Nel testo si ipotizza l'abolizione dell'obbligo per i titolari di notificare i trattamenti di dati personali, sostituito da quello di nominare un *data protection officer* (incaricato della protezione dati, secondo la terminologia della direttiva 95/46/CE) per tutti i soggetti pubblici e per quelli privati al di sopra di un certo numero di dipendenti (per dettagli sull'*iter* delle proposte modifiche v. *infra* par. 19.1).

# 16 La trattazione dei ricorsi

## 16.1. *I profili generali*

È difficile riassumere in una sola parola il senso complessivo del lavoro svolto nello scorso anno. Se si guarda al numero complessivo dei ricorsi trattati e all'insieme dei temi affrontati, i termini "assestamento" e "consolidamento" sembrano i più rispondenti alla realtà complessiva. Il numero delle decisioni adottate, duecentoventidue (cfr. sez. IV, tab. 4 e 5), è stato pressoché uguale all'anno precedente e le tipologie principali dei procedimenti instaurati corrispondono grosso modo agli ambiti intorno ai quali da diversi anni si concentrano la maggior parte dei fascicoli in trattazione (e che saranno oggetto di specifico esame nei paragrafi successivi).

Uno sguardo più approfondito (che tenga conto non solo del contenuto immediato delle richieste formulate, ma anche delle ragioni sostanziali che muovono i ricorrenti) permette però di cogliere un filo rosso (a volte curioso, sicuramente sorprendente) che consente di ricondurre molte vicende esaminate alle varie sfaccettature determinate da quel complesso di azioni e reazioni che va sotto il nome (riassuntivo e semplificatorio) di "crisi economica globale". Ne sono testimonianza, prima di tutto, i numerosissimi ricorsi rivolti nei confronti dell'intera galassia degli istituti di credito e delle società finanziarie. In un quadro di persistente crisi economica appare, infatti, di estrema importanza disporre di uno strumento di tutela capace di assicurare (in tempi celeri e con minimo esborso di denaro) la possibilità di ricostruire il quadro completo dei rapporti bancari che fanno capo ad una persona singola o ad un'imprenditore individuale (o alle posizioni riconducibili ad un defunto, grazie alle potenzialità racchiuse nel disposto dell'art. 9, comma 3, del Codice). L'art. 7 del Codice diventa così strumento per ricostruire l'assetto e l'evoluzione di patrimoni e rapporti bancari personali, familiari, imprenditoriali, ed è spesso il punto di partenza per contestare le condizioni contrattuali dei rapporti in essere con il sistema creditizio o, più in dettaglio, per verificare la congruità degli interessi praticati.

Più spesso le potenzialità di acquisizione di dati e informazioni messe a disposizione dal Codice sono lo strumento indispensabile per verificare la liceità del trattamento operato nell'ampio settore della centralizzazione dei rischi di credito e in quello ancora più esteso delle banche dati che forniscono elementi di informazione sulle imprese (e più specificamente sulle persone ad esse preposte), sulla correttezza e tempestività di queste nell'onorare le scadenze dei pagamenti e, più in generale, sulla loro affidabilità economica.

Non è un caso, quindi, che ormai da anni, il Garante sia diventato un punto di riferimento in questa materia grazie agli orientamenti espressi in relazione, in particolare, al settore (assai ampio) che comprende i trattamenti effettuati presso i sistemi di informazioni creditizie, la Centrale dei rischi della Banca d'Italia e la Centrale d'allarme interbancaria.

Se quello descritto è il profilo positivo e fisiologico dell'utilizzo della normativa sulla protezione dei dati personali a tutela delle posizioni degli attori "deboli" del sistema economico, in un momento di crisi economica diffusa, non si può però sottacere che gli stessi strumenti a volte appaiono usati in modo strumentale per finalità prevalentemente dilatorie. Su questo confine, a volte contrassegnato da chiaroscuri, si

deve esercitare il senso di responsabilità dell'Autorità, chiamata a fornire interpretazioni e ad adottare decisioni che salvaguardino le effettive esigenze di tutela degli interessati senza dimenticare però le ragioni delle imprese e le necessità di tutela del sistema bancario e finanziario in genere.

### 16.2. *Uno sguardo ai dati statistici*

Una conferma di questo panorama generale si desume anche dall'analisi dei dati statistici riferiti al 2013, sia prestando attenzione alla tipologia di decisioni adottate, sia con riguardo alle categorie di titolari del trattamento.

Dal primo punto di vista, si conferma con assoluta evidenza l'alto numero di decisioni di non luogo a provvedere (pari al 60% del totale), cioè di procedimenti conclusisi con il soddisfacimento, nel corso dell'istruttoria, delle richieste degli interessati/ricorrenti (procedimenti spesso imperniati su quelle istanze di accesso a dati e informazioni economico-finanziarie cui sopra si è fatto riferimento) (cfr. sez. IV, tab. 4). Una percentuale così significativa di procedimenti conclusisi celermente e positivamente senza dubbio depone a favore dell'utilità e dell'efficacia dello strumento del ricorso, anche se, di riflesso, segnala ancora la persistenza di ambiti di "resistenza" da parte dei titolari del trattamento o (quantomeno) di non conoscenza dei diritti previsti e tutelati dall'art. 7 del Codice, tenendo conto, peraltro, che l'attivazione del ricorso dinanzi all'Autorità è passaggio necessariamente successivo rispetto alla proposizione di un apposito interpello rivolto previamente al soggetto detentore dei dati.

Sul piano della tipologia delle decisioni va comunque sottolineato un incremento significativo dei casi di accoglimento (totale o parziale) delle richieste dei ricorrenti (cfr. sez. IV, tab. 4). Spesso dietro queste vicende si celano istanze articolate (non esclusivamente imperniate su semplici domande di accesso) che attestano una ormai diffusa conoscenza dell'ampio ventaglio delle situazioni giuridiche soggettive riconosciute dalla disciplina di protezione dei dati personali.

Non meno significativo è lo sguardo alle principali categorie di titolari del trattamento (cfr. sez. IV, tab. 5). Pur nella grande varietà di ambiti (praticamente l'intero spettro immaginabile dei soggetti pubblici e privati) emergono in modo evidente le macro-categorie (banche e società finanziarie, sistemi di informazioni creditizie, altri archivi centralizzati relativi alla verifica della affidabilità delle imprese) che sono già state indicate in apertura di questo paragrafo. E a conferma della "sensibilità" dell'ampia casistica dei trattamenti di dati personali connessi allo svolgimento dell'attività economica, va notato anche il numero significativo di procedimenti attivati nei confronti dei datori di lavoro pubblici e privati (circostanza questa che trova conferma anche dal panorama che si ricava dalle segnalazioni e dai reclami pervenuti in questa materia: cfr. par. 11.4). È una casistica che riflette le difficoltà occupazionali del momento, che evidenzia le dinamiche conflittuali diffuse nelle fabbriche e negli uffici e che pone spesso in luce, rispetto all'utilizzo delle nuove tecnologie, il rapporto complesso fra tutela della riservatezza e della dignità dei singoli e le esigenze dell'impresa.

Non può essere sottaciuto, in conclusione, il persistente flusso, già segnalato lo scorso anno, di ricorsi che vengono tuttora proposti (in veste di "interessati") da società commerciali ed enti vari, non ancora consapevoli che le modifiche normative (intervenute alla fine del 2011) alle nozioni di "interessato" e di "dato personale", contenute nell'art. 4 del Codice privano ormai questi soggetti della possibilità di utilizzare gli strumenti di tutela previsti dal Codice, di cui proprio negli ultimi anni erano state

colte le potenzialità. È un fenomeno che va messo in luce, se non altro per segnalare al legislatore e alle associazioni di categoria, il rischio insito in alcune proposte di modifica normativa che, in nome di una malintesa semplificazione, possono sottrarre ulteriori ambiti della vita economica (*in primis* quelle degli imprenditori individuali) alle tutele specifiche della normativa in materia di protezione dei dati personali, riportando in un'area di opacità i trattamenti di dati personali che interessano le realtà imprenditoriali (specie piccole e medie) rispetto al grado di trasparenza alle stesse assicurato dalla disciplina previgente.

### 16.3. *I profili procedurali*

La varietà dei temi e dei soggetti implicati nella trattazione dei ricorsi e la stessa "elasticità" di molte delle posizioni giuridiche contemplate dall'art. 7 del Codice ha portato da sempre ad un utilizzo ampio dello strumento del ricorso che, lungi dall'essere solo il rimedio al mancato, positivo esercizio del diritto di accesso, ha finito per costituire spesso una sorta di "cavallo di Troia" per utilizzare i rimedi (e la tempistica) prevista in materia di protezione di dati personali al fine di "esplorare" e influenzare la decisione di profili più propriamente pertinenti ad altri ambiti dell'ordinamento giuridico. In questo senso vanno evidenziate le non poche decisioni che hanno permesso di fare luce su diversi aspetti procedurali (a volte anche inediti) fissando quindi i "paletti" dell'area potenzialmente interessata dall'utilizzo dello strumento ricorso.

Vanno anzitutto ricordate le decisioni che hanno messo in luce alcuni profili rispetto ai quali il legislatore ha espliciteamente escluso la possibilità di utilizzare lo strumento del ricorso. In un caso (provv. 27 giugno 2013, n. 324, doc. web n. 2615218) veniva in gioco l'installazione di un impianto di videosorveglianza a tutela di un'abitazione privata che riprendeva però una zona soggetta al transito dell'interessato/ricorrente: in tale fattispecie va fatto riferimento al significativo disposto dell'art. 5, comma 3, del Codice, secondo cui "il trattamento di dati personali effettuato da persone fisiche per fini esclusivamente personali è soggetto all'applicazione del presente Codice solo se i dati sono destinati ad una comunicazione sistematica o alla diffusione". Ne deriva che situazioni analoghe a quella rappresentata, in cui possono darsi ingerenze nella vita privata di singoli, (non rientrando nell'ambito di applicazione del Codice) non possono (neanche) costituire oggetto di richieste *ex* art. 7, né tantomeno di proposizione di ricorso.

Profilo diverso è quello affrontato nella decisione del 21 febbraio 2013, n. 83 (doc. web n. 2413109) concernente una richiesta di "integrazione" dei dati personali dell'interessato contenuti in un'informativa redatta da ufficiali di polizia giudiziaria e rivolta alla procura della Repubblica. Si tratta di fattispecie che, ai sensi del combinato disposto degli artt. 8, comma 2, lett. *h)* e 53 del Codice, rientra fra i trattamenti svolti da "organi di pubblica sicurezza [...] per finalità di [...] prevenzione, accertamento e repressione dei reati" per i quali non è possibile utilizzare lo strumento di tutela di cui agli artt. 145 e ss. (interpello preventivo e successiva, eventuale, proposizione del ricorso).

L'ampia casistica relativa al 2013 ha messo in luce anche alcune situazioni nelle quali i ricorsi sono stati dichiarati inammissibili in quanto proposti da soggetti non legittimati o rivolti a soggetti che di tale particolare strumento di tutela non possono essere destinatari. È il caso della decisione del 6 giugno 2013, n. 285 (doc. web n. 2603890) con la quale, in riferimento ad una richiesta di accesso a informazioni pertinenti ad una controversia in materia bancaria, l'Autorità ha avuto modo di sottolineare che, ai sensi dell'art. 147 del Codice, il ricorso può essere proposto esclu-

sivamente nei confronti del "rirolare del trattamenro" e non anche del soggerto qualificato formalmente come "responsabile" ai sensi dell'art. 29 del Codice (come avvenuto nel caso di specie).

Interessanre anche la vicenda, decisa il 28 novembre 2013, n. 539 (doc. web n. 2943920) nella quale l'Autorità ha ritenuto inammissibile il ricorso proposto da un curatore (privo però di espressa procura) nell'interesse di un soggetto inabilitato. Ciò, seguendo un ormai consolidato orientamento della Corte di cassazione secondo cui "l'inabilitato può stare in giudizio come attore e come convenuto con l'assistenza del curatore [...] atteso che il curatore ha istituzionalmente solo funzioni di assistenza e di supporto, non di rappresentanza o di sostituzione processuale del suo assistito, cui spettano le manifestazioni di volontà processuale" (Cass. civ., sez. I, n. 5359/1992).

Significative e ricche di spunti procedimenrali sono state anche le diverse pronunce incentrate sull'esercizio del diritto di accesso ai dati riferiti ai defunti (che abbiamo già segnalato come efficace strumento per l'impostazione o la risoluzione di complesse controversie ereditarie). Basti ricordare al riguardo le decisioni del 6 giugno 2013, n. 289 (doc. web n. 2605463) e del 26 settembre 2013, n. 419 (doc. web n. 2745548) che hanno permesso di mettere in luce l'ampia platea dei soggetti che possono avere titolo a richiedere le informazioni riferite al defunto, atteso il disposto dell'art. 9, comma 3, del Codice che legittima "chi ha un interesse proprio, o agisce a tutela dell'interessato o per ragioni familiari meritevoli di protezione", formula di evidente ampiezza che, in particolare, è svincolata dalla configurazione in capo all'interessato della qualità di erede.

Non si può sottacere che l'utilizzo di questa ampia possibilità di accesso (innestata sulle già segnalate rilevanti potenzialità dell'art. 7 del Codice) ha dato luogo a forme di abuso e a richieste di tipo esplorativo che hanno comportato oneri significativi (si pensi al caso degli istituti di credito). È stata così riaffermata (provv. 21 novembre 2013, n. 525, doc. web n. 2936729) la proposta di superare la tendenziale gratuità dell'esercizio del diritto di accesso, dando attuazione al disposto dell'ultima parte dell'art. 10, comma 8, del Codice. Si tratta di tema delicato, che potrà essere oggetto di approfondimento, cui l'Autorità si è fino ad ora accostata con doverosa prudenza e con riferimento al solo ambito dei sistemi di informazioni creditizie.

### 16.4. *La casistica più significativa*

Merita ora passare rapidamente in rassegna alcuni degli ambiti più significativi interessati dai ricorsi nel 2013. L'elenco (come detto, parziale) mira a segnalare alcuni provvedimenti che, in ragione della loro valenza generale, possono fornire utili indicazioni ai soggetti interessati ad attivare le tutele di cui all'art. 7 del Codice in relazione ad ambiti analoghi.

**Trattamenti presso società fornitrici di servizi telefonici e telematici**

Lo sviluppo delle tecnologie e la diffusione di apparecchiature informatiche a tutti i livelli e per tutti i tipi di attività ha ovviamente moltiplicato le possibilità di trattamento dei dati personali e il relativo contenzioso. Va però evidenziato che i ricorsi proposti in questa materia nell'ultimo anno si sono concentrati su un aspetto che in passato era stato più volte all'attenzione del Garante: la possibilità di accedere ai cd. dati di traffico. Le norme di riferimento sono rappresentate, come noto, dagli artt. 123 e 132 del Codice, che prevedono un'articolata tempistica di conservazione di tali dati e delimitano in modo puntuale la possibilità di avervi accesso. La consapevolezza della particolare delicatezza di queste informazioni (tenuto conto delle garanzie che assistono la libertà e segretezza delle comunicazioni) e dei diversi soggetti che possono essere interessati da una medesima comunicazione (abbonati e

utenti chiamati o chiamanti) giustifica una disciplina che è, sul punto, attenta e giustamente restrittiva. Disciplina che però non appare molto conosciuta, come dimostrano diversi ricorsi che sono stati dichiarati infondati in quanto formulati con riferimento a iporesi che si pongono al di fuori dei limiti consentiti dal citato art. 132. A tal proposito, si può ricordare la decisione del 28 febbraio 2013, n. 90 (doc. web n. 2414766) relativa ad una richiesta di dati di traffico telefonico già piuttosto risalenti nel tempo. Nel caso di specie, infatti, la richiesta riguardava informazioni rispetto alle quali era già trascorso il termine massimo di conservazione di ventiquattro mesi e, inoltre, l'istanza non era stata formulata con riferimento alle finalità di accertamento e repressione dei reati. Quest'ultimo, indispensabile elemento sta alla base dell'infondatezza anche del ricorso deciso il 26 settembre 2013, n. 421 (doc. web n. 2746125). In tal caso i dati risultavano ancora conservati dall'operatore telefonico ma, essendo già decorsi i sei mesi previsti per la conservazione dei dati a fini di fatturazione ed essendo la richiesta connessa a profili di tutela contrattuali (o comunque civilistica), si esulava dalle previsioni del citato art. 132.

Va infine ricordata la decisione dell'11 aprile 2013, n. 194 (doc. web n. 2544003) che ha visto il positivo esito di una richiesta di accesso a dati di tipo telematico, necessari all'interessato al fine di chiarire i sospetti relativi all'accesso fraudolento da parte di terzi alla propria casella di posta elettronica.

**Trattamenti in ambito bancario e finanziario**

Si è già avuto modo di sottolineare come sia questo l'ambito rispetto al quale è pervenuto il maggior numero di ricorsi anche nel 2013. Ciò, considerando, naturalmente, questo settore in una accezione larga che comprende non solo le istanze specificamente rivolte nei confronti degli istituti di credito (con particolare riguardo all'esercizio del diritto di accesso), ma anche tutti i procedimenti rivolti (oltre che nei confronti delle banche) nei riguardi dei soggetti (con funzioni di gestione di banche dati o di controllo sulle stesse) che svolgono il ruolo di titolari del trattamento dei dati conservati in alcuni delicati archivi, sia pubblici, sia privati. Il riferimento, naturalmente, è alla Centrale dei rischi istituita presso la Banca d'Italia, alla Centrale d'allarme interbancaria, ma anche e soprattutto, ai soggetti gestori dei sistemi di informazioni creditizie, cui tuttora si indirizzano numerosi ricorsi in relazione al delicato ambito del "credito al consumo". Si tratta peraltro di micro settori caratterizzati da specifiche normative (primarie e/o secondarie) o disciplinate, come nel caso dei sistemi di informazioni creditizie, da fonti atipiche come i codici di deontologia e buona condotta che stabiliscono le modalità di trattamento e la tempistica di conservazione delle informazioni. Sono questi i parametri di riferimento cui il Garante si richiama nell'esaminare questi ricorsi e nel verificarne la liceità dei relativi trattamenti (cfr. provv. 11 aprile 2013, n. 193, doc. web n. 2542632 e provv. 17 ottobre 2013, n. 465, doc. web n. 2925010).

Al di là dei procedimenti che hanno fatto riferimento alle problematiche interpretative di questo complesso di disposizioni (rispetto ai quali nell'anno trascorso non sono emersi profili innovativi ma sostanzialmente una riproposizione di temi sui quali si sono ormai consolidati gli orientamenti del Garante) vi sono però da segnalare alcuni casi che hanno portato all'attenzione dell'Autorità problematiche diverse, e in parte, nuove. In particolare, la decisione del 17 ottobre 2013, n. 463 (doc. web n. 2914255) ha permesso di affrontare per la prima volta il tema dell'accesso alle informazioni trattate nell'ambito delle operazioni (normalmente effettuate con l'ausilio di appositi programmi informatici) di cd. *credit scoring*, cioè il calcolo matematico che precede e (in misura rilevante) condiziona la possibile concessione di un finanziamento o (come nel caso di specie) il rilascio di una carta di credito. Nel caso in esame, la società emittente la carta (che ne aveva negato l'attivazione all'interessato) nel corso del procedimento ha integrato le proprie comunicazioni e, venendo incontro alle richieste del ricorrente volte a conoscere sulla base di quali specifiche informazioni si

era formulato un giudizio "negativo" nei suoi confronti, ha precisato quali dati avevano concorso al calcolo del *credit scoring*, che, nel caso di specie, era risultato inferiore a quello minimo stabilito dalla società per l'emissione del prodotto richiesto.

Interessanti, su altro versante, sono poi due decisioni (del 14 febbraio 2013, n. 70, doc. web n. 2413087 e del 30 ottobre 2013, n. 493, doc. web n. 2929960) con le quali l'Autorità ha avuto la possibilità di confrontarsi con il tema del cd. furto d'identità (realtà purtroppo in costante espansione, tanto da frenare in modo significativo lo sviluppo delle transazioni *online*). Anche in questo caso si è potuta cogliere l'utilità dell'esercizio del diritto di accesso ai dati personali che ha permesso di ricostruire le informazioni da cui la truffa subita dall'interessato ha avuto inizio, attraverso l'acquisizione dei dati (solo parzialmente corrispondenti al vero) riportati sui documenti d'identità contraffatti della vittima del raggiro.

**Trattamenti in ambito giornalistico e archivi *online***

In relazione al giornalismo, l'anno 2013 ha confermato in pieno come ormai la quasi totalità delle vicende sottoposte al vaglio dell'Autorità attenga al giornalismo *online*, o riguardi l'ambito televisivo, o interessi il settore, in rapidissima espansione, degli archivi storici digitali delle testate giornalistiche (accessibili gratuitamente e, in alcuni casi, dotati di una profondità temporale di decenni). Da questo punto di vista è anche largamente cambiata la tipologia di contenzioso che si affronta. Sono sempre meno numerose le vicende che vengono portate all'attenzione dell'Autorità per valutazioni sui "contenuti" delle notizie date (profili peraltro che un'autorità amministrativa, per quanto indipendente come il Garante, ha sempre esaminato con prudenza, considerate le particolari guarentigie costituzionali di cui all'art. 21 Cost.), mentre si moltiplicano le ipotesi in cui il trattamento dei dati e, in particolare, le disposizioni del codice di deontologia e buona condotta del settore giornalistico vengono messe in discussione in relazione alle modalità (sotto il profilo della correttezza e liceità delle stesse) con le quali, grazie alle nuove tecnologie, le notizie vengono acquisite, trattate e diffuse. Se questo è già il nuovo fronte dell'informazione, che supera barriere spazio-temporali e professionali (aprendo una rinnovata stagione al giornalismo d'inchiesta anche attraverso l'irruzione del "*citizen journalism*"), non meno rilevanti sono le problematiche (ormai sottoposte al vaglio del Garante con frequenza pressoché quotidiana) legate alla persistenza sulla rete internet ed alla connessa facile reperibilità (in ragione dell'azione dei motori di ricerca) di notizie, anche molto risalenti nel tempo, che possono contenere informazioni (in alcuni casi molto delicate o comunque quasi sempre negative). Tali notizie, inizialmente giustificate da un corretto esercizio del diritto di cronaca, poi sicuramente legittimate nella loro conservazione da esigenze di memoria storica, finalizzata ad assicurare anzitutto la libertà di informazione nonché di studio e ricerca, non di rado, però, riverberano (per un tempo indefinito) un influsso negativo e spesso condizionante sulla vita e le aspettative future di molte persone (che pur possono essere state protagoniste con un ruolo "negativo" di vicende giudiziarie o di cronaca). In questo senso, già da alcuni anni l'Autorità, con una serie numerosa e rilevante di decisioni, ha indicato (significativamente seguita dalla giurisprudenza) la strada della deindicizzazione dei contenuti contestati come strada maestra per assicurare il giusto contemperamento fra le diverse esigenze (ed i connessi valori) sopra evidenziate e le istanze (pressanti e comprensibili) di tante persone comuni che, riassumendo nel concetto evocativo di "diritto all'oblio", le ansie e le negatività indotte da una "esposizione telematica" continua e incancellabile, hanno spinto l'Autorità ad intervenire su questa materia.

Fra le tante decisioni adottate in materia, si possono segnalare quelle del 24 aprile 2013, n. 224 (doc. web n. 2547890) e del 18 dicembre 2013, nn. 597 e 600 (doc. web nn. 2957134 e 2956995) (cfr. par. 9.5). Se questi esempi riflettono un orientamento ormai consolidato, cui sembra peraltro corrispondere un atteggiamento colla-

borativo sempre più diffuso da parte degli editori, non bisogna trascurare i casi (più complessi e delicati) nei quali l'Autorità, oltre al profilo della persistenza in rete degli articoli ormai inseriti negli archivi storici, ha affrontato il problema della pubblicazione di dati avvenuta in modo illecito, in particolare, in violazione delle disposizioni contenute nel codice deontologico di settore, con riferimento, ad esempio, alla diffusione di informazioni, anche dettagliate, sullo stato di salute di una persona (provv. 12 dicembre 2013, n. 578, doc. web n. 2956950) o con riguardo alla pubblicazione di dati identificativi di minori coinvolti, seppure indirettamente, in gravi fatti di cronaca (provv. 18 dicembre 2013, n. 594, doc. web n. 2957346).

Per quanto non attinente alla materia del giornalismo, va infine segnalata una decisione (provv. 21 novembre 2013, n. 516, doc. web n. 2914227) che è strettamente connessa alla materia della deindicizzazione degli articoli dai motori di ricerca. In quesro caso, oggetto delle richieste dell'interessato non era un "pezzo" giornalistico, bensì un'interrogazione parlamentare contenente dati giudiziari (molto risalenti nel tempo e superati da successivi sviluppi processuali) del ricorrente. Pur trattandosi formalmente di una declaratoria di inammissibilità (in ragione della pertinenza dell'attività in questione con lo svolgimento delle funzioni parlamentari assistite nell'ordinamento da una "indipendenza guarentigiata nei confronti di qualsiasi altro potere"), la vicenda ha coinciso con un ripensamento della Camera dei deputati sulle modalità di trattamento di tali questioni. I competenti organi della Camera hanno, infatti, adottato apposite disposizioni procedurali interne (cfr. Deliberazioni dell'Ufficio di Presidenza n. 46/2013 e n. 53/2013, Procedura in ordine a richieste concernenti dati personali contenuti in atti parlamentari) che, recependo linee interpretative e metodologiche già utilizzate in contesti simili (deindicizzazione di notizie disponibili negli archivi storici *online* delle principali testate giornalistiche), hanno offerto anche a queste particolari fattispecie una tutela effettiva e adeguata.

# 17 Il contenzioso giurisdizionale

## 17.1. *Considerazioni generali*

Come riferito nella Relazione 2012, il d.lgs. n. 150/2011 con l'art. 34 ha abrogato l'art. 152 del Codice – con l'eccezione del comma 1 –, dettando all'art. 10 nuove regole procedurali concernenti le controversie in materia di applicazione delle disposizioni del Codice in materia di protezione dei dati personali. In particolare, l'art. 34 ha abrogato anche 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 continua a far 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 ricorsi notificati nel 2011 e dei 78 nel 2012, nel 2013 sono stati notificati all'Autorità e da questa trattati 32 ricorsi (cfr. sez. IV, tab. 1).

Attesa l'accertata validità di tale strumento posto a disposizione degli interessati, volto alla 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 quindi 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 strumento, unitamente alle notifiche dei ricorsi proposti direttamente davanti al giudice che l'autorità giudiziaria riterrà di effettuare, potrà consentire al Garante di continuare ad avere conoscenza sull'evoluzione della giurisprudenza in materia di protezione dei dati personali e di svolgere il ruolo di segnalazione al Parlamento e al Governo degli interventi normativi necessari per la tutela dei diritti degli interessati (come previsto dall'art. 154, comma 1, lett. *f*), del Codice).

## 17.2. *I profili procedurali*

L'art. 152 devolve tutte le controversie riguardanti l'applicazione del Codice, comprese quelle inerenti ai provvedimenti del Garante, all'autorità giudiziaria ordinaria (comma 1), con ricorso da depositare nella cancelleria del Tribunale del luogo ove ha la residenza il titolare del trattamento (art. 10, comma 2, d.lgs. n. 150/2011).

Una pronuncia ha affrontato il problema dell'individuazione del giudice territorialmente competente nel giudizio di opposizione a provvedimenti dell'Autorità nel caso in cui il titolare del trattamento sia una società avente una pluralità di filiali sul territorio nazionale (si trattava, nel caso di specie, di un importante istituto di credito).

Secondo l'art. 152, comma 2, del Codice, applicabile *ratione temporis* alla fattispecie, "l'azione si propone con ricorso depositato nella cancelleria del Tribunale del luogo ove risiede il titolare del trattamento". Il giudice ha reputato che la disposizione citata fosse intesa a radicare la competenza rispetto al luogo di residenza del titolare

"in concreto": il verbo "risiede" non evocherebbe una localizzazione in senso statico del titolare, ma la localizzazione in senso dinamico del suo concreto operare. Assumerebbe rilievo infatti, dal punto di vista dell'interessato, il luogo in cui il trattamento dei dati è stato concretamente percepito. Tale interpretazione è stata sostenuta anche avuto riguardo alle finalità di tutela della normativa in materia di protezione di dati personali: sarebbe infatti irragionevole costringere l'interessato ad esercitare i propri diritti non già nel luogo in cui gli effetti del trattamento si evidenziano e, quindi rivelano la loro capacità lesiva, bensì nel luogo, potenzialmente molto distante, ove ha sede il titolare del trattamento.

Sulla base di tali premesse, è stato ritenuto corretto incardinare la controversia nel luogo dove si trovava la filiale della banca che effettivamente aveva esercitato il trattamento dei dati della ricorrente, escludendo la competenza del tribunale del luogo ove si trova la sede centrale dell'istituto (Trib. Catania, sez. distaccata di Paternò, sentenza 10 giugno 2013, n. 1139).

La menzionata disposizione del Codice, secondo quanto si accennava, è stata successivamente abrogata e sostituita dall'art. 10, comma 2, d.lgs. n. 150/2011, il quale la riproduce nella sostanza, anche se con diverso tenore testuale: "è competente il tribunale del luogo in cui ha la residenza il titolare del trattamento dei dati". Tale modifica dovrebbe definitivamente deporre a favore della competenza del tribunale del luogo dove si trova la sede legale della società, con l'eccezione del caso in cui una sede decentrata, per le particolari caratteristiche che la contraddistinguono, possa essere considerata come autonoma titolare del trattamento dei dati.

Due decisioni si sono occupate della competenza territoriale nei casi in cui una controversia in materia di protezione di dati personali si inserisca nell'ambito di un rapporto di consumo: l'art. 33, lett. *u*), d.lgs. n. 205/2006 (cd. codice del consumo) stabilisce infatti la competenza del giudice del luogo di residenza o di domicilio elettivo del consumatore (derogabile contrattualmente ma, in tal caso, con presunzione di vessatorietà). Sulla scorta di una decisione della Corte di cassazione (ordinanza 14 ottobre 2009, n. 21814), i giudici hanno affermato che il foro previsto dal d.lgs. n. 206/2005 prevale su quello individuato dal Codice, perché la sopravvenienza del primo ha derogato al secondo (Trib. Chieti, sentenza 30 dicembre 2012, n. 833; Trib. Roma, sentenza 18 giugno 2013, n. 12550). Sotto questo profilo, si rileva che – in applicazione del medesimo criterio cronologico indicato dalla Suprema Corte e confermato nelle due pronunce citate – il successivo intervento da parte del d.lgs. n. 150/2011 potrebbe allora indurre a modificare la soluzione prospettata nel senso della prevalenza del foro indicato dalla normativa in materia di tutela dei dati personali.

In tema di giurisdizione, analogamente a quanto accaduto 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.

### 17.3. *I profili di merito*

Nel 2013 si sono riperute più decisioni emesse dall'autorità giudiziaria, 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 p.a. e il loro trattamento da parte di alcuni istituti di credito. Le fartispecie oggetto dei giudizi concernevano l'illiceità del riferimento da parte dell'ente pubblico erogatore, nella

causale di accredito dei fondi confluiti nei conti correnti bancari dei ricorrenti, beneficiari di presrazioni indennitarie, al titolo giustificativo costituto dalla l. n. 210/1992 (concernente l'indennizzo a favore dei soggetti danneggiati da complicanze di tipo irreversibile a causa di vaccinazioni obbligatorie, trasfusioni e somministrazione di emoderivati) nonché 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.

La maggioranza di tali pronunce hanno rigettato le domande, avendo l'adito Tribunale di Napoli escluso che l'ente pubblico avesse 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 ove era stato aperto il conto, che, essendo stato preventivamente autorizzato sulla base del contratto di conto corrente stipulato dall'interessato, riveste il ruolo, unitamente all'ente pubblico, di titolare del trattamento cui comperono le decisioni in ordine alle finalità, alle modalità del trattamento dei dati personali ed agli strumenti utilizzati, ivi compreso il profilo della sicurezza. In tali casi, anche nei confronti degli istituti di credito il Tribunale non ha ritenuto dimostrato alcun illecito, essendosi verificato che l'unica condotta della banca denunciata come illecita dai ricorrenti e provata *per tabulas* consisteva nella descrizione, effettuata in esecuzione di un preciso obbligo contrattuale, della causale del bonifico disposto dall'ente erogatore nei certificati di estratto conto inoltrati periodicamente alla medesima persona fisica a cui si riferisce il dato personale (Trib. Napoli, sentenze nn. 6383 e 6384 del 16 maggio 2013; in precedenza, sentenze nn. 12068 e 12098 dell'8 novembre 2012).

Può aggiungersi che in passato una sola pronuncia, emessa nel 2011 ma pervenuta al Garante nel 2013, invece, ha accolto il ricorso, evidenziando una diversità di orientamento giurisprudenziale all'interno della medesima sezione del Tribunale di Napoli. In tale decisione, il giudice, confermando che il riferimento alla l. n. 210/1992, contenuto nella causale di accredito in relazione al pagamento dell'indennizzo previsto dalla stessa legge, integra sicuramente un dato sensibile e che costituisce obbligo di legge che i mandati di pagamento contengano la precisa indicazione dell'oggetto della spesa, ha tuttavia ritenuto che debba applicarsi l'art. 22, comma 6, del Codice, il quale stabilisce che i dati sensibili debbano essere trattati, da parte dei soggetti pubblici, con tecniche di cifratura o mediante l'utilizzo di codici identificativi o di altre soluzioni che, considerato il numero e la natura dei dati trattati, li rendano temporaneamente non intellegibili anche a chi è autorizzato ad accedervi (sentenza 7 giugno 2011, n. 7157).

A sostegno di questo orientamento, il giudice ha citato il provvedimento del Garante che, in un caso analogo, ha chiesto al Ministero dell'economia e delle finanze di individuare una modalità di pagamento più rispettosa della riservatezza dei dati sulla salute degli interessati.

Un'altra pronuncia ha riguardato la richiesta di risarcimento del danno (patrimoniale e non) nei confronti di due società operanti nel campo finanziario da parte della persona titolare di una società operante nel medesimo settore e che aveva svolto la propria attività quale agente delle società convenute, le quali avevano comunicato a soggetti terzi dati di natura giudiziaria relativi alla ricorrente. L'illiceità dei comportamenti posti in essere dalle convenute era stata sancita dal provvedimento del Garante del 2 aprile 2008 (doc. web n. 1519711), a seguito di reclamo dell'attrice. In particolare, il Garante aveva rilevato che le comunicazioni lamentate erano state effettuate in assenza della prevista informativa ed erano eccedenti rispetto alle finalità perseguite. Il giudice, nel valutare la sussistenza dei requisiti per il risarcimento del danno, ha ritenuto che, ai fini della prova dell'*an debeatur*, debba ritenersi vincolante la pronuncia del Garante.

Rispetto al *quantum debeatur*, ha ritenuto che la ricorrente non avesse fornito alcuna prova dei danni patrimoniali e non conseguiti, non potendosi considerare sussistente nella specie un danno in *re ipsa*, in adesione con l'orientamento della Suprema Corte (Trib. Napoli, sentenza 12 febbraio 2013, n. 2036).

### 17.4. *Le opposizioni ai provvedimenti del Garante*

L'anno 2013 ha registrato una lieve flessione nella proposizione delle opposizioni a provvedimenti dell'Autorità: a fronte dei 73 ricorsi del 2012, nel 2013 sono state proposte sessantasette opposizioni (cfr. sez. IV, tab. 1). Di queste, trentotto si riferiscono a opposizioni a ordinanze ingiunzioni, così registrando un aumento rispetto al 2012, nel quale le impugnazioni di tale natura erano state trentaquattro.

Complessivamente, l'Autorità ha avuto notizia di quarantuno decisioni dell'autorità giudiziaria relative a opposizioni a provvedimenti del Garante, che si è sempre costituito in questi giudizi, tramite l'Avvocatura dello Stato territorialmente competente.

Ventuno sentenze hanno avuto ad oggetto opposizioni ad ordinanze ingiunzioni; in prevalenza, si è trattato di violazioni dell'art. 13 del Codice (omessa o inidonea informativa agli interessati), talvolta unitamente alla mancata acquisizione del consenso e, più raramente, ad altre violazioni della normativa in materia di protezione dei dati personali.

Al riguardo, va rilevato che, rispetto al 2012, si è manifestata una maggiore tendenza dei giudici a ridurre l'importo delle sanzioni irrogate dall'Autorità.

Tra le opposizioni alle ordinanze ingiunzioni, due decisioni hanno riguardato provvedimenti irroganti sanzioni in relazione a trattamenti di immagini raccolte mediante impianti di videosorveglianza, rispettivamente, in un'area portuale e presso una farmacia. In entrambi i casi le valutazioni dell'Autorità sono state confermate ed i ricorsi rigettati (Trib. Vibo Valentia, sez. distaccata di Tropea, sentenza 6 novembre 2012, n. 227; Trib. Piacenza, sentenza 23 maggio 2013, n. 368).

Anche in un altro caso, inerente l'invio, da parte di una società, di comunicazioni indesiderate di carattere promozionale via fax in assenza di informativa e consenso, è stato integralmente confermato il provvedimento del Garante (Trib. Padova, sentenza 4 aprile 2013, n. 877).

In tema di *e-mail* promozionali, il Tribunale di Milano ha confermato l'ordinanza ingiunzione emanata per sanzionare l'invio di tali comunicazioni senza che fossero stati assolti gli obblighi di legge. L'organo giudicante, peraltro, ha ritenuto di ridurre la sanzione, avuto riguardo alle condizioni soggettive del trasgressore (una società artigianale, operante nei confronti di una platea ristretta di utenti) e, per quanto concerne la condotta contestata, il numero assai contenuto di messaggi elettronici inviati (sentenza 17 giugno 2013, n. 8373).

Il Tribunale di Montepulciano, in analoga fattispecie, confermato il provvedimento ingiuntivo nel merito, ha ridotto l'entità della sanzione irrogata, rilevato che non vi era stata né diffusione, né conservazione dei dati trattati nonché la circostanza che l'interessato era stato messo in condizione di consultare l'informativa dopo la ricezione del messaggio di posta elettronica e di comunicare la volontà di non riceverne ulteriori (sentenza 4 aprile 2013, n. 75).

Anche il Tribunale di Santamaria Capua Vetere ha pienamente condiviso le valutazioni svolte dall'Autorità in un caso di omessa informativa relativamente alla raccolta di dati personali dei contribuenti mediante questionari, nell'ambito del servizio di riscossione dei tributi comunali (sentenza 8 maggio 2013, n. 317).

È stato altresì confermato il provvedimento ingiuntivo a carico di una azienda di trasporti per una raccolta di dati personali tramite un *form online*: il giudice si è inserito nel solco di una pacifica giurisprudenza secondo cui, in tema di sanzioni amministrative, è sufficiente e necessaria la coscienza e la volontà della condotta omissiva, senza che occorra la concreta dimostrazione del dolo o della colpa, giacché la norma pone una presunzione (relativa) di colpevolezza a carico del trasgressore. Si è reputato equo, tuttavia, ridurre la sanzione, attesa la minore gravità della violazione ed avuto riguardo al servizio pubblico svolto dall'azienda (Trib. Verona, sentenza 15 marzo 2013, n. 587).

Il Tribunale di Cosenza ha rigettato il ricorso contro un provvedimento emanato nei confronti di un'azienda ospedaliera, con cui il Garante aveva sanzionato una pluralità di violazioni del Codice. Accogliendo le osservazioni della difesa dell'Autorità, il giudice ha rilevato che il pagamento già effettuato non avesse efficacia estintiva dell'obbligazione perché versato dall'azienda, in luogo dell'obbligato, a norma dell'art. 169, comma 2, del Codice, al fine di estinguere il reato di cui al comma 1 del medesimo articolo (sentenza 22 ottobre 2013, n. 1921).

Anche in un'altra controversia vi è stata integrale conferma della sussistenza degli illeciti sanzionati dal Garante: violazione di un provvedimento dell'Autorità, omessa informativa, mancata acquisizione del consenso, mancato riscontro alle richieste di informazioni ed esibizione di documenti effettuate dal Garante, pluralità di violazioni in relazione a banche dati di particolare rilevanza o dimensioni. Il giudice ha ritenuto di operare una riduzione della sanzione, in ragione delle qualità soggettive del trasgressore, come la mancanza di precedenti specifici e le precarie condizioni economiche in cui versava (Trib. Milano, sentenza 15 ottobre 2013, n. 7555).

In materia di rilevazione di dati biometrici, è stato confermato nel merito il provvedimento del Garante che sanzionava l'omessa notificazione all'Autorità dell'avvenuta installazione, all'ingresso del palazzo di un ente pubblico territoriale, di uno strumento di riconoscimento delle impronte digitali, al fine di disciplinare l'accesso all'edificio medesimo.

Il giudice ha ritenuto di ridurre la sanzione pecuniaria, applicando la diminuente di cui all'art. 164-*bis*, comma 1, del Codice, considerato lo scopo perseguito dal ricorrente, la circostanza che il sistema non avesse mai funzionato secondo le intenzioni e, soprattutto, che il lettore non fosse idoneo ad individuare la posizione geografica delle persone mediante una rete di comunicazione elettronica (Trib. Sanremo, sez. distaccata di Ventimiglia, sentenza 6 maggio 2013, n. 75).

È stata altresì confermata l'ordinanza ingiunzione con la quale veniva sanzionata l'omessa risposta ad una richiesta di informazioni del Garante *ex* art. 157 del Codice. Il giudice adito ha respinto la censura relativa al mancato rispetto del termine di novanta giorni per la notifica della contestazione di violazione amministrativa. In conformità ad una consolidata giurisprudenza di merito e di legittimità, richiamata dalla difesa dell'Autorità, si è ribadito che il *dies a quo* va individuato non già in quello della commissione dell'infrazione, bensì nella data di accertamento della medesima da parte dell'organo procedente: la durata dell'istruttoria, peraltro, va valutata in relazione al caso concreto e sulla base della complessità delle indagini tese a riscontrare la sussistenza dell'infrazione e ad acquisire piena conoscenza della condotta illecita, sì da valutarne l'esatta consistenza agli effetti della formulazione della contestazione. L'entità della sanzione è stata tuttavia ridotta a causa delle condizioni economiche del contravventore (Trib. Milano, sentenza 4 luglio 2013, n. 9510).

Un'altra pronuncia ha confermato l'ordinanza ingiunzione emessa sulla base dell'art. 162, comma 2-*bis*, in relazione all'art. 33 del Codice (misure minime di sicurezza). Il Giudice ha ridotto l'ammontare della sanzione al minimo edittale, considerando l'importo già versato dal trasgressore in sede penale e considerato soprattutto il

successivo adeguamento della società ricorrente alla normativa in materia di protezione dei dati personali (Trib. Cagliari, sentenza 15 maggio 2013, n. 1610).

Il Tribunale di Milano ha pienamente confermato nel merito un provvedimento ingiuntivo con cui il Garante aveva sanzionato il trattamento dei dati personali dopo la revoca del consenso dell'interessato da parte di un'agenzia di viaggi *online* ed il mancato riscontro alla richiesta di informazioni dell'Autorità. Il giudice ha tuttavia deciso di operare una leggera riduzione dell'importo della sanzione, in base ad una differente valutazione sulla gravità della condotta (sentenza 16 aprile 2013, n. 5637).

È stato invece dichiarato inammissibile, per difetto di legittimazione, il ricorso sollevato in proprio da soggetto che aveva ricevuto l'ordinanza ingiunzione quale legale rappresentante di una casa di cura che aveva commesso la violazione di cui all'art. 164 del Codice. Per completezza, peraltro, il giudice ha ritenuto di respingere le censure anche nel merito e di confermare la piena legittimità del provvedimento del Garante (Trib. Torino, sentenza 29 novembre 2012, n. 6973).

Due decisioni hanno parzialmente accolto le opposizioni, revocando una delle due sanzioni che l'Autorità aveva irrogato con unico provvedimento.

In tema di messaggi sms contenenti propaganda elettorale, il Tribunale di Milano ha confermato la sanzione per mancata acquisizione del consenso, aderendo alla interpretazione, prospettata dalla difesa del Garante, secondo cui i dati personali non possono essere utilizzati in assenza di manifestazione di volontà dell'interessato solo perché reperibili nella rete internet, essendo necessario che siano inseriti in pubblici registri, elenchi, atti o documenti che sono sottoposti ad una disciplina di conoscibilità da parte di chiunque. Il giudice ha invece ritenuto che fosse applicabile alla fattispecie quanto statuito nel cd. decalogo elettorale del Garante, che esclude l'obbligo di informativa quando si tratti di materiale propagandistico di dimensione ridotte, annullando la relativa sanzione (sentenza 4 dicembre 2013). Contro tale pronuncia, il Garante ha proposto ricorso per cassazione.

In altra decisione, relativa ad una vicenda di rilevazione di dati biometrici dei dipendenti della soprintendenza locale per i beni architettonici, si è ritenuto che il titolare del trattamento, contrariamente a quanto sostenuto nell'ordinanza ingiunzione, avesse assolto l'obbligo di notificazione del trattamento mediante corrispondenza intercorsa con l'Autorità, poiché all'epoca dell'attivazione del sistema non erano ancora state individuate forme specifiche per adempiere a tale obbligo. Il giudice ha invece confermato la sussistenza della violazione relativa all'omessa informativa, ma ha ridotto l'ammontare della sanzione, in base alla minore gravità della condotta e allo scopo perseguito dal trasgressore (Trib. Napoli, sentenza 4 aprile 2013, n. 4358).

Quattro pronunce hanno invece accolto le opposizioni ad altrettanti provvedimenti ingiuntivi emanati dal Garante che, per l'effetto, sono stati annullati.

Due di esse riguardavano ordinanze ingiunzioni adottate a seguito della violazione dell'obbligo di notificazione al Garante del trattamento di dati sensibili (artt. 37 e ss. del Codice).

Nella prima, il giudice ha ritenuto che l'Ausl ricorrente non fosse tenuta a procedere alla notifica in quanto: il trattamento in questione non aveva carattere sistematico; l'esenzione dall'obbligo, formalmente riferita solo ai medici di famiglia e ai pediatri di libera scelta, era applicabile anche alle aziende sanitarie; la ricorrente non era riuscita ad effettuare la notificazione a causa di problemi tecnici legati al sito internet dell'Autorità (Trib. Piacenza, sentenza n. 108 del 27 marzo 2013). Contro tale decisione, il Garante ha proposto ricorso alla Corte di cassazione.

Nel secondo caso, giudicando sulla opposizione proposta da una casa di cura, si è ritenuto, sulla base dell'art. 37, comma 1, lett. *b*), del Codice, che l'obbligo di notifica del trattamento dei dati sensibili non sia imposto in ogni caso di effettuazione di pre-

stazioni sanitarie, ma solo quando sussista una delle finalità previste dalla norma, non rientrandovi i casi di erogazione dei servizi di diagnosi e cura compresi nell'ordinaria attività sanitaria che non siano indirizzati ai fini indicati (Trib. Pescara, sentenza 2 maggio 2013, n. 673).

In una vicenda concernente una sanzione per inidonea informativa a fronte di impianti di videosorveglianza, l'organo giudicante ha dichiarato, disattendendo la ricostruzione in punto di fatto dell'Autorità, che le misure concretamente adottate dal ricorrente erano effettivamente conformi all'art. 3.1 del provvedimento generale del Garante del 29 aprile 2004 (doc. web n. 1003482), applicabile *ratione temporis* alla fattispecie (Trib. Bari, 23 settembre 2013, n. 2798).

In un'altra vicenda si è statuito che la pubblicazione sul sito internet di un ente pubblico territoriale del nome di un individuo e della causa della sua richiesta di riconoscimento dell'infermità da causa di servizio non comportasse un illecito trattamento di dati, in quanto riconducibile all'esigenza di trasparenza amministrativa, legata all'interesse generale a conoscere del procedimento per l'incidenza dell'eventuale esito favorevole sulle risorse patrimoniali della collettività. Il trattamento, secondo il Tribunale, si è svolto nel rispetto dei principi di necessità e proporzionalità dell'azione amministrativa, atteso anche il generico richiamo ad una tabella contenente una elencazione di numerose patologie, tale da non consentire la sicura identificazione dello stato di salute dell'istante (Trib. di Foggia, sentenza 19 novembre 2013, n. 1638). L'Autorità proporrà ricorso in cassazione avverso tale decisione.

La Corte di cassazione ha, infine, dichiarato inammissibili i ricorsi proposti dall'Autorità e dalla controparte avverso una sentenza del Tribunale di Milano di parziale riforma (sul *quantum debeatur*) di una ordinanza ingiunzione emessa dal Garante per violazione dell'obbligo di informativa, sulla base dell'erronea prospettazione del vizio di motivazione della sentenza impugnata e per il tentativo di sollecitare, di fatto, un nuovo giudizio di merito (VI sez. civ., ordinanza 14 giugno 2013, n. 14938).

In un solo caso, risalente al 2012 ma pervenuto all'Autorità l'anno successivo, invece, l'impugnazione è stata proposta 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 idonea a costituire titolo per la riscossione della sanzione (Trib. Sassari, sez. distaccata di Alghero, sentenza 16 ottobre 2012, n. 170).

È giunta a conclusione, con il giudizio della Suprema Corte, una controversia relativa alla raccolta dei dati genetici in assenza di consenso dell'interessato: si trattava, in particolare, di mozziconi di sigaretta utilizzati per lo svolgimento di accertamenti biologici di compatibilità genetica, in vista di una successiva azione di disconoscimento della paternità. Il giudice della nomofilachia ha confermato la sentenza del Tribunale di Roma che aveva respinto il ricorso contro il provvedimento inibitorio del Garante (27 novembre 2008, doc. web n. 1581365). Per risolvere il caso, peraltro, la Corte si è pronunciata per l'assoggettamento dei dati genetici alla più ampia disciplina della *privacy* (con riferimento anche all'autorizzazione generale del Garante *ratione temporis* applicabile) affermando i seguenti principi: 1) i dati genetici sono i dati personali dotati del maggior grado di esclusività; 2) essi non si esauriscono in quelli di natura sanitaria od attinenti alla vita sessuale; 3) i dati genetici possono essere dati sensibili, ma hanno una potenzialità predittiva che ne determina l'ontologica diversità; 4) la collocazione dell'art. 90 del Codice nel titolo V dedicato ai dati sanitari e in un capo *ad hoc* dedicato ai dati genetici rappresenta plasticamente tale peculiarità, in quanto stabilisce in via generale un regime derogatorio rispetto agli altri dari personali anche di carattere sanitario che siano fondati su indagini genetiche; 5) al trattamento dei dati

genetici a carattere non sanitario non si applica l'art. 24, comma 1, lett. *f*), del Codice, disciplinante le ipotesi in cui i dati personali possono, previa autorizzazione del Garante, essere utilizzati senza consenso: rispetto a tale disciplina generale, infatti, l'art. 90 si pone come norma derogatoria; 6) al trattamento dei dati genetici di carattere sanitario può invece applicarsi l'art. 26, comma 4, lett. *c*), del Codice.

Nella vicenda in questione, si è affermato che il trattamento, oltre a non avere alcuna finalità sanitaria, non era neanche astrattamente riconducibile all'esercizio in sede giudiziale di un diritto della personalità di rango quanto meno pari a quello dell'interessato (art. 26, comma 4, lett. *c*), del Codice), in quanto non può essere equiparata una valutazione di opportunità *ante causam* diretta a verificare le probabilità di successo in una futura azione di disconoscimento della paternità con la necessaria utilizzazione di alcuni dati come strumenti indispensabili per ottenere tutela giurisdizionale (Corte di cassazione, I sez. civ. sentenza 13 settembre 2013, n. 21014).

La medesima Corte ha, inoltre, respinto il ricorso proposto avverso una sentenza del Tribunale di Milano che aveva confermato, in sede di giudizio di opposizione, un provvedimento emanato dall'Autorità (5 ottobre 2006, doc. web n. 1357375). La vicenda riguardava l'acquisizione da parte del datore di lavoro (nel caso di specie, un istituto bancario) di alcuni dati inerenti ai conti correnti, alle disposizioni di pagamento, all'acquisizione di titoli da parte di un proprio dipendente onde verificare la possibilità di aprire un procedimento disciplinare e, eventualmente, di far valere i propri diritti nelle competenti sedi giudiziarie. Nella sentenza, ribadito come la disciplina posta a tutela dell'interesse alla riservatezza dei dati sia derogabile quando il relativo trattamento sia esercitato per la difesa di un interesse giuridicamente rilevante e nei limiti in cui ciò sia necessario, si richiama la giurisprudenza di legittimità secondo cui la produzione in giudizio di documenti contenenti dati personali è sempre consentita ove necessaria per esercitare il proprio diritto di difesa, anche in assenza del consenso dell'interessato e quali che siano le modalità con cui è stata acquisita la loro conoscenza (I sez. civile, sentenza 11 luglio 2013, n. 17204).

Una controversia ha avuto ad oggetto il sistema di controllo del traffico internet dei dipendenti durante l'orario di lavoro; mediante un apposito *software*, infatti, una società procedeva a memorizzare l'accesso ai siti svolto da ciascun lavoratore, generando *report* individuali e quotidiani, con conservazione dei dati per un tempo variabile tra i sei mesi ed un anno; memorizzava la posta elettronica dei dipendenti e la rendeva accessibile agli amministratori del sistema informatico; controllava il traffico effettuato tramite la tecnologia VoIP.

Il Tribunale è pervenuto alla conferma del provvedimento inibitorio e prescrittivo del Garante (21 luglio 2011, n. 308, doc. web n. 1829641), tramite una ampia e precisa ricostruzione dell'evoluzione della giurisprudenza in tema di controlli cd. difensivi sull'attività del lavoratore e sul rapporto di essi con le garanzie previste dall'art. 4 dello Statuto dei lavoratori (Trib. Roma, sentenza 4 aprile 2013, n. 1196).

Il Tribunale di Pescara ha confermato il provvedimento con il quale il Garante aveva dichiarato illecito il trattamento dei dati personali effettuato a mezzo del sistema di videosorveglianza installato all'interno di un'azienda, con conseguente inutilizzabilità dei dati trattati, e aveva prescritto la designazione di incaricati o, se del caso, responsabili del relativo trattamento (4 ottobre 2012, n. 267, doc. web n. 2066968). Il giudice di merito si è uniformato alla giurisprudenza della Corte di cassazione, evocata dalla difesa del Garante, secondo cui in materia di videosorveglianza le garanzie procedurali imposte dallo Statuto dei lavoratori e dal Codice non trovano applicazione solo quando i controlli (cd. difensivi) riguardino la tutela di beni estranei al rapporto di lavoro e non siano invece anche volti ad accertare comportamenti riguardanti l'esatto adempimento delle obbligazioni discendenti dal rapporto stesso (sentenza 10 ottobre 2013).