In altra controversia è stato rigettato il ricorso di una società avverso il provvedimento con il quale il Garante aveva dichiarato illecito, e conseguentemente vietato, l'invio di fax promozionali ad operatori turistici o titolari di agenzie di viaggi in assenza di una informativa e di un consenso espresso documentato per iscritto e aveva prescritto le misure necessarie ed opportune per rendere il trattamento conforme alla normativa in materia di protezione di dati personali (21 marzo 2012, n. 113, doc. web n. 1895176). Il giudice ha integralmente accolto la ricostruzione, in fatto e in diritto, che ha condotto all'adozione del provvedimento (Trib. Milano, sentenza 10 aprile 2013, n. 4978).

È stato altresì respinto il ricorso contro un provvedimento di infondatezza dell'Autorità (14 luglio 2011, n. 293, doc. web n. 1835222). In quella circostanza, il Garante aveva ritenuto che non vi fosse stata violazione della normativa in materia di protezione di dati personali da parte di una banca che, ricevuto un reclamo per *mobbing* (da cui sarebbero discesi problemi di salute per la reclamante) nei confronti di uno dei propri dipendenti, ne aveva dato notizia al medesimo dipendente nel corso dello svolgimento degli accertamenti interni di natura disciplinare e fornito copia a fini di tutela nelle sedi competenti. Il Tribunale ha confermato la liceità dell'uso dei dati fatto in attività contenziose e precontenziose, condividendo peraltro la posizione dell'Autorità secondo cui il generico riferimento, fatto dallo stesso interessato, a problemi di salute non costituisca di per sé dato sensibile ai fini della più esigente disciplina codicistica (Trib. Roma, sentenza 26 luglio 2013, n. 10817).

Una vicenda ha riguardato la pubblicazione su un quotidiano nazionale di un documento, formato all'interno di una grande azienda radiotelevisiva, contenente l'organigramma della stessa, nel quale i nomi dei dirigenti erano stampati con colori diversi a seconda della loro presunta affiliazione partitica: nell'articolo di commento, inoltre, si denunciava l'occupazione e la lottizzazione della società da parte dei partiti politici. Il Garante, adito separatamente da alcuni dirigenti e dall'azienda stessa, aveva adottato, per quanto qui interessa, provvedimenti di infondatezza (rispettivamente, 30 ottobre 2008 e 12 febbraio 2009, doc. web nn. 1571719 e 1598380). Il Tribunale di Roma, in sede di opposizione ad entrambi i provvedimenti, si è pronunciato sulla vicenda con due distinte sentenze di analogo tenore. Accogliendo le argomentazioni del Garante, il giudice, dopo aver ben distinto gli eventuali profili di rilevanza penale da quelli attinenti alla protezione dei dati personali, ha sottolineato come il trattamento dei dati nell'esercizio di attività giornalistica possa prescindere dal consenso dell'interessato e dall'autorizzazione del Garante, avendo ritenuto il legislatore di dover fornire, quando l'informazione sia essenziale rispetto a fatti di interesse pubblico, una sorta di attenuazione del grado di tutela del diritto alla protezione dei dati personali. Si è ritenuta dunque la pubblicazione non eccedente le finalità del trattamento ma, al contrario, del tutto pertinente ed indispensabile per sostenere il ragionamento seguito (Trib. Roma, sentenze 3 aprile 2013, nn. 13269 e 13268).

Il medesimo ufficio giudiziario, inoltre, ha confermato un provvedimento di non luogo a provvedere del Garante (10 novembre 2010, doc. web n. 1776249): in relazione a delle intercettazioni telefoniche a carico di un dirigente di una società, disposte dall'autorità giudiziaria ed inviate al datore di lavoro per eventuali valutazioni disciplinari, un terzo non destinatario di tale procedimento, che vi compariva in quanto interlocutore, lamentava – a seguito della trasmissione delle intercettazioni al consiglio d'amministrazione dell'azienda – l'indebito trattamento dei propri dati personali. Il giudice ha confermato le valutazioni dell'Autorità, secondo cui non vi erano i presupposti per aprire un autonomo procedimento volto a verificare la sussistenza di eventuali profili di illiceità. Premessa la liceità dell'utilizzo delle intercettazioni telefoniche a fini disciplinari, il Tribunale ha affermato l'inscindibilità del contenuto dell'intercet-

tazione, che coinvolge necessariamente anche un soggetto diverso dal diretto destinatario dell'azione, la cui posizione non può essere separata od oscurata se non a pena di rendere incomprensibile il significato della conversazione. L'interessato, peraltro, aveva ricevuto adeguati ragguagli sul trattamento, essendo egli stesso membro del Cda (Trib. Roma, sentenza 10 luglio 2013, n. 15198).

Una pronuncia, di cui si è già dato conto nel paragrafo riguardante i profili procedurali (cfr. *supra*, par. 17.2), ha confermato il provvedimento (20 settembre 2012, n. 259, doc. web n. 2106524) con cui l'Autorità ha dichiarato il non luogo a provvedere, alla luce dell'esaustivo riscontro inviato dal titolare del trattamento. Il giudice ha inoltre evidenziato, come correttamente il Garante avesse distinto ai fini della propria decisione, la richiesta di comunicazione dei dati personali di cui agli artt. 7 e ss. del Codice e diritto di accesso a documenti bancari previsto dall'art. 119 del Testo unico bancario, diversi nella disciplina e nelle finalità (Trib. di Catania, sez. distaccata di Paternò, sentenza 10 giugno 2013, n. 1139).

È stata dichiarata improcedibile una opposizione avverso un provvedimento di inammissibilità del Garante (4 novembre 2010, doc. web n. 1774912), per la non corretta instaurazione del contraddittorio, ed esattamente per mancato rispetto, da parte del ricorrente, del termine perentorio per la notificazione stabilito dal giudice istruttore a norma dell'art. 152, comma 7, del Codice (successivamente abrogato). Il Tribunale adito non si è pertanto pronunciato sul merito del provvedimento opposto (Trib. Perugia, sentenza 22 febbraio 2013, n. 139).

Una pronuncia si è occupata del tema delle cd. telefonate mute nell'ambito dell'attività di chiamata plurima da parte dei *call center*, ossia di quelle chiamate nelle quali il destinatario, dopo aver sollevato il ricevitore, non viene messo in comunicazione con alcun interlocutore (in merito v. par. 10.4): il Garante, con proprio provvedimento (6 dicembre 2011, n. 474, doc. web n. 1857326), aveva tra l'altro prescritto a due società che il contatto del destinatario di una telefonata muta non venisse richiamato per almeno trenta giorni. Il Tribunale di Roma ha confermato che il procedimento di raccolta, registrazione, consultazione, selezione, utilizzo e blocco della comunicazione che conduce alla telefonata muta è da considerarsi a tutti gli effetti un trattamento di dati personali. L'uso dei dati per una telefonata muta, inoltre, contrasta con il canone della correttezza di cui all'art. 11 del Codice, dal momento che tutto il sistema di selezione e formulazione delle chiamate passate agli operatori fa cadere il rischio e il disagio non su chi effettua la telefonata ma sui destinatari. Il giudice ha conclusivamente ritenuto che il provvedimento del Garante non fosse lesivo della possibilità di condurre campagne commerciali telefoniche, rigettando le censure di difetto di proporzionalità e ragionevolezza (sentenza 26 settembre 2013, n. 18977).

Il Tribunale di Padova ha confermato una nota con cui l'Ufficio aveva chiuso un'istruttoria preliminare, non avendo rilevato, in tema di videosorveglianza stradale, alcun profilo di violazione della disciplina posta a tutela dei dati personali. Il giudice ha ritenuto provata l'esistenza di uno specifico cartello che informava gli utenti che percorrevano il tratto di strada oggetto di controllo; a nulla è valso al ricorrente opinare che, nel senso opposto di marcia, da lui non percorso, non fosse presente alcuna segnaletica informativa. Si è infatti sottolineato che, anche in materia di tutela della riservatezza, chi agisce in giudizio non può agire a tutela della *privacy* indifferenziata degli utenti, ma solo a tutela di un proprio, specifico interesse alla protezione dei dati personali (sentenza 7 agosto 2013, n. 1330).

Il Tribunale di Roma ha invece ritenuto illecita la condotta dell'Agenzia delle dogane, la quale aveva inviato il provvedimento di trasferimento di un lavoratore, motivato sulla base di alcune indagini che la Procura della Repubblica stava svolgendo in ordine a gravi ipotesi di reato ad esso ascrivibili, non soltanto al direttore

dell'ufficio ove era impiegato, in quanto titolare del trattamento dei dati personali, ma genericamente all'ufficio, utilizzando un protocollo ordinario e non riservato e rendendo, di fatto, la nota di pubblico dominio tra i colleghi ed i superiori dell'interessato. Il giudice, discostandosi dalle valutazioni dell'Autorità (provv. 6 maggio 2010, doc. web n. 1724717), ha ritenuto che il datore di lavoro avrebbe dovuto adottare le più opportune cautele per prevenire la conoscibilità ingiustificata dei dati personali da parte di terzi, considerando infatti che, a norma dell'art. 22 del Codice, il trattamento di dati *sensibili* e *giudiziari* deve avvenire con modalità volte a prevenire violazioni dei diritti, delle libertà fondamentali e della dignità dell'interessato (sentenza 20 maggio 2013, n. 8437).

Il Tribunale di Torino ha confermato un provvedimento (11 ottobre 2012, n. 289, doc. web n. 2131862) con cui il Garante aveva dichiarato inammissibile un ricorso sul presupposto che il Codice non consente di chiedere la conferma di dati di cui è *sub iudice* la stessa giuridica esistenza, né di ottenere l'integrazione di informazioni o la rielaborazione delle stesse secondo modalità indicate dal ricorrente (si trattava, nel caso di specie, di una polizza assicurativa). Il giudice ha confermato che fino a quando l'esistenza del dato personale non sarà accertata con sentenza passata in giudicato, nessun diritto di accesso a tale dato potrà essere attribuito al ricorrente (ordinanza *ex* art. 702-*bis* c.p.c. del 23 aprile 2013).

È stato altresì confermato il provvedimento (17 aprile 2012, n. 149, doc. web n. 1905893) di infondatezza di un ricorso con cui un soggetto lamentava il presunto utilizzo di dati personali da parte del proprio precedente datore di lavoro, con il quale era pendente una controversia davanti all'autorità giudiziaria: il Tribunale ha ribadito, oltre alla liceità del trattamento al fine di far valere o difendere un diritto in sede giudiziaria, l'inammissibilità di richieste di tutela di dati personali meramente esplorative o congetturali (Trib. Prato, sentenza 29 marzo 2013).

In una interessante pronuncia il Tribunale di Firenze ha confermato un provvedimento inibitorio del Garante (26 ottobre 2011, n. 407, doc. web n. 1851750), reso in materia di trattamento di dati da parte di una società che si occupava di selezionare, nell'ambito di banche dati che raccolgono i dati personali di clienti di società committenti, gruppi di clienti a cui inviare *e-mail* per conto delle medesime committenti. Il Garante aveva adottato il proprio provvedimento rilevando come, non essendo stata designata la società in questione come responsabile del trattamento da parte delle committenti, essa dovesse ritenersi autonomo titolare e quindi tenuta a rendere l'informativa e ad acquisire il consenso degli interessati.

Il Tribunale ha ricordato che – per evitare che si renda necessaria una duplicazione degli obblighi informativi e di acquisizione del consenso nelle ipotesi in cui il titolare del trattamento decida di demandare a terzi la gestione dei dati – è stata prevista la possibilità di nominare per iscritto un responsabile del trattamento, la cui legittimazione al trattamento discende dall'adempimento degli obblighi di legge da parte del titolare. Il giudice ha inoltre sottolineato come costituiscano dati personali anche quelli che, pur non consentendo una identificabilità diretta, possano rendere comunque identificabile la persona a cui si riferiscono, mediante l'aggregazione dei dati relativi al sesso, alla fascia di età, alla regione e provincia di residenza e ad altre informazioni (sentenza 11 marzo 2013, n. 826).

La Corte suprema di cassazione è intervenuta in una controversia relativa alla pubblicazione, nell'ambito di un *dossier online* relativo ad alcuni soggetti, formato da una società operante nel settore delle informazioni commerciali, della notizia del fallimento di una società nella quale essi avevano ricoperto il ruolo di soci e di consiglieri di amministrazione, in epoca precedente alla dichiarazione di fallimento. Il Garante aveva accolto il ricorso degli interessati e, per l'effetto, disposto il divieto di

rendete ulteriormente disponibile l'informazione relativa alla dichiarazione di fallimento della società laddove figurasse direttamente associata agli interessati (11 febbraio 2010, doc. web n. 1705084).

In una articolata motivazione, oltre a confermare la legittimità del provvedimento opposto, il giudice della nomofilachia ha anche rammentato che la tutela dei dati personali comprende anche quelli già pubblici o pubblicati poiché colui che compie operazioni di accostamento, comparazione, esame, analisi, congiunzione, rapporto o incrocio, può ricavare ulteriori informazioni e quindi un valore informativo aggiuntivo, non estraibile dai dati isolatamente considerati, potenzialmente lesivo della dignità dell'interessato, la quale costituisce valore sommo nel nostro ordinamento. Nella gerarchia dei valori costituzionali, infatti, esso risulta preminente rispetto all'iniziativa economica privata di cui all'art. 41 della Costituzione, che infatti non può svolgersi in modo da recare danno alla dignità umana (I sez. civ., sentenza 8 agosto 2013, n. 18981).

Nel corso del 2013 è, infine, pervenuta all'Autorità una sentenza resa nel 2005 dalla Suprema Corte in tema di trattamento di dati personali nell'ambito di investigazioni difensive finalizzate a far valere un diritto in sede giurisdizionale (più esattamente, in sede di arbitrato rituale). Con provvedimento del 19 febbraio 2002 (doc. web n. 1063652) l'Autorità aveva affermato, tra l'altro, che il temporaneo differimento del diritto dell'interessato ad opporsi al trattamento ed ottenere la cancellazione dei dati è legittimo solo nel periodo in cui ciò potrebbe arrecare un effettivo pregiudizio per lo svolgimento delle investigazioni o per l'esercizio del diritto; non appena ultimate le operazioni di raccolta e trattamento e versata la relativa documentazione nel giudizio (ivi compreso quello arbitrale), non vi è più ragione di operare un ulteriore rinvio dell'esercizio dei diritti dell'interessato. Tale impostazione era stata confermata dal Tribunale di Bergamo. La Corte di cassazione, nel respingere il ricorso, ha ritenuto che tale soluzione costituisca "un ragionevole e soddisfacente punto di equilibrio tra gli interessi confliggenti, quello dell'interessato e quello degli autori e committenti della raccolta e del trattamento di tali dati" (I sez. civ. sentenza 15 luglio 2005, n. 15076).

17.5. *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, l'Autorità ha comunque seguito con attenzione tutti i contenziosi nei quali non ha ritenuto opportuno intervenire, chiedendo alle avvocature distrettuali dello Stato di essere comunque informata sullo svolgimento delle vicende processuali e di riceverne comunicazione in merito agli esiti.

18 L'attività ispettiva e le sanzioni

18.1. *La programmazione dell'attività ispettiva*

L'attività ispettiva è lo strumento istruttorio necessario per accertare *in loco* situazioni di fatto che devono essere oggetto di valutazione da parte dell'Autorità in relazione a specifici casi. Essa però è spesso utilizzata anche con lo scopo di acquisire conoscenze in relazione a fenomeni nuovi in vista di una successiva regolazione da parte del Garante attraverso i cc.dd. provvedimenti generali.

Le ispezioni, 411 nel 2013 (cfr. sez. IV, tab. 1), sono state effettuate sulla base di programmi ispettivi semestrali secondo linee di indirizzo stabilite dal Collegio con delibere di programmazione che indicano gli ambiti del controllo e gli obiettivi numerici da conseguire. Le linee generali della programmazione dell'attività ispettiva vengono quindi rese pubbliche attraverso il sito web del Garante (cfr. *newsletter* n. 369 del 14 febbraio 2013 e n. 376 del 2 agosto 2013) e, sulla base dei criteri così fissati, l'Ufficio individua i titolari dei trattamenti da sottoporre a controllo e istruisce i conseguenti procedimenti.

Il programma relativo al primo semestre 2013 ha previsto che l'attività ispettiva fosse, tra l'altro, indirizzata nei seguenti settori:

- grandi banche dati pubbliche: per controllare i trattamenti di dati personali effettuati da enti previdenziali, mediante i propri sistemi informativi, e dall'amministrazione finanziaria, mediante il sistema informativo della fiscalità (cd. Anagrafe tributaria). Questa attività è condotta con continuità da diversi anni con lo scopo di garantire che gli accessi ai dati contenuti in queste enormi banche dati gestite da soggetti pubblici avvenga solo ed esclusivamente nel rispetto dei presupposti fissati dal legislatore e che vengano costantemente aggiornate le misure per prevenire qualunque forma di violazione della sicurezza dei dati;
- Fascicolo sanitario elettronico: (attività differita al fine di tenere presente i recenti sviluppi normativi) per rilevare l'impostazione dei trattamenti di dati personali effettuati dagli enti pubblici in relazione all'istituzione del Fse che rappresenta lo strumento di raccolta e di condivisione delle informazioni e dei documenti clinici afferenti al cittadino, generati dai vari attori del sistema sanitario;
- *telemarketing*: per accertare la liceità dei trattamenti di dati personali effettuati anche mediante sistemi automatizzati, in relazione alle attività di *marketing* telefonico realizzata mediante *call center* operanti anche all'estero. Questa attività si inserisce organicamente nel complesso di iniziative istruttorie con le quali l'Autorità si è preposta l'obiettivo di contrastare fenomeni di illecito trattamento dei dati connessi alle attività di *marketing* (che sono purtroppo ancora oggetto di frequente segnalazione);
- *mobile remote payment* (sistema che consente l'acquisto di beni digitali quali ad es., quotidiani *online*, libri elettronici, giochi, *etc.* pagando con il credito telefonico): per verificare la correttezza dei trattamenti di dati personali effettuati da tutti i soggetti coinvolti nella gestione di sistemi di *mobile payment* (in particolare, gli operatori telefonici, che mettono a disposizione il

credito disponibile sulle schede prepagate o procedono all'addebito in bolletta, nel caso degli abbonamenti; il gestore dell'infrastruttura tecnologica attraverso la quale viene fornito il servizio che consente l'acquisto; i venditori (cd. *merchant*);

- sistemi di informazione creditizia: per rilevare, attraverso ispezioni presso i principali gestori delle banche dati private in cui sono raccolte le informazioni utilizzate ai fini dell'erogazione del credito al consumo o comunque riguardanti l'affidabilità e la puntualità dei pagamenti e presso alcune società che conferiscono dati all'interno dei sistemi informativi creditizi (cc.dd. partecipanti), il rispetto e l'attualità delle misure contenute nel codice di deontologia e di buona condotta allegato al Codice, sulla base di quanto disposto con il provvedimento dell'Autorità del 16 novembre 2004.

Con riferimento, invece, al secondo semestre 2013, oltre alla prosecuzione dei controlli nei confronti degli enti previdenziali e dell'amministrazione finanziaria, l'attività ispettiva di iniziativa è stata finalizzata ad accertamenti nell'ambito di:

- *WiFi* pubblico: per esaminare le modalità e le cautele attuate dai soggetti pubblici che offrono ai cittadini l'accesso gratuito ad internet mediante connessioni *WiFi*, in particolare per quel che riguarda le misure di sicurezza implementate, la completezza delle informative sul trattamento dei dati, la rispondenza delle finalità del trattamento dei dati alla natura pubblica dell'ente che fornisce il servizio e le modalità e le garanzie con le quali gli enti pubblici hanno affidato i servizi ai soggetti privati che forniscono le infrastrutture tecnologiche;
- violazioni di sicurezza (cd. *data breach*): per constatare il rispetto, da parte dei fornitori di servizi di comunicazione elettronica, delle recenti linee guida adottate dall'Autorità in materia di *data breach* (provv. 4 aprile 2013, n. 161, doc. web n. 2388260), con particolare riferimento alla corretta gestione delle violazioni di sicurezza verificatesi e al rispetto degli obblighi di comunicazione sia nei confronti delle persone i cui dati sono stati violati, sia nei confronti del Garante che è chiamato ad effettuare una immediata valutazione sulla violazione e sulle contromisure adottate dal fornitore per attenuare le possibili conseguenze negative per gli interessati;
- attivazione di servizi non richiesti a seguito di interazione con inserzioni pubblicitarie *online* (cd. *banner*): per appurare la correttezza dei trattamenti di dati personali effettuati da società che offrono servizi a pagamento attivati a seguito dell'interazione dell'utente con collegamenti pubblicitari (*banner*) inseriti all'interno di applicazioni o pagine web. In particolare, con tale attività, tuttora in corso, si intende verificare se siano state implementate modalità di attivazione dei servizi non rispettose della volontà degli interessati con conseguente trattamento illecito dei rispettivi dati personali;
- recupero crediti: per riscontrare, alla luce dell'intensificarsi di segnalazioni concernenti le modalità operative utilizzate dagli operatori del settore, l'adeguamento da parte di questi ultimi alle prescrizioni adottate dal Garante con il provvedimento generale del 30 novembre 2005 (doc. web n. 1213644). Con questa attività, tuttora in corso, il Garante, oltre ad analizzare la liceità e la correttezza dei trattamenti effettuati, si propone di valutare l'attualità delle prescrizioni adottate nell'ottica di un loro eventuale aggiornamento.

Come specificato al successivo paragrafo 18.3, nel periodo di riferimento sono state anche effettuate in diversi settori verifiche:

- sull'adozione delle misure minime di sicurezza da parte di soggetti, pubblici e privati, che effettuano trattamenti di dati sensibili;

- concernenti l'adempimento dell'obbligo di notificazione da parte di soggetti, pubblici e privati, individuati mediante raffronto con il registro generale dei trattamenti;
- 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.

18.2. *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 ancora una volta la meritoria attività svolta dal Nucleo speciale *privacy*, che ha provveduto direttamente ad effettuare gli accertamenti delegati, avvalendosi anche, ove necessario, dei reparti del Corpo territorialmente competenti.

Sulla base della prassi operativa ormai consolidata, le informazioni e i documenti acquisiti nell'ambito degli accertamenti dal Corpo sono trasmessi all'Autorità per le successive verifiche in ordine alla liceità del trattamento e al rispetto dei princìpi previsti dalla legge.

Nei casi in cui sono emerse violazioni penali o amministrative, la Guardia di finanza ha provveduto a informare l'autorità giudiziaria competente e ad avviare i procedimenti sanzionatori amministrativi mediante la redazione della "contestazione", in conformità alla legge 24 novembre 1981, n. 689.

Grazie alla sinergia ormai collaudata con il Nucleo speciale *privacy* della Guardia di finanza, il Garante utilizza un dispositivo di controllo flessibile ed articolato, in grado di integrare l'attività ispettiva svolta direttamente dal competente Dipartimento dell'Autorità, consentendo così l'effettuazione, efficace e tempestiva, di tutte le verifiche *in loco* che si rendono necessarie per garantire il rispetto della protezione dei dati personali su tutto il territorio nazionale.

È proseguita l'attività di formazione del personale del Corpo al fine di approfondire la conoscenza delle disposizioni del Codice e dei provvedimenti dell'Autorità anche da parte del personale impiegato nei reparti territoriali, ordinariamente impiegato in altri servizi istituzionali.

In questo quadro, sono stati realizzati due corsi presso la Scuola di polizia tributaria, denominati "Collaborazione della Guardia di finanza con il Garante per la protezione dei dati personali", cui hanno partecipato circa quaranta tra ufficiali e ispettori.

18.3. *I principali settori oggetto di controllo*

Oltre a quanto già riportato al paragrafo 18.1, nel 2013 le ispezioni effettuate dall'Autorità hanno riguardato i titolari del trattamento che:

- hanno notificato il trattamento di dati che indicano la posizione geografica di persone od oggetti mediante una rete di comunicazione elettronica per appurare: se il trattamento riguarda clienti o dipendenti; le modalità con le quali

gli interessati vengono informati sul trattamento e ne viene acquisito il consenso (ove necessario); nel caso in cui il trattamento sia connesso all'uso di sistemi di localizzazione dei veicoli nell'ambito del rapporto di lavoro, il rispetto di quanto prescritto dal Garante nel provvedimento generale del 4 novembre 2011, n. 370 (doc. web n. 1850581) e di quanto stabilito all'art. 4 dello Statuto dei lavoratori;

- hanno notificato il trattamento di dati personali idonei a rivelare la vita sessuale o la sfera psichica degli interessati, per rilevare le modalità e le finalità del trattamento nonché le misure di sicurezza adottate;
- forniscono servizi di comunicazione elettronica accessibili al pubblico su reti pubbliche di comunicazione, per verificare il rispetto di quanto stabilito dall'art 132 del Codice, con riferimento alla conservazione dei dati di traffico telefonico e telematico per finalità di prevenzione e accertamento dei reati (cd. *data retention*). In questa attività è stata posta particolare attenzione: alla verifica dei dati conservati; al rispetto dei termini tassativi di conservazione stabiliti dalla legge (il cui mancato rispetto, oltre a rendere illecito il trattamento, è sanzionato amministrativamente sia in caso di superamento del termine che di conservazione per tempi inferiori a quelli stabiliti dall'art. 132 del Codice); alla corretta attuazione delle misure e degli accorgimenti prescritti dal Garante nell'ambito del provvedimento del 17 gennaio 2008 (doc. web n. 1482111). Tra questi ricordiamo: la limitazione dell'accesso ai dati e ai locali dove gli stessi sono custoditi; il tracciamento dell'attività del personale incaricato di accedere ai dati; la conservazione separata dei dati e la loro cancellazione una volta decorso il termine di conservazione stabilito dalla legge; l'effettuazione di controlli interni sulla legittimità degli accessi ai dati da parte degli incaricati e l'adozione di sistemi di cifratura;
- raccolgono dati personali *online*, con riferimento all'iscrizione di interessati ai cc.dd. gruppi di acquisto, per accertare: la completezza delle informative rese agli interessati; la correttezza delle modalità di acquisizione del consenso; la congruenza tra le finalità indicate nell'informativa ed i trattamenti effettivamente svolti sui dati;
- sviluppano o distribuiscono applicazioni per dispositivi mobili di comunicazione (cc.dd. "*app*") per rilevare: i trattamenti di dati personali effettuati e le modalità attraverso le quali viene resa l'informativa agli interessati; la tipologia di dati raccolti al momento della registrazione dell'interessato al servizio e, successivamente, al momento dell'installazione dell'*app* sul dispositivo e durante il suo effettivo utilizzo;
- operano nel settore del *marketing*, con particolare riferimento ai trattamenti relativi alla profilazione degli interessati (cd. *market profiling*). In questo caso le verifiche hanno riguardato la tipologia dei dati raccolti, la completezza delle informative fornite agli interessati, la correttezza delle modalità utilizzate per raccogliere il consenso nonché l'effettuazione della notificazione del trattamento;
- prestano servizi di assistenza fiscale ai cittadini. Anche in questo caso le ispezioni avevano come obiettivo quello di verificare le modalità del trattamento dei dati, il rispetto degli adempimenti previsti dalla normativa e, in particolare, le misure adottate per garantire agli interessati che i dati fossero accessibili solo alle persone specificamente autorizzate e, più in generale, fossero adottate tutte le misure di sicurezza;
- operano in ambito sanitario. In questo caso si è data particolare attenzione al controllo delle modalità del trattamento con riferimento alle informative for-

nite agli interessati e alla corretta acquisizione del consenso richiesto dalla legge per il trattamento di dati idonei a rivelare lo stato di salute, nonché alla corretta gestione degli archivi (sia cartacei che informatizzati) in cui sono custoditi i dati sanitari;

- gestiscono sale giochi ove sono installati sistemi del tipo *videolottery*, con particolare riferimento alla verifica degli obblighi di informativa e consenso degli interessati i cui dati vengono raccolti dagli operatori talvolta per molteplici finalità (ad esempio fidelizzazione e *marketing*);
- forniscono servizi per il recupero di anni scolastici, con particolare riferimento al rispetto degli adempimenti connessi all'informativa che deve essere resa ai sensi dell'art. 13 del Codice all'atto della raccolta dei dati degli iscritti e alla manifestazione del consenso, quando necessario;
- gestiscono concessionarie "plurimarca" per la vendita di autoveicoli, al fine di appurare il rispetto della disciplina con particolare riferimento ai profili dell'informativa resa agli interessati nonché al consenso degli stessi, ove necessario;
- offrono servizi di intrattenimento ed effettuano trattamenti mediante sistemi di videosorveglianza, per verificare il rispetto di quanto prescritto dal Garante con il provvedimento generale in materia di videosorveglianza dell'8 aprile 2010 (doc. web n. 1712680).

Particolarmente rilevante per complessità e significatività di risultato è stata l'attività condotta nei confronti dei gestori delle grandi banche dati pubbliche, l'Agenzia delle entrate, con riferimento al sistema informativo della fiscalità (Anagrafe tributaria), e l'Inps.

Nel primo caso (Agenzia delle entrate) le verifiche ispettive hanno avuto ad oggetto l'acquisizione di informazioni necessarie per la definizione delle misure e degli accorgimenti che l'Autorità ha prescritto, in base all'art. 17 del Codice, a seguito della verifica preliminare richiesta dalla stessa Agenzia in relazione all'avvio dell'attività di profilazione dei contribuenti ai fini dell'accertamento sintetico del reddito delle persone fisiche di cui all'art. 38, commi 4 e 5, del d.P.R. 29 settembre 1973, n. 600, modificato dall'art. 22 del d.l. 31 maggio 2010, n. 78, convertito, con modificazioni, dalla l. 30 luglio 2010, n. 122 (cd. redditometro) (cfr. *supra* par. 4.7).

Con riferimento invece all'Inps, gli accertamenti hanno riguardato le modalità con le quali l'ente gestisce l'accesso da parte degli utenti esterni all'istituto (patronati, c.a.f., liberi professionisti, *etc.*) ai dati contenuti nel proprio sistema informativo, al fine di rilevare profili di criticità delle procedure, nell'ottica di incrementare le garanzie affinché i dati degli interessati siano effettivamente oggetto di trattamento solo ed esclusivamente su loro delega e per la fornitura delle prestazioni richieste. In questo caso, come per l'Anagrafe tributaria, una gestione oculata della sicurezza degli accessi, la loro tracciabilità e la rigorosa definizione dell'ambito del trattamento consentito alle migliaia di utenti abilitati costituiscono elementi essenziali per ridurre al minimo i rischi di utilizzi impropri da parte degli utenti abilitati di banche dati di particolare rilevanza e dimensioni quali sono sicuramente quelle degli enti previdenziali e dell'Anagrafe tributaria.

Sono stati effettuati altresì controlli nei confronti di specifici titolari del trattamento per esigenze istruttorie connesse alle segnalazioni, ai reclami e ai ricorsi pervenuti 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, come riportato nel prossimo paragrafo, ha adottato alcuni provvedimenti particolarmente significativi per i cittadini.

18.4. *I provvedimenti adottati dall'Autorità a seguito dell'attività ispettiva*

Attraverso le ispezioni l'Autorità svolge una penetrante attività istruttoria che può essere finalizzata, a seconda dei casi, a uno o più dei seguenti obiettivi:

- intervenire sui trattamenti illeciti da chiunque effettuati adottando i provvedimenti cautelari previsti dalla legge (blocco e divieto) e/o definendo le misure da prescrivere per rendere il trattamento conforme alla legge (contrasto dell'illecito);
- verificare lo stato di attuazione delle prescrizioni adottate dal Garante nei diversi contesti e sanzionare gli eventuali inadempimenti al fine di prevenire futuri illeciti (attività preventiva);
- acquisire tutti gli elementi utili a comprendere nuovi fenomeni emergenti che impattano notevolmente sul diritto alla protezione dei dati personali degli interessati (ad es., il tema del *mobile remote payment*) in modo da definire tempestivamente le misure e gli accorgimenti che devono essere adottati da tutti i soggetti che sono coinvolti nei trattamenti (attività conoscitiva).

Occorre tenere presente che, al di là della/e finalità che la sottendono, l'ispezione è pur sempre un procedimento amministrativo di controllo all'esito del quale, ove vengano accertate illiceità, l'Autorità è tenuta ad adottare i necessari provvedimenti per rendere il trattamento conforme alla legge e a contestare le sanzioni eventualmente rilevate.

Con riferimento all'anno 2013, tra i provvedimenti più rilevanti adottati dal Garante sulla base degli elementi istruttori acquisiti in sede ispettiva, si segnalano, in ordine cronologico, i provvedimenti con i quali il Garante ha:

- dichiarato illecito il trattamento dei dati personali mediante un sistema di videosorveglianza effettuato, per finalità antitaccheggio presso un esercizio commerciale, da parte di soggetti non autorizzati ad effettuare tale attività (sulla base di quanto previsto dall'art. 134, r.d. 18 giugno 1931, n. 773 Tulps), la cui osservanza costituisce presupposto di liceità del trattamento (provv. 17 gennaio 2013, n. 16, doc. web n. 2291893);
- dato specifiche prescrizioni a società esercenti l'attività di fornitura di servizi di comunicazione elettronica accessibili al pubblico su reti pubbliche di comunicazione, in relazione alla verifica del mancato rispetto delle misure e degli accorgimenti da adottare a garanzia degli interessati, con riferimento ai dati di traffico telefonico e telematico che tali soggetti devono conservare per finalità di accertamento e repressione dei reati (cd. *data retention*), già prescritti dall'Autorità con il provvedimento generale del 17 gennaio 2008 (doc. web n. 1482111), successivamente integrato con il provvedimento generale del 24 luglio 2008 (doc. web n. 1538237) (provv.ti 21 febbraio 2013, n. 74, doc. web n. 2338534 e 3 ottobre 2013, n. 429, doc. web n. 2740948);
- dichiarato illecito il trattamento dei dati personali effettuato da una società mediante l'utilizzo di telecamere e di un sistema di geolocalizzazione installati sui veicoli aziendali, anteriormente alla conclusione dell'accordo con le rappresentanze sindacali, con la conseguente inutilizzabilità dei dati trattati in violazione di legge ai sensi dell'art. 11, comma 2, del Codice (provv. 7 marzo 2013, n. 103, doc. web n. 2471134);
- disposto il divieto del trattamento dei dati personali acquisiti da una società mediante apparati di ripresa occultati all'interno di un rilevatore di fumo e di una lampada d'allarme nonché dichiarato illecito il trattamento dei dati personali effettuato in generale dalla stessa società a mezzo del sistema di video-

sorveglianza in quanto effettuato senza accordo con le rappresentanze sindacali, né l'autorizzazione del competente ufficio periferico del Ministero del lavoro, in violazione quindi degli artt. 114 del Codice e 4, l. n. 300/1970 (provv. 4 aprile 2013, n. 164, doc. web n. 2439178);

- dichiarato illecito il trattamento dei dati personali mediante un sistema di videosorveglianza effettuato da titolari del trattamento, pubblici e privati, in assenza dell'accordo con le rappresentanze sindacali e dell'autorizzazione del competente ufficio periferico del Ministero del lavoro, in violazione quindi degli artt. 114 del Codice e 4, l. n. 300/1970 (provv.ti 18 aprile 2013, nn. 199 e 200, doc. web nn. 2476068 e 2483269; 4 luglio 2013, n. 335, doc. web n. 2577227, n. 334, doc. web n. 2577203, n. 336, doc. web n. 2578071; 18 luglio 2013, n. 361, doc. web n. 2605290; 5 settembre 2013, n. 385, doc. web n. 2683203; 12 settembre 2013, n. 398, doc. web n. 2705679; 30 ottobre 2013, n. 483, doc. web n. 2851973 e n. 484, doc. web n. 2908871);
- disposto il divieto del trattamento dei dati personali acquisiti, per finalità di profilazione e *marketing*, in assenza del rilascio di un'idonea informativa e dell'acquisizione del necessario consenso, da parte di una società esercente l'attività di fornitura di servizi di comunicazione elettronica accessibili al pubblico su reti pubbliche di comunicazione (provv. 3 ottobre 2013, n. 430, doc. web n. 2745497);
- dichiarato illecito il trattamento dei dati personali effettuato da un ente pubblico per aver consentito la messa a disposizione e consultazione del fascicolo personale di una dipendente, contenente in particolare dati personali idonei a rivelare lo stato di salute dell'interessata, a soggetti non designati incaricati del trattamento, in violazione degli artt. 11, comma 1, lett. *d*), 20, commi 1 e 2, e 22, commi 3 e 5, del Codice (provv. 24 ottobre 2013, n. 469, doc. web n. 2799174);
- stabilito, nell'ambito di una verifica preliminare richiesta dall'Agenzia delle entrate, le misure e gli accorgimenti a garanzia dei diritti degli interessati sul trattamento di dati personali effettuato dall'ente richiedente ai fini dell'accertamento sintetico del reddito delle persone fisiche di cui all'art. 38, commi 4 e 5, d.P.R. 29 settembre 1973, n. 600 (cd. redditometro), modificato dall'art. 22 del d.l. 31 maggio 2010, n. 78, convertito, con modificazioni, dalla l. 30 luglio 2010, n. 122 (provv. 21 novembre 2013, n. 515, doc. web 2765110);
- vietato a una società il trattamento dei dati personali raccolti *online*, con finalità di intermediazione tra domanda e offerta di lavoro, in quanto risultavano effettuati in violazione di legge in assenza dell'autorizzazione prevista dal d.lgs. n. 276/2003 e sulla base di un'informativa inidonea (provv. 5 dicembre 2013, n. 547, doc. web n. 2865637);
- adottato uno schema di provvedimento recante "Provvedimento generale in materia di trattamento di dati personali nell'ambito dei servizi di *mobile remote payment*", sottoponendo a consultazione pubblica (provv. 12 dicembre 2013, n. 561, doc. web 2830145).

In molti dei provvedimenti sopra citati l'Autorità, accertata la violazione di norme del Codice per le quali la legge prevede una sanzione amministrativa, ha avviato anche un procedimento sanzionatorio. In diversi casi inoltre l'Autorità, rilevando condotte punite come reato, ha disposto anche la trasmissione degli atti alla competente Procura della Repubblica.

18.5. *L'attività sanzionatoria del Garante*

18.5.1. Le violazioni penali e i procedimenti relativi alle misure minime di sicurezza

Nell'anno 2013, in relazione alle istruttorie effettuate, sono state inviate 71 segnalazioni di violazioni penali all'autorità giudiziaria di cui:

- ventinove per la mancata adozione delle misure minime di sicurezza;
- ventitré per violazioni della l. n. 300/1970 (Statuto dei lavoratori), ora punite come reato dall'art. 171 del Codice;
- cinque per trattamento illecito dei dati;
- tre per inosservanza di un provvedimento del Garante;
- due per falsità nelle dichiarazioni e notificazioni al Garante;
- nove in relazione ad altre violazioni penali.

Come dimostrano i dati sopra riportati (cfr. tab. 7), permangono numerose le violazioni delle misure minime di sicurezza; ciò nonostante si tratti di adempimenti di non particolare complessità, in vigore da più di dieci anni, che dovrebbero essere stati oramai "metabolizzati" sia dalle imprese che dagli enti pubblici. Deve essere nuovamente segnalata la ormai indifferibile esigenza di aggiornare il "Disciplinare tecnico in materia di misure minime di sicurezza", All. B al Codice in vigore dal 2003, le cui prescrizioni appaiono in buona parte non più adeguate allo stato dell'evoluzione tecnica, anche alla luce della ormai consistente esperienza maturata dall'Autorità in sede di controllo. Tale revisione dovrebbe essere ispirata a criteri di semplificazione, rispetto ad adempimenti di natura prettamente burocratica oggi previsti dalle disposizioni, e di maggiore effettività delle misure, prevedendo adeguati accorgimenti tecnici che intervengano in modo progressivo in funzione della quantità e della qualità dei dati, nonché della complessità della struttura tecnologica utilizzata e del numero di incaricati che vi hanno accesso.

Al di là dei risvolti sanzionatori, occorre sottolineare che la mancata osservanza delle disposizioni relative alle misure minime di sicurezza è particolarmente grave perché espone, almeno potenzialmente, i dati personali degli interessati all'accesso da parte di persone non autorizzate e a trattamenti non consentiti, intaccando il naturale affidamento degli interessati nei confronti del titolare del trattamento.

Sotto il profilo procedurale, 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 All. B al Codice), in base al disposto dell'art. 169, comma 2, del Codice, il Garante impartisce una prescrizione alla persona individuata come responsabile della predetta violazione e, successivamente, 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 valutazioni in ordine all'estinzione del reato.

Come per l'anno precedente, anche nel 2013 si è avuta una notevole incidenza dell'accertamento di violazioni penali relative allo Statuto dei lavoratori connesse, nella maggior parte dei casi, all'installazione di sistemi di videosorveglianza in assenza delle garanzie previste dall'art. 4, comma 2, l. n. 300/1970. Occorre tenere presente che la disciplina prevista dallo Statuto e relativa all'utilizzo di impianti audiovisivi e di altre apparecchiature per finalità di controllo a distanza dell'attività dei lavoratori (art. 4) e al divieto di indagini sulle opinioni ai fini dell'assunzione (art. 8), costituisce ormai parte integrante delle disposizioni del Codice (artt. 113 e 114) ed è sanzionata dall'art. 171.

L'entità delle violazioni accertate in questo settore dipende:

- dalla circostanza che pervengono all'Autorità numerose segnalazioni da parte di dipendenti o di organizzazioni sindacali;

- dalla costituzione, a partire dall'aprile del 2011 (v. p. 117 della Relazione annuale 2011) di una specifica unità organizzativa che cura anche queste istruttorie che presuppongono quasi sempre un accertamento in fatto per il quale si rende necessario lo svolgimento di ispezioni *in loco* (effettuate sia direttamente dall'Ufficio che dal Nucleo speciale *privacy* della Guardia di finanza).

18.5.2. Le sanzioni amministrative

Il dato relativo ai procedimenti sanzionatori amministrativi nell'anno 2013 (850; cfr. sez IV, tab. 6) attesta una rilevante crescita delle violazioni (+ 47% rispetto al 2012).

Per apprezzare compiutamente questo dato occorre tenere presente che all'accertamento delle violazioni amministrative previste dal Codice può procedere:

- il personale dell'Ufficio del Garante addetto all'attività ispettiva a cui, sulla base di quanto previsto dall'art. 156, comma 9, del Codice, nei limiti del servizio cui è destinato e secondo le rispettive attribuzioni, è attribuita la qualifica di ufficiale o agente di polizia giudiziaria;
- chiunque rivesta, nell'esercizio delle proprie funzioni, la qualifica di ufficiale o agente di polizia giudiziaria, in base a quanto previsto dall'art. 13, l. 24 novembre 1981, n. 689.

L'art. 13, l. n. 689/1981 prevede: "Gli organi addetti al controllo sull'osservanza delle disposizioni per la cui violazione è prevista la sanzione amministrativa del pagamento di una somma di denaro possono, per l'accertamento delle violazioni di rispettiva competenza, assumere informazioni e procedere a ispezioni di cose e di luoghi diversi dalla privata dimora, a rilievi segnaletici, descrittivi e fotografici e ad ogni altra operazione tecnica [...]. All'accertamento delle violazioni punite con la sanzione amministrativa del pagamento di una somma di denaro possono procedere anche gli ufficiali e gli agenti di polizia giudiziaria".

I procedimenti sanzionatori iniziano, pertanto, con la contestazione in relazione ad istruttorie effettuate direttamente dall'Autorità ma anche sulla base di accertamenti effettuati autonomamente da corpi dello Stato quali la Guardia di finanza, i Carabinieri, la Polizia di Stato che possono accertare le violazioni amministrative in materia di protezione dei dati personali in occasione di attività svolte sulla base dei propri poteri, anche di polizia giudiziaria. Questo "doppio binario" risulta complessivamente efficace, considerata l'amplissima platea di soggetti tenuti all'osservanza delle regole previste dal Codice, che renderebbe velleitario un sistema di accertamento delle violazioni accentrato solo nell'Autorità.

L'assicurazione di una uniformità di giudizio e di interpretazione è peraltro assicurata, in quanto la legge affida invece al solo Garante il compito dell'applicazione delle sanzioni in tutti i casi nei quali, a seguito dell'accertamento, il contravventore, non avvalendosi della possibilità di definire il procedimento con il pagamento entro sessanta giorni dalla notifica del doppio del minimo della sanzione, decida di proseguire il procedimento medesimo inviando scritti difensivi o chiedendo l'audizione. In tutti questi casi è infatti l'Autorità a prendere la decisione finale circa l'applicazione della sanzione adottando l'atto finale dell'ordinanza ingiunzione, quantificandone l'importo o l'archiviazione.

Le violazioni in relazione alle quali sono stati avviati procedimenti sanzionatori nel 2013 hanno riguardato (cfr. sez. IV, tab. 6):

- l'omessa o inidonea informativa – art. 161 (n. 476);
- il trattamento illecito amministrativo – art. 162, comma 2-*bis* (n. 277);
- l'omessa adozione delle misure minime di sicurezza di cui all'art. 33 del Codice – art. 162, comma 2-*bis* (n. 24);

- l'utilizzo illecito dei dati delle persone iscritte al Registro pubblico delle opposizioni per finalità di *marketing* – art. 162, comma 2-*quater* (n. 19);
- l'omessa informazione o esibizione al Garante – art. 164 (n. 18);
- l'inosservanza di un provvedimento del Garante – art. 162, comma 2-*ter* (n. 17);
- l'omessa o incompleta notificazione – art. 163 (n. 12);
- la conservazione di dati di traffico telefonico e telematico per un tempo superiore a quello stabilito dall'art. 132 del Codice – art. 162-*bis* (n. 7).

Un approfondimento merita il dato relativo alle 277 violazioni di cui all'art. 162, comma 2-*bis* che si è definito "trattamento illecito amministrativo". La disposizione prevede una sanzione pecuniaria, da 10.000 a 120.000 euro in relazione alla violazione delle disposizioni di cui all'art. 167. Quest'ultima disposizione, a sua volta, richiama numerose disposizioni del Codice, estremamente eterogenee, e, in particolare, gli artt: 17 (verifica preliminare), 18, 19, 20, 21, 22, commi 8 e 11 (disposizioni concernenti il trattamento dei dati da parte di soggetti pubblici), 23, 25, 26, 27 (disposizioni concernenti il trattamento dei dati da parte dei soggetti privati), 45 (trasferimenti all'estero vietati), 123, 126, 129 e 130 (disposizioni specifiche per le comunicazioni elettroniche). Nel 2013 le violazioni concernenti il "trattamento illecito amministrativo" accertate hanno riguardato:

- in 179 casi, la violazione del consenso dell'interessato in rapporto agli artt. 23 e 130 del Codice;
- in 36 casi, violazioni commesse da enti pubblici (nella maggior parte dei casi comunicazioni o diffusioni di dati non sensibili senza i necessari presupposti di legge o regolamento);
- in 51 casi, violazioni commesse da enti pubblici con riferimento a dati sensibili;
- in 8 casi, violazioni delle misure e degli accorgimenti prescritti dal Garante nell'ambito di una verifica preliminare sulla base dell'art. 17 del Codice;
- in 3 casi, violazioni commesse da soggetti privati in relazione al trattamento di dati sensibili o giudiziari.

Analizzando i dati statistici sopra riportati si può rilevare che:

- in senso assoluto, anche per l'anno di riferimento, il maggior numero di violazioni accertate ha riguardato l'obbligo di fornire all'interessato tutte le informazioni sul trattamento dei dati, al fine di renderlo pienamente consapevole dell'effettivo utilizzo dei suoi dati personali; ciò si spiega alla luce del fatto che l'obbligo di informativa costituisce l'adempimento più generale previsto dal Codice;
- sommando le violazioni riguardanti il consenso dell'interessato (n. 179) a quelle relative all'utilizzo illecito dei dati delle persone iscritte al Registro pubblico delle opposizioni per finalità di *marketing* (n. 19), si arriva ad un totale di circa 200 violazioni commesse da soggetti privati che hanno utilizzato i dati personali dei clienti senza (o contro) la volontà degli interessati. Nella gran parte dei casi queste violazioni attengono a trattamenti effettuati da aziende per finalità di *marketing* e rientrano in quel fenomeno definito *marketing* selvaggio in relazione al quale pervengono centinaia di segnalazioni di cittadini disturbati in particolare da chiamate indesiderate sulle proprie utenze telefoniche.

Infine appare opportuno evidenziare il numero di violazioni in materia di conservazione di dati di traffico telefonico e telematico da parte dei fornitori di servizi di comunicazione elettronica accessibili al pubblico per finalità di accertamento e repressione dei reati; si tratta di dati molto delicati ai quali si può accedere solo in forza di specifici decreti adottati dall'autorità giudiziaria nell'ambito delle indagini penali.

Seppure non elevato in termini assoluti (n. 7 contestazioni), il dato è rilevante se si tiene conto dell'estrema specificità di tale violazione, dell'elevata incidenza in relazione al numero di controlli effettuati (n. 12), della regolamentazione specifica e dettagliata prevista dal Codice e dai provvedimenti del Garante che evidentemente non sono stati ancora compiutamente attuati dagli operatori del settore.

I procedimenti che non si sono chiusi con il pagamento spontaneo da parte del contravventore (e sono stati quindi definiti con ordinanza dall'Autorità) sono stati 527. Di questi 420 hanno comportato l'applicazione di una sanzione (per un ammontare complessivo di somme ingiunte pari a 4.709.400 euro) e 107 si sono invece conclusi con l'archiviazione in quanto la parte ha potuto dimostrare nel procedimento di non aver commesso la violazione contestata o che la violazione non era a lei imputabile.

Tra le ordinanze più rilevanti adottate si segnalano, per rilevanza economica, quella nei confronti di una primaria società internazionale che opera nel settore della pubblicità *online* e delle ricerche web, in relazione all'omessa informativa agli interessati in conseguenza di una raccolta di dati attuata sistematicamente su tutto il territorio nazionale (ordinanza di ingiunzione del 18 dicembre 2013, n. 583, doc. web n. 2954309) e quelle nei confronti di due importanti società italiane operanti nel settore della fornitura di servizi per il *marketing*, in relazione all'utilizzo illecito di ingenti banche dati per finalità di *marketing* (ordinanza di ingiunzione del 10 gennaio 2013, n. 6, doc. web n. 2438949 e ordinanza di ingiunzione del 5 dicembre 2013, n. 549, doc. web n. 2954335). Fattore comune di queste ordinanze è stata l'applicazione della sanzione, prevista dall'art. 164-*bis*, comma 2, del Codice, a seguito dell'accertamento di plurime violazioni commesse in relazione a banche dati che possono essere qualificate "di particolare rilevanza o dimensioni", in armonia con i criteri e i principi già illustrati nella Relazione annuale 2012 (cfr. p. 265).

Per quanto invece riguarda l'interpretazione degli aspetti giuridici, si citano i seguenti casi.

- Propaganda elettorale: i trattamenti di dati personali nell'ambito di propagande elettorali, benché possano essere in senso lato assimilati alle comunicazioni commerciali tradizionali e al *marketing*, hanno una propria specificità di cui il Garante ha tenuto conto nel provvedimento generale adottato il 7 settembre 2005 (doc. web n. 1165613), attualizzato varie volte e, da ultimo, con provvedimento del 10 gennaio 2013, n. 1 (doc. web n. 2181429). L'Autorità ha definito i casi nei quali non è necessario richiedere il consenso degli elettori per l'invio del materiale di propaganda. In particolare, è stato confermato che il consenso è necessario in caso di utilizzo di particolari modalità di comunicazione elettronica come sms, mms, *e-mail* e per telefonate pre-registrate e fax, in virtù di quanto previsto dall'art. 130 del Codice. In questo ambito l'Autorità ha applicato la sanzione prevista dall'art. 162, comma 2-*bis*, del Codice, in relazione all'invio di sms di propaganda elettorale da parte di un candidato alle elezioni regionali ad una persona che aveva manifestato, in maniera espressa e specifica, la propria opposizione al trattamento. In assenza di un documentato consenso dell'interessato, il trattamento dei suoi dati personali è risultato illecito, indipendentemente dal fatto che i dati utilizzati (in questo caso il numero di cellulare) fossero stati reperiti sul web, o acquisiti nell'espletamento dell'attività istituzionale (provv. 21 febbraio 2013, n. 78, doc. web n. 2462289). Il Tribunale di Milano, pur riducendo in sede di ricorso l'ammontare della sanzione irrogata, con la sentenza del 4 dicembre 2013 ha pienamente confermato l'impostazione dell'Autorità.

- Notificazione dei trattamenti di geolocalizzazione: in ragione del fatto che la maggior parte dei sistemi *gps*, utilizzati per la geolocalizzazione, funziona mediante l'utilizzo di una scheda telefonica tramite la quale, inviando un sms, si attiva il localizzatore, indicando la posizione del mezzo sul quale è applicato, questa modalità sostanzia, così come specificato al punto 2 del parere del 23 aprile 2004 (doc. web n. 993385), il requisito della continuità di funzionamento, atteso che il sistema è in grado di fornire la posizione del mezzo (e, di regola, quantomeno indirettamente, dell'interessato) su cui è applicato il localizzatore in qualsiasi momento (cfr. provv. 18 dicembre 2013, n. 604, doc. web n. 2954181).
- I trattamenti di dati personali effettuati per mezzo di un sistema di videosorveglianza dal libero professionista persona fisica: quando il trattamento di dati personali viene effettuato, quale titolare, da una persona fisica nell'ambito della propria attività professionale non sussistono infatti le finalità esclusivamente personali che consentirebbero di escludere il trattamento dall'ambito di applicazione del Codice ai sensi dell'art. 5, comma 3, così come illustrato anche al punto 6.1 del provvedimento generale sulla videosorveglianza adottato dal Garante l'8 aprile 2010 (doc. web n. 1712680) (provv. 21 marzo 2013, n. 146, doc. web n. 2922669).
- Documentazione del consenso al trattamento dei dati personali in ambito sanitario: i trattamenti di dati personali idonei a rivelare lo stato di salute effettuati dagli esercenti le professioni sanitarie e dagli organismi sanitari pubblici rientrano tra quelli per i quali il Codice richiede il consenso informato degli interessati; in tale ambito sono previsre specifiche modalità semplificate per rendere l'informativa agli interessati medesimi ed acquisirne il consenso (art. 77). In particolare, rispetto alla regola generale che richiede la forma scritta per il rilascio del consenso al trattamento di dati sensibili (art. 23, comma 4), l'art. 81 del Codice prevede che il consenso in ambito sanitario possa essere manifestato anche oralmente ma che, in tal caso esso debba essere documentato, anziché con atto scritto dell'interessato, con annotazione scritta dell'esercente la professione sanitaria o dell'organismo sanitario pubblico. L'Autorità ha, dunque, chiarito il rapporto di genere a specie esistente tra la disposizione di cui all'art. 23, che, in quanto norma di carattere generale, individua gli elementi atti a connotare un valido consenso, e l'art. 81 che, nel caso di trattamenti in ambito sanitario, specifica le modalità con cui questo debba essere raccolto, applicando la sanzione prevista dall'art. 162, comma 2-*bis* nei confronti di un organismo sanitario che aveva omesso di documentare l'acquisizione del consenso degli interessati secondo quanto previsto dall'art. 81 del Codice (provv. 22 maggio 2013, n. 254, doc. web n. 2616474).
- Attività di *marketing* e vincolo di finalità: l'utilizzo di dati provenienti da pubblici registri, elenchi, atti o documenti conoscibili da chiunque può avvenire senza il preventivo consenso degli interessati, purché nel rispetto dei limiti e delle modalità stabilite dalla legge (art. 24, comma 1, lett. *c*), del Codice); tra questi rientra, in particolare, il cd. vincolo di finalità, in base al quale i dati possono essere raccolti e registrati per scopi determinati, espliciti e legittimi e possono essere utilizzati in altri trattamenti in termini compatibili con tali scopi, tenuto conto del dettato dell'art. 11, comma 1, lett. *b*), del Codice. Il caso riguardava una società che aveva inviato *e-mail* promozionali ritenendo erroneamente che i dati tratti da un elenco pubblico (estrapolato dal sito dell'Ordine degli avvocati) potessero essere liberamente utilizzati per finalità