell'Arma dei carabinieri

2 aprile 2008 [doc. *web* n. 1519667]

Tecnologie per la formazione a distanza e controllo a distanza dei lavoratori

2 aprile 2008 [doc. *web* n. 1519695]

L'azienda non può comunicare a terzi i dati giudiziari riferiti ai collaboratori

2 aprile 2008 [doc. *web* n. 1519711]

Programmi di fidelizzazione: trattamento di dati personali riferiti al dipendente e loro utilizzo a fini disciplinari

2 aprile 2008 [doc. *web* n. 1519679]

Comunicazioni illecite di dati sulla salute dei dipendenti

2 aprile 2008 [doc. *web* n. 1519902]

Limiti al controllo sulla posta elettronica del dipendente

2 aprile 2008 [doc. *web* n. 1519703]

Prove di ammissione a corsi di laurea ad accesso programmato per l'anno accademico 2008/2009

10 aprile 2008 [doc. *web* n. 1519655]

Trattamento di dati sensibili e giudiziari da parte della Provincia di Roma. Nuova finalità di rilevante interesse pubblico

10 aprile 2008 [doc. *web* n. 1507195]

Regole tecniche per la firma digitale

15 aprile 2008 [doc. *web* n. 1519647]

Iscrizione al registro nazionale delle imprese operanti nel settore degli armamenti

24 aprile 2008 [doc. *web* n. 1514260]

Accesso agli atti delle imprese assicuratrici derivanti dalla circolazione dei veicoli a motore e natanti

30 aprile 2008 [doc. *web* n. 1514729]

Pubblicazione Internet degli elenchi dei contribuenti da parte dell'Agenzia delle entrate

30 aprile 2008 [doc. *web* n. 1510761]

Graduatorie di concorsi pubblici e dati sensibili

8 maggio 2008 [doc. *web* n. 1521716]

Marketing via *e-mail*: necessaria l'informativa per il trattamento di dati personali

13 maggio 2008 [doc. *web* n. 1521775]

Vendita a domicilio e trattamento di dati a fini di *marketing* in violazione di legge

19 maggio 2008 [doc. *web* n. 1526956]

Autonomia della comunicazione di dati rispetto alle altre operazioni di trattamento

19 maggio 2008 [doc. *web* n. 1523347]

Uso di strumenti informatici e telematici nel processo civile

19 maggio 2008 [doc. *web* n. 1521729]

Ministero della giustizia. Tenuta dei registri informatizzati negli uffici

19 maggio 2008 [doc. *web* n. 1521788]

Immigrazione, condizione dello straniero e ricongiungimento familiare

5 giugno 2008 [doc. *web* n. 1526943]

Esercizio di attività giornalistica e comunicazione all'interessato dei dati che lo riguardano

5 giugno 2008 [doc. *web* n. 1542403]

Trattamento dei dati completi e aggiornati tratti dai pubblici registri

5 giugno 2008 [doc. *web* n. 1535726]

Giornalismo: rispetto del principio di essenzialità dell'informazione nel caso di vittime di reato

5 giugno 2008 [doc. *web* n. 1527037]

Informazioni commerciali: qualità dei dati

12 giugno 2008 [doc. *web* n. 1537684]

Modifiche e integrazioni allo schema tipo di regolamento per i trattamenti dei dati sensibili e giudiziari svolti presso le regioni e le province autonome

12 giugno 2008 [doc. *web* n. 1537639]

Uso di dati biometrici nelle operazioni di trasfusione

19 giugno 2008 [doc. *web* n. 1532480]

Telemarketing: banche dati precedenti al 1° agosto 2005 - Provvedimento inibitorio

26 giugno 2008 [doc. *web* n 1544326]

26 giugno 2008 [doc. *web* n.1544315]

26 giugno 2008 [doc. *web* n. 1544338]

25 settembre 2008 [doc. *web* n. 1562780]

25 settembre 2008 [doc. *web* n. 1562758]

Attività giornalistica: diffusione di dati su minori vittime di violenza sessuale

10 luglio 2008 [doc. *web* n. 1536583]

2 ottobre 2008 [doc. *web* n. 1557470]

16 febbraio 2009 [doc. *web* n. 1590076]

Schema di linee-guida in tema di insediamenti di comunità nomadi nelle regioni Campania, Lazio e Lombardia

17 luglio 2008 [doc. *web* n. 1537659]

Individuazione dei soggetti certificatori della Cns

24 luglio 2008 [doc. *web* n. 1545983]

Trattamento dei dati sensibili nell'ambito di attività di informazione scientifica e di sperimentazione clinica di medicinali

24 luglio 2008 [doc. *web* n. 1544575]

Recepimento normativo in tema di dati di traffico telefonico e telematico

24 luglio 2008 [doc. *web* n. 1538224]

Social card: *privacy* garantita per i meno abbienti

18 settembre 2008 [doc. *web* n. 1553367]

Videosorveglianza: limiti e garanzie per il trattamento dei dati

2 ottobre 2008 [doc. *web* n. 1581352]

Identità personale e sistemi di informazione creditizia

13 ottobre 2008 [doc. *web* n. 1562822]

6 novembre 2008 [doc. *web* n. 1571531]

Società di informazioni commerciali: tutela dell'interessato nei casi di possibile omonimia

13 ottobre 2008 [doc. *web* n. 1571459]

Giornalismo: diffusione di dati su vittime di violenza sessuale

13 ottobre 2008 [doc. *web* n. 1563958]

Aggiornamento 2009/2010 del Programma statistico nazionale

22 ottobre 2008 [doc. *web* n. 1565063]

Informazioni commerciali: si possono trattare solo dati pertinenti

30 ottobre 2008 [doc. *web* n. 1570327]

Programmi di fidelizzazione: trattamento di dati personali riferiti al dipendente e loro utilizzo a fini disciplinari

6 novembre 2008 [doc. *web* n. 1573780]

Contratti di locazione: vietata la diffusione a terzi dei dati personali del conduttore

20 novembre 2008 [doc. *web* n. 1576139]

Dati genetici: limiti al trattamento a fini giudiziari

27 novembre 2008 [doc. *web* n. 1581365]

Attività giornalistica: dati relativi a minori

27 novembre 2008 [doc. *web* n. 1582436]

Esercizio dei diritti dell'interessato e difesa in giudizio

27 novembre 2008 [doc. *web* n. 1580262]

Videosorveglianza: vietata negli spogliatoi di poliambulatorio

4 dicembre 2008 [doc. *web* n. 1576125]

Archivi storici *on-line* dei quotidiani: accoglimento dell'opposizione dell'interessato alla reperibilità delle proprie generalità attraverso i motori di ricerca

11 dicembre 2008 [doc. *web* n. 1582866]

19 dicembre 2008 [doc. *web* n. 1583152]

Operazioni di scissione e fusione per incorporazione: prescrizioni in tema di aggiornamento dell'informativa a Banca Nazionale del Lavoro S.p.A. ed Artigiancassa

11 dicembre 2008 [doc. *web* n. 1584328]

Agenzia delle entrate: modalità e termini per la segnalazione da parte delle società di gestione del risparmio dei soggetti che hanno omesso la comunicazione necessaria ai fini dell'applicazione dell'imposta patrimoniale
19 dicembre 2008 [doc. *web* n. 1584260]

Frodi comunitarie: trattamento di dati sensibili e giudiziari da parte della Presidenza del Consiglio dei ministri
19 dicembre 2008 [doc. *web* n. 1584241]

Persone disperse in montagna: si può localizzare il cellulare per rintracciarle
19 dicembre 2008 [doc. *web* n. 1580543]

Accesso all'Indice dei nati in Trentino: intesa tra la Provincia autonoma di Trento e l'Arcidiocesi di Trento
19 dicembre 2008 [doc. *web* n. 1584224]

Operazione di fusione per incorporazione: prescrizioni in tema di aggiornamento dell'informativa a Banca Monte dei Paschi di Siena S.p.A.
19 dicembre 2008 [doc. *web* n. 1584272]

Operazione Cai/Alitalia: informativa semplificata per i clienti e trattamento dei dati personali
8 gennaio 2009 [doc. *web* n. 1580603]

Archivi storici *on-line* dei quotidiani: condizioni che rendono legittima la riproposizione di un articolo su Internet
12 febbraio 2009 [doc. *web* n. 1601624]

Conservazione dei dati di traffico: proroga dei termini
29 aprile 2009 [doc. *web* n. 1612508]

Principali attività internazionali

42. Unione europea

Sistema europeo di informazione visti (VIS)

Decisione 2008/633/Gai del Consiglio relativa all'accesso per la consultazione al sistema di informazione visti (Vis) da parte delle autorità designate degli Stati membri e di Europol ai fini della prevenzione, dell'individuazione e dell'investigazione di reati di terrorismo e altri reati gravi
23 giugno 2008 [doc. *web* n. 1623022]

Regolamento 767/2008 del Parlamento europeo e del Consiglio concernente il sistema di informazione visti (Vis) e lo scambio di dati tra Stati membri sui visti per soggiorni di breve durata (regolamento Vis)
9 luglio 2008 [doc. *web* n. 1623026]

Cooperazione giudiziaria e di polizia

Decisione 2008/615/Gai del Consiglio sul potenziamento della cooperazione transfrontaliera, soprattutto nella lotta al terrorismo e alla criminalità transfrontaliera
23 giugno 2008 [doc. *web* n. 1621998]

Decisione 2008/616/Gai del Consiglio relativa all'attuazione della Decisione 2008/615/Gai sul potenziamento della cooperazione transfrontaliera, soprattutto nella lotta al terrorismo e alla criminalità transfrontaliera
23 giugno 2008 [doc. *web* n. 1623035]

Decisione quadro 2008/977/Gai del Consiglio sulla protezione dei dati personali trattati nell'ambito della cooperazione giudiziaria e di polizia in materia penale
27 novembre 2008 [doc. *web* n. 1620574]

MANDATO EUROPEO DI RICERCA DELLE PROVE

Decisione quadro 2008/978/Gai del Consiglio relativa al mandato europeo di ricerca delle prove diretto all'acquisizione di oggetti, documenti e dati da utilizzare nei procedimenti penali

18 dicembre 2008 [doc. *web* n. 1620578]

CARTELLE CLINICHE

Raccomandazione della Commissione europea 2008/594/Ce sull'interoperabilità transfrontaliera dei sistemi di cartelle cliniche elettroniche

2 luglio 2008 [doc. *web* n. 1623030]

AREA DI LIBERTÀ, SICUREZZA, GIUSTIZIA

Relazione del Gruppo consultivo informale ad alto livello sul futuro della politica europea in materia di affari interni ("Gruppo del futuro")

9 luglio 2008 [doc. *web* n. 1622002]

CENSIMENTO SU BASE ETNICA

Risoluzione del Parlamento europeo sul censimento dei rom su base etnica in Italia

10 luglio 2008 [doc. *web* n. 1620664]

SICUREZZA E LIBERTÀ SU INTERNET

Raccomandazione del Parlamento europeo destinata al Consiglio sul rafforzamento della sicurezza e delle libertà fondamentali su Internet

26 marzo 2009 [doc. *web* n. 1622010]

EUROPOL

Decisione 2009/371/Gai del Consiglio che istituisce l'Ufficio europeo di polizia (Europol)

6 aprile 2009 [doc. *web* n. 1621994]

43. Corte di giustizia delle Comunità europee

DATI FISCALI E LIBERTÀ DI ESPRESSIONE

Court of Justice of the European Communities, Case of Tietosuojavaltuutettu v. Satakunnan Markkinapörssi Oy, Satamedia Oy

(C-73/07)

16 dicembre 2008 [doc. *web* n. 1622031]

LIBERA CIRCOLAZIONE E PROTEZIONE DEI DATI

Court of Justice of the European Communities, Case of Heinz Huber v. Bundesrepublik Deutschland

(C-524/06)

16 dicembre 2008 [doc. *web* n. 1623041]

ANNULLAMENTO DIRETTIVA SULLA CONSERVAZIONE DEI DATI DI TRAFFICO

Court of Justice of the European Communities, Case of Ireland v. Council of the European Union, European Parliament

(C-301/06)

10 febbraio 2009 [doc. *web* n. 1620668]

44. Gruppo art. 29

PROGRAMMA DI LAVORO 2008-2009

WP 146 - Work Programme 2008-2009, Article 29 Working Party

18 febbraio 2008 [doc. *web* n. 1610768]

PROTEZIONE DEI DATI RELATIVI AI MINORI

WP 147 - Working Document 1/2008 on the protection of Children's Personal Data

18 febbraio 2008 [doc. *web* n. *1610778*]

MOTORI DI RICERCA

WP 148 - Opinion 1/2008 on data protection issues related to search engines

4 aprile 2008 [doc. *web* n. 1610786]

CONTROLLI E SORVEGLIANZA DELLE FRONTIERE ESTERNE

WP 149 - Lettera al Commissario Barrot relativa al commento congiunto del Gruppo Art. 29 e del *Working Party on Police and Justice* sulle iniziative della Commissione europea in materia di controlli e sorveglianza delle frontiere esterne

29 aprile 2008 [doc. *web* n. 1610793]

RIESAME DELLA DIRETTIVA RELATIVA ALLA VITA PRIVATA E ALLE COMUNICAZIONI ELETTRONICHE

WP 150 - Parere 2/2008 sul riesame della Direttiva 2002/58/Ce relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (direttiva relativa alla vita privata e alle comunicazioni elettroniche)

15 maggio 2008 [doc. *web* n. 1610799]

DATI RELATIVI AI PASSEGGERI

WP 151 - Parere 2/2007 sull'informazione dei passeggeri in merito al trasferimento di dati Pnr alle autorità statunitensi

24 giugno 2008 [doc. *web* n. 1619505]

BINDING CORPORATE *RULES*

WP 153 - Working Document setting up a table with the elements and principles to be found in Binding Corporate Rules

24 giugno 2008 [doc. *web* n. 1619530]

WP 154 - Working Document Setting up a framework for the structure of Binding Corporate Rules

24 giugno 2008 [doc. *web* n. 1619588]

WP 155 - Working Document on Frequently Asked Questions (FAQs) related to Binding Corporate Rules

8 aprile 2009 [doc. *web* n. 1619607]

AZIONE CONGIUNTA DI ACCERTAMENTO

WP 152 - Mandate to the Enforcement Subgroup to proceed to the 2nd joint investigation action

17 luglio 2008 [doc. *web* n. 1619517]

ANTI-DOPING

WP 156 - Parere 3/2008 sul progetto di *standard* internazionale del codice mondiale *anti-doping* per la protezione della *privacy*

1 agosto 2008 [doc. *web* n. 1619614]

PROPOSTE DI MODIFICA DELLA DIRETTIVA RELATIVA ALLA VITA PRIVATA E ALLE COMUNICAZIONI ELETTRONICHE

WP 159 - Parere 1/2009 sulle proposte recanti modifica della Direttiva 2002/58/Ce relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (direttiva relativa alla vita privata e alle comunicazioni elettroniche)

10 febbraio 2009 [doc. *web* n. 1620306]

PRE-TRIAL DISCOVERY

WP 158 - Working Document 1/2009 on pre-trial discovery for cross border civil litigation

11 febbraio 2009 [doc. *web* n. 1620296]

PROTEZIONE DEI DATI RELATIVI A MINORI

WP 160 - Opinion 2/2009 on the protection of children's personal data (General Guidelines and the special case of schools)

11 febbraio 2009 [doc. *web* n. 1620315]

CLAUSOLE CONTRATTUALI TIPO

WP 161 - Opinion 3/2009 on the Draft Commission Decision on standard contractual clauses for the transfer of personal data to processors established in third countries, under Directive 95/46/EC (data controller to data processor)

5 marzo 2009 [doc. *web* n. 1620329]

ANTI-DOPING

WP 162 - Second opinion 4/2009 on the World Anti-Doping Agency (WADA) International Standard for the Protection of Privacy and Personal Information, on related provisions of the WADA Code and on other privacy issues in the context of the fight against doping in sport by WADA and (national) anti-doping organizations

6 aprile 2009 [doc. *web* n. 1620339]

45. Autorità di controllo Europol

RELAZIONE DI ATTIVITÀ DELL'AUTORITÀ DI CONTROLLO COMUNE DELL'EUROPOL

Quarta relazione di attività dell'autorità di controllo comune dell'Europol novembre 2006 - novembre 2008

[doc. *web* n. 1624648]

46. Unità di controllo Eurodac

rapporto di attività eurodac

Coordinated supervision of Eurodac – Activity Report 2006-2008

In corso di pubblicazione

47. Autorità comune di controllo Schengen

relazione di attività dell'autorità comune di controllo schengen

Relazione sulle attività – dicembre 2005 - dicembre 2008

[doc. *web* n. 1625267]

48. Gruppo di lavoro in materia di attività giudiziarie e di polizia - *Working Party on Police and Justice*

rapporto di attività

2007-2008 Annual activity report of the working party on police and justice

16 dicembre 2008 [doc. *web* n. 1623172]

49. Corte europea dei diritti dell'uomo

TUTELA DEI MINORI *ON-LINE*

European Court of Human Rights, Case of K.U. v. Finland

(Application no. 2872/02)

2 dicembre 2008 [doc. *web* n. 1620370]

IMPRONTE DIGITALI E DNA NELLA LOTTA ALLA CRIMINALITÀ

European Court of Human Rights, Case of Marper v. the United Kingdom

(Applications nos. 30562/04 and 30566/04)

4 dicembre 2008 [doc. *web* n. 1620374]

FOTO DI UN NEONATO E TUTELA DELLA VITA PRIVATA

European Court of Human Rights, Affaire Reklos et Davourlis c. Gréce

(Requête no. 1234/05)

15 gennaio 2009 [doc. *web* n. 1620656]

50. 30ma Conferenza internazionale dei garanti *privacy*

ACCREDITAMENTO

Accreditation Resolution

17 ottobre 2008 [doc. *web* n. 1619248]

PRIVACY *ON-LINE* DEI MINORI

Resolution on children's *on-line* privacy

17 ottobre 2008 [doc. *web* n. 1566072]

"GIORNO O SETTIMANA MONDIALE SULLA PRIVACY"

Resolution to explore establishing an International Privacy/Data Protection Day or Week

17 ottobre 2008 [doc. *web* n. 1623189]

***STANDARD* INTERNAZIONALI IN MATERIA DI *PRIVACY* E PROTEZIONE DEI DATI PERSONALI**

Resolution on the urgent need for protecting privacy in a borderless world, and for reaching a Joint Proposal for setting International Standards on Privacy and Personal Data Protection

17 ottobre 2008 [doc. *web* n. 1566053]

TUTELA DELLA *PRIVACY* NEL *SOCIAL NETWORK*

Resolution on Privacy Protection in Social Network Services

17 ottobre 2008 [doc. *web* n. 1560428]

CREAZIONE DI UN COMITATO DIRETTIVO PERMANENTE PER LA RAPPRESENTANZA IN OCCASIONE DI INCONTRI TENUTI DA ORGANISMI INTERNAZIONALI

Resolution concerning the Establishment of a Steering Group on Representation at Meetings of International Organisations

17 ottobre 2008 [doc. *web* n. 1566088]

GRUPPO DI LAVORO PER IL SITO *WEB*

Resolution of the Website Working Group

17 ottobre 2008 [doc. *web* n. 1619256]

51. Conferenza di primavera 2008 (1)

DICHIARAZIONE SUL CONTROLLO DEI PASSEGGERI

18 aprile 2008 [doc. *web* n. 1531404]

52. Conferenza di primavera 2009 (2)

IL FUTURO DELLA PROTEZIONE DEI DATI IN EUROPA

Declaration on leadership and the future of data protection in Europe

23 aprile 2009 [doc. *web* n. 1622018]

ACCORDI BILATERALI E MULTILATERALI NELLE ATTIVITÀ GIUDIZIARIA E DI POLIZIA

Resolution on bilateral and multilateral agreements between European states and third countries in the area of police and judicial co-operation in criminal matters

23 aprile 2009 [doc. *web* n. 1623162]

SEMINARIO SUL CONTENZIOSO PRESSO LE AUTORITÀ PER LA PROTEZIONE DEI DATI

The future of the case handling workshops

23 aprile 2009 [doc. *web* n. 1623166]

(1) Conferenza delle autorità europee per la protezione dei dati tenutasi a Roma dal 17 al 18 aprile 2008
(2) Conferenza delle autorità europee per la protezione dei dati tenutasi a Edimburgo dal 23 al 24 aprile 2009

53. OCSE

IL FUTURO DI INTERNET

The Seul Declaration for the future of Internet economy

18 giugno 2008 [doc. *web* n. 1623176]

RFID

Radio frequency identification (Rfid): a focus on information security and privacy

14 gennaio 2008 [doc. *web* n. 1623180]

SICUREZZA IN INTERNET

Measuring security and trust in the on-line enviroment: a view using official data

29 gennaio 2008 [doc. *web* n. 1623184]

54. GRUPPO INTERNAZIONALE SULLA *PRIVACY* NELLE TELECOMUNICAZIONI

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]

55. Consiglio d'Europa

Privacy e lotta al terrorismo

Protecting the right to privacy in the fight against terrorism

Documento pubblicato dal Commissario del Consiglio d'Europa per i diritti umani, Thomas Hammarberg

4 dicembre 2008 [doc. *web* n. 1622006]

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

Redazione
Garante per la protezione dei dati personali

Piazza di Monte Citorio, 121
00186 Roma
tel. 06 696771 - fax 06 69677785
www.garanteprivacy.it
www.dataprotection.org
e-mail: garante@garanteprivacy.it

progetto grafico:
maurizio leante