dal SIC, anche la condanna al risarcimento del danno dell'istituto o della società che ha effettuato la segnalazione.

I casi decisi hanno riguardato la segnalazione: del fideiussore del terzo debitore in mancanza di prova dell'esistenza di un credito esigibile e del ritardato pagamento da parte del debitore principale (Tribunale di Milano, sentenza n. 13640 del 25 novembre 2010), di un omonimo del soggetto effettivamente inadempiente, con condanna al risarcimento del danno, in solido, anche della società che gestisce il SIC che non aveva verificato l'esattezza dei dati forniti dall'intermediario finanziario (Tribunale di Milano, sentenza n. 5351 del 28 aprile 2010), del sottoscrittore di un contratto di locazione finanziaria, in mancanza di prova dell'effettiva sottoscrizione del contratto (Tribunale di Roma, sentenza n. 6687 del 28 settembre 2010), dell'interessato erroneamente segnalato dall'operatore di una società finanziaria in relazione ad un contratto proposto telefonicamente e non accettato dal ricorrente (Tribunale di Brescia, sentenza n. 3764 del 16 dicembre 2010), di un correntista, in relazione ad un credito residuo a seguito della chiusura del conto corrente, a cui non era stata fornita idonea comunicazione sull'esistenza del debito, che è poi stato immediatamente saldato, mentre l'istituto aveva tardato a procedere alla cancellazione del nominativo dell'interessato dal SIC (Tribunale di Milano, sentenza n. 3716 del 22 marzo 2010).

18.4. LE OPPOSIZIONI AI PROVVEDIMENTI DEL GARANTE

L'anno 2010 ha registrato un leggero incremento delle opposizioni a provvedimenti del Garante: a fronte dei 56 ricorsi del 2009, nel 2010 sono state proposte 65 opposizioni. Di queste, 19 si riferiscono a opposizioni ad ordinanze ingiunzioni, con una sostanziale equivalenza rispetto al 2009, nel quale si erano registrate 17 opposizioni di tale natura.

L'Autorità ha avuto notizia di 17 decisioni dell'autorità giudiziaria relative a opposizioni a provvedimenti del Garante, che si è sempre costituito in questi giudizi.

Quattro pronunce concernono opposizioni ad ordinanze ingiunzioni. Tutte hanno avuto ad oggetto violazioni dell'art. 13 del Codice per omessa o tardiva informativa agli interessati (Tribunale di Arezzo, sentenza n. 197 del 18 febbraio 2010; Tribunale di Milano, sentenza n. 12973 del 16 novembre 2010 e sentenza n. 3972 del 25 marzo 2010;

Tribunale di Varese, sentenza n. 942 del 1° febbraio 2010). Tutte queste pronunce hanno respinto le opposizioni, confermando i provvedimenti del Garante. In un caso la sanzione è stata ridotta a causa della precaria situazione economica della società sanzionata.

Per quanto attiene al trattamento di dati personali effettuato in ambito giornalistico, devono essere segnalate 3 pronunce. In un caso l'Autorità, con *provvedimento* del 25 luglio 2007, aveva respinto il ricorso volto ad ottenere la cancellazione ed il blocco dell'ulteriore trattamento dei dati diffusi in un articolo pubblicato su un quotidiano [doc. *web* n. 1435059]. Il Tribunale di Verona ha respinto l'opposizione proposta dall'interessato in quanto la notizia oggetto dell'articolo è stata ritenuta di indubbia rilevanza pubblica e la sua pubblicazione rientrava nella scelta discrezionale della testata giornalistica (sentenza n. 647 del 9 febbraio 2009).

Un altro caso ha riguardato il *provvedimento* 28 maggio 2009 con il quale il Garante ha respinto il ricorso volto ad ottenere il blocco del trattamento dei dati personali in relazione ad un articolo consultabile, anche in versione informatica, nell'archivio storico di un noto quotidiano [doc. *web* n. 1635910]. Il Tribunale di Milano ha confermato il *provvedimento* del Garante, ritenendo che l'articolo contenga fatti di pubblico interesse e rispetti il limite dell'essenzialità dell'informazione (sentenza n. 4302 del 6 aprile 2010).

Infine, il Tribunale di Milano ha respinto il ricorso avverso il *provvedimento* 3 novembre 2009 con cui una società aveva chiesto l'adozione delle misure necessarie per la cancellazione, rettifica e aggiornamento delle informazioni ricavabili da un motore di ricerca di un noto sito Internet relativamente ad una notizia pubblicata su di un quotidiano *online* inerente una vicenda giudiziaria che aveva coinvolto la ricorrente [doc. *web* n. 1687662]. Il Tribunale di Milano, condividendo le argomentazioni dell'Autorità, ha affermato il difetto di legittimazione passiva della società italiana citata in giudizio, rilevando che la gestione dei servizi del motore di ricerca viene effettuata dalla società capogruppo con sede all'estero, limitandosi la società italiana ad un'attività di supporto nel campo del *marketing* (sentenza n. 10756 del 25 ottobre 2010).

L'esercizio del diritto di accesso ai dati personali ha riguardato 5 pronunce.

In 2 casi si è trattato di un'istanza di accesso ai dati relativi a una persona defunta.

Nel primo caso, l'erede aveva chiesto di poter avere accesso al nominativo del beneficiario di una polizza assicurativa sottoscritta dal *de cuius*. Il Tribunale di Roma, conformemente a quanto stabilito dal Garante con *provvedimento* 26 marzo 2009 [doc. *web* n. 1608042], ha ritenuto che l'impresa assicuratrice, in qualità di titolare del trattamento, ha l'obbligo di fornire all'erede tutte le informazioni relative alle polizze stipulate dal dante causa, ma con esclusivo riferimento agli atti contenenti i dati personali del medesimo e non anche di terzi beneficiari che non vi abbiano acconsentito (sentenza n. 13713 del 15 dicembre 2010).

Nel secondo caso il Garante, con *provvedimento* 28 settembre 2006, ha ritenuto applicabile la disciplina dell'accesso ai dati personali dettata dal Codice alla richiesta rivolta dall'erede all'istituto bancario di avere copia degli assegni rilasciati dal *de cuius*, [doc. *web* n. 1348677]. Il Tribunale di Pisa, sezione distaccata di Pontedera, ha, invece, stabilito che la movimentazione bancaria relativa ai suddetti titoli di credito non contiene dati personali e ha ritenuto applicabile la disciplina disposta dal t.u. bancario in materia di accesso alla documentazione bancaria (sentenza n. 173 del 14 aprile 2010).

Altre 2 pronunce hanno riguardato l'accesso ai dati personali in tema di lavoro.

Nel primo caso (sentenza n. 462 del 24 febbraio 2010), il Tribunale di Lecce ha respinto il ricorso proposto avverso il *provvedimento* 19 dicembre 2008 [doc. *web* n. 1582051], con il quale l'Autorità ha ordinato alla società datrice di lavoro di consentire al dipendente l'accesso ai dati personali che lo riguardano inerenti il rapporto di lavoro.

Nel secondo caso, il Garante, con *provvedimento* 21 gennaio 2010, ha ordinato ad una società di consentire ad una dipendente licenziata l'accesso alla propria casella di posta elettronica presso la sede lavorativa, nonché di trasporre i dati personali ivi contenuti su supporto cartaceo o informatico in presenza di personale appositamente incaricato dalla resistente [doc. *web* n. 1701577]. Il Tribunale di Milano ha confermato il *provvedimento* del Garante, ritenendo che le informazioni contenute nelle e-mail inviate e ricevute sulla casella di posta elettronica aziendale dal dipendente costituiscono dati personali del medesimo, che in relazione ad essi è quindi possibile chiedere l'accesso ai sensi dell'art. 7 del Codice e che le modalità di accesso delineate nel *provvedimento* sono idonee a preservare la riservatezza dell'azienda (sentenza n. 8188 del 2 settembre 2010).

Con altra pronuncia, il Tribunale di Milano ha confermato il *provvedimento* 25 marzo 2008 con il quale il Garante [doc. *web* n. 1507012] ha respinto, in quanto presentata oltre il termine previsto dalla legge, la richiesta di una società volta ad ottenere da un gestore di telefonia mobile, al fine della difesa in giudizio, i dati relativi al traffico telefonico di un'utenza (sentenza n. 13750 del 30 novembre 2010).

Una decisione ha riguardato la richiesta di un privato nei confronti di un istituto bancario, di prescrivere tutte le misure necessarie per il ripristino dei diritti del ricorrente, di conoscere dell'esistenza, della conservazione e delle modalità di gestione dei propri dati personali presso il suddetto istituto e di dichiarare l'illegittimità della diffusione dei dati e la cessazione del comportamento illegittimo. Il Tribunale di Bologna, nel respingere il ricorso, ha confermato il provvedimento 18 aprile 2008, rilevando la genericità e l'indeterminatezza della domanda, nonché l'assenza di violazioni della normativa in materia di protezione dei dati personali (sentenza n. 7997 del 4 novembre 2010).

In tema di misure di sicurezza, il Garante, con *provvedimento* 26 marzo/2 aprile 2009 ha prescritto ad un'associazione, in relazione ad un illecito utilizzo dei dati degli iscritti a fini propagandistici-elettorali da parte di un terzo, di adottare misure idonee a contenere i rischi di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta, e di designare gli incaricati del trattamento [doc. *web* n. 1606059]. Il Tribunale di Roma ha confermato integralmente il provvedimento con sentenza n. 19186 del 7 ottobre 2010.

Un'ulteriore pronuncia del Tribunale di Roma (sentenza n. 24978 del 6 aprile 2010) ha accolto il ricorso proposto da una società che gestisce banche dati nell'ambito della *cd.* "*business information*", ritenendo che alcune specifiche informazioni riferite ad un soggetto censito nella banca dati costituiscono dati pertinenti al medesimo e non eccedenti lo scopo del trattamento, e annullando il *provvedimento* 19 dicembre 2008 [doc. *web* n. 1583124].

Con un'altra decisione il Tribunale di Grosseto, annullando il *provvedimento* 14 ottobre 2009 [doc. *web* n. 1658058], ha accolto il ricorso presentato da un dirigente scolastico, ritenendo lecito il trattamento dei dati personali di un'insegnante, contenuti in un verbale

di accertamento sanitario redatto dalla commissione medica di verifica, consistito nella trasmissione, in busta chiusa, dei dati all'istituzione scolastica individuata come competente (sentenza n. 502 del 11 novembre 2010).

Infine, come già riportato (*supra*, par. 18.2.), il Tribunale di Perugia, sezione distaccata di Todi, ha dichiarato la propria incompetenza territoriale in favore del Tribunale di Roma, in applicazione dell'art. 152, comma 2, del Codice, che prevede la competenza a conoscere della controversia del Tribunale del luogo ove ha la sede legale il titolare del trattamento (sentenza n. 15 del 19 febbraio 2008).

18.5. L'INTERVENTO DEL GARANTE NEI GIUDIZI RELATIVI ALL'APPLICAZIONE DEL CODICE

Conformemente agli indirizzi giurisprudenziali e al parere espresso dall'Avvocatura generale dello Stato –che si è pronunciata in termini favorevoli alla costituzione in giudizio del Garante, ritenendo essenziale che l'Autorità possa far valere le proprie ragioni, a tutela unicamente dell'interesse pubblico, tenendo conto delle sue specifiche e caratteristiche funzioni–, il Garante ha limitato la propria attiva presenza, nei giudizi che non coinvolgono direttamente pronunce dell'Autorità, ai soli casi in cui sorge, o può sorgere, la necessità di difendere o comunque far valere particolari questioni di diritto.

In questo quadro, nel quale l'Autorità ha seguito con attenzione tutti i contenziosi nei quali non ha ritenuto opportuno intervenire, chiedendo alle avvocature distrettuali dello Stato di essere comunque informata sullo svolgimento delle vicende processuali e di ricevere comunicazione in merito agli esiti, il Garante è intervenuto in un caso in cui aveva ricevuto da un Internet *service provider* la segnalazione di una presunta attività di monitoraggio del traffico telematico dei suoi utenti da parte della Federazione antipirateria audiovisiva, desunta dagli elementi prodotti dalla Federazione nel giudizio di urgenza promosso nei confronti della segnalante presso il Tribunale civile di Roma per la asserita illecita acquisizione da parte degli utenti di opere audiovisive protette tramite la rete Internet.

L'intervento del Garante ha riguardato i profili della vicenda attinenti alla protezione dei dati personali, e in particolare:

- la possibilità che gli elementi posti a fondamento del ricorso giudiziale della Federazione fossero il risultato di un illecito trattamento di dati personali degli utenti del *provider* e, come tali, inutilizzabili, anche in sede giudiziaria (art. 11, comma 2, del Codice);
- la possibilità che la richiesta della ricorrente al giudice adito di ordinare al *provider* di comunicare alle autorità di pubblica sicurezza tutti i dati idonei alla repressione dei reati di illecita riproduzione di opere protette si sostanziasse nell'obbligo per il *provider* di effettuare un monitoraggio delle attività compiute in rete dai propri utenti e quindi di compiere un trattamento di dati personali illecito, per la sua contrarietà alle vigenti disposizioni, nazionali e comunitarie, in tema di tutela della riservatezza; trattamento che il Garante aveva già espressamente vietato (*Provv.* 10 gennaio 2008 [doc. *web* n. 1524263]).

Con ordinanza depositata il 15 aprile 2010 il Tribunale di Roma ha accolto parzialmente il ricorso cautelare della Federazione, ma ha confermato, nella sostanza, la tesi principale sostenuta dall'Autorità secondo la quale non è ammissibile, allo stato della legislazione in materia di protezione dei dati personali, che il giudice civile ordini ad un *provider* di monitorare la navigazione in rete dei propri utenti, acquisendo dati anche sui siti visitati, al fine di individuare eventuali comportamenti violativi del diritto di autore.

19. L'ATTIVITÀ ISPETTIVA E LE SANZIONI

19.1. LA PROGRAMMAZIONE DELL'ATTIVITÀ ISPETTIVA

Nel 2010 sono state effettuate 474 ispezioni sulla base dei programmi ispettivi semestrali disposti dall'Autorità.

Come evidenziato anche nelle precedenti Relazioni, l'attività di controllo è stata essenzialmente volta a verificare il rispetto dei principali adempimenti previsti dal Codice da parte di:

- enti pubblici o aziende che gestiscono banche dati di particolare rilevanza o dimensioni, in cui vengono trattati dati di ampie categorie di interessati (ad es., anagrafe tributaria, patronati, enti previdenziali, banche, comuni con riferimento all'anagrafe della popolazione, società che gestiscono banche dati per finalità di *marketing*);
- soggetti che effettuano trattamenti di dati sensibili e, in particolare, idonei a rivelare lo stato di salute degli interessati (ad es., ospedali e cliniche private e trattamenti relativi alla realizzazione del fascicolo sanitario elettronico);
- società che effettuano trattamenti di dati personali facendo ricorso a particolari tecnologie (ad es., trattamento di dati biometrici);
- società che effettuano trattamenti di dati per i quali il Codice prevede l'obbligo di notificazione (ad es., attività di profilazione o di gestione di banche dati relative al rischio di solvibilità economica, al corretto adempimento di obbligazioni, a comportamenti illeciti o fraudolenti).

Le linee di indirizzo dell'attività ispettiva sono stabilite, con cadenza semestrale, dal Collegio attraverso delibere di programmazione che indicano gli ambiti del controllo e gli obiettivi numerici da conseguire.

Sulla base di tali criteri, l'Ufficio individua i titolari dei trattamenti da sottoporre a controllo e istruisce i conseguenti procedimenti.

Le linee generali della programmazione dell'attività ispettiva vengono rese pubbliche attraverso la rivista settimanale (*Newsletter*) pubblicata sul sito *www.garanteprivacy.it*.

Lo svolgimento dell'attività ispettiva permette di acquisire importanti elementi di valutazione in ordine ad alcuni importanti profili quali il grado di adeguamento alla legge di

categorie omogenee di operatori, la sussistenza di fenomeni di ampia portata che possono costituire presupposto per l'adozione di provvedimenti generali nonché la verifica dell'impatto dei provvedimenti adottati.

In tal modo l'attività ispettiva acquisisce una valenza conoscitiva e di indirizzo oltre che repressiva. Nell'anno 2010, il programma relativo al primo semestre (gennaio-giugno) ha previsto che l'attività ispettiva fosse indirizzata a:

- trattamenti di dati personali effettuati presso istituti di credito relativamente alla legittimità della consultazione e del successivo utilizzo di dati da parte di soggetti aventi diritto, anche in riferimento al tracciamento degli accessi e a correlate misure di protezione;
- trattamenti di dati personali effettuati da società che gestiscono pagamenti attraverso carte di credito;
- trattamenti di dati personali effettuati da enti previdenziali mediante i propri sistemi informativi;
- trattamenti di dati personali effettuati dall'amministrazione finanziaria mediante il sistema informativo della fiscalità (anagrafe tributaria);
- trattamenti di dati personali effettuati da enti pubblici in relazione all'adozione dei regolamenti sui dati sensibili e alla realizzazione del fascicolo sanitario elettronico;
- trattamenti di dati personali in relazione alla formazione e commercializzazione di banche dati, per finalità di *marketing* effettuato anche attraverso l'invio di *Sms* ed *Mms*.

Con riferimento, invece, al secondo semestre (luglio-dicembre), l'attività ispettiva di iniziativa è stata finalizzata ad accertamenti nell'ambito di:

- trattamenti di dati personali effettuati da società che gestiscono pagamenti attraverso carte di credito;
- trattamenti di dati personali effettuati da enti previdenziali mediante i propri sistemi informativi;
- trattamenti di dati personali effettuati da società attraverso sistemi di rilevamento biometrici;

- trattamenti di dati personali in relazione alla formazione e commercializzazione di banche dati per finalità di *marketing* effettuato anche attraverso l'invio di *Sms* ed *Mms*;
- trattamenti di dati personali effettuati dai comuni con riferimento all'anagrafe della popolazione residente.

Nel periodo di riferimento sono state altresì effettuate:

- verifiche sull'adozione delle misure minime di sicurezza da parte di soggetti, pubblici e privati, che effettuano trattamenti di dati sensibili;
- altre verifiche di iniziativa concernenti, in particolare, l'adempimento dell'obbligo di notificazione da parte di soggetti, pubblici e privati, individuati mediante raffronto con il registro generale dei trattamenti;
- verifiche sulla liceità e correttezza dei trattamenti di dati personali con particolare riferimento al rispetto dell'obbligo di informativa, alla pertinenza e non eccedenza nel trattamento, alla libertà e validità del consenso, nei casi in cui questo è necessario, nonché alla durata della conservazione dei dati nei confronti di soggetti, pubblici o privati, appartenenti a categorie omogenee. Ciò, prestando anche specifica attenzione a profili sostanziali del trattamento che spiegano significativi effetti sulle persone da esso interessate.

In base ai regolamenti dell'Autorità, l'istruttoria preliminare relativa alle ispezioni effettuate d'ufficio sulla base dei criteri fissati dal Collegio spetta al dipartimento attività ispettive e sanzioni.

Effettuati gli accertamenti sulle presunte violazioni, il dipartimento procede direttamente alle contestazioni di sanzioni amministrative e inoltra gli atti alla competente unità organizzativa per il seguito di trattazione, che concerne profili diversi dall'applicazione di sanzioni (adozione di provvedimenti prescrittivi o inibitori).

Il dipartimento attività ispettive e sanzioni cura, altresì, i controlli nell'ambito delle istruttorie preliminari e dei procedimenti amministrativi comunque avviati presso altre unità organizzative (di norma sulla base di segnalazioni, ricorsi o reclami), cui è restituito l'esito per la successiva trattazione.

19.2. LA COLLABORAZIONE CON LA GUARDIA DI FINANZA

Anche nell'anno di riferimento l'Autorità si è avvalsa della preziosa collaborazione della Guardia di finanza per lo svolgimento dell'attività di controllo in applicazione del protocollo di intesa siglato nel 2005. Al riguardo si fa rinvio a quanto nel dettaglio riferito nelle precedenti edizioni (cfr., da ultimo, *Relazione* 2009, p. 240 ss.), evidenziando la meritoria attività svolta dal Nucleo speciale *privacy*, che ha provveduto direttamente a effettuare gli accertamenti, avvalendosi anche, ove necessario, dei reparti del Corpo territorialmente competenti.

Come già accade da alcuni anni, le informazioni e i documenti acquisiti nell'ambito degli accertamenti sono stati trasmessi all'Autorità per le successive verifiche in ordine alla liceità del trattamento e al rispetto dei princìpi previsti dalla legge. Laddove siano emerse violazioni penali o amministrative, la Guardia di finanza ha direttamente segnalato la notizia di reato all'autorità giudiziaria e contestato la sanzione amministrativa.

Si è registrato inoltre un importante coinvolgimento nell'attività di controllo della componente territoriale della Guardia di finanza (nuclei di polizia tributaria, gruppi, compagnie e tenenze) e un rafforzamento del ruolo di coordinamento del Nucleo speciale *privacy* rispetto all'attività subdelegata a tali reparti.

In tal modo l'Autorità ha fruito di un dispositivo di controllo flessibile ed articolato, idoneo a espletare l'attività di controllo sul territorio in modo più efficace e tempestivo.

19.3. I SETTORI OGGETTO DEI CONTROLLI E I CASI PIÙ RILEVANTI

Nel 2010 sono state effettuate, suddivise per settore, le seguenti attività ispettive:

- 85 controlli nei confronti di cliniche private, ospedali e case di cura pubbliche, centri di chirurgia estetica e società che gestiscono cartelle cliniche che trattano dati relativi alla salute, con riferimento alla liceità dei trattamenti effettuati e all'adozione delle misure minime di sicurezza;
- 35 controlli nei confronti di centri di riabilitazione, con riferimento al trattamento dei dati degli utenti;
- 34 controlli nei confronti di società telefoniche, *dealer* e altri soggetti, con riferimento

alle modalità di attivazione delle schede telefoniche (*Sim card*), al fine di verificare il rispetto delle prescrizioni contenute nel *provvedimento* 16 febbraio 2006 [doc. *web* n. 1242592] in tema di servizi telefonici non richiesti;

- 30 controlli nei confronti di esercizi ricreativi, con riferimento al trattamento dei dati dei clienti effettuato anche mediante raccolte di dati via *web*;
- 25 controlli nei confronti di soggetti vari che hanno effettuato la notificazione al registro generale dei trattamenti;
- 20 controlli nei confronti di scuole ed istituti di formazione, con riferimento al trattamento dei dati dei discenti effettuato anche mediante raccolte di dati via *web*;
- 20 controlli nei confronti di soggetti fornitori di servizi di ricezione ed ospitalità, con riferimento al trattamento dei dati dei clienti effettuato anche mediante raccolte di dati via *web*;
- 17 società di noleggio, con riferimento al trattamento dei dati dei clienti effettuato anche mediante raccolte di dati via *web*;
- 14 controlli nei confronti di società che commercializzano banche dati a terzi per finalità di *marketing* anche attraverso l'invio di *Sms*, *Mms* ed e-mail, volti a rilevare la liceità del trattamento, con particolare riferimento al consenso degli interessati all'utilizzo dei propri dati;
- 13 controlli nei confronti di chiromanti, con riferimento al trattamento dei dati dei clienti effettuato anche mediante raccolte di dati via *web*;
- 11 controlli nei confronti di università *online*, con riferimento al trattamento dei dati degli studenti;
- 10 controlli nei confronti di istituti di credito, con riferimento alla legittimità della consultazione e del successivo utilizzo dei dati da parte di soggetti aventi diritto, anche in riferimento al tracciamento degli accessi e a correlate misure di protezione;
- 8 controlli nei confronti di società che effettuano attività di *marketing* attraverso l'invio di fax, volti a rilevare la liceità del trattamento, con particolare riferimento al consenso degli interessati all'utilizzo dei propri dati per tali finalità;

- 3 controlli nei confronti di enti previdenziali e patronati che utilizzano i sistemi informativi dei predetti enti volti a rilevare la liceità dei trattamenti e le misure di sicurezza adottate;
- 3 controlli nei confronti di società che gestiscono pagamenti attraverso carte di credito con riferimento alle modalità di trattamento dei dati dei clienti;
- 2 controlli nei confronti di soggetti pubblici che utilizzano i sistemi informativi della fiscalità mediante l'anagrafe tributaria volti a rilevare la liceità dei trattamenti e le misure di sicurezza adottate;
- 2 controlli nei confronti di comuni con riferimento ai trattamenti di dati personali effettuati attraverso l'anagrafe della popolazione residente e l'anagrafe degli italiani residenti all'estero.

A questi si aggiungono i 109 controlli effettuati nei confronti di altri soggetti, per esigenze istruttorie connesse a specifiche segnalazioni pervenute all'Autorità.

In relazione a quanto emerso dagli accertamenti, sono state effettuate numerose proposte di adozione di provvedimenti inibitori e/o prescrizioni per conformare il trattamento alla legge, a fronte delle quali l'Autorità ha adottato alcuni provvedimenti di particolare rilievo per le garanzie nei confronti dei cittadini.

Tra i più rilevanti, in ordine cronologico, si segnalano:

- il *provvedimento* con il quale il Garante, a conclusione dell'istruttoria svolta nei confronti di INPS, INPDAP, ENPALS, AVCP, camere di commercio ed AGEA, ha prescritto all'Agenzia delle entrate specifiche misure, di carattere prevalentemente tecnico, idonee ad assicurare che l'accesso all'anagrafe tributaria effettuato dai predetti enti attraverso la nuova classe di *web* service predisposta dall'Agenzia avvenga nel rispetto del Codice. Nel medesimo *provvedimento* è stata altresì prescritta ai predetti enti, utilizzatori dei *web* service dell'Agenzia delle entrate, l'adozione di ulteriori misure da seguire nella fase di integrazione di tali strumenti nell'ambito dei propri applicativi (*Provv.* 26 marzo 2010 [doc. *web* n. 1713453]);
- il nuovo *provvedimento* generale in materia di videosorveglianza, di cui si è riferito nella *Relazione* 2009, p. 25 ss. (*Provv.* 8 aprile 2010 [doc. *web* n. 1712680]);

- il *provvedimento* con il quale il Garante ha vietato ad una società che gestisce un portale che promuove la prenotazione di servizi turistici qualunque trattamento a fini di profilazione effettuato senza il consenso preventivo, specifico e informato degli interessati ed ha prescritto alla medesima società di rendere conforme alle disposizioni del Codice l'informativa data attraverso il proprio sito *web* (*Provv.* 8 aprile 2010 [doc. *web* n. 1721205]);
- il *provvedimento* con il quale il Garante ha disposto il blocco del trattamento dei dati personali effettuato da una ditta individuale a mezzo videosorveglianza presso un proprio punto vendita, in attesa dell'eventuale espletamento delle procedure previste dalla l. n. 300/1970 (Statuto dei lavoratori) per i casi in cui tali strumenti siano idonei a configurare un controllo a distanza dei lavoratori (*Provv.* 10 giugno 2010 [doc. *web* n. 1736167]);
- il *provvedimento* con il quale il Garante ha disposto il blocco del trattamento delle immagini riprese nelle aree interne, per mezzo di un sistema di videosorveglianza, da un centro per la riabilitazione, nelle more dell'espletamento delle procedure previste dalla l. n. 300/1970 (Statuto dei lavoratori) per i casi in cui tali strumenti siano idonei a configurare un controllo a distanza dei lavoratori, invitando il medesimo soggetto ad adottare, medio tempore, adeguate misure alternative per garantire l'incolumità di pazienti, operatori sanitari e dipendenti (*Provv.* 24 giugno 2010 [doc. *web* n. 1738396]);
- il *provvedimento* con il quale il Garante ha vietato a un importante gruppo societario, operante nel settore radiofonico e nella gestione dei siti Internet delle proprie emittenti e dei concorsi a premi da queste effettuati, il trattamento di dati personali degli utenti raccolti attraverso i siti *web* delle emittenti, finalizzato all'invio di comunicazioni commerciali, ad operazioni di profilazione e alla comunicazione a terzi dei dati personali senza il necessario consenso specifico, libero e informato. Nel medesimo *provvedimento* sono state altresì prescritte le misure necessarie per rendere conforme il trattamento alle disposizioni del Codice con riferimento alle modalità con le quali viene resa l'informativa, al relativo contenuto e agli adempimenti in tema di notificazione per i trattamenti effettuati a fini di profilazione (*Provv.* 22 luglio 2010 [doc. *web* n. 1741988]);

- il *provvedimento* con il quale l'Autorità ha tra l'altro prescritto ad una società, operante nel settore del mailing postale per finalità di comunicazione commerciale e di *marketing*, di pubblicare almeno una volta l'anno l'informativa prevista dall'art. 13 del Codice, con la specifica ed aggiornata indicazione delle fonti da cui i dati sono tratti, compresa l'ipotesi in cui gli stessi siano acquisiti da società terze, tramite un avviso su tre quotidiani ad ampia diffusione nazionale, nonché di pubblicare la medesima informativa anche sul proprio sito *web*, in un'apposita sezione dedicata alla *privacy*, adeguatamente evidenziata in autonomi riquadri e di immediata consultazione (*Provv.* 16 dicembre 2010 [doc. *web* n. 1781973]).

19.4. L'ATTIVITÀ SANZIONATORIA DEL GARANTE

19.4.1. Violazioni penali e procedimenti relativi alle misure minime di sicurezza

A seguito delle ispezioni effettuate e, più in generale, dall'esame degli atti delle istruttorie effettuate dall'Autorità si sono rilevati gli estremi per l'invio all'autorità giudiziaria di 55 informative (di cui 25 direttamente da parte dell'Autorità e 30 da parte della Guardia di finanza).

Le segnalazioni relative a presunte violazioni penali hanno riguardato:

- in 34 casi la mancata adozione delle misure minime di sicurezza;
- in 7 casi l'inosservanza di un *provvedimento* del Garante;
- in 4 casi la falsità nelle dichiarazioni e notificazioni al Garante;
- in 3 casi il trattamento illecito dei dati;
- in 7 casi violazioni della l. n. 300/1970 (Statuto dei lavoratori) ora punite come reato dall'art. 171 del Codice, o violazioni penali previste da disposizioni non contenute nel Codice in materia di protezione dei dati personali.

Come dimostrano i dati sopra riportati, la violazione penale più frequentemente accertata riguarda il mancato rispetto delle disposizioni concernenti le misure minime di sicurezza che devono essere adottate da coloro che trattano dati personali (titolari, responsabili ed incaricati) per assicurare agli interessati di cui trattano i dati un livello di sicurezza adeguato predefinito dalle norme.

Come noto, in base all'art. 169, comma 2, del Codice, nel caso in cui venga rilevata

una violazione di una o più delle misure minime di sicurezza specificatamente previste dal Disciplinare tecnico sulle misure di sicurezza (Allegato B. al Codice), il Garante impartisce una prescrizione alla persona individuata come responsabile della predetta violazione e, verificato il ripristino delle misure violate, ammette il destinatario della prescrizione al pagamento del quarto del massimo della sanzione prevista (pari a 30.000 euro). L'adempimento alla prescrizione ed il pagamento della somma, vengono comunicati all'autorità giudiziaria competente per le valutazione in ordine all'estinzione del reato.

Con riferimento a questa complessa procedura, i procedimenti definiti nell'anno 2010 connessi al *cd.* "ravvedimento operoso" in materia di misure minime di sicurezza, sono stati 17 e hanno determinato il pagamento all'Autorità di 457.500 euro da parte delle persone responsabili delle violazioni.

19.4.2. Sanzioni amministrative

A seguito delle ispezioni effettuate e delle istruttorie curate dall'Ufficio, sono stati avviati 424 procedimenti sanzionatori amministrativi (di cui 220 direttamente dal Garante e 204 da parte della Guardia di finanza e di altri organi accertatori).

Le sanzioni amministrative contestate hanno riguardato le seguenti violazioni:

- omessa o inidonea informativa (239);
- trattamento dei dati in violazione dell'art. 33 o delle disposizioni indicate nell'art. 167 (124);
- omessa informazione o esibizione al Garante (19);
- omessa o incompleta notificazione (20);
- inosservanza di un *provvedimento* del Garante (12);
- sanzioni in materia di conservazione dei dati di traffico (4);
- più violazioni da parte di soggetti che gestiscono banche dati di particolare rilevanza o dimensioni (6).

Sotto il profilo economico, le sanzioni contestate nell'anno 2010 prevedono la possibilità di applicare pene pecuniarie da un minimo di circa 5.200.000 euro a un massimo di circa 31.100.000 euro.

Gli importi relativi alle sanzioni applicate dal Garante sono versati sul bilancio dello Stato.

Sulla base di quanto previsto dall'art. 166 del Codice, tali proventi, nella misura del 50% del totale annuo sono riassegnati al fondo stanziato per le spese di funzionamento dell'Autorità previsto dall'art. 156, comma 10, del Codice e sono utilizzati unicamente per l'esercizio della attività ispettiva e di divulgazione della disciplina della protezione dei dati personali.

Complessivamente le entrate relative all'attività sanzionatoria per l'anno 2010 sono effettivamente state pari a 3.809.000 euro in relazione a:

- 319 procedimenti sanzionatori spontaneamente definiti mediante pagamento dai contravventori (per un importo di 3.046.001 euro);
- 132 ordinanze-ingiunzione adottate dall'Autorità sulla base dell'esame delle memorie e delle audizioni delle parti (per un importo di 306.400 euro);
- 17 ammissioni al pagamento in relazione a procedimenti sulle misure minime di sicurezza (per un importo di 457.500 euro).

Occorre evidenziare che la gran parte dei procedimenti sanzionatori definitisi nell'anno 2010 riflette ancora violazioni commesse in epoca anteriore all'entrata in vigore del d.l. 30 dicembre 2008, n. 207 (convertito nella l. 27 febbraio 2009, n. 41), e per le quali l'ammontare delle pene pecuniarie era sensibilmente inferiore a quello attuale.

Sono stati 86 i procedimenti sanzionatori definitisi in senso favorevole al contravventore con l'adozione di ordinanze di archiviazione.

Come evidenziano i dati, il maggior numero di sanzioni erogate ha riguardato la violazione dell'obbligo di fornire all'interessato tutte le informazioni riguardanti il trattamento dei dati, al fine di renderlo pienamente consapevole dell'effettivo utilizzo dei suoi dati personali.

In particolare, tale violazione è stata riscontrata sui siti *web*, a fronte di una raccolta dei dati effettuata mediante *form* e spesso finalizzata a raccogliere richieste di utenti. Tale circostanza ha indotto i gestori dei siti Internet a ritenere che non fosse necessario indicare l'informativa in calce ai predetti *form*, sul presupposto che i dati erano forniti