apprendere notizie impersonali che non siano riferibili ad un interessato identificato o identificabile.

7.2. Accesso ai dati per ragioni di giustizia

Il Garante ha nuovamente rilevato, in occasione di una decisione su un ricorso presentato nei confronti di un ufficio giudiziario (procura della Repubblica), che ai trattamenti effettuati per "ragioni di giustizia" (v., ora, art. 47 d.lg. n. 196/2003) alcune disposizioni in materia di protezione dei dati personali non sono applicabili o sono applicate con alcuni adattamenti.

Modalità di esercizio dei diritti

In particolare, non è previsto l'esercizio in forma diretta del diritto di accesso e degli altri diritti degli interessati, né la presentazione di un ricorso all'Autorità. È invece possibile esercitare tali diritti in forma diversa dalla richiesta rivolta al titolare o al responsabile del trattamento, presentando un'istanza al Garante per sollecitare la verifica della conformità del trattamento ai requisiti stabiliti (*Provv.* 5 novembre 2003).

Il Codice ha poi confermato l'inesperibilità del ricorso al Garante, prevedendo che il diritto di accesso e gli altri diritti degli interessati possano essere esercitati anche nei confronti dei trattamenti effettuati per "ragioni di giustizia" attraverso una segnalazione a questa Autorità. Le diverse modalità di esercizio dei diritti non incidono, quindi, sul sostanziale livello di tutela garantito agli interessati, poiché il Garante mantiene il potere di verificare la liceità e la correttezza dei trattamenti, con modalità peraltro adeguate alla specificità del contesto in cui questi sono effettuati, ovvero nel rispetto delle reciproche attribuzioni e della particolare collocazione istituzionale dell'organo giudiziario procedente (artt. 8, 47 e 160 d.lg. n. 196/2003).

7.3. Associazioni

Nel 2003 sono pervenute numerose segnalazioni relative all'accesso, da parte di soci o iscritti, a dati personali di altri aderenti ad un ente o associazione.

Dati non sensibili degli associati

Come in passato, l'Ufficio del Garante ha evidenziato che il trattamento dei dati personali non sensibili degli associati è consentito senza il loro consenso quando persegue finalità lecite sulla base di quanto previsto dall'atto costitutivo o dallo statuto dell'associazione o ente, oppure se ricorre uno degli ulteriori presupposti del trattamento equipollenti al consenso, previsti dalla normativa vigente (ad esempio, per adempiere ad un obbligo di legge o per esigenze di difesa di un diritto in sede giudiziaria).

Tale impostazione è stata ribadita dal Codice con riferimento al trattamento dei dati effettuato da associazioni od organismi senza scopo di lucro, anche non riconosciuti, in riferimento agli aderenti ed ai soggetti che con essi hanno contatti regolari (artt. 24, comma 1, lett. *h)* e 26, comma 4, lett. *a),* d.lg. n. 196/2003).

7.4. Dati di traffico: fatturazione dettagliata

Il Garante ha ribadito la piena applicabilità dell'art. 13 della legge n. 675/1996 (ora, art. 7 del Codice) alle informazioni incluse nella fatturazione, trattandosi di dati di carattere personale. In particolare, con una decisione del 30 aprile 2003

l'Autorità, nell'accogliere un ricorso, ha ordinato ad un fornitore di servizi di telecomunicazione di comunicare gratuitamente al ricorrente i dati di traffico "in uscita" con l'indicazione integrale delle cifre dei numeri chiamati, che nel caso di specie erano relativi ad una carta prepagata intestata all'interessato.

Chiamate "in uscita"

Non possono, invece, trovare accoglimento le richieste, rivolte ai gestori telefonici, di conoscere gli estremi identificativi e gli indirizzi dei soggetti cui corrispondono i numeri telefonici riportati nel tabulato delle chiamate "in uscita" (*Provv.* 22 settembre 2003). Esercitando il diritto di accesso, l'interessato può infatti conoscere i dati personali che lo riguardano, ma non può chiedere di acquisire dati e informazioni relativi a terzi, come ora precisa espressamente il Codice (art. 10, comma 5, d.lg. n. 196/2003).

Sempre con riferimento alle chiamate "in uscita", l'Autorità ha precisato che il titolare deve fornire idoneo riscontro soltanto alle istanze di accesso formulate dalla persona cui si riferiscono i dati personali oggetto della richiesta. In un caso è stato, pertanto, ritenuto illecito il riscontro fornito dal titolare ad un'istanza di accesso presentata da una persona che non risultava essere il reale utilizzatore dell'utenza telefonica (*Provv.* 30 dicembre 2003).

Con decisione del 13 novembre 2003, il Garante ha altresì chiarito che l'accesso dell'interessato deve essere garantito anche nei confronti dei dati relativi a chiamate verso numeri a tariffazione speciale (ad es., quelli che iniziano con il prefisso "709").

7.5. Dati di traffico: chiamate in entrata e chiamate di disturbo

La problematica dei giusti limiti da porre all'esercizio del diritto d'accesso ai dati identificativi delle cd. chiamate in entrata ha trovato una soluzione di conferma nel Codice, il quale precisa che l'accesso a tali dati non è previsto per esercitare un diritto in sede civile ed è lecito soltanto quando, omettendo di darne comunicazione, si determinerebbe un pregiudizio "effettivo e concreto" per lo svolgimento delle investigazioni difensive in ambito penale (art. 8, comma 2, lett. *f)*, d.lg. n. 196/2003; l. 7 dicembre 2000, n. 397).

Questa previsione del Codice, come ha nuovamente constatato l'Autorità con una decisione del 18 febbraio 2004, traccia un bilanciamento tra il diritto dell'interessato ad accedere ai dati che lo riguardano e il diritto alla riservatezza di terzi (gli utenti-persone fisiche chiamanti e i soggetti chiamati), circoscrivendo il diritto di accesso alle sole comunicazioni "in entrata" di cui sia realmente necessaria la conoscenza, negando le quali si arrecherebbe un pregiudizio reale per lo svolgimento delle investigazioni difensive, che deve risultare comprovato, in concreto, caso per caso.

Anche con riferimento alle chiamate in entrata, è stato ribadito che il diritto d'accesso può essere esercitato dall'interessato soltanto nei confronti dei dati che lo riguardano. Nel decidere su un ricorso, il Garante ha pertanto dichiarato inammissibile la richiesta volta ad identificare utenze diverse da quella dell'interessato (e le relative coordinate delle chiamate), da cui erano originate alcune chiamate effettuate a nome di quest'ultimo verso il *call-center* di una società di telefonia mobile (*Provv.* 5 novembre 2003).

Riguardo, invece, all'accesso alle chiamate di disturbo, specie quando non sia possibile identificare sull'apparecchio la linea chiamante, il Codice conferma il diritto dell'abbonato di richiedere al fornitore del servizio di rendere temporaneamente inefficace la soppressione dell'identificazione della linea chiamante (e di conservare i dati relativi alla provenienza della chiamata ricevuta) e riconosce espressamente il diritto di venirne a conoscenza (art. 127 d.lg. n. 196/2003).

7.6. Messaggi di posta elettronica indesiderati

Anche al destinatario di messaggi di posta elettronica non sollecitati sono riconosciuti i diritti di cui all'art. 7 del Codice, fra i quali il diritto di conoscere da quale fonte siano stati ricavati i propri dati, di far interrompere in qualsiasi momento la loro ulteriore utilizzazione a fini commerciali o pubblicitari e, ancora, di far cancellare quelli trattati in violazione di legge.

Ferma restando la tutela che su un altro piano, quello penalistico, è data dalla natura di reato dello *spamming* (art. 167 del Codice), l'interessato può, gratuitamente e senza particolari formalità, rivolgere comunque un'esplicita richiesta al mittente del messaggio indesiderato e, ove non riceva un soddisfacente riscontro nel termine di quindici giorni (o di trenta giorni, se sono necessarie operazioni di particolare complessità), può rivolgersi all'autorità giudiziaria ordinaria oppure proporre ricorso al Garante (che resta incompetente riguardo ad eventuali pretese risarcitorie del danno subito).

Accesso ai dati relativi ai terzi

Negli innumerevoli ricorsi esaminati in materia di *spamming* l'Autorità ha peraltro precisato che l'esercizio del diritto di accesso e la successiva proposizione di un ricorso al Garante non sono consentiti con riferimento a dati personali relativi a terzi. Sono stati pertanto dichiarati inammissibili alcuni ricorsi, una volta accertata la loro proposizione da parte di soggetti privi della relativa legittimazione, in quanto si trattava di persone diverse da quelle cui erano riferiti i dati concernenti gli indirizzi di posta elettronica dei quali era stato lamentato l'illecito trattamento (*Provv.* 25 luglio, 5 e 16 dicembre 2003).

7.7. Credito

Con riferimento al trattamento dei dati personali in ambito bancario, un profilo delicato ha riguardato l'esercizio del diritto di accesso ai dati personali di persone decedute, il quale è qui approfondito in un apposito paragrafo (cfr. subito parag. 7.10.).

Gratuità del riscontro all'interessato

Per quanto concerne la disciplina del diritto di accesso dell'interessato ai dati personali che lo riguardano detenuti da istituti di credito, va ricordato che il titolare è tenuto ad assicurare un riscontro gratuito alle richieste di accesso rivoltegli dagli interessati.

In alcune occasioni, taluni istituti di credito hanno invece subordinato tale riscontro al versamento, da parte del cliente, di somme occorrenti per ricercare e mettere a disposizione i documenti richiesti: ciò per far fronte alle spese che gli istituti sostenevano di dover affrontare per il reperimento dei dati e la loro comunicazione all'interessato.

Tale comportamento è stato giudicato illegittimo dal Garante in alcune decisioni su ricorsi (*Newsletter* n. 199, 3-9 novembre 2003; v. anche *Provv.* 10 dicembre 2003) poiché, nel vigore della legge n. 675/1996, il contributo spese poteva essere richiesto all'interessato solo nel caso in cui presso il titolare non fosse risultata confermata l'esistenza di suoi dati personali. Pertanto, si è affermato che l'esercizio del diritto di accesso vantato dal ricorrente doveva essere garantito gratuitamente e non poteva essere condizionato, nelle sue modalità di esercizio, a quanto stabilito, a ben altri fini, dal testo unico in materia bancaria e creditizia (d.lg. n. 385/1993). È stato quindi ordinato alle banche resistenti di estrarre dagli atti e dai documenti da essa detenuti tutte le informazioni personali richieste, concernenti le movimentazioni effettuate, e di comunicarle in breve termine agli interessati in modo intelligibile.

7.8. "Centrali rischi" private

Al Garante sono pervenute ancora numerose richieste da parte di cittadini per il tramite di associazioni e studi legali, indirizzate direttamente o per semplice conoscenza all'Autorità ed aventi ad oggetto l'esercizio dei diritti di cui all'art. 13 della legge n. 675/1996 (ora, art. 7 del Codice) in merito al trattamento dei dati da parte delle "centrali rischi" private. Sul punto si è ribadito che gli interessati possono rivolgersi direttamente al titolare o al responsabile del trattamento dei dati al fine di esercitare i diritti in esame, non risultando indispensabile, nella prima fase di questo interpello, rivolgersi subito al Garante, anche solo per conoscenza.

"Messa in chiaro" dei dati

In numerosi casi, i riscontri forniti alle richieste di accesso rivolte a banche e società finanziarie sono risultati lacunosi, in quanto limitati alla comunicazione dei dati solo per categorie od a un semplice rinvio agli estratti conto forniti mensilmente, senza nessun riferimento alle "centrali rischi". Al riguardo l'Autorità ha ripetutamente invitato le società ad integrare i riscontri già forniti in modo generico, provvedendo alla "messa in chiaro" di tutte le notizie di carattere personale oggetto di trattamento relative anche ai rapporti finanziari con i clienti, pur se provenienti da "centrali rischi". Di queste ultime, infatti, nella modulistica relativa ai contratti di finanziamento anteriori al provvedimento generale del Garante del 31 luglio 2002, spesso non sono indicati i puntuali estremi identificativi e i recapiti.

Credit scoring

Anche il riscontro fornito dalle "centrali rischi" in caso di accesso esercitato direttamente nei loro confronti è risultato in più casi parziale e insoddisfacente. Ad esempio, una società non aveva comunicato, come invece specificamente richiesto dall'interessato, i dati personali detenuti in forma di punteggi sul grado di affidabilità/solvibilità, qualificati genericamente come "indicatori numerici o punteggi diretti a fornire una rappresentazione sintetica, in termini predittivi o probabilistici, del complessivo profilo di rischio di un determinato interessato, della sua affidabilità o solvibilità". Pertanto, la società è stata invitata ad integrare la risposta fornita con riferimento all'integralità dei propri archivi, comunicando tutti gli ulteriori dati personali relativi all'interessato, anche se appunto espressi in forma di punteggio (cd. *credit scoring*, v. *Provv.* 29 dicembre 2003).

7.9. Assicurazioni

In ambito assicurativo, l'Autorità ha ribadito il principio che le informazioni personali comprese nelle valutazioni e negli altri elementi di giudizio riportati nelle perizie medico-legali delle compagnie di assicurazione rientrano nella sfera dei dati

personali e vanno pertanto comunicate all'interessato quando questi ne faccia richiesta: così nel caso del cittadino che, a seguito di un sinistro di cui era rimasto vittima, si era rivolto all'impresa assicuratrice della controparte per avere conferma dell'esistenza di dati personali che lo riguardavano.

L'art. 8, comma 4, del Codice ha, poi, individuato opportune soluzioni in riferimento all'accesso a dati di tipo valutativo, relativi a giudizi, opinioni o altri apprezzamenti di tipo soggettivo, confermando però il diritto di accesso, che trova riconoscimento anche nel successivo regolamento sull'accesso agli atti delle imprese di assicurazione (art. 5 comma 2, d.m. 20 febbraio 2004, n.74).

Comunicazione all'interessato di dati sulla salute

Il Garante aveva inoltre riaffermato in passato che in caso di comunicazione all'interessato di dati che riguardano la sua salute acquisiti nell'ambito di una visita medica dal consulente sanitario della compagnia, tale comunicazione doveva avvenire per il tramite di un medico designato dall'interessato o dalla compagnia assicuratrice titolare del trattamento (*Provv.* 7 maggio 2003; *Newsletter* n. 195, 8-21 dicembre 2003); la questione è ora diversamente disciplinata dall'art. 84 del Codice.

Differimento temporaneo dell'accesso

Per altro verso, la normativa consente ancora al titolare del trattamento di differire temporaneamente l'esercizio del diritto di accesso, per il periodo durante il quale potrebbe derivargli un pregiudizio per lo svolgimento delle cd. indagini difensive o, comunque, per far valere o difendere un diritto in sede giudiziaria (*Provv.* 21 marzo 2003; *Provv.* 29 dicembre 2003). Come già osservato, la valutazione dell'esistenza di un effettivo pregiudizio, tale da giustificare il temporaneo differimento dell'accesso, deve essere effettuata caso per caso sulla base di elementi concreti allegati dal titolare del trattamento o comunque presenti in atti (v. ora art. 8, comma 2, lett. *e)*, del Codice).

7.10. Accesso ai dati di persone decedute

Uno degli aspetti più delicati affrontati nella materia dell'accesso ai dati personali è stato quello dell'accesso ai dati del defunto.

Settore bancario

La questione si è posta in primo luogo, come accennato, nel settore bancario. L'art. 13, comma 3, della legge n. 675/1996, riconosceva tale diritto a chiunque vi avesse interesse: in base a tale disposizione, si è ammesso il diritto degli eredi di accedere ai dati personali del defunto, inclusi eventuali dati riferiti a terzi (ad es., cointestatari del conto corrente o soggetti delegati ad operare sul conto medesimo), nel caso in cui quelli relativi all'interessato e le notizie relative a terzi fossero intrecciati al punto da rendere i primi, se presi isolatamente, incomprensibili, oppure snaturati nel loro contenuto (v. *Provv.* 8 ottobre 2003 e *Provv.* 10 dicembre 2003, che richiamano sul punto il *Provv.* 23 giugno 1998). Al contrario, non poteva essere accolta la richiesta di accesso a dati personali trattati da una banca e riferiti ad una persona deceduta, se volta a conoscere specificamente e direttamente l'identità della persona delegata dal defunto ad effettuare determinate operazioni bancarie (*Provv.* 13 novembre 2003).

La disposizione, come modificata dal Codice (v. l'art. 9, comma 3), specifica ora l'ambito dei soggetti legittimati ad accedere ai dati personali di persone decedute in favore di chi ha un interesse proprio, o agisce a tutela dell'interessato, o per ragioni familiari meritevoli di protezione.

Settore assicurativo

Nel 2003, il Garante è stato chiamato a pronunciarsi sulla questione dell'accesso ai dati relativi al defunto anche in ambito assicurativo: in proposito si è affermato che il diritto di accesso ai dati personali di un defunto non riguarda le informazioni relative a terzi, come ad es. i terzi beneficiari di polizze assicurative (*Provv.* 31 marzo 2003; *Provv.* 22 settembre 2003; *Provv.* 13 novembre 2003): pertanto, sebbene all'erede legittimo spetti il diritto ad accedere a tutte le informazioni personali che riguardano il defunto, non è tuttavia consentito alla società assicuratrice di comunicargli il nome del beneficiario della polizza.

Nei casi a suo tempo esaminati, l'Autorità ha riconosciuto legittima la richiesta di alcuni eredi di accedere ai dati personali riconducibili ai familiari deceduti, benché impropriamente formulata (sul piano della protezione dei dati personali), nella parte in cui si chiedeva l'accesso ad interi documenti detenuti dalle imprese di assicurazioni. La messa a disposizione dell'intera documentazione da parte del titolare del trattamento, in copia o in visione, può essere infatti disposta dal Garante, in applicazione del Codice, qualora sussistano reali, oggettive difficoltà di estrapolazione dei dati richiesti all'interno di documenti, ed avendo comunque cura di oscurare i dati personali eventualmente riferiti a terzi. È stato quindi intimato alle società di estrarre dagli atti e dai documenti detenuti, comprese le eventuali polizze sottoscritte, tutte le informazioni personali relative al defunto, comunicandole in modo intelligibile all'erede legittimo, con esclusione di tutte le informazioni non direttamente riferite al medesimo defunto (e, quindi, nello specifico, non comunicando i dati personali relativi al beneficiario della polizza).

La tematica va ora considerata anche da un diverso angolo visuale, alla luce dell'ulteriore diritto di accesso agli atti delle imprese di assicurazione, disciplinato innovativamente dal già citato d.m. 20 febbraio 2004, n.74.

Un'altra questione ha riguardato la legittimità del rifiuto, opposto da un ufficio delle imposte, di rilasciare copia della dichiarazione dei redditi presentata, a suo tempo, da un parente deceduto del richiedente. In questo caso, il Garante ha riconosciuto al richiedente stesso il diritto di accedere ai dati personali relativi al congiunto deceduto contenuti nella dichiarazione dei redditi di quest'ultimo, ribadendo che tale diritto può essere esercitato da chiunque vi abbia interesse (*Nota* 12 febbraio 2004).

7.11. Giornalismo

Il Garante ha riaffermato il principio in base al quale i diritti di accesso e gli altri diritti ora previsti dall'art. 7 del Codice –esercitabili pure nei confronti degli editori e dei direttori responsabili delle testate giornalistiche (cfr. *Provv.* 26 marzo e 23 aprile 2003)– possono essere fatti valere anche in riferimento a fotografie e ad altri dati personali diffusi attraverso pubblicazioni consultabili via Internet (*Provv.* 8 ottobre 2003 e 8 gennaio 2004).

7.12. Rai

Con la decisione del 19 novembre 2003 è stata dichiarata inammissibile la richiesta dell'interessato volta a conoscere il nominativo della persona incaricata dalla Rai –Radiotelevisione Italiana S.p.A.– di effettuare una visita presso il domicilio dell'interessato stesso nell'ambito delle attività relative alla gestione e riscossione del canone di abbonamento. In proposito, va ricordato che l'art. 7, comma 2, lett. *e)*,

del Codice consente ora, all'interessato, di ottenere dal titolare anche l'indicazione dei soggetti che in qualità di responsabili o incaricati possono venire a conoscenza dei dati che lo riguardano.

8 Cancellazione dei dati

8.1. Cancellazione dei dati trattati dalla pubblica amministrazione

Il diritto ad ottenere la cancellazione dei dati personali trattati da una pubblica amministrazione ha formato oggetto di numerosi ricorsi.

Delibera di giunta comunale

Va ricordata in particolare la decisione su un ricorso con il quale era stata domandata la cancellazione di dati personali contenuti in una deliberazione di giunta comunale, affissa all'albo pretorio, che faceva riferimento ad una controversia in cui era coinvolto il ricorrente (*Provv.* 12 gennaio 2004).

L'Autorità non ha accolto la richiesta dell'interessato, ritenendo la diffusione dei dati che lo riguardavano necessaria allo svolgimento delle funzioni istituzionali dell'ente e conforme alle vigenti disposizioni sullo svolgimento dei procedimenti amministrativi e sulla pubblicazione degli atti (cfr. art. 124 d.lg. n. 267/2000). Nella deliberazione, peraltro, non venivano riportati dati di carattere giudiziario e le informazioni contenute risultavano esatte e non eccedenti rispetto all'esigenza di trasparenza delle deliberazioni comunali. Il Garante ha però riaffermato la necessità di rispettare i principi di pertinenza e non eccedenza, nel bilanciare le esigenze di riservatezza e di trasparenza dell'attività amministrativa.

Quesito referendario

Analogamente, è stata ritenuta infondata la richiesta volta ad eliminare dal testo di un quesito referendario (concernente il progetto di ristrutturazione di una scuola elementare), le generalità del ricorrente, lì indicate in quanto si trattava dell'autore di un progetto che era contestato nella vicenda referendaria. I dati in questione non sono stati ritenuti eccedenti rispetto alla finalità di illustrare l'iniziativa alla popolazione, considerata pure l'esattezza e l'obiettività con cui essi erano stati riportati, come anche l'ampia conoscibilità che queste informazioni avevano già avuto nella comunità locale (*Provv.* 25 settembre 2003).

8.2. Cancellazione dei dati concernenti i comportamenti debitori

La problematica dei limiti entro cui si può ottenere la cancellazione dei dati relativi ai comportamenti debitori si è posta più volte nel periodo considerato, con riferimento sia ai dati personali contenuti in banche dati pubbliche, sia a quelli registrati in banche dati private, "alimentate" peraltro con dati tratti da registri o elenchi accessibili a tutti.

Trascrizione di pignoramenti

Con riferimento all'esercizio dei diritti riconosciuti dalla normativa sulla protezione dei dati nei confronti dei pubblici registri immobiliari, l'Autorità, in una decisione del 30 dicembre 2003, ha affermato che la tutela della riservatezza non può essere invocata per ottenere la cancellazione di una trascrizione di pignoramento

immobiliare in difformità dalle specifiche ipotesi e particolari procedure previste dalla normativa di settore.

Su questa base il Garante ha giudicato infondato il ricorso presentato da un cittadino che lamentava di non aver ricevuto riscontro ad una sua istanza presentata all'Agenzia del territorio, nella quale aveva chiesto l'immediata cancellazione dei dati personali relativi una procedura esecutiva immobiliare promossa nei suoi confronti.

L'art. 2668 c.c. consente all'interessato di presentare domanda per la cancellazione delle trascrizioni quando ritiene che sussistano le condizioni per esercitare questo suo diritto. I competenti uffici possono apporre l'annotazione di cancellazione della trascrizione nel pubblico registro immobiliare solo dopo aver verificato la completezza della documentazione richiesta ed accertato la regolarità formale e sostanziale della domanda stessa.

Nel caso in esame, la richiesta di immediata cancellazione è stata quindi giudicata infondata, poiché non era emerso, da parte dell'Agenzia, un uso dei dati personali difforme dalla disciplina in materia, sia rispetto alle modalità di annotazione e tenuta dei registri immobiliari, sia rispetto alle formalità richieste dalla normativa per la cancellazione delle trascrizioni.

Banche dati private contenenti dati raccolti da elenchi pubblici

Sempre in materia di registri immobiliari, l'Autorità ha esaminato la richiesta di cancellazione di dati personali contenuti non in registri pubblici, bensì in banche di dati create e gestite da società private ed alimentate da informazioni estratte da fonti pubbliche accessibili da chiunque. La vicenda, sollevata in un ricorso, riguarda la problematica della pertinenza e completezza delle informazioni a contenuto economico in rapporto al diritto dell'interessato alla conservazione limitata nel tempo dei dati che lo riguardano, ossia per il tempo necessario al perseguimento delle finalità per le quali i dati stessi sono raccolti e successivamente trattati (art. 9 legge n. 675/1996; ora, art. 11 d.lg. n. 196/2003).

Nella decisione (*Provv.* 22 settembre 2003), il Garante ha ricordato che il trattamento di dati provenienti da pubblici registri può essere effettuato anche in assenza del consenso dell'interessato ed ha richiamato la disciplina introdotta in materia dal Codice, il quale, nel confermare la prossima adozione di un codice deontologico in materia, demanda a quest'ultimo il compito di individuare nuovi limiti temporali di conservazione dei dati relativi al comportamento debitorio (art. 119 d.lg. n. 196/2003).

Nelle more dell'adozione di tali fonti, il trattamento dei dati consistente nell'estrazione e comunicazione di informazioni accessibili a chiunque può ritenersi lecito; di qui l'infondatezza del ricorso, fermo restando il riconoscimento del diritto dell'interessato di ottenere, nei modi di legge, l'integrazione e/o l'aggiornamento delle informazioni che lo riguardano (per es., in ordine ad eventuali sentenze di riabilitazione pronunciate in suo favore).

Omonimie

Con un altro ricorso l'Autorità è stata chiamata a pronunciarsi su una richiesta di cancellazione di dati personali da un pubblico registro, motivata da una pretesa omonimia tra il ricorrente e il soggetto cui si riferivano i dati relativi ad un assegno protestato. Nel caso di specie non è stato possibile accertare inequivocabilmente nel procedimento se i dati riportati nell'elenco dei protestati corrispondessero a quelli

del ricorrente: tuttavia, nel disporre l'apertura di un autonomo procedimento, il Garante ha affermato che la situazione soggettiva dell'interessato doveva ritenersi comunque meritevole di tutela. Pertanto, l'Autorità ha disposto il blocco del trattamento effettuato dalla camera di commercio con riferimento alle informazioni che si contestava essere riconducibili al ricorrente, riservandosi ulteriori accertamenti sul punto (*Provv.* 12 gennaio 2004).

9 Opposizione al trattamento

9.1. Attività tributarie

Con importante decisione del 12 gennaio 2004, e in senso analogo a quanto disposto in passato, l'Autorità ha accolto l'opposizione di un contribuente alla comunicazione, da parte di una concessionaria provinciale del servizio riscossione tributi, di informazioni concernenti la posizione debitoria dell'interessato a terzi con i quali l'interessato stesso aveva intrattenuto rapporti professionali. La comunicazione veniva effettuata tramite l'invio a questi ultimi di una "richiesta di dichiarazione stragiudiziale" circa l'esistenza di eventuali crediti vantati dall'interessato nei loro confronti. Poiché tale particolare procedura è risultata non legittimata da alcuna specifica previsione normativa e non rispondente ai principi di pertinenza e non eccedenza dei dati rispetto alle finalità perseguite, nelle more degli ulteriori accertamenti (in corso) sulla questione è stato disposto, quale misura cautelare, il blocco dei dati oggetto di trattamento (cfr. *infra*, parag. 26.).

Diffusione degli elenchi dei contribuenti

In merito al regime di pubblicità dell'elenco dei contribuenti l'Autorità ha ribadito che non vi è incompatibilità tra la protezione dei dati personali e determinate forme di pubblicità di dati previste per finalità di interesse pubblico o della collettività. In particolare, con decisione del 2 luglio 2003, il Garante ha rilevato che la disciplina contenuta nel d.P.R. n. 600/1973 (art. 69), in base alla quale gli elenchi nominativi dei contribuenti che hanno presentato la dichiarazione dei redditi sono consultabili da chiunque presso alcuni uffici finanziari e i comuni interessati, non è stata abrogata, né modificata dalla disciplina sulle modalità di presentazione e trasmissione delle dichiarazioni per via telematica (d.P.R. 22 luglio 1998, n. 322). Pertanto, l'istanza di opposizione per motivi legittimi alla diffusione dei dati personali contenuti nelle dichiarazioni dei redditi attraverso la pubblicazione degli elenchi in questione non poteva essere accolta, poiché il regime di pubblicità previsto risponde ad una scelta normativa di carattere generale operata per favorire la trasparenza in materia di dati raccolti dalla pubblica amministrazione attraverso le dichiarazioni fiscali

9.2. Attività investigative

In una decisione dell'8 gennaio 2004 l'Autorità ha affrontato la questione della liceità del trattamento di dati personali contenuti nel materiale raccolto nell'ambito di indagini investigative e successivamente prodotto in un procedimento giudiziario.

In proposito, il Garante ha ribadito il principio in base al quale il trattamento dei dati a fini di esercizio di un diritto in sede giudiziaria è ammesso, anche in man-

canza del consenso dell'interessato, soltanto quando risulti strettamente "necessario" per la tutela del diritto esercitato. Una volta conclusa l'attività investigativa, il trattamento deve cessare in ogni sua forma, fatta salva l'immediata comunicazione dei dati al difensore o al soggetto che ha conferito l'incarico.

In particolare, nell'ambito di un procedimento di modifica delle condizioni economiche della separazione consensuale tra coniugi è stata ritenuta illecita la produzione di relazioni investigative e di fotografie, precedentemente commissionate ad un'agenzia d'investigazione, riguardanti una pretesa relazione extraconiugale mai stata oggetto di accertamento giudiziario.

9.3. Condominio

Nel 2003 sono stati esaminati dall'Autorità diversi ricorsi aventi ad oggetto il diritto di opposizione al trattamento di dati personali riguardanti situazioni di morosità di singoli condomini. Al riguardo, è stato ribadito che la normativa sulla protezione dei dati personali non ha modificato la disciplina sul condominio degli edifici prevista dal codice civile (art. 1117 s. c.c.), precisando che il condominio può tuttavia trattare solo i dati pertinenti e non eccedenti rispetto alle finalità di gestione. In particolare, i singoli condomini, che sono contitolari di un unico trattamento di cui l'amministratore ha la concreta gestione, hanno diritto di conoscere le informazioni utili riguardanti l'amministrazione ed il funzionamento del condominio, comprese quelle concernenti posizioni debitorie e creditorie dei condomini nei confronti del condominio stesso.

Comunicazione e diffusione dei dati sulle morosità dei condomini

Così, la comunicazione di informazioni relative alla morosità di un condomino nel corso dell'assemblea di condominio e la successiva trascrizione di queste informazioni in un verbale inviato ai soli condomini è stata giudicata dal Garante conforme ai principi di pertinenza e non eccedenza dei dati raccolti o successivamente trattati (*Provv.* 16 luglio 2003).

L'opposizione alla diffusione (tramite affissione nella bacheca condominiale) di dati personali concernenti presunte posizioni di morosità relative ad alcuni condomini è stata oggetto di un'ulteriore decisione dell'Autorità. In tale occasione, il Garante ha, però, ritenuto infondato il ricorso, in quanto l'istanza di opposizione era stata avanzata al titolare in un momento successivo alla rimozione dell'elenco dei morosi dalla bacheca condominiale (*Provv.* 19 novembre 2003).

I doveri

10 Rapporto di lavoro

Il Codice sulla protezione dei dati personali ha introdotto nel contesto lavorativo importanti novità ispirate, in particolar modo, alla semplificazione di alcuni adempimenti da parte del datore di lavoro. Ad esempio, per i dati sensibili, quando il trattamento è necessario per eseguire specifici obblighi o compiti previsti dalla legge, da un regolamento o dalla normativa comunitaria per la gestione del rapporto di lavoro, anche in materia di igiene e sicurezza del lavoro e della popolazione e di previdenza e assistenza, non è più necessario acquisire il consenso scritto del lavoratore interessato, fermo restando il rispetto dell'autorizzazione del Garante e delle regole che saranno individuate mediante il codice di deontologia in materia di lavoro e previdenza (art. 26, comma 4, lett. *d)*, d.lg. n. 196/2003).

Raccordo con il d.lg. n. 276/2003

A prescindere dagli sviluppi a breve termine di tale codice deontologico, questo nuovo quadro normativo va peraltro raccordato con i recenti mutamenti introdotti dal d.lg. n. 276/2003 in attuazione delle deleghe in materia di occupazione e mercato del lavoro di cui alla legge n. 30/2003 (cd. riforma Biagi).

Sotto questo profilo, assume rilievo, in primo luogo, la previsione di un ulteriore divieto di indagini sulle opinioni e trattamenti discriminatori (art. 10 d.lg. n. 276/2003), sul quale sono già state avanzate all'Autorità richieste di chiarimenti da parte di talune organizzazioni sindacali. Rilevano inoltre la disposizione sull'ambito di diffusione dei dati relativi all'incontro tra domanda ed offerta di lavoro (art. 8 d.lg. n. 276 cit.) e quella sulle comunicazioni a mezzo stampa, Internet, televisione o altri mezzi di informazione (art. 9 d.lg. n. 276 cit.).

In particolare, con quest'ultima disposizione è stato recepito, a livello normativo, il consolidato orientamento dell'Autorità in materia di modalità dell'informativa ai candidati interessati ad una selezione o ricerca di personale, che deve essere in sostanza resa, sin dal momento della pubblicazione degli annunci di lavoro (cfr. *Provv.* 10 gennaio 2002).

Settori di intervento

Tra i diversi settori in cui l'Autorità è dovuta intervenire, vanno ricordati poi: il controllo a distanza dei lavoratori a mezzo di apparecchiature di videosorveglianza; le modalità di custodia e conservazione dei dati dei dipendenti a cura dei datori di lavoro; l'accesso dei lavoratori ai dati che li riguardano.

In relazione al divieto di controllo a distanza dei lavoratori, l'Autorità ha curato vari approfondimenti e si pronuncerà a breve con un provvedimento di carattere generale concernente le verifiche effettuate dai datori di lavoro sull'uso, da parte dei lavoratori, degli strumenti informatici e telematici loro assegnati per ragioni di servizio e, in particolare, sulle navigazioni in Internet e sulla gestione della posta elettronica.

Sul piano del contenzioso al riguardo merita di essere ricordata la delicata questione, portata all'attenzione del Garante, dell'impugnativa (da parte del dipendente

di una banca) di un licenziamento disciplinare motivato dall'uso irregolare delle infrastrutture informatiche fornitegli quali strumenti di lavoro.

In particolare, a fronte della domanda del lavoratore di tutela d'urgenza avverso il licenziamento, la banca ha sostenuto l'assenza di *periculum in mora* per l'avvenuta corresponsione del trattamento di fine rapporto. Tra il materiale probatorio prodotto in proposito, la banca ha tuttavia inserito anche la documentazione di cui aveva la disponibilità in qualità di parte non del rapporto di lavoro, bensì del rapporto di conto corrente che era stato instaurato con il medesimo dipendente.

L'Ufficio ha pertanto deciso di verificare in tempi brevi il rispetto, nel caso di specie, sia dei principi pertinenza e non eccedenza dei dati utilizzati e di liceità e correttezza del trattamento, sia delle norme in tema di informativa, consenso e relativi casi di esclusione (artt. 11, 13, 23 e 24 d.lg. n. 196/2003).

Eguale urgente approfondimento istruttorio è stato disposto sull'avvenuta conoscenza, da parte di alcuni dipendenti della medesima banca, dei dati personali dell'interessato emersi nell'ambito delle attività ispettive svolte nei suoi confronti, nonché sulle misure di sicurezza adottate con riferimento alle informazioni contenute nei documenti ed altri supporti presi in custodia in esito a tali attività.

Vari sono stati, poi, i reclami inviati al Garante da parte di organizzazioni sindacali (in particolare a livello aziendale), in merito all'installazione di impianti di videosorveglianza sul luogo di lavoro. In molti casi (riguardanti, soprattutto, apparecchiature installate a protezione del patrimonio aziendale, ma che riprendono anche postazioni di lavoro dei dipendenti), sono state impartite indicazioni ai datori di lavoro ai fini del pieno rispetto delle vigenti disposizioni in materia e del primo "decalogo" del Garante (v. la parte di *Relazione* inerente alla sorveglianza e ai sistemi biometrici: parag. 37.-38.).

È poi da segnalare, tra gli altri, un caso relativo alla modalità di recapito, da parte di un'azienda, di una comunicazione di contestazione disciplinare al domicilio privato di un dipendente, contenuta in un foglio ripiegato per errore in modo da rendere possibile la conoscenza dell'oggetto della lettera.

Il datore di lavoro è stato richiamato ad impartire precise istruzioni a tutti gli uffici e dipendenti incaricati di analoghi trattamenti di dati, al fine di assicurare una corretta applicazione della disciplina sulla protezione dei dati personali e garantire la riservatezza di comunicazioni contenenti dati relativi ai lavoratori interessati, in particolare per evitare la conoscenza, anche casuale, alle informazioni riportate al loro interno da parte di terzi estranei.

Cedolini delle buste paga

Il Garante è tornato ad occuparsi anche della questione relativa alla modalità di redazione e consegna dei cedolini delle buste paga ai dipendenti. Con decisione del 16 luglio 2003, l'elaborazione e la consegna dei cedolini in busta chiusa sigillata da parte di appositi incaricati del trattamento è stata ritenuta conforme ai principi della disciplina sulla protezione dei dati personali.

Indirizzo *e-mail* aziendale dell'ex dipendente

Infine, il Garante si è pronunciato sull'istanza volta a ottenere la chiusura dell'indirizzo di posta elettronica aziendale attivato a nome di un ex dipendente durante il rapporto di prestazione d'opera con una società. L'Autorità, ritenendo la

richiesta rilevante anche quale sostanziale opposizione per motivi legittimi, ha giudicato soddisfacente il riscontro fornito all'interessato da parte dell'ex datore di lavoro: quest'ultimo aveva infatti creato un nuovo indirizzo *e-mail* ed aveva inserito all'indirizzo dell'interessato un messaggio di risposta automatica che dava comunicazione dell'avvenuta disattivazione della casella di posta oggetto di contestazione (*Provv.* 22 dicembre 2003).

11 Sicurezza dei dati e dei sistemi

E-banking

Nel periodo di riferimento l'Autorità si è occupata di un caso assai significativo per la materia in esame, relativo alla sicurezza dei dati personali concernenti i rapporti bancari con i clienti, trattati da un istituto di credito nell'ambito di servizi di *e-banking*.

Il caso ha suscitato viva attenzione nel settore bancario e spiega effetti rilevanti, come caso pilota, per il livello di futuro sviluppo e di affidabilità dei servizi bancari prestati per via telematica.

È infatti accaduto che un cliente, il quale usufruiva di questi servizi via Internet, dopo un primo accesso ai dati che lo riguardavano, ricollegandosi a distanza di poco tempo al sito per controllare nuovamente la propria posizione contabile, si è trovato accidentalmente a consultare anche *file* relativi a conti correnti di altri clienti. I dati in tal modo visualizzati e memorizzati in appositi prospetti riguardavano operazioni bancarie, inclusi i numeri di conto corrente o delle carte di pagamento utilizzate per effettuare le singole transazioni (nonché, a volte, i dati dei relativi titolari), e recavano l'indicazione del pagamento di utenze domiciliate, tasse, imposte e persino emolumenti erogati da datori di lavoro. In molti casi le informazioni riguardavano anche familiari dei titolari dei conti correnti oggetto dell'accidentale consultazione, nonché terzi con i quali i correntisti avevano effettuato singole transazioni bancarie.

La banca ha fornito alcune giustificazioni sostenendo, tra l'altro, che l'unico caso di accesso indebito era stato quello oggetto di segnalazione, e che esso si era verificato solo per un breve arco temporale.

Il Garante, a conclusione di complesse verifiche, ha invece rilevato che l'erronea configurazione del sistema e dei programmi per l'accesso al servizio di *e-banking* aveva violato l'obbligo di garantire la riservatezza dei dati personali relativi a numerosi clienti e la loro protezione da accessi non autorizzati, con un abbassamento della sicurezza del sistema al di sotto della soglia minima di tutela prescritta dalla legge, rilevante non solo sul piano dell'eventuale responsabilità civile, ma anche a livello penale.

Nel caso di specie, inoltre, l'indebita comunicazione a terzi dei dati dei correntisti, realizzata mediante la messa a disposizione di informazioni caratterizzate da un'elevata confidenzialità (soprattutto in considerazione del rischio di utilizzo abusivo o illecito degli stessi dati da parte di terzi), ha configurato una violazione del cd. segreto bancario, inteso come obbligo per la banca di mantenere il riserbo su operazioni, conti e posizioni degli utenti dei servizi bancari.

Per prevenire il ripetersi delle violazioni contestate, il Garante ha segnalato alla banca l'esigenza di aggiornare l'analisi dei rischi connessi alla prestazione dei servizi di *e-banking*, in modo da adottare preventivamente misure di sicurezza idonee a garantire un livello di protezione elevato dei dati accessibili attraverso tali servizi. L'Autorità ha inoltre prescritto alla banca di verificare e di confermare l'utilizzo di codici identificativi personali e parole chiave da parte sia dei dipendenti incaricati, sia degli utenti del servizio di *e-banking*; ha poi disposto contestualmente la comunicazione all'autorità giudiziaria penale di copia degli atti. Da ultimo, a seguito dell'adempimento alle prescrizioni impartite, la banca è stata ammessa dall'Ufficio del Garante al pagamento di una somma pari al quarto del massimo dell'ammenda stabilita per la contravvenzione, con conseguente dichiarazione di estinzione del reato, in conformità alla normativa vigente (cfr. ora l'art. 169 del Codice).

L'attivazione di analoghi accertamenti si è poi resa necessaria in altri due casi riguardanti la sicurezza dei dati degli utenti trattati da società concessionarie del servizio di erogazione dell'energia elettrica e del gas, mediante l'installazione di contatori per il monitoraggio dei consumi della clientela, il cui procedimento è in procinto di essere concluso.

Alla fine del 2003 sono stati inoltre instaurati alcuni procedimenti relativi alle misure adottate da datori di lavoro per la custodia di comunicazioni contenenti dati personali di lavoratori, al fine di renderne il contenuto inaccessibile ad eventuali terzi estranei alle vicende oggetto di comunicazione o di contestazione.

Da ultimo, va ricordato che, a chiarimento del nuovo quadro normativo in materia di misure di sicurezza introdotto dal Codice, e alla luce dei numerosi quesiti e richieste di proroga inviate da molte imprese, il Garante ha predisposto apposite istruzioni.

Codice e misure di sicurezza: le istruzioni del Garante (Nota 22 marzo 2004)

In particolare, il 22 marzo scorso il Garante ha fornito diverse indicazioni sui tempi e sulle modalità per una corretta applicazione delle novità normative introdotte dal Codice in materia di "misure minime" per la sicurezza dei dati e dei sistemi informatici.

L'Autorità ha sottolineato come il Codice abbia confermato la disciplina in materia di sicurezza dei dati personali introdotta nel 1996, ribadendo il principio in base al quale le "misure minime", la cui mancata adozione costituisce reato, sono solo una parte degli accorgimenti obbligatori in materia di sicurezza. Vi è, infatti, il dovere più generale, rilevante anche sul piano della responsabilità civile, di custodire i dati personali per contenere il più possibile il rischio che essi siano distrutti, dispersi, trattati in modo illecito, ovvero che diventino conoscibili fuori dei casi consentiti, come pure il dovere di introdurre ogni utile dispositivo di protezione legato alle nuove conoscenze tecniche.

L'elenco delle "misure minime" di sicurezza è stato aggiornato dal Codice, il quale ha specificato alcune modalità di applicazione in un apposito disciplinare tecnico. Analogamente a quanto avveniva in passato, le "misure minime" sono diverse a seconda che il trattamento sia effettuato o meno con strumenti elettronici, nonché a seconda che riguardi o meno dati sensibili o giudiziari.

Premesso che le "misure minime" obbligatorie anche in passato, devono essere ulteriormente mantenute senza attendere il decorso di termini transitori, in considerazione delle novità introdotte il Codice ha invece stabilito che, in sede di prima applicazione

del mutato quadro normativo, le nuove misure possono essere adottate entro il 30 giugno 2004. Un periodo più ampio per l'adeguamento (1° gennaio 2005) è previsto solo nel caso particolare in cui ricorrano obiettive e documentate ragioni di natura tecnica, che non consentano di installare immediatamente le nuove misure rispetto agli elaboratori e ai programmi utilizzati.

Il documento programmatico sulla sicurezza (Dps)

Con la recente comunicazione, l'Autorità ha ricordato che tra le "misure minime" di sicurezza rientra anche la redazione del documento programmatico sulla sicurezza (Dps) da parte dei soggetti che effettuano un trattamento di dati sensibili o giudiziari con l'ausilio di strumenti elettronici.

Si tratta di una misura non nuova; tuttavia, è cambiato parzialmente il contenuto del documento ed è aumentato il numero dei casi e dei soggetti destinatari dell'obbligo.

Proprio per questi motivi il Garante ha ritenuto che, solo in sede di prima applicazione della nuova disciplina, il Dps possa essere predisposto al più tardi entro il 30 giugno 2004: ciò permetterà di utilizzare il modello base semplificato predisposto dall'Autorità per effettuare, soprattutto presso realtà medio-piccole, l'analisi dei rischi che incombono sui dati personali, per individuare gli accorgimenti da adottare al fine di prevenire la loro distruzione o eventuali accessi abusivi e per pianificare gli interventi formativi nei riguardi del personale.

Dal 2005, decorso il periodo transitorio connesso all'entrata in vigore del Codice, il termine per redigere annualmente il Dps aggiornato rimarrà fissato ad un'unica scadenza, quella del 31 marzo di ogni anno, come dispone la regola tecnica n. 19 che disciplina tale misura.

Obbligo di riferire della redazione o aggiornamento del Dps

Il Garante ha inoltre precisato le modalità da seguire per l'attuazione di un'altra rilevante "misura minima" introdotta dal Codice, quella relativa all'obbligo di riferire, nella relazione di accompagnamento al bilancio di esercizio, dell'avvenuta redazione o aggiornamento del Dps. Questa misura, diretta a sensibilizzare e responsabilizzare gli organi di vertice aziendali o amministrativi sulla programmazione annuale degli adempimenti in tema di sicurezza, deve essere rispettata già nel 2004. Per questo primo anno, si è considerato il menzionato regime transitorio e la circostanza che alcuni soggetti non erano tenuti a redigere o aggiornare il Dps in base alla legge n. 675/1996. Sono state fornite varie indicazioni relative ai singoli casi, che si possono sintetizzare nel seguente specchietto riassuntivo che è stato accluso alla risposta data a Confindustria, Confcommercio e a diversi altri operatori pubblici e privati:

Disposizioni transitorie

Termini	Adempimenti
30 giugno 2004	Adozione per il 2004 di tutte le "misure minime" non previste dalla precedente disciplina. Termine ultimo di predisposizione del documento a data certa per descrivere le obiettive ragioni tecniche che non consentono di applicare immediatamente alcune nuove "misure minime" *(documento utilizzabile unicamente nel caso del tutto particolare previsto dall'art. 180, comma 2, del Codice per i soli strumenti elettronici).*
1° gennaio 2005	Adozione nuove "misure minime" su strumenti elettronici non previste in base alla precedente disciplina (solo per i soggetti legittimati a predisporre il predetto documento a data certa).

Relazione accompagnatoria del bilancio esercizio 2003

Misure	Soggetti già tenuti a redigere o aggiornare il Dps [1]	Soggetti non obbligati a redigere o aggiornare il Dps in base alla previgente disciplina
Dps 2004	Aggiornamento Dps entro il 30 giugno 2004	Redazione Dps entro il 30 giugno 2004
Relazione accompagnatoria del bilancio esercizio 2003	Riferimento al Dps redatto o aggiornato nel 2003 (con facoltà di indicazione aggiuntiva dell'aggiornamento 2004 *in itinere*), oppure menzione dell'aggiornamento eventualmente già effettuato nel 2004	Nessun riferimento se il Dps 2003 o il Dps 2004 non sono stati adottati, oppure riferimento al Dps eventualmente già adottato nel 2004. Facoltà di indicazione del Dps eventualmente predisposto nel 2003 e facoltà di indicazione dell'aggiornamento 2004 *in itinere*

Ulteriori indicazioni pratiche sono state fornite nel corso della prima edizione del ciclo di seminari di formazione curati dal Garante presso la propria sede (2 aprile 2004) e nel *Cd-Rom* multimediale in fase di predisposizione con i materiali del seminario.

12 Notificazione

Casi sottratti alla notificazione: il provvedimento del 31 marzo 2004

Con il provvedimento del 31 marzo 2004 (pubblicato in *G.U.*, Serie generale, 6 aprile 2004, n. 81 e che è riportato tra gli allegati di questa *Relazione*), il Garante ha individuato i trattamenti di dati personali che non sono oggetto di notificazione all'Autorità, in conformità a quanto stabilito dall'art. 37, comma 2, del Codice.

Come è stato già evidenziato, quest'ultimo ha introdotto una robusta semplificazione in argomento, individuando alcune specifiche categorie di trattamento per le quali vige l'obbligo di notificare preventivamente all'Autorità l'avvio di un trattamento di dati.

Fin dalle prime settimane di applicazione del Codice, e in vista del termine transitorio del 30 aprile 2004 per la presentazione delle notificazioni, il Garante ha ritenuto necessario individuare nuove semplificazioni che interessano, a date condizioni, imprese, enti locali, operatori sanitari (in particolare medici di medicina generale e pediatri), liberi professionisti, datori di lavoro e gestori di impianti di videosorveglianza.

Con tale provvedimento il Garante ha recepito diversi suggerimenti formulati, in questi primi mesi di vigenza del Codice, da alcuni operatori e associazioni di categoria, ravvisando che i trattamenti effettuati nelle predette ipotesi, specialmente in ragione delle relative modalità, potessero essere sottratti all'obbligo di notificazione, ferma restando, ovviamente, l'osservanza degli ulteriori principi ed obblighi previsti dal Codice.

(1) Titolari di un trattamento di dati sensibili o relativi a provvedimenti giudiziari di cui agli artt. 22 e 24 della legge n. 675/1996, effettuato per mezzo di elaboratori accessibili mediante una rete di telecomunicazione disponibili al pubblico