

elevatissimo numero di soggetti (tutto il sistema imprenditoriale che viene censito per offrire informazioni sulla solidità e affidabilità delle imprese a chi a vario titolo deve operare con le stesse) dove la precisione e la completezza delle informazioni hanno un valore essenziale, poiché un dato errato può compromettere, a volte, la stessa sopravvivenza sul mercato di un operatore. È innegabile, però, la complessità della materia e la conseguente difficoltà di una *reductio ad unitatem* della stessa.

Se infatti i Sic sono caratterizzati da una sostanziale omogeneità di dati (rapporti finanziari riconducibili al cd. “credito al consumo” concessi alla platea dei consumatori-persone fisiche), il settore delle informazioni commerciali, da una parte, fa riferimento ad un *target* più limitato (le imprese commerciali) dall'altra, però, associa a tale platea una quantità di informazioni eterogenee (ad es., fatte dal registro delle imprese, dagli archivi dei tribunali concernenti le procedure fallimentari, dal catasto, dal registro dei protesti) che scontano una disciplina di riferimento diversa, nonché modalità di trattamento e tempi di conservazione differenziati, anche in ragione delle funzioni diverse cui i vari archivi sono funzionalmente preposti. Ne deriva l'esigenza di fare chiarezza, apprestando una serie di regole condivise che contemperino la necessità di informazioni sempre più estese e complete che viene dal sistema economico e finanziario e l'obbligo di assicurare che i dati siano esatti, completi, aggiornati, qualitativamente significativi.

In questo quadro si collocano le iniziative del Garante per giungere alla redazione di un codice deontologico di settore, che hanno incontrato il favore degli operatori, ma che sicuramente scontano la difficoltà di un quadro normativo instabile. È di tutta evidenza che le già segnalate modifiche alle nozioni base di “dato personale” e di “interessato”, incidendo sulla collocazione, nel sistema *privacy*, delle società commerciali, hanno di fatto precluso la possibilità di estendere la disciplina deontologica a quel complesso di *report e dossier* esplicitamente riferiti a società ed enti pubblici e privati di ogni tipo. Ma suscitano perplessità i recenti tentativi, in sede parlamentare, di sottrarre all'ambito di applicazione del Codice anche i trattamenti di dati concernenti le persone fisiche preposte ai ruoli di vertice nelle gerarchie societarie.

Trattamenti in  
ambito  
assicurativo

Nel settore assicurativo l'esame del contenzioso fa emergere il delicato ruolo di equilibrio del Garante di contemperamento fra contrastanti interessi: nel caso di specie, da un lato, il

diritto di accesso rivendicato dagli interessati cui i dati si riferiscono, dall'altro le esigenze di tutela delle compagnie di assicurazione.

È tipica infatti della dinamica dei rapporti assicurativi la contrapposizione fra i soggetti che hanno subito danni, o che comunque chiedono risarcimenti, e le compagnie chiamate all'eventuale liquidazione di tali richieste.

Nell'intreccio di questi rapporti, inevitabilmente conflittuali, si inseriscono acquisizione di informazioni e testimonianze, raccolta di dati medici, svolgimento di perizie medico-legali, tutte operazioni che comportano un esteso utilizzo di dati sensibili e, a volte, giudiziari.

È evidente che, nel momento in cui le reciproche posizioni o pretese non trovano una composizione bonaria e sfociano in una vertenza giudiziaria o anche solo in una dialettica pre-contenziosa, la tempestiva disponibilità di determinati dati personali può assumere un rilievo determinante per l'esito di una vertenza. Perciò tutela (o meglio possibilità di disporre) dei dati di un interessato e necessità di non compromettere le esigenze difensive e processuali del titolare del trattamento (che ha interesse non a nascondere o distruggere certe informazioni, ma sicuramente a differirne l'ostensione in un momento processualmente propizio) si confrontano e si scontrano, anche davanti all'Autorità.

È un contrasto inevitabile, in qualche modo preventivato dallo stesso legislatore che, nell'art. 8 del Codice, ha ipotizzato la possibilità di invocare, da parte del titolare del trattamento, il differimento dell'accesso ai dati proprio nell'ipotesi in cui il "disvelamento" delle informazioni determini "*un pregiudizio effettivo e concreto per lo svolgimento delle investigazioni difensive o per l'esercizio del diritto in sede giudiziaria*". Da ciò la necessità di effettuare un'attenta valutazione in concreto, per verificare l'esistenza di questi elementi "escludenti" il normale esercizio del diritto di accesso (prov. 8 marzo 2012 [doc. web n. 1889056]). Senza dimenticare che l'art. 8, comma 4, più radicalmente esclude dall'ambito di applicazione della disciplina l'indicazione di decisioni in via di assunzione da parte del titolare del trattamento o considerazioni a carattere difensivo o di strategia contrattuale o processuale, magari espresse in pareri resi dai legali di fiducia o da qualche consulente incaricato (prov. 29 novembre 2012 [doc. web n. 2286291]).

Trattamenti di dati  
in ambito bancario

Come già detto, il settore bancario ha visto la presentazione del più elevato numero di ricorsi, specie in relazione all'esercizio del diritto di accesso. In qualche modo, l'utilizzo di tale diritto ha prima affiancato e poi quasi surclassato gli strumenti di tutela previsti dal Testo unico bancario (T.u.b.). Tale fenomeno ha determinato qualche incomprensione e qualche confusa sovrapposizione fra le diverse previsioni, in relazione alle quali il Garante è dovuto più volte intervenire per chiarire i diversi ambiti di applicazione. In particolare, dinanzi all'Autorità può essere fatto valere solo il diritto di accesso ai dati personali riferiti all'interessato/ricorrente, che non deve essere confuso con l'accesso a documenti bancari disciplinato dall'art. 119 del citato T.u.b. (prov. 20 settembre 2012 [doc. web n. 2106524]). In questo quadro va ricordata l'inammissibilità di richieste di accesso volte soprattutto a conoscere dati di terzi (ad es., beneficiari di determinate operazioni bancarie), oppure ad acquisire la copia di documenti che in realtà non contengono neppure dati personali (ad es., prospetti informativi relativi alla quotazione in borsa di una società), oppure richieste finalizzate ad ottenere un'aggregazione di dati, anche personali, non nelle forme in cui gli stessi risultano conservati negli archivi del titolare, ma secondo criteri e modalità suggeriti dalle particolari esigenze del richiedente.

Merita poi di essere considerato il profilo relativo all'onere connesso al riscontro delle predette richieste di accesso. Al riguardo si deve ricordare che tali richieste devono essere riscontrate gratuitamente, senza addossare all'interessato oneri previsti per altri tipi di operazioni e servizi bancari (prov. 26 luglio 2012 [doc. web n. 2104639]). Il tema viene spesso riproposto visto che, in effetti, questo tipo di richieste si sta diffondendo e a volte la loro estensione temporale e la loro complessità determina, da parte degli istituti di credito, l'impiego di mezzi e risorse non indifferenti.

Va infine posta attenzione ai tempi di conservazione dei dati. Le richieste formulate nei confronti degli istituti di credito sono infatti caratterizzate da un'ampia profondità temporale, nel tentativo, sotteso a molte istanze, di ricostruire integralmente i rapporti con una banca fin dall'instaurazione del rapporto. Va però ricordato che non è prevista una conservazione per un tempo indefinito dei dati e delle informazioni bancarie (situazione che si porrebbe in evidente contrasto con il principio generale di conservazione limitata nel

tempo di cui all'art. 11, comma 1, lett. e), del Codice). Anzi esiste, sulla base di specifici obblighi normativi, la previsione di un termine decennale di conservazione che rappresenta, quindi, il limite massimo di tempo rispetto al quale formulare un'istanza di accesso.

Come già segnalato (cfr. *supra* par. 18.1.) ormai l'attenzione e la sensibilità degli interessati si rivolgono sempre più spesso nei confronti dei periodici *online* o comunque delle nuove forme di manifestazione del pensiero disponibili sulla rete (*blog, forum* di discussione, siti internet della più varia natura ed altro). È un terreno nuovo, in larga misura inesplorato, sul quale ancora una volta il Garante è chiamato a fare da apripista, in qualche misura anche in vista della eventuale definizione di adeguati parametri legislativi (problema che peraltro non riguarda solo l'Italia, poiché le incertezze al riguardo dominano il dibattito a livello mondiale). In questo quadro già complesso ha determinato un effetto moltiplicativo delle problematiche la rapida diffusione degli archivi *online*, che permettono di disporre permanentemente e di accedere con semplicità (tramite i motori di ricerca generalisti) alle raccolte complete dei quotidiani e dei periodici di informazione, con una profondità temporale addirittura di decenni, che permette quindi di riportare ad attualità anche il più lontano passato. È evidente infatti che, in questa situazione, alcuni valori, tutti costituzionalmente rilevanti, entrano in forte tensione e tendono a confliggere. Dalla libertà di manifestazione del pensiero e in particolare dall'esercizio del diritto di cronaca e di critica che aveva ispirato *ab origine* determinate pubblicazioni (gli articoli originari, spesso risalenti nel tempo, che, in ipotesi, contengono informazioni delicate, negative, sgradite...) al diritto di libera ricerca, in particolare storica, fondato sulla possibilità di disporre di archivi quanto più estesi e completi (che ovviamente si avvantaggia di tecnologie che permettono comodamente e gratuitamente l'accesso ad archivi di tali dimensioni) fino al contrapposto interesse di tanti soggetti citati nella miriade di articoli messi in rete che ben possono ricevere nocumento da questa sorta di "ripubblicazione virtuale permanente" e che aspirano quindi a veder riconosciuto quel "diritto all'oblio" che nell'era di internet presenta profili particolarmente problematici.

Fin dal 2009 (come segnalato anche nelle precedenti Relazioni annuali) il Garante ha individuato una possibile soluzione nella cd. "deindicizzazione", dai motori di ricerca generalisti, di quelle informazioni che, volta a volta, sulla base di un'accurata analisi del caso

Trattamento dei  
dati in ambito  
giornalistico

specifico, potevano incidere in modo effettivamente sproporzionato sui diritti degli interessati citati nelle cronache giornalistiche. Tutto ciò tenendo conto di alcuni criteri di ragionevolezza e buon senso ricavati dall'ampia casistica che si è presentata in questi anni (attenzione alle richieste delle persone non note, delle vittime di reato, dei terzi incidentalmente citati; valutazione del tempo trascorso dalla vicenda narrata e della posizione di notorietà o meno, nell'ambito geografico di riferimento della testata giornalistica, della persona citata e soprattutto accertamento sulla attuale persistenza di elementi che giustificano tuttora un'ampia divulgazione di notizie pur datate). Il panorama è complesso e difficilmente suscettibile in schemi di carattere generale, sicché il Garante ha preferito procedere caso per caso senza elaborare, fino a questo momento, linee di condotta predefinite e astratte.

Anche il 2012 ha portato significative decisioni in merito (provvti 4 ottobre 2012 [doc. web n. 2108032] e 18 ottobre 2012 [doc. web n. 2130029]), ma soprattutto ha indotto l'Autorità a deliberare su un profilo diverso e per certi aspetti ulteriore rispetto a quello fin qui analizzato. Sono infatti pervenuti diversi ricorsi nei quali la richiesta volta ad ottenere che un determinato articolo non venisse più indicizzato dai motori di ricerca esterni al cd. "sito sorgente" (normalmente quello dell'editore di una testata giornalistica dotato di un archivio storico *online*) veniva accompagnata o da una richiesta di cancellazione integrale dell'informazione dal sito web dello stesso giornale, o da una parallela richiesta di integrazione e aggiornamento dell'informazione a suo tempo fornita.

Sono evidenti le implicazioni delicate e significative di questo nuovo "fronte". Per quanto concerne il primo aspetto, non può sfuggire l'effetto che una cancellazione "totale" di una notizia può apportare sull'integrità di una fonte, sulla completezza e sulla ricostruibilità di una pubblicazione storicamente avvenuta, specie quando la stessa dovesse essere disponibile esclusivamente in formato digitale. È chiaro quindi che interventi di "rimozione" devono trovare una base giuridica e una giustificazione fondata. Sono parametri che, ad esempio, non si riscontrano quando le informazioni riportate sono veritiere, i fatti sono recenti e la vicenda narrata (magari di tipo processuale) è ancora in corso e suscettibile di ulteriori sviluppi e aggiornamenti (provv. 8 marzo 2012 [doc. web n. 1887094]).

Non meno delicato è il secondo problema (quello dell'aggiornamento di una notizia) che inevitabilmente comporta riflessi su normative e competenze che eccedono il terreno esclusivo della protezione dei dati personali. Sicuramente le ipotesi sulle quali si è focalizzata l'attenzione non sono quelle nelle quali si voglia discutere di una "rettifica" di una notizia pubblicata, profilo per il quale la legge sulla stampa ha apprestato strumenti utilizzabili (almeno in riferimento alle testate giornalistiche registrate) né quelle nelle quali si faccia questione di lesioni all'onore e alla reputazione di un soggetto, profili questi che rimandano al giudice penale o all'attivazione di azioni risarcitorie in sede civile.

Gli aspetti che hanno coinvolto direttamente il Garante riguardano piuttosto l'esercizio di quei diritti (integrazione e aggiornamento dei dati) che rientrano pienamente nel campo di applicazione della legge sulla protezione dei dati personali. Si tratta di situazioni nelle quali la deindicizzazione degli articoli in questione dai motori di ricerca generalisti era già stata effettuata, ma il ricorrente aveva messo in luce la necessità di aggiornare le cronache comunque disponibili in modo integrale nel cd. "sito sorgente", alla luce dei rilevanti sviluppi che la vicenda in origine raccontata aveva avuto, ma che non erano stati oggetto di successiva cronaca giornalistica.

La situazione è abbastanza tipica di quei casi di cronaca giudiziaria che, per le più varie ragioni, godono, nella fase iniziale, da parte dei *mass media*, di una grande attenzione, che però generalmente tende a sfumare con l'andare del tempo e non segue pertanto molte vicende fino alla loro conclusione. Le conseguenze sulla vita e sull'identità personale degli interessati, nonché sul loro profilo professionale sono chiaramente pesanti, specie quando si tratta di professionisti affermati o di persone attive nel campo economico-finanziario, ambiti nei quali la reputazione personale è un valore non negoziabile.

È significativo che il tema sia stato oggetto nello stesso periodo di un importante pronunciamento della Corte di Cassazione che con la sentenza n. 5525/2012 ha affrontato la medesima problematica, sottolineando la necessità di dar conto di successive evoluzioni di una vicenda già oggetto di cronaca giornalistica. Ciò perché non si può prescindere dall'informazione su tali sviluppi *"giacché altrimenti la notizia, originariamente completa e vera, diviene non aggiornata risultando quindi parziale e non esatta, e pertanto sostanzialmente non*

*vera*”. Anche ispirandosi a questo importante pronunciamento, il Garante in due occasioni ha accolto ricorsi aventi ad oggetto la richiesta di aggiornare, sulla base di significativi sviluppi avvenuti *medio tempore*, gli articoli (già deindicizzati) presenti sul sito di un’importante testata giornalistica. In particolare si è ordinato all’editore resistente di predisporre un idoneo sistema nell’ambito dell’archivio storico *online* in cui gli articoli sono conservati per segnalare, appunto (ad es., con un’annotazione a margine dei singoli articoli) l’esistenza del “seguito”, o dello “sviluppo” della notizia, in modo da assicurare, da un lato, all’interessato il rispetto della propria (attuale) identità personale, quale risultato della completa visione di una serie di fatti che lo hanno visto protagonista (anche se solo in parte oggetto di cronaca giornalistica), dall’altro, ad ogni lettore, un’informazione attendibile e completa (provv.ti 20 dicembre 2012 [doc. web n. 2286432] e 24 gennaio 2013 [doc. web n. 2286820]).

È evidente che decisioni di questa portata devono essere sottoposte ad un vaglio critico attento, specie tenendo conto delle difficoltà della loro esecuzione (basti pensare ad ipotizzabili dispute sui contenuti concreti delle integrazioni da effettuare, o alle ipotesi in cui non sia chiaramente desumibile, da atti e documenti, l’esistenza stessa di un reale aggiornamento di cui dar conto). Al riguardo potrebbe essere utile esaminare la tematica in un confronto aperto, in particolare, a giornalisti ed editori, per “gestire” quello che, prima di essere un problema di contenzioso, è in realtà una nuova frontiera dell’informazione.

## **19. IL CONTENZIOSO GIURISDIZIONALE**

### **19.1. CONSIDERAZIONI GENERALI**

Come riferito nella Relazione 2011 (p. 161), l'art. 34 del d.lgs. n. 150/2011 ha abrogato l'art. 152 del Codice -con l'eccezione del comma 1- dettando all'art. 10 nuove regole procedurali concernenti le controversie sull'applicazione del Codice.

È stato altresì abrogato il comma 7 dell'art. 152, che prevedeva esplicitamente l'obbligo della notifica al Garante dei ricorsi proposti direttamente davanti all'autorità giudiziaria, non coinvolgenti le pronunce dell'Autorità.

Tale abrogazione ha fatto sentire i suoi effetti negativi sul numero delle notifiche relative a tale tipologia di giudizi effettuate al Garante, che in alcuni casi l'autorità giudiziaria ha continuato a ritenere necessarie; a fronte dei 170 nel 2011, nel 2012 sono stati notificati all'Autorità e da questa trattati 78 ricorsi.

Attesa la accertata utilità della tutela giurisdizionale del diritto alla protezione dei dati personali in alternativa al ricorso presentato in sede amministrativa al Garante, attestata dal costante aumento del numero delle notifiche all'Autorità effettuate negli anni precedenti, assume sempre maggiore rilevanza 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).

Tale trasmissione, unitamente alle notifiche dei ricorsi proposti direttamente davanti al giudice che l'autorità giudiziaria riterrà necessarie, potrà consentire al Garante di continuare ad avere conoscenza dell'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).

### **19.2. I PROFILI PROCEDURALI**

L'art. 152 devolve tutte le controversie riguardanti l'applicazione del Codice all'autorità giudiziaria ordinaria (comma 1), con ricorso da depositare nella cancelleria del tribunale del luogo ove risiede il titolare del trattamento (art. 10, comma 2, d.lgs. n. 150/2011).

In particolare, il comma 3 dell'art. 10 del d.lgs. n. 150/2011, riportando pedissequamente il testo dell'abrogato art. 152, comma 3, del Codice, ricomprende in dette controversie quelle proposte avverso i provvedimenti del Garante.

Nonostante tale chiara attribuzione di competenza, è stata proposta un'opposizione davanti al Giudice di pace di Milano avverso un atto istruttorio adottato dal Garante nell'ambito di un procedimento su ricorso proposto ai sensi dell'art. 145 del Codice, con il quale l'istante aveva avanzato richiesta di accesso ai dati relativi al nominativo del soggetto che aveva richiesto l'emissione di un assegno circolare. In giudizio, l'Autorità aveva eccepito l'incompetenza sia funzionale sia territoriale del giudicante, essendo competente il Tribunale di Torino, ove ha sede l'istituto di credito titolare del trattamento. Con la sentenza n. 100.029 del 7 gennaio 2013, con cui ha respinto l'opposizione, il Giudice di pace ha invece ritenuto sussistente la propria competenza, sul rilievo che l'attore non era cliente della banca, ma solo giratario dell'assegno.

In tema di giurisdizione, analogamente a quanto accaduto nel 2011, nel 2012 l'Autorità non ha avuto notizia di ricorsi concernenti il trattamento dei dati personali proposti avanti al giudice amministrativo.

Non si sono altresì riscontrate pronunce che hanno dichiarato un difetto di competenza per materia.

È giunto invece a conclusione il procedimento introdotto dal ricorso straordinario al Presidente della Repubblica nei confronti del provvedimento del 22 dicembre 2009 [doc. web n. 1695144], con il quale l'Autorità aveva respinto il ricorso con cui l'interessato aveva chiesto la cancellazione di dati sensibili riportati in una nota contenuta nel suo fascicolo personale detenuto dal Ministero dell'interno. Confermando l'orientamento precedentemente espresso (sez. prima, n. 4468/2007, v. Relazione 2008 p. 210; sez. prima, n. 3754/2009, v. Relazione 2009 p. 230), il Consiglio di Stato ha ritenuto il ricorso inammissibile (sez. prima, n. 170/2011; v. d.P.R. del 29 ottobre 2012), in quanto avverso atti dell'amministrazione oggetto di tutela giurisdizionale, quale quella prevista dall'art. 152 del Codice, qualificabile come esclusiva e funzionale.

### 19.3. I PROFILI DI MERITO

Nel 2012 l'autorità giudiziaria ha emesso alcune pronunce, nell'ambito di giudizi nei quali non erano in discussione provvedimenti adottati dal Garante, con riferimento alla divulgazione di dati personali di natura sensibile da parte di una pubblica amministrazione ed al loro trattamento da parte di alcuni istituti di credito.

I ricorrenti, beneficiari di prestazioni indennitarie, contestavano, in particolare, il riferimento da parte dell'ente pubblico erogatore, nella causale di accredito dei fondi ricevuti, al titolo giustificativo costituito dalla l. n. 210/1992 (relativa all'indennizzo a favore dei soggetti danneggiati da complicanze di tipo irreversibile a causa di vaccinazioni obbligatorie, trasfusioni e somministrazioni di emoderivati) e la detenzione di tale dato da parte delle banche ove erano stati aperti i conti. Gli istanti chiedevano l'inibitoria della divulgazione di dati personali sensibili e il risarcimento dei danni subiti.

Nel rigettare le domande, il Tribunale di Napoli ha escluso che l'ente pubblico abbia illecitamente propagato i dati sensibili portandoli a conoscenza di soggetti indeterminati, essendosi invece limitato a trasmetterli attraverso una rete informatica ad accessibilità ristretta ad un unico soggetto, ovvero l'istituto di credito che, sulla base del contratto di conto corrente riveste il ruolo, unitamente all'ente pubblico, di titolare del trattamento. Anche nei confronti degli istituti di credito il Tribunale non ha ravvisato alcun illecito, poiché la banca si era limitata, in esecuzione di un preciso obbligo contrattuale, a descrivere la causale del bonifico nei certificati di estratto conto (Trib. di Napoli, sentenza n. 7896 dell'8 luglio 2012; sentenze nn. 5115, 5116 e 5117 del 4 maggio 2012).

Alcune pronunce dell'autorità giudiziaria hanno riguardato, in particolare, le segnalazioni degli interessati come cattivi pagatori, da parte di istituti di credito o società finanziarie ai soggetti che gestiscono i sistemi di informazioni creditizia (Sic) o alla Banca d'Italia, materia che genera frequente contenzioso per il rilievo che assume per gli interessati.

In tre casi la segnalazione è stata riconosciuta non corretta, con condanna dell'istituto o della società che l'aveva effettuata al risarcimento del danno in favore dell'interessato. I casi concernono: un soggetto che era stato segnalato da una società di finanziamento quale garante di un prestito erogato ad altra persona (Trib. di Milano, I sez. civ., sentenza n. 5395

del 10 maggio 2012); una persona segnalata alla Centrale d'allarme interbancaria (Cai), istituita presso la Banca d'Italia, a cui la società emittente aveva revocato la carta di credito (Trib. di Roma, sez. X civile, sentenza n. 23732 del 5 dicembre 2012); un interessato a cui era stato rifiutata la sottoscrizione di un contratto di mutuo fondiario con garanzia ipotecaria, essendovi una segnalazione di sofferenza a suo carico presso la Centrale rischi della Banca d'Italia (Trib. di Milano, I sez. civ., sentenza n. 6265 del 28 maggio 2012).

Nel terzo caso l'ente resistente, oltre al risarcimento del danno, è stato condannato anche alla cancellazione dei dati personali del ricorrente.

In due casi, invece, la segnalazione è stata ritenuta corretta, con conseguente rigetto delle domande di cancellazione e di risarcimento del danno. I casi concernono: ritardi nei pagamenti dovuti all'utilizzo della carta di credito (Trib. di Milano, sentenza n. 6478 del 29 maggio 2012); segnalazione alla Centrale rischi della Banca d'Italia di inadempimenti nei pagamenti relativi ad un contratto di finanziamento (Trib. di Milano, sentenza n. 719 del 28 febbraio 2012).

In un altro caso, pur ritenendo ingiustificata la segnalazione, il giudice ha respinto la domanda di risarcimento del danno, ritenuta non dimostrata (Trib. di Milano, sentenza n. 2887 del 5 luglio 2012).

#### **19.4. LE OPPOSIZIONI AI PROVVEDIMENTI DEL GARANTE**

L'anno 2012 ha registrato una sostanziale stabilità nella proposizione delle opposizioni a provvedimenti del Garante: a fronte dei settantadue ricorsi del 2011, nel 2012 sono state proposte settantatré opposizioni. Di queste, trentaquattro si riferiscono a opposizioni a ordinanze ingiunzioni, così registrando un calo rispetto al 2011, nel quale si erano registrate quarantacinque opposizioni di tale natura.

Complessivamente l'Autorità ha avuto notizia di trentacinque decisioni dell'autorità giudiziaria relative a opposizioni a provvedimenti del Garante, che si è sempre costituito in questi giudizi.

Ventidue sentenze hanno avuto ad oggetto opposizioni a ordinanze ingiunzioni; di queste, quindici hanno riguardato violazioni dell'art. 13 del Codice per omessa o inidonea informativa agli interessati, talvolta unitamente all'omessa acquisizione del loro consenso.

Cinque pronunce, riguardanti trattamenti di dati svolti attraverso siti internet da parte di una università telematica, di un esercizio commerciale, di un ente teatrale, di un'azienda di trasporti e, mediante la compilazione di *form*, di un'azienda municipalizzata per la raccolta di rifiuti urbani hanno respinto le opposizioni, confermando i provvedimenti del Garante (Trib. di Roma, sentenza n. 3739 del 4 luglio 2012; Trib. di Busto Arsizio, sentenza n. 143 del 26 aprile 2012; Trib. di Roma, sentenza n. 10729 del 24 maggio 2012).

Nel quarto caso, per l'entità del fatto (in particolare, le finalità non commerciali perseguite con il trattamento dei dati e la circostanza che l'azienda si era prontamente attivata per inserire una corretta informativa sul proprio sito) e nel quinto per le condizioni economiche dell'azienda e l'attività di servizio pubblico espletata, l'accertata violazione è stata considerata di "minore gravità" (art. 164-*bis*, comma 1, del Codice), con conseguente riduzione dell'importo della sanzione (Trib. di Trento, sentenza n. 110 dell'8 febbraio 2012; Trib. di Taranto, sentenza n. 807 del 23 aprile 2012).

Due pronunce, concernenti trattamenti di dati effettuati attraverso la compilazione di *form* sui siti internet di altrettante società per i quali non era stata fornita l'obbligatoria informativa e non era stato acquisito il consenso, hanno respinto l'opposizione, nel primo caso confermando integralmente il provvedimento del Garante e, nel secondo, rideterminando l'ammontare della sanzione pecuniaria (Trib. di Udine, sentenza n. 1332 del 7 novembre 2012; Trib. di Roma, sentenza n. 2969 del 22 febbraio 2012).

In altra pronuncia, anch'essa concernente il rilascio di un'inidonea informativa agli interessati al momento del conferimento di incarico da parte di un intermediario immobiliare, il giudice ha confermato il provvedimento ingiuntivo (Trib. di Perugia, sentenza n. 1221 del 2 ottobre 2012).

Uguale conferma, ma con riduzione della sanzione, è stata decisa dal Tribunale di Reggio Emilia in fattispecie di omessa informativa da parte di un circolo privato (sentenza del 20 febbraio 2012).

Ulteriori due pronunce, aventi ad oggetto il trattamento di dati personali realizzato attraverso l'uso di sistemi automatizzati di chiamata senza l'intervento di operatore e di fax per i quali era stata omessa l'informativa, hanno visto la conferma dei provvedimenti del

Garante (Trib. di Marsala, sentenza n. 175 del 28 febbraio 2012; Trib. di Roma, sentenza n. 8834 del 4 maggio 2012).

Una ulteriore pronuncia, riguardante due ordinanze ingiunzioni emanate nei confronti di una società che aveva inviato fax promozionali senza previamente fornire un'ideonea informativa agli interessati e senza avere acquisito il loro consenso, ha confermato entrambi i provvedimenti dell'Autorità (Trib. di Roma, sentenza n. 21089 del 18 aprile 2012).

In un caso, concernente l'omesso adempimento di un provvedimento emanato dall'Autorità (artt. 150, comma 2, e 162, comma 2-ter, del Codice), il ricorso è stato proposto avverso il verbale di contestazione di violazione amministrativa.

In sintonia con il consolidato orientamento della Corte di Cassazione, richiamato dal Garante, il ricorso è stato dichiarato inammissibile, in quanto la contestazione non è autonomamente impugnabile, non essendo decisione finale dell'Autorità sulla irrogazione della sanzione, costituita dalla eventuale ordinanza-ingiunzione (Trib. di Roma, sentenza n. 1041 del 18 giugno 2012).

In due opposizioni, riguardanti trattamenti di immagini raccolte attraverso sistemi di videosorveglianza posti all'ingresso di due esercizi commerciali, i giudici aditi, nel confermare i provvedimenti del Garante, hanno però rideterminato l'importo della sanzione pecuniaria (Trib. di Lamezia Terme, sentenza n. 843 del 29 maggio 2012; Trib. di Monza, ordinanza ex art. 702-bis e ss., c.p.c., del 28 marzo 2012).

Una pronuncia ha avuto ad oggetto la violazione degli artt. 37 e 38 del Codice per omessa o incompleta notificazione del trattamento da parte di una casa di cura. La decisione ha respinto l'opposizione e confermato il provvedimento del Garante (Trib. di Catania, sentenza n. 3241 del 20 febbraio 2012).

La mancata adozione da parte di una società delle misure minime di sicurezza, consistente nella omessa designazione per iscritto degli incaricati del trattamento in violazione dell'art. 30 del Codice e nella mancata adozione di *password* aventi otto caratteri, è stata oggetto della sentenza del Tribunale di Bologna, che ha confermato il provvedimento del Garante. La società aveva lamentato la violazione del principio del *ne bis in idem*, ritenendo che il Garante avesse già irrogato, per lo stesso fatto, un'altra sanzione. Accogliendo le osservazioni del

Garante, il giudice ha invece rilevato che era stata impugnata l'ordinanza-ingiunzione emessa nei confronti della società per la violazione amministrativa prevista dall'art. 162 del Codice, mentre l'importo a cui l'opponente faceva riferimento costituiva atto interno del procedimento penale instaurato, ai sensi dell'art. 169 del Codice, per gli stessi fatti, nei confronti della persona fisica autore della violazione.

Nella specie, quindi, non sussisteva la lamentata violazione del principio del *ne bis in idem* trattandosi di profili e di soggetti diversi (sentenza n. 20333 dell'8 marzo 2012).

Cinque pronunce hanno accolto le opposizioni ad altrettanti provvedimenti ingiuntivi emanati dal Garante.

La prima ha avuto ad oggetto il mancato rispetto, da parte dell'Autorità, del termine di novanta giorni dall'accertamento entro il quale deve avvenire la notificazione della contestazione di violazione amministrativa (Trib. di Bolzano, sentenza n. 199 del 17 febbraio 2012).

La seconda, concernente la raccolta di dati personali tramite un *forum online*, è stata accolta in quanto il provvedimento ingiuntivo era stato adottato nei confronti di uno studio professionale quale autore dell'illecito e non come soggetto tenuto in via solidale al pagamento della somma (Trib. di Latina, sez. di Terracina, sentenza n. 1231 del 26 aprile 2012). Avverso tale pronuncia il Garante ha proposto ricorso per Cassazione.

Con la terza, riguardante la mancata adozione di una misura minima di sicurezza, consistente nell'omessa designazione, in violazione dell'art. 30 del Codice, di un incaricato del trattamento da parte di una società commerciale, sono state accolte le argomentazioni della società ingiunta, in quanto non è risultata dimostrata la violazione dell'art. 33 del Codice (Trib. di Roma, sentenza n. 10863 del 24 maggio 2012). Anche avverso tale pronuncia il Garante ha proposto ricorso per Cassazione.

Nella quarta, relativa ad un caso di inidonea informativa riguardo l'utilizzo di una particolare tecnologia per mezzo della quale era possibile identificare gli utenti di un impianto di risalita, il Giudice ha ritenuto esaustiva l'informativa rilasciata dalla società agli utenti in relazione alla raccolta ed all'uso dei dati personali (Trib. di Sondrio, sentenza n. 102 del 12 aprile 2012). Il Garante ha proposto ricorso avanti alla Corte di Cassazione.

Nella quinta, infine, concernente il trattamento svolto da un ente pubblico territoriale tramite il sito internet istituzionale di dati personali idonei a rivelare lo stato di salute dei soggetti inseriti nelle graduatorie provinciali degli iscritti negli elenchi del collocamento obbligatorio dei disabili e dei centralinisti non vedenti, il Tribunale ha ritenuto che, in tema di sanzioni amministrative, autore della violazione è solo la persona fisica che ha commesso il fatto e non la persona giuridica (nei cui confronti era stata emessa l'ordinanza-ingiunzione) che può rispondere solo a titolo di obbligato in solido con l'autore, trattandosi di soggetto nei cui confronti non può essere compiuta alcuna valutazione dell'elemento soggettivo dell'illecito, dell'imputabilità e dell'esistenza di cause di esclusione della responsabilità (Trib. di Avellino, sentenza n. 374 del 29 febbraio 2012). Anche in questo caso il Garante ha proposto ricorso avanti alla Corte di Cassazione.

Ambito territoriale  
di applicazione del  
Codice

Particolare interesse presenta, anche per i complessi profili tecnici coinvolti, una sentenza del Tribunale di Milano con riferimento all'art. 5, comma 2, del Codice, ai sensi del quale le norme del Codice stesso non si applicano al trattamento di dati personali effettuato da chi è stabilito nel territorio di un Paese non appartenente all'Unione europea anche se impiega per il trattamento strumenti situati nel territorio dello Stato, ma solo ai fini di transito nel territorio dell'Unione.

A seguito di numerose segnalazioni ricevute relative alla ricezione di fax non richiesti a carattere promozionale, il Garante, a seguito di una complessa attività istruttoria, aveva individuato la società che per conto di terzi aveva trasmesso tali comunicazioni dichiarando illecito il trattamento dei dati (prov. 7 aprile 2011 [doc. web n. 1810207]).

La società aveva impugnato il provvedimento sostenendo che l'intero processo dei messaggi pubblicitari era gestito su *server* collocati negli Stati Uniti e che parte del servizio fax diretto verso l'Italia veniva indirizzato presso un *delivery node* in Italia, gestito da una società telefonica ivi stabilita, sicché a parte il mero transito della comunicazione, nessun trattamento sui messaggi veniva realizzato in Italia, con conseguente applicabilità dell'esimente di cui all'art. 5, comma 2, del Codice.

Il Garante ha rilevato in giudizio che, in base alla normativa italiana (delibera Agcom 417/06/CONS, in G.U. 7 settembre 2006, n. 208; delibera 180/10/CONS, in G.U. 28

maggio 2010, n. 123), il “servizio di transito” consiste nel mero trasporto di traffico da una rete di origine a una di terminazione.

La società, invece, effettuava il trattamento dati attraverso una struttura informatica complessa, che inoltrava al mittente (cioè al terzo nel cui interesse erano svolte le attività promozionali), per ogni destinatario, un messaggio contenente l’esito della spedizione del singolo fax, tracciando le informazioni relative all’invio, in particolare l’utenza e l’indirizzo *Ip* del mittente, il numero del fax del destinatario, l’esito dell’invio, il numero dei fax inviati e il contenuto del messaggio. Il sistema realizzava, pertanto, una interconnessione tra la rete internet e la rete telefonica, attuabile, secondo le attuali conoscenze tecniche, attraverso uno specifico dispositivo di interconnessione, noto come *fax gateway* che, per la realizzazione del servizio offerto dalla società resistente, deve necessariamente trattare alcuni dati personali, tra i quali la conversione di un identificativo di utente della rete internet in un numero di abbonato della rete telefonica pubblica; la ricezione del fax al fine di acquisirne l’immagine; la conversione del formato dell’immagine. Il Garante ha, altresì, accertato che il *fax gateway* si trovava nel territorio italiano ed era gestito direttamente dalla società.

Tutto ciò ha consentito di provare che la società ispezionata era titolare di un trattamento di dati personali effettuato in Italia, ancorché con dati detenuti all’estero (cioè nei *server* dove i clienti della ricorrente caricano le informazioni) che, pertanto, ricadeva sotto l’applicazione del Codice.

Il Tribunale di Milano, con sentenza n. 3352 del 2 aprile 2012, ha accolto interamente le tesi sostenute dal Garante.

Si ritiene utile dare diffusamente conto anche di un’interessante decisione del Tribunale di Udine, sezione distaccata di Cividale del Friuli che, per quanto depositata nel 2010, è pervenuta al Garante nel luglio 2012.

In particolare, il Tribunale ha affrontato il tema dell’obbligo di informativa posto dall’art. 13 del Codice in un caso nel quale il titolare di un’azienda individuale si era rivolto ad una società di intermediazione per il reperimento di rappresentanti di commercio attraverso il sito internet dell’intermediario. L’azienda, che era stata sanzionata per non avere reso l’informativa agli agenti che producevano il loro *curriculum*, aveva impugnato il provvedimento

Informativa  
nell’intermediazione  
per la ricerca del  
personale