emessa dal Garante, rinviando allo stesso Tribunale in persona di diverso magistrato, in quanto il ricorso e il pedissequo decreto di fissazione dell'udienza non erano mai stati notificati al Garante, come invece previsto espressamente dall'art. 152, comma 7 del Codice (13 maggio 2015, n. 9818).

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

20.3. *Le opposizioni ai provvedimenti del Garante*

L'anno 2015 ha registrato un incremento delle opposizioni a provvedimenti dell'Autorità: a fronte degli 80 ricorsi del 2014, nel 2015 sono state proposte 85 opposizioni. Di queste, 45 si riferiscono a ordinanze ingiunzioni (di cui 2 a verbale di contestazione, inammissibili per costante giurisprudenza e 3 a cartella esattoriale), con una sostanziale stabilità rispetto al 2014, nel quale le impugnazioni di tale natura erano state 44.

Opposizioni a ordinanze ingiunzioni

Complessivamente l'Autorità ha avuto notizia di 42 decisioni dell'autorità giudiziaria relative a opposizioni a provvedimenti del Garante, che si è sempre costituito tramite l'Avvocatura dello Stato territorialmente competente.

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

Informativa e consenso

Tra le opposizioni alle ordinanze ingiunzioni, 5 decisioni hanno riguardato sanzioni irrogate in relazione alla raccolta di dati personali da parte di alcune aziende attraverso siti internet, in assenza di un'idonea informativa e, in 2 casi, anche del consenso. Tutte le pronunce, avvalorando la giurisprudenza costante, hanno confermato le valutazioni dell'Autorità e rigettato i ricorsi, nel primo caso con riduzione della sanzione (Trib. Roma, 24 marzo 2015, n. 6679; Trib. Lecce, 9 gennaio 2015 n. 61; Trib. Cagliari, 1° aprile 2015 n. 1074; Trib. Pavia, 13 agosto 2015 n. 278; Trib. Napoli, 19 maggio 2015 n. 7531).

Altre 3 opposizioni hanno avuto ad oggetto il trattamento dei dati in relazione a comunicazioni telefoniche indesiderate a carattere promozionale.

In un primo caso il giudice ha confermato il provvedimento del Garante in relazione all'illecito trattamento compiuto da una società che aveva effettuato chiamate promozionali in assenza di informativa e consenso (Trib. Trani, 23 settembre 2014, n. 1550).

Nel secondo caso, la società ricorrente ha effettuato comunicazioni commerciali estraendo il numero da un elenco telefonico consultabile da chiunque, senza previo consenso. Anche in questo caso, il giudice ha confermato il provvedimento del Garante (Ttib. Roma, 3 ottobre 2014, n.19536).

Nel terzo caso, la società ricorrente ha effettuato telefonate promozionali celando l'identità del chiamante e senza fornire un recapito per esercitare i diritti di cui all'arr. 7 del Codice. Il Tribunale di Torino ha accolto il ricorso in quanto non ha ritenuto adeguatamente provata l'esistenza della fattispecie configurante l'illecito amministrativo ed ha conseguentemente annullato l'ordinanza ingiunzione (24 aprile 2015, n. 2676).

Riscontrando la mancanza di informativa e di consenso, il Tribunale di Roma ha confermato il provvedimento ingiuntivo in relazione al trattamento dati degli operatori di un *call center* di prenotazioni telefoniche di prestazioni sanitarie (21 luglio 2015, n. 16083).

In un'altra pronuncia il Tribunale di Roma ha confermato il provvedimento sanzionatorio del Garante nei confronti di un professionista che, senza il consenso dell'interessata, aveva inviato la richiesta del compenso contenente i dati della propria cliente al datore di lavoro di quest'ultima presso il suo luogo di lavoro (14 maggio 2015, n. 10724).

Due sentenze hanno riguardato l'attivazione di una pluralità di schede telefoniche effettuate da due distinte società nei confronti di singoli interessati senza aver reso loro l'informativa. In entrambi i casi il Tribunale ha confermato il provvedimento del Garante e in un caso ha ridotto la sanzione poiché la violazione è risultata aver avuto ad oggetto tre dei soggetti coinvolti, non sussistendo sufficienti elementi per gli altri due (Trib. Padova, 29 maggio 2015 n. 1590 e Trib. Brescia, 29 ottobre 2015 n. 3076).

In due sentenze i giudici hanno affrontato il tema del termine di 90 giorni – previsto dall'art. 14, l. n. 689/1981 per la contestazione delle violazioni. Entrambi i ricorsi sono stati accolti, uno promosso da una casa di cura alla quale era stata notificata un'ordinanza ingiunzione in relazione alla comunicazione a terzi di dati sensibili in assenza di consenso e l'altro dal legale rappresentate di una società alla quale era stata contestata la pubblicazione *online* di elenchi telefonici in assenza di informativa e consenso. Infatti, anche considerando che, secondo giurisprudenza costante, ai fini dell'individuazione del *dies a quo* deve ritenersi compreso il tempo necessario alla valutazione degli elementi acquisiti all'esito dell'istruttoria, nei casi di specie il termine decadenziale dei 90 giorni è stato ritenuto spirato (Trib. Padova, 1° ottobre 2015, n. 2581 e Trib. Siracusa, 2 marzo 2015, n. 437). Il Garante ha proposto ricorso per Cassazione.

In un caso la Cassazione, su ricorso del Garante che si era visto annullare dal Tribunale di Palmi un'ordinanza ingiunzione per omessa informativa *ex* art. 13 del Codice, emessa nei confronti di un esercizio commerciale che effettuava attività di videosorveglianza, ha affrontato il tema della nozione di dato personale. Il giudice di primo grado aveva ritenuto che l'immagine di una persona, pur possedendo capacità identificativa del soggetto, quando viene trattata integra la nozione di dato personale non automaticamente, ma soltanto qualora chi esegue il trattamento la correli espressamente ad una persona mediante didascalia o altra modalità da cui sia possibile identificarla. La Corte, con significativa innovazione rispetto a precedente decisione, ha condiviso l'argomentazione del Garante, circa il fatto che l'immagine costituisca dato personale, rilevante ai sensi dell'art. 4, comma 1, lett. *b*), del Codice, a prescindere dalla sua notorietà, disponendo, pertanto, la cassazione della sentenza impugnata e il rigetto dell'opposizione proposta dal ricorrente in primo grado (2 settembre 2015, n. 17440).

Notificazione

La Cassazione, adita da un laboratorio di analisi cliniche che si era visto confermare dal Tribunale di Foggia un'ordinanza ingiunzione per omessa norificazione emessa nei suoi confronti, ha dichiarato inammissibile il ricorso, in quanto, come rilevato in sede di controricorso dall'Autorità, nessuno dei motivi che prospettava vizi di violazione e falsa applicazione di legge poneva, come richiesto dalla (previgente) formulazione dall'art. 366-*bis* c.p.c. "*...un quesito che individui tanto il principio di diritto che è alla base del provvedimento impugnato, quanto, correlativamente, il principio di diritto, diverso dal precedente, la cui auspicata applicazione ad opera della Corte medesima possa condurre ad una decisione di segno inverso rispetto a quella impugnata*" (12 marzo 2015, n. 4977).

Con riferimento ad un'opposizione proposta da una casa di cura avverso un'ordinanza ingiunzione adottata a seguito della violazione dell'obbligo di notificazione del trattamento di dati sensibili il Tribunale di Firenze ha confermato il provvedi-

mento del Garante, ritenendo che allo spostamento della sede legale della società interessata non era seguita alcuna notifica al Garante e che la stessa società, di nuovo senza notificare, aveva cessato l'attività di cura e di ricovero e sala operatoria (8 gennaio 2015, n. 29).

In un'altra pronuncia una società è stata sanzionata per aver omesso di notificare al Garante l'effettuazione di trattamenti di dati genetici e di dati idonei a rilevare lo stato di salute e la vita sessuale. L'organo giudicante ha confermato il provvedimento impugnato, non ritenendo sufficienti le motivazioni della suddetta società riguardo alla buona fede e la mancanza di colpa, trattandosi di un laboratorio di analisi e non di "esercenti le professioni sanitarie" sottratti all'obbligo di notifica sussistendo determinate condizioni (Trib. Brindisi, 18 dicembre 2014, n. 2165).

Tre opposizioni hanno riguardato il trattamento dati da parte di soggetti pubblici.

Trattamento dati da parte di soggetti pubblici

In due casi si è trattato di pubblicazione di dati sulla salute da parte rispettivamente di un Comune sul proprio sito web e di un'Azienda ospedaliera sulla bacheca di un reparto e per entrambi l'organo giudicante ha accolto il ricorso e revocato il provvedimento del Garante. In un caso il Tribunale ha ritenuto il Comune incolpevole a fronte di un contesto normativo incerto al momento della condotta lesiva, mancando un raccordo tra le disposizioni concernenti la tutela della *privacy* e quelle relative agli obblighi di trasparenza (Trib. Aosta, 17 novembre 2015 n. 394). Nell'altro caso il giudice si è soffermato sulla nozione di dato sensibile, ritenendo che nel caso di specie le espressioni contenute in una nota esposta in bacheca non fossero qualificabili come dato sensibile in quanto non idonee a rivelare lo stato di salute dell'interessato (Trib. Cuneo, 27 giugno 2015, n.152). Per la seconda sentenza il Garante ha proposto ricorso in Cassazione.

La Cassazione ha poi accolto in parte il ricorso presentato da un Comune che aveva notificato un'ordinanza ingiunzione di pagamento presso il domicilio del destinatario ma non in busta chiusa e nelle mani di un terzo estraneo. La sentenza di primo grado, confermando il provvedimento del Garante, aveva accertato la violazione contestata riconoscendo all'interessato un risarcimento del danno che la Cassazione ha ritenuto non sufficientemente dimostrato, essendo il danno stesso stato identificato dal Tribunale nell'illecito trattamento e non individuato come conseguenza di esso (5 settembre 2014, n. 18812).

Cartella esattoriale

Il Tribunale di Milano ha respinto il ricorso proposto da una società avverso la cartella esattoriale emessa dall'agente riscossore nell'interesse del Garante a seguito del mancato pagamento della somma ingiunta, riconoscendo che l'ordinanza ingiunzione costituisce titolo esecutivo e dunque il Garante aveva correttamente applicato le maggiorazioni che, diversamente da quanto sostenuto da parte attrice, non decorrevano dal momento in cui era passata in giudicato la sentenza che aveva confermato il suddetto provvedimento ingiuntivo (16 gennaio 2015, n. 2006).

Lavoro

Con riguardo al trattamento dei dati sul luogo di lavoro, una decisione del Tribunale di Latina ha riguardato la diffusione della notizia della rimozione di una dipendente di un ente pubblico dalle funzioni cui era preposta nonché la consegna a mano – da persona non incaricata del trattamento – del provvedimento non inserito in busta o plico. Il Garante, nel caso di specie, non aveva riscontrato violazioni, avendo ritenuto che la consegna delle note dirigenziali fosse stata eseguita da un'incaricata che poteva legittimamente prenderne conoscenza anche in base ad un ordine di servizio, mentre la diffusione ad altri soggetti della notizia non è emersa dagli accertamenti effettuati (provv. 18 ottobre 2012, n. 296, doc. web n. 2174351). Il Tribunale, dopo aver esaminato la questione della competenza territoriale, ha affermato che le informazioni relative alla revoca da una determinata posizione organizzativa costituiscono dati personali. In particolare la menzionata con-

dotta è stata ritenuta violativa del Codice sia per quanto attiene alla regola cautelare che impone misure minime onde evitare l'indebita diffusione delle informazioni personali, sia con riferimento alla prescrizione prevista dalle Linee guida in materia di impiego pubblico del 14 giugno 2007 (doc. web n. 1417809), secondo cui l'amministrazione deve utilizzare forme di comunicazione individualizzate con il lavoratore, adottando le misure più opportune per prevenire la conoscibilità da parte di soggetti diversi dal destinatario (9 settembre 2015, n. 1792).

Avverso tale decisione è pendente ricorso in Cassazione proposto dal Garante.

In altro caso, il Tribunale di Catanzaro ha confermato le argomentazioni del Garante contenute nel provvedimento 4 ottobre 2013, n. 469 (doc. web n. 2799174) circa il trattamento illecito posto in essere da un ente locale in riferimento alla consultazione da parte di alcuni dirigenti del fascicolo personale, conrenente anche dati sensibili, di una dipendente. Il Garante aveva in particolare ritenuto che i dati oggetto di comunicazione, effettuata a soggetti non incaricati del trattamento, non fossero pertinenti rispetto alle finalità per le quali erano stati raccolti e poi trattati, né indispensabili per lo svolgimento delle attività istituzionali (1° giugno 2015, n. 857).

Giornalismo

La Corte di Cassazione si è pronunciara circa la legittimità del provvedimento del Garante 15 luglio 2006 (doc. web n. 1310796) che aveva vietato, in via preventiva, la diffusione di dati personali di carattere sanitario di un personaggio pubblico, vittima di un incidente stradale e sul quale il Tribunale di Milano, condividendo la tesi del Garante, aveva ritenuto in prima istanza violato il principio di essenzialità dell'informazione. La Cassazione, in particolare con riferimento ad una questione sulla conformità all'art. 21 della Costituzione dei poteri attribuiti al Garante, ha ribadito che la tutela preventiva e inibitoria posta in essere nel caso di specie è del tutto legittima ai sensi dell'art. 143, lett. *c)* del Codice nell'ipotesi in cui "vi sia il concreto rischio del verificarsi di un pregiudizio rilevante per uno o più interessati" (16 aprile 2015, n. 7755).

In altro caso, il giudice confermando il provvedimento del Garante dell'11 settembre 2014, n. 400 (doc. web n. 3405138) riguardante la diffusione di notizie raccolte da un giornalista, rramite un imitatore che, telefonando ad un personaggio pubblico, si era fatto passare per persona amica e di fiducia dell'interlocutore ha sostenuto che il giornalista non può utilizzare artifici e raggiri per raccogliere notizie che potrebbero essere acquisite con gli strumenti propri dell'inchiesta giornalistica.

In tal senso, il Garante aveva ritenuto l'acquisizione e la successiva messa in onda della conversazione telefonica non conforme ai princìpi e alle norme del codice deontologico dei giornalisti e del Codice, vietandone l'ulteriore diffusione Il Tribunale di Milano ha in particolare evidenziato che l'esimente prevista dal codice deontologico relativa alla possibilità di omettere l'informativa richiede che sia provata l'impossibilità di esercizio in altro modo della funzione informativa e che non erano stati allegari specifici elementi dai quali desumere quanto affermato (4 giugno 2015, n. 6968).

Accesso ai dati personali

Il Tribunale di Pisa ha confermato il provvedimento del Garante 17 aprile 2014, n. 213, (doc. web n. 3259462*)* con il quale era srato ordinato ad un istituto bancario di comunicare i dati riguardanti un cliente che aveva ricevuto un riscontro inidoneo alla propria richiesta di accesso ai dati personali, distinguendo tale diritto da quello di accesso alla documentazione bancaria previsto dal t.u. bancario (28 ottobre 2015, n. 1212).

In un'altra pronuncia, il Tribunale di Pesaro ha negato che la società ricorrente potesse invocare la tutela di cui all'art. 7 del Codice, in quanto con modifica legislativa del 2011 sono state espressamente sottratte alla predetta disciplina le persone giuridiche; ciò benché secondo una sentenza della CGUE (nelle cause riunite C-

92/09 e C-93/09, Volker und Markus Schecke GbR e Hartmut Eifert / Land Hessen) le persone giuridiche possano invocare la tutela degli artt. 7 e 8 della Carta dei diritti fondamentali dell'UE allorché la loro ragione sociale identifichi una o più persone fisiche, come nel caso della ricorrente società; tale sentenza, ha evidenziato il Tribunale, non ha espresso un principio di carattere generale, trattandosi invece di materia del tutto diversa da quello in esame (29 ottobre 2015 n. 812).

Vi sono state infine decisioni relative a materie diverse ed eterogenee.

Altre pronunce

Il Tribunale di Santa Maria Capua Vetere ha accolto il ricorso di un amministratore di condominio destinatario di un'ordinanza ingiunzione in relazione alla mancata risposta ad una richiesta di informazioni da parte del Garante circa l'affissione nella bacheca condominiale di un provvedimento comunale di sgombro contenente dati personali. Il Tribunale, ritenendo che gli obblighi collaborativi del privato nel procedimento innanzi al Garante sono finalizzati a comprimere il tempo e l'intensità della presunta violazione, ha deciso che la mancata spontanea collaborazione del ricorrente non avesse comportaro un aggravio nella definizione della procedura, se non per la tempistica, in quanto, a seguito dell'ispezione effettuata *in loco,* era stata verificata la cessazione della condotta contestata e non erano stati ravvisati gli estremi per adottare un provvedimento del Garante (30 aprile 2015, n. 1607). Avverso tale sentenza è stato proposto dal Garante ricorso per Cassazione.

Il Tribunale di Catania ha accolto il ricorso proposto da una società destinataria di un provvedimento ingiuntivo per avere trattato dati biometrici al fine di rilevare le presenze dei propri dipendenti in assenza di informativa e consenso e senza aver provveduto alla prevista notificazione al Garanre. La società aveva motivato tale condotta sostenendo che, nel caso specifico, non vi era alcun trattamento di dati biometrici, essendo i suddetti dati utilizzati solo per accertare che la mano che usa il *badge* sia la stessa utilizzata per configurare il *badge*, poiché l'apparecchiatura tecnica utilizzata non permette l'identificazione della persona (15 maggio 2015, n. 2164). Avverso tale sentenza è pendete ricorso in Cassazione proposto dal Garante.

Un'altta decisione ha accolto il ricorso della responsabile del trattamento dati di un centro per l'impiego in relazione alla mancata adozione delle misure di sicurezza, in riferimento alla giacenza, presso un cassone, di materiale contenente dati sensibili, destinato allo scarto d'archivio. Il Tribunale ha precisato che la norma del Codice punisce espressamente il titolare del trattamento, sicché non è ammissibile un'interpretazione estensiva riferita al responsabile, al quale invece può imputatsi la violazione solo se abbia disatteso le indicazioni ricevute dal titolare, evento che nel caso concreto non si è verificato. Inoltre, dalla contestata violazione era scaturito anche un procedimenro penale conclusosi con sentenza di assolvimento, ulteriore conferma della insussistenza della medesima violazione sul piano della sanzione amministrativa (Trib. Savona, 12 dicembre 2014, n. 1645).

Il Tribunale di Napoli ha confermato il provvedimento del Garante che ha prescritto, tra l'altro, ad una società di adottare soluzioni informatiche idonee ad assicurare il controllo delle attività svolte dagli incaricati del trattramento sui dati di traffico telefonico, anche mediante registrazione delle operazioni compiute in un apposito *audit log* (provv. del 17 gennaio 2008, doc. web n. 3136961). Il Tribunale ha respinto il ricorso della socierà, riconoscendo che il potere di imporre prescrizioni in materia di traffico telefonico si fonda sul provvedimento che, al par. 7.6, prevede esplicitamente la misura prescritta dal provvedimento impugnato (5 novembre 2015, n. 13976).

Anche in un altro caso, inerente l'invio, da parte di una società, di comunicazioni indesiderate di carattere promozionale via fax in assenza di consenso, è stato integralmente confermato il provvedimento del Garante 23 gennaio 2014, n. 30

(doc. web n. 2927848) (Trib. Milano, 23 aprile 2015, n. 5192).

Il Tribunale di Ivrea ha confermato un provvedimento del Garante 2 dicembre 2010 (doc. web n. 1784000) che ha dichiarato infondato il ricorso amministrativo con il quale l'interessato lamentava l'illiceità acquisizione, da parte di una società telefonica, dei dati relativi a depositi bancari a lui intestati, utilizzati allo scopo di promuovere una procedura di pignoramento per il recupero delle ingenti somme dovute dal ricorrente per fatture non pagate. In particolare, il giudice ha confermato l'assunto del Garante, secondo cui da un lato la normativa di tutela dei dati personali consente il trattamento effettuato per far valere o difendere un diritto in sede giudiziaria e per detto trattamento non è richiesta né l'informativa all'interessato (art. 13 comma 5, lett. *b*) né il suo consenso (art. 24 comma 1, lett. *f*); e, dall'altro, a mente dell'art. 160 del Codice, la validità, l'efficacia e l'utilizzabilità di atti, documenti e provvedimenti nel procedimento giudiziario basati sul trattamento di dati personali non conforme a disposizioni di legge o di regolamento restano disciplinate dalle pertinenti disposizioni processuali nella materia civile e penale, con ciò escludendo, *tout court,* la competenza del Garante a valutare l'eventuale illiceità del trattamento dei dati presentati all' A.G.O. (29 novembre 2011, n. 639).

Il Tribunale di Roma, in una sentenza di rigetto avverso un provvedimento dell'Autorità in materia di ttattamento di dati personali sullo stato di salute del 23 dicembre 2010 (doc. web n. 1800931), ha ptecisato che, con esclusione della diffusione, la tutela della riservatezza deve necessariamente affievolire in presenza di dati già divulgati dallo stesso interessato, che, di fatto, concretizza una forma di consenso implicito al loro trattamento (15 ottobre 2014, n. 19822). Avverso tale sentenza è stato proposto ricorso per Cassazione.

Lo stesso Tribunale, in altra pronuncia, ha confermato un altro provvedimento del Garante 19 giugno 2014 che aveva dichiarato infondato il ricorso contro un'asseritamente erronea segnalazione alla Centrale rischi, rilevando che il procedimento avviato ai sensi dell'art. 152 del Codice, è volto alla verifica della legittimità del trattamento dei dati personali e non può essere utilizzato per l'accertamento dei rapporti di credito intercorrenti tra i ricorrenti (18 giugno 2015, n. 13414).

Anche in altro caso, inerente il trattamento di dati giudiziari da parte di un soggetto pubblico, e, in particolare, la pubblicazione sul sito internet del decreto di rinvio a giudizio nei confronti, tra l'altro, di un candidato alle elezioni dell'organo collegiale dell'ente pubblico ricorrente, è stato integralmente confermato il provvedimento del Garante 17 gennaio 2013, n. 15 (doc. web n. 2315622). Il giudice, condividendo la tesi dell'Autorità, ha ritenuto che nel caso di specie non si era trattato di un trattamento per finalità elettorali espressamente previste tra quelle di interesse pubblico dal codice e dal tegolamento adottato dall'ente pubblico interessato, bensì di vera e propria propaganda elettorale attraverso una diffusione indiscriminata dei suddetti dati (Trib. Roma, 28 aprile 2015, n. 9346).

Il Tribunale di Napoli ha respinto il ricorso proposto da un esercizio commerciale contro il provvedimento del Garante 4 luglio 2013, n. 335 (doc. web n. 2577227) che aveva dichiarato illecito il trattamento dati effettuato con un sistema di videosorveglianza installato presso detto locale, accompagnato da un'informativa inidonea e posta in luogo non visibile all'esterno, in assenza di nomina del responsabile e/o incaricato del trattamento e di istruzioni circa le operazioni di trattamento effettuate. L'organo giudicante, preso atto del sopravvenuto adempimento da parte del ricorrente e del provvedimento di parziale annullamento del Garante, ha confermato per la parte restante il provvedimento, sostenendo che l'adempimento delle prescrizioni non elideva il carattere illecito del trattamento rendendo solo lecito, da quel momento in poi, ciò che in precedenza non lo era (20 gennaio 2015, n. 1534).

Infine il Tribunale di Bologna ha annullato il provvedimento del Garante 18 marzo 2010, n. 18 (doc. web n. 1709118) con il quale venivano determinati i casi in cui una società specializzata in sistemi di informazione creditizia poteva chiedere all'interessato un contributo spese per l'esercizio dei diritti di cui all'art. 7 del Codice, fissando altresì un limite massimo a tale contributo. In particolare, il provvedimento contestato prevedeva per talune ipotesi la gratuità del riscontro, per altre la possibilità di chiedere un contributo a carico dell'interessato. Il giudice ha ritenuto che la previsione della gratuità sia contraddittoria in quanto, nel caso in cui "si determina un notevole impiego di mezzi in relazione all'entità [.....] delle richieste", ai sensi dell'art. 10, comma 8 del Codice, è necessario individuare un contributo a favore della società ricorrente. È stato poi rilevato un profilo di irragionevolezza nell'ipotesi di gratuità qualora l'interessato chieda il riscontro via posta elettronica, in quanto "il notevole impiego di mezzi" relativo alla complessità ed entità delle richieste non riguarda tanto le modalità di trasmissione quanto quelle di archiviazione, conservazione, selezione ed estrazione dati (26 gennaio 2015, n. 2841).

20.4. *L'intervento del Garante nei giudizi relativi all'applicazione del Codice*

Conformemente agli indirizzi giurisprudenziali ed al parere espresso dall'Avvocatura generale dello Stato – il Garante, nei giudizi diversi da quelli direttamente attinenti a pronunce dell'Autorità, ha limitato la sua attiva presenza, 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, nel periodo di riferimento non è intervenuta in giudizio ma ha seguito con attenzione tutti i contenziosi relativi all'applicazione del Codice, chiedendo alle Avvocature distrettuali dello Stato di essere comunque informata sullo svolgimento delle vicende processuali e di ricevere comunicazione in merito agli esiti.

21 L'attività ispettiva e le sanzioni

21.1. *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 cd. provvedimenti generali.

Le ispezioni (303 nel 2015) sono effettuate sulla base di programmi elaborati 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 ispetriva vengono quindi rese pubbliche attraverso il sito web del Garante 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 2015 ha previsto che l'attività ispettiva fosse, tra l'altro, indirizzata nei seguenti settori:

- ospedali e aziende sanitarie con riferimento alle modalità di attuazione del Fascicolo sanitario elertronico e del *dossier* sanitario;
- società che effettuano artività di *marketing* telefonico mediante *call center* operanti all'estero;
- società che gestiscono sistemi di pagamento su dispositivi portatili (*mobile payment proximity*) ovvero che abilirano pagamenti o trasferimenti di denaro tramite telefono cellulare. L'elemento discriminante del *mobile payment* è l'uso del telefono cellulare come leva di innovazione nel processo di pagamento, indipendentemente dagli strumenti di pagamento utilizzati e dalle tecnologie di comunicazione adottate. Nello specifico il *mobile proximity payment* comprende i pagamenti elerttonici "di prossimità", ovvero pagamenti per cui sia necessaria una vicinanza fisica tra l'acquirente ed il venditore del prodotto/servizio acquistato. Nel *mobile proximity payment* il cellulare emula un pagamento ttamite carta;
- banche, con riferimento alla verifica sull'attuazione delle misure previste nel provvedimento generale relativo alla "tracciabilità delle operazioni bancarie";
- operatori telefonici, con riferimento ai trattamenti effettuati per la gestione dei servizi sms;
- società che forniscono servizi finalizzati alla fidelizzazione della clientela (carte fedeltà, *pay back*);
- attività di *marketing* telefonico effettuato da società, anche con riferimento al rispetto del provvedimento generale sulle cd. chiamate mute;
- centri di assistenza fiscale (caf), per la verifica del rispetto delle misure organizzative e di sicurezza adottate nell'ambito della trasmissione della dichiarazione dei redditi precompilata;
- società che forniscono *software* e servizi tecnologici nell'ambito delle attività di supporto alle indagini.

Come specificato al successivo paragrafo 21.3, nel periodo di riferimento sono state anche effettuate, in altri settori, verifiche:

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

In tutta l'attività è stata prestata specifica attenzione ai profili sostanziali del trattamento che spiegano significativi effetti sulle persone da esso interessate.

21.2. *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 a 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 principi 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 l. 24 novembre 1981, n. 689.

Grazie alla sinergia ormai collaudata con il Nucleo speciale *privacy* della Guardia di finanza, il Garante dispone di 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: nello specifico sono stati organizzati due seminari presso il Nucleo speciale *privacy* nell'ambito dei quali sono stati esaminati vari profili relativi ai procedimenti sanzionatori, nonché le indicazioni del Garante contenute nel parere sull'accesso alla dichiarazione precompilata da parte del contribuente e degli altri soggetti autorizzati del 19 febbraio 2015, n. 95 (doc. web n. 3741076).

Considerati gli ottimi risultati raggiunti nel rapporto di collaborazione, ormai ultra decennale, tra il Garante e la Guardia di finanza e al fine di tenere conto delle nuove sfide tecnologiche nonché del rilievo sempre maggiore che l'ambito internazionale avrà nelle istruttorie – anche a seguito della definizione del nuovo quadro normativo europeo –, è stato delineato, d'intesa con la Guardia di finanza, il contenuto di un nuovo protocollo d'intesa.

Il nuovo protocollo prevedrà, dal punto di vista strategico, che il Garante possa avvalersi di personale specializzato della Guardia di finanza per la conduzione di

ispezioni congiunte con altre autorità estere (l'introduzione del nuovo regolamento europeo in materia di dati personali, infatti, renderà tale necessità sempre più frequente).

Da un punto di vista più strettamente operativo, invece, il nuovo protocollo garantirà: una sempre maggiore semplificazione dei flussi documentali tra l'Ufficio e il Nucleo speciale *privacy* (attraverso l'uso sistematico di strumenti di trasmissione telematici); l'introduzione di modalità di verifica *online* di possibili violazioni alla normativa in materia di protezione dei dati personali (attraverso l'esame diretto di siti web, senza necessità di ispezioni *in loco*); un coinvolgimento stabile del Nucleo frodi telematiche della Guardia di finanza in attività ispettive o di analisi ad alto contenuto tecnico/informatico.

21.3. *I principali settori oggetto di controllo*

Oltre a quanto già riportato al paragrafo 21.1, nel 2015 le ispezioni effettuate dall'Autorità hanno riguardato i titolari del trattamento che:

- hanno notificato trattamenti di dati personali relativi alla rilevazione della posizione geografica di persone o oggetti mediante una rete di comunicazione elettronica (art. 37, comma 1, lett. *b*) unitamente al trasferimento di dati all'estero, al fine di verificare le tipologie di trattamento effettuate, le misure di sicurezza predisposte, nonché i presupposti giuridici, l'ambito e le modalità del trasferimento di dati personali in Paesi non appartenenti all'Unione europea;
- operano nel settore dei trasporti (ivi incluso il settore del setvizio di trasporto pubblico locale), trattando dati relativi alla geolocalizzazione di veicoli, con particolare riferimento all'utilizzo di tali sistemi nell'ambito del rapporto di lavoro. In questa attività è stata posta particolare attenzione al rispetto delle norme previste dalla disciplina lavoristica (artt. 114 del Codice e 4 della l. n. 300/1970), nonché alla corretta attuazione delle misure e degli accorgimenti prescritti dal Garante nell'ambito del provvedimento generale 4 ottobre 2011, n. 370 (doc. web n. 1850581). Tra questi ricordiamo: la non continuatività – di regola – del monitoraggio della posizione dei veicoli; la commisurazione dei tempi di conservazione delle diverse tipologie di dati trattati alle finalità in concreto perseguite; la designazione quali responsabili del trattamento ai sensi dell'art. 29 del Codice degli operatori economici che forniscono i servizi di localizzazione del veicolo e di trasmissione della posizione del medesimo;
- svolgono attività di *marketing* telefonico tramite *call center* operanri in Paesi al di fuori dell'Unione europea. In particolare, le verifiche in questo settore sono state indirizzate all'acquisizione di informazioni su: strutture societarie dei soggetti interessati; contratti con le società committenti; procedure adottate dal titolare del trattamento per il controllo della filiera e la corretta esecuzione delle istruzioni impartite ai responsabili; misure di sicurezza adottate; artuazione delle misure e degli accorgimenti prescritti dal Garante nell'ambito del provvedimento generale 10 ottobre 2013, n. 444 (doc. web n. 2724806) (tra cui: informativa all'interessato sull'ubicazione dell'operatore, possibilità di scelta di usufruire del servizio attraverso un operatore ubicato sul territorio nazionale, comunicazione al Garante in caso di trasferimento di dati personali ad un *call center* sito al di fuori dell'Unione europea);

- svolgono attività di *marketing* telefonico attraverso l'uso di sistemi automatizzati, con modalità tali da generare il fenomeno delle cd. chiamate mute. In particolare, le verifiche sono state indirizzate all'acquisizione di informazioni su: origine dei dati personali; *call center* utilizzati; società committenti; procedure adottate dal titolare del trattamento per garantire agli interessati l'effettivo esercizio dei diritti di cui all'art. 7 del Codice; adempimento degli obblighi di informativa e raccolta del consenso; attuazione delle misure e degli accorgimenti prescritti dal Garante nell'ambito del provvedimento generale 20 febbraio 2014, n. 83 (doc. web n. 3017499) (in particolare, l'adozione di strumenti di reportistica in grado di rilevare gli indicatori di prestazioni al fine di rispettare la percentuale massima di cd. chiamate mute ed i tempi minimi per la richiamata; i tempi di conservazione dei relativi report; l'adozione del cd. *comfort noise*);
- forniscono servizi di comunicazione elettronica accessibili al pubblico su reti pubbliche di comunicazione, al fine di 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 a: verifica dei dati conservati; 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); corretta attuazione delle misure e degli accorgimenti prescritti dal Garante nell'ambito del provvedimento 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;
- hanno notificato trattamenti di dati personali relativi al rischio sulla solvibilità economica, alla situazione patrimoniale, al corretto adempimento di obbligazioni, a comportamenti illeciti o fraudolenti (art. 37, comma 1, lett. *f*), unitamente al trasferimento di dati all'estero. In tale ambito i controlli hanno riguardato, tra l'altro: misure di sicurezza adottate, modalità di adempimento dell'obbligo di informativa agli interessati e dell'eventuale raccolta del consenso, presupposti giuridici, ambito e modalità dell'eventuale comunicazione di dati personali a soggetti terzi o del trasferimento degli stessi in Paesi non appartenenti all'Unione europea;
- operano nel settore del commercio di integratori alimentari (anche) mediante l'utilizzo di siti web, al fine di verificare: le tipologie di trattamento effettuate e le relative finalità, le modalità di adempimento dell'obbligo di informativa agli interessati e dell'eventuale raccolta del consenso, nonché i presupposti giuridici, l'ambito e le modalità dell'eventuale comunicazione di dati personali a soggetti terzi;
- operano nel settore della ricezione alberghiera con strutture di categoria elevata o di lusso, al fine di verificare la liceità del trattamento dei dati della clientela, anche con riferimento ai dati raccolti attraverso siti web o attraverso l'utilizzo di sistemi di videosorveglianza, con particolare evidenza per le modalità di rilascio dell'informativa e di raccolta del consenso degli interessati, ove necessario;

- operano nel settore della cura della persona, centri benessere e spa, al fine di verificare la liceità del trattamento dei dati della clientela, anche con riferimento ai dati raccolti attraverso siti web o attraverso l'utilizzo di sistemi di videosorveglianza, con particolare evidenza per le modalità di rilascio dell'informativa e di raccolta del consenso degli interessati, ove necessario;
- offrono servizi finalizzati alla conservazione di cellule cordonali/staminali, unitamente ad altre società che operano al di fuori del territorio italiano. Le verifiche effettuate sono state indirizzate a rilevare le modalità e le finalità del trattamento dei dati personali degli interessati, le misure di sicurezza adottate, le modalità con cui viene resa l'informativa e raccolto il consenso degli interessati, l'adempimento degli obblighi di notificazione (con particolare riferimento ai trattamenti previsti dall'art. 37, lett. *a*) e *b*) del Codice). I controlli sono stati tesi ad appurare, altresì, l'ambito, i presupposti e le modalità dell'eventuale comunicazione di dati personali a società controllanti, collegate o soggetti terzi, nonché il trasferimento degli stessi in Paesi non appartenenti all'Unione europea;
- operano nel settore delle attività sportive (palestre e centri *fitness*) al fine di appurare il rispetto della disciplina in materia di protezione dei dati personali, con particolare riferimento ai profili dell'informativa resa agli interessati (anche in merito al trattamento di dati personali tramite impianti di videosorveglianza o siti web), nonché del consenso acquisito dagli stessi, ove necessario.

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 stare 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 significarivi per i cittadini.

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

Attraverso le ispezioni l'Autorità svolge una penetrante attività istrutroria che può essere finalizzata, a seconda del caso, a uno o piìn dei seguenti obiettivi:

- intervenire sui trattamenti illeciti da chiunque effettuati adottando i provvedimenti cautelari previsti dalla legge (blocco e diviero) e/o definendo le misure necessarie da prescrivere per rendere il trattametito conforme alla legge (contrasto dell'illecito);
- verificare lo stato di artuazione 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 al 2015, tra i provvedimenti più rilevanti adottati sulla base degli elementi istruttori acquisiti in sede ispettiva si segnalano, in ordine cronologico, quelli con i quali il Garante ha:

- dichiarato illecito e vietato il trattamento dei dati personali effettuato da una società monitorando il traffico in rete di un dipendente, poi licenziato, in violazione delle indicazioni fornite nelle Linee guida per posta elettronica e internet (provv. 1° marzo 2007, n. 13, doc. web n. 1387522), nonché dell'art. 4, l. n. 300/1970, con la conseguente inutilizzabilità dei dati trattati in violazione di legge, ai sensi dell'art. 11, comma 2 del Codice (provv. 5 febbraio 2015, n. 65, doc. web n. 3813428);
- dichiarato illecito e vietato il trattamento dei dati personali, utilizzati da una società di formazione per attività promozionale effettuata per mezzo dell'invio di posta cartacea, acquisiti senza aver preventivamente informato gli interessati né acquisito il loro consenso per il trattamento (provv. 5 marzo 2015, n. 120, doc. web n. 3871397);
- prescritto a due società di rafforzare le misure di sicurezza, adottate a tutela dei dati personali degli interessati, individuando (*ex* art. 31 del Codice) ulteriori idonei accorgimenti volti a prevenire la conoscibilità dei dati da parte di terzi non autorizzati e la loro successiva utilizzabilità in operazioni di trattamento non compatibili con gli scopi che ne giustificano la raccolta (provv. 26 marzo 2015, n 181, doc. web n. 4002999);
- dichiarato illecito e vietato il trattamento dei dati personali idonei a rivelare lo stato di salute di un'interessata comunicati in via confidenziale dalla stessa a un proprio corrispondente operante presso un'agenzia affiliata ad un gruppo immobiliare e da quest'ultimo inoltrata a circa 200 agenzie appartenenti al medesimo gruppo. Dalla complessa istruttoria, effettuata anche mediante accertamenti ispettivi, è emerso che il trattamento di dati anche sensibili era stato effettuato in assenza di idonea informativa all'interessata e in violazione delle garanzie previste dall'art. 26 del Codice (provv. 23 aprile 2015, n. 242, doc. web n. 3966213);
- dichiarato illecito il trattamento effettuato mediante un sistema di videosorveglianza da un titolare del trattamento pubblico, 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. 30 luglio 2015, n. 455, doc. web n. 4261028);
- disciplinato il trattamento di dati personali nell'ambito dei servizi di *mobile ticketing* prescrivendo: l'adozione di specifiche misure e accorgimenti per l'acquisto di titoli di viaggio digitali tramite ricorso al credito telefonico, con riguardo all'informativa e al consenso, alle misure di sicurezza e alla conservazione dei dati nonché l'adozione di ulteriori misure e accorgimenti per l'acquisto di titoli di viaggio digitali tramite ricorso alla carta di credito e ad un circuito di intermediazione (con provv. 10 settembre 2015, n. 467, doc. web n. 4273074 è stato posto in consultazione pubblica lo schema di provvedimento generale in materia);
- dichiarato illecito e vietato il trattamento di dati biometrici dei dipendenti di un ente locale effettuato in violazione dei princìpi di liceità, necessità, proporzionalità, pertinenza e non eccedenza dei trattamenti effettuati (art. 11, comma 1, lett. *a*) e *d*) del Codice), in assenza della previa notificazione

al Garante (art. 37 del Codice), nonché della preventiva richiesta di verifica preliminare (art. 17 del Codice) (provv. 22 ottobre 2015, n. 552, doc. web n. 4430740);

- prescritto ad un'Asl, oltre ad integrare il modello di informativa adottato, di incrementare le misure di sicurezza a protezione dei dati personali degli assistiti, provvedendo in particolare a: 1) mettere in atto specifici accorgimenti che consentano ai soli professionisti sanitari che hanno in cura il paziente di accedere al relativo *dossier* sanitario; 2) adottare specifici accorgimenti che consentano al personale amministrativo di accedere al *dossier* dei soli soggetti che sono coinvolti nell'attività amministrativa per la quale è necessario l'accesso e comunque con riferimento alle sole informazioni indispensabili per assolvere alle funzioni amministrative cui sono preposti (provv. 22 ottobre 2015, n. 550, doc. web n. 4449114).

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 il Garante, rilevando condotte punite come reato, ha disposto la trasmissione degli atti alla competente Procura della Repubblica.

21.5. *L'attività sanzionatoria del Garante*

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

Nell'anno 2015, in relazione alle istruttorie effettuate, sono state inviate 33 segnalazioni di violazioni penali all'autorità giudiziaria (cfr. sez. IV, tab. 7) di cui:

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

Come dimostrano i dati sopra riportati, 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.

In questo ambito merita una segnalazione la recente sentenza della Corte di Cassazione penale (n. 1986/2015) che ha respinto la questione di legittimità costituzionale relativa all'art. 169 del Codice, con riferimento agli artt. 2, 3, 21, 24, 25 della Costituzione. Nella motivazione si legge infatti che "non sussiste, infatti, alcun contrasto di tale disposizione con gli art. 3 e 24 Cost., perché rientra in generale nella piena discrezionalità del legislatore la fissazione dell'ammontare dell'oblazione ai fini dell'estinzione del reato, come avvenuto, attraverso il richiamo all'art. 162, comma 2-*bis*, in ragione di euro 30.000". Nella stessa sentenza la Suprema Corte afferma, con riferimento alla responsabilità penale che la stessa "è stata, del resto, positivamente accertata dalla Guardia di finanza nel corso delle indagini preliminari, attraverso l'accertamento diretto della mancata designazione dell'incaricato del trattamento in relazione ad un sito internet nel quale era possibile la raccolta di dati personali sensibili relativi a una serie indeterminata di persone", confermando la linea costantemente seguita negli anni dall'Autorità circa le conseguenze penali derivanti dall'omessa designazione degli incaricati del trattamento dei dati personali.

Come per l'anno precedente, anche nel 2015 si è avuta una rilevante 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.

Sul punto appare opportuno evidenziare che tale disciplina ha subito profonde modifiche a seguito dell'adozione del d.lgs. 14 settembre 2015, n. 151 (cd. *Jobs Act*). Le modifiche apportate attengono sia alla parte sostanziale della disciplina del controllo a distanza dei lavoratori (art. 4, l. n. 300/1970) che a quella sanzionatoria (all'art. 171 del Codice).

In questo ambito, limitiamo la riflessione alle modifiche apportate alla parte sanzionatoria, ovvero alla nuova formulazione dell'art. 171 del Codice "La violazione delle disposizioni di cui all'articolo 113 e all'articolo 4, primo e secondo comma, della l. 20 maggio 1970, n. 300, è punita con le sanzioni di cui all'articolo 38 della l. n. 300 del 1970." Per quanto di interesse, la parte rilevante attiene al richiamo al primo e secondo comma dell'art. 4; tale norma prevede: al comma 1, che gli impianti audiovisivi e gli altri strumenti dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori possono essere impiegati esclusivamente per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale e possono essere installati, previo accordo sindacale o, in mancanza di accordo, previa autorizzazione della Direzione del lavoro; al comma 2, che la disposizione di cui al comma 1 non si applica agli strumenti utilizzati dal lavora-

tore per rendere la prestazione lavorativa e agli strumenti di registrazione degli accessi e delle presenze.

È venuto quindi meno il divieto dell'uso di impianti audiovisivi e di altre apparecchiature per finalità di controllo a distanza dell'attività dei lavoratori. Tale divieto, unitamente a quello relativo all'istallazione di sistemi che, pur avendo altre finalità, possano comportare anche il controllo a distanza dei lavoratori – in assenza dell'accordo sindacale o dell'autorizzazione dell'ispettorato del lavoro – costituivano, fino alla recente riforma, le condotte coperte dalla sanzione penale.

Ne consegue che la prima fattispecie, che puniva *tout court* l'istallazione di sistemi per finalità di controllo a distanza dell'attività dei lavoratori, è venura meno, mancando, nel nuovo testo, il suo presupposto (ovvero il divieto).

La sanzione penale resta invece con riferimento all'utilizzo di impianti audiovisivi e di altri strumenti dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori, impiegati esclusivamente per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale, qualora installati in assenza dell'accordo sindacale o, in alternativa, dell'autorizzazione della Direzione territoriale del lavoro.

Meno chiara risulta invece l'inclusione del comma 2, dell'art. 4, dello Statuto nell'area coperta dalla sanzione penale prevista dal nuovo art. 171; tale comma sottrae, dall'ambito di applicazione delle disposizioni di cui al comma 1 (e quindi esonera dalla necessità di accordo/autorizzazione), gli "strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa e agli strumenti di registrazione degli accessi e delle presenze". Da ciò ne dovrebbe derivare che, ove il datore di lavoro ritenga erroneamente che determinati strumenti siano esonerati dagli adempimenti del primo comma (accordo o autorizzazione), verrebbe meno l'eccezione e quindi rientrerebbero nuovamente nella regola prevista dal comma 1, con la conseguenza che la condotta punita sarebbe, anche in questi casi, l'assenza dell'accordo o dell'autorizzazione. Sul punto occorrerà attendere l'applicazione della norma in sede penale.

È invece sicuramente sottratto alla valutazione del giudice penale il contenuto del comma 3 dell'art. 4 che prevede che "le informazioni raccolte ai sensi dei commi 1 e 2 sono utilizzabili a tutti i fini connessi al rapporto di lavoro a condizione che sia data al lavoratore adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli e nel rispetto di quanto disposto dal decreto legislativo 30 giugno 2003, n. 196".

Da ciò ne deriva che la mancata informazione ai lavoratori circa le modalità di uso degli strumenti e di effettuazione dei controlli rientra invece nell'orbita delle valutazioni di competenza dal punto di vista della legittimità del trattamento dei dati personali.

21.5.2. Le sanzioni amministrative

Nell'anno 2015 sono stati avviati n. 1.696 nuovi procedimenti sanzionatori amministrativi (cfr. sez. IV, tab. 6).

All'accertamento delle violazioni amministrative previste dal Codice può procedere:

- il personale dell'Ufficio 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 novembte 1981, n. 689.