ai molteplici soggetti coinvolti (collaboratori, *franchisor*, società appaltatrici e subappaltatrici), il ruolo effettivamente svolto da ciascuno nella vicenda e le relative eventuali responsabilità – il Garante ha ritenuto, anche sulla base dei rapporti in essere tra le singole società, che i collaboratori avessero agito per finalità, nell'interesse e a tutela, anzitutto, del *franchisor* e che a tale soggetto (unitamente ad una delle società appaltatrici coinvolte, operante in piena autonomia) doveva essere ascritta la responsabilità del relativo operato. Muovendo da tali premesse, accertata l'assenza di idonei presupposti per il trattamento dei dati personali e sensibili dell'interessata, ha provveduto a dichiararne l'illiceità, vietando al *franchisor* e alla società co-titolare l'ulteriore trattamento dei medesimi dati, fatta salva la loro conservazione a fini di giustizia. Ha inoltre prescritto alle due società di adottare idonee misure atte a garantire una scrupolosa vigilanza sui soggetti incaricati di operare nel loro interesse e/o per loro conto, sensibilizzando costoro al puntuale rispetto delle istruzioni ricevute nella veste di incaricati del trattamento (art. 30 del Codice); è stato prescritto, infine, al *franchisor* di designare una delle società appaltatrici coinvolte nella vicenda quale responsabile *ex* art. 29 del Codice (provv. 23 aprile 2015, n. 242, doc. web n. 3966213).

Esonero dell'informativa

A seguito di un'avvenuta cessione di ramo di azienda, l'Autorità ha esonerato una compagnia aerea dall'obbligo di rendere l'informativa agli interessati (in particolare, ai clienti, alle altre controparti contrattuali ed i ai dipendenti della società cedente).

Al riguardo – come già sostenuto in altre occasioni - ha rilevato che in ragione della peculiare disciplina che regola la cessione di ramo di azienda (artt. 2558, 2559, 2560 e 2112 c.c.) sul piano sostanziale, si viene a determinare una successione legale del nuovo imprenditore in tutti i rapporti giuridici e in tutte le posizioni attive e passive facenti capo al cedente, sicché, subentrando l'acquirente nella stessa posizione dell'alienante, il trattamento dei dati personali connessi alla gestione dei rami di azienda ceduti, non necessita di alcun consenso, trovando applicazione il presupposto equipollente di cui all'art. 24, comma 1, lett. *b*), del Codice, che consente di prescindere da esso nel caso in cui il trattamento sia necessario per eseguire obblighi derivanti da un contratto di cui sia parte lo stesso interessato. Ciò premesso, restando comunque doveroso il rispetto dell'obbligo di informativa posto dall'art. 13 del Codice che, nell'ipotesi in cui i dati personali non siano raccolti direttamente presso l'interessato, impone al titolare del trattamento di rendere l'informativa "all'atto della registrazione dei dati o, quando è prevista la loro comunicazione, non oltre la prima comunicazione" (comma 4), - dopo aver verificato l'impossibilità di rendere l'informativa a tutti gli interessati in forma individuale in ragione della natura sproporzionata dei mezzi astrattamente impiegabili - ha accolto la richieste di esonero, ai sensi dell'art. 13, comma 5, lett. *c*), del Codice, prescrivendo specifiche modalità alternative e semplificate (provv. 19 febbraio 2015, n. 97, doc. web n. 3864423).

14 I dati biometrici

14.1. *Il trattamento dei dati biometrici nel settore societario e professionale*

Sono pervenute al Garante numerose richieste di verifica preliminare (art. 17 del Codice) relativamente al trattamento di dati biometrici connesso all'utilizzo di soluzioni di firma di atti e documenti informatici.

In un caso, il trattamento – benché riconducibile nelle ipotesi di esonero contemplate dal provvedimento generale 12 novembre 2014, n. 513 (doc. web n. 3556992) – ha formato comunque oggetto di attenzione da parte del Garante per espressa volontà della richiedente, società ideatrice e fruitrice del sistema dalla stessa realizzato. Tale sistema, con riferimento al correlato trattamento di dati personali e biometrici, è risultato sostanzialmente conforme, sulla base delle indicazioni fornite, alle prescrizioni contenute nel richiamato provvedimento generale. L'Autorità, tuttavia, ha prescritto alla società di provvedere, se necessario, alla designazione di tutti i soggetti preposti al trattamento dei dati anche biometrici degli interessati quali incaricati *ex* art. 30 del Codice, nonché di trattare questi ultimi solo dopo aver adempiuto all'obbligo di notifica di cui agli artt. 37 e 38 dello stesso Codice (provv. 17 settembre 2015, n. 478, doc. web n. 4373152).

In un altro caso l'Autorità è stata chiamata a pronunciarsi su un trattamento connesso all'utilizzo di un sistema di firma "grafometrica" in ambito notarile. Tale sistema, preordinato alla raccolta dei dati biometrici dei partecipanti all'atto (parti, fidefacienti, interpreti, testimoni) in termini sostanzialmente conformi al menzionato provvedimento generale, non sarebbe stato riconducibile, tuttavia, alle soluzioni di firma elettronica avanzata poste a base del medesimo provvedimento generale, in ragione dei "limiti d'uso" connessi a quest'ultima (art. 60 d.P.C.M., 22 febbraio 2013). L'Autorità, nel ritenere che tale aspetto non incidesse significativamente rispetto ai sistemi in precedenza esaminati, ha ammesso il trattamento oggetto dell'istanza (proposta dal Consiglio nazionale del notariato in ragione della rilevanza per l'intera categoria professionale), prescrivendo comunque ai titolari alcune misure aggiuntive a garanzia degli interessati, tra cui l'adozione di idonei meccanismi di autenticazione "forte" per l'accesso alle postazioni e adeguati tempi di *time-out* automatico per l'applicazione utilizzata. È stata invece respinta, per altro verso, la contestuale richiesta di esonero dalla notificazione formulata ai sensi dell'art. 37, comma 2, del Codice, attesa la peculiare natura dei dati trattati e l'oggettiva rischiosità del trattamento (provv. 25 novembre 2015, n. 619, doc. web n. 4538440).

Non consta di precedenti, invece, la pronuncia in tema di riconoscimento facciale applicato a un sistema di selezione delle immagini dei passeggeri ritratti a bordo delle navi da crociera (provv. 18 giugno 2015, n. 360, doc. web n. 4170232). Tale sistema, basato sul confronto (consensuale) delle caratteristiche biometriche dei volti estratte da apposite foto-campione con quelle ricavate dagli scatti quotidianamente effettuati dal fotografo di bordo, avrebbe permesso ai passeggeri di visionare le sole immagini di propria pertinenza, evitando così accessi indistinti e generalizzati alle fotografie altrui. Inoltre, la soluzione descritta avrebbe consentito di ridurre significativamente l'impatto ambientale derivante dai processi di smaltimento dell'ingente quantitativo di fotografie invendute (pari a circa il 92%, su un totale

approssimativo di 11.300.000 scatti annuali). L'Autorità, nel valutare positivamente l'istanza presentata, ha ritenuto che il trattamento dei dati biometrici dei passeggeri, effettuato su base volontaria e secondo le modalità indicate, non fosse illecito, né sproporzionato rispetto alla finalità dichiarata; nondimeno, è stato prescritto alla società di adottare opportuni accorgimenti atti a rendere compiutamente informati gli interessati in ordine al trattamento dei loro dati anche biometrici, nonché di provvedere all'effettiva e irreversibile cancellazione, al termine del periodo di riferimento, delle foto scattate e dei codici associati ai volti ivi presenti (lecitamente trattati dal titolare per effetto del bilanciamento di interessi disposto dall'Autorità con il medesimo provvedimento). Ha inoltre raccomandato alla società di assicurare che le registrazioni degli accessi al *database* contenente i predetti codici presentassero le medesime caratteristiche di quelle richieste dal provvedimento generale sugli amministratori di sistema (provv. 27 novembre 2008, doc. web n. 1577499).

Meritano di essere citate inoltre, soprattutto per i complessi profili tecnologici esaminati, le richieste di verifica preliminare riguardanti il trattamento di dati biometrici nell'ambito di un servizio di firma digitale remota con autenticazione biometrica da parte di un istituto bancario (provv. 28 maggio 2015, n. 318, doc. web n. 4167873); il trattamento di dati biometrici nell'ambito di un sistema di firma elettronica avanzata realizzata attraverso firma grafometrica da un istituto bancario (provv. 17 dicembre 2015, n. 662, doc. web n. 4645479); il trattamento di dati biometrici connesso a una soluzione di firma elettronica avanzata basata su bio–penna (provv. 4 giugno 2015, n. 336, doc. web n. 4172308).

14.2. *Il trattamento dei dati biometrici nel rapporto di lavoro*

Con il provvedimento generale prescrittivo in tema di biometria 12 novembre 2014, n. 513 (doc. web n. 3556992) il Garante ha ribadito che il trattamento di dati biometrici, in considerazione della loro stretta (e stabile) relazione con l'individuo e la sua identità, può essere effettuato solo previa adozione di particolari cautele. In particolare, tutti coloro che intendano effettuare tale tipologia di trattamenti sono tenuti a presentare un'istanza di verifica preliminare al Garante, salvi alcuni casi di esonero puntualmente individuati, sempre che vengano adottate specifiche misure e accorgimenti tecnici e che siano rispettati i principi generali di liceità, finalità, necessità e proporzionalità dei trattamenti.

Accesso ad aree riservate

In un caso specifico l'Autorità ha ritenuto lecito il trattamento dei dati biometrici dei lavoratori (impronte digitali), prospettato da una società che gestisce spazi commerciali all'interno di alcuni aeroporti internazionali, allo scopo di consentire ai soli dipendenti previamente autorizzati l'accesso a determinate aree (ove vengono depositate merci di particolare valore o collocate particolari apparecchiature informatiche). Considerato che alla luce delle specificità del sistema prescelto non è stato ritenuto applicabile l'esonero dall'obbligo di attivazione del procedimento di verifica preliminare, con il provvedimento sono state altresì prescritte alcune cautele ritenute necessarie per rafforzare le misure di sicurezza e per tenere distinte le basi di dati relative, rispettivamente, ai riferimenti biometrici ed agli altri dati personali dei dipendenti (provv. 18 giugno 2015, n. 361, doc. web n. 4173465).

Finalità di rilevazione delle presenze

In relazione, invece, all'utilizzo di un sistema biometrico da parte di un Comune per finalità di rilevazione delle presenze in servizio dei dipendenti, all'esito di una valutazione effettuata alla luce dei principi di necessità e proporzionalità rispetto alle finalità perseguite, il Garante non ha rinvenuto ragioni specifiche in base alle quali altri e diversi strumenti automatizzati (es. il *badge*, se del caso associato ad un pin

individuale) dovessero essere ritenuti inadatti a realizzare legittimi obiettivi di efficienza nell'attività di gestione del personale, né nel caso concreto sono emersi specifici motivi per i quali il personale direttivo sarebbe srato impossibilitato a svolgere l'ordinaria attività di controllo sulla corretta esecuzione della prestazione lavorativa. Non sono, peraltro, emerse concrete ipotesi di violazione dei doveri d'ufficio da parte dei dipendenti o elementi tali da ritenere fondato il timore di abusi. È stato, altresì, rilevato che il titolare del trattamento non aveva ottemperato all'obbligo di effettuare la notificazione del ttattamento e di presentare la richiesta di verifica preliminare. Conseguentemente l'Autorità ha disposto il divieto dell'ulteriote trattamento dei dati biometrici riferiti ai dipendenti (provv. 22 ottobre 2015, n. 552, doc. web n. 4430740).

15 Attività di normazione tecnica internazionale e nazionale

Nel 2015 l'Autorità ha collaborato, armonizzando la propria posizione con quelle delle altre autorità di protezione dati per il tramite del WP29, all'elaborazione di norme tecniche nell'ambito dell'ente di standardizzazione internazionale ISO, sia all'interno del Working Group 5 - Sottocomitato 27 (SC27), competente in materia di sicurezza di gestione delle identità, biometria e *privacy*, sia e del *Joint Technical Committee* (JTC1), sulla sicurezza delle informazioni.

In particolare si menzionano:

- ISO 29134 - *Privacy Impact Assessment -Guidelines*: linea guida per condurre un *Privacy Impact Assessment* (PIA) allo scopo di valutare e mitigare i rischi relativi al trattamento di dati personali attraverso un approccio di gestione del rischio ispirato alla norma tecnica ISO 31000 e definire i controlli di sicurezza (ISO/IEC 27002) relativi alla protezione dei dati personali (ISO/IEC 29151);
- ISO 29151- *Code of practice for the protection of personally identifiable information*: catalogo di controlli per la protezione dei dati personali, sul modello dei controlli di sicurezza previsti dalla ISO/IEC 27002, nonché di controlli relativi alla protezione dei dati personali derivati dai princìpi della ISO/IEC 29100 (*Privacy Framework*).

L'Autorità, inoltre, ha contribuito ai lavori di UNINFO - l'ente di normazione federato con UNI (Ente Nazionale Italiano di Unificazione) - riguardanti:

- l'elaborazione di una metodologia basata sul sistema e-CF per definire i profili professionali di terza generazione relativi alla gestione della *privacy*;
- la revisione della traduzione italiana della ISO 29100 (*Privacy Framewok*) in cui si è tenuto conto delle definizioni presenti nella legislazione italiana e in uso corrente al momento della conclusione dei lavori (ottobre 2015);
- la stesura di una norma tecnica sui "Criteri d'identificazione delle *app* nel mondo socio-sanitario della salute" per una corretta identificazione e caratterizzazione delle *app* nonché per favorire una maggiore consapevolezza da parte degli utilizzatori.

16 Il trattamento dei dati nel condominio

In materia di condominio l'attività dell'Autorità nel 2015 è stata prevalentemente indirizzata all'analisi delle implicazioni della riforma entrata in vigore nel giugno del 2013 (l. 11 dicembre 2012, n. 220, recante modifiche alla disciplina del condominio negli edifici), al fine di fornire ulteriori chiarimenti rispetto ai profili attineuti il tema del trattamento di dati personali (cfr. Relazione annuale 2014, p. 121).

In particolare sono state nuovamente oggetto di attenzione da parte del Garante le norme inerenti le nuove "Attribuzioni dell'amministratore" relative, tra l'altro, alla tenuta di vari registri, tra i quali è ricompreso anche il cd. "registro di anagrafe condominiale" (cfr. art. 1130, comma 1, punto 6, c.c.). Al riguardo, il Garante – nel sottolineare l'alterità tra l'esercizio del diritto di accesso ai dati personali disciplinato dagli artt. 7 ss. del Codice e il diverso diritto di prendere visione e di ottenere eventualmente copia del registro nella sua interezza, ai sensi dell'art. 1129 c.c. – ha chiarito che il registro può essere visionato, previa richiesta all'amministratore, dagli interessati gratuitamente e che gli stessi possono ottenerne eventualmente copia, previo rimborso della relativa spesa. L'Autorità ha dunque colto l'occasione per ribadire, in termini generali, quanto già indicato nel provvedimento del 18 maggio 2006 in materia di trattamento di dati personali nell'ambito dell'amministrazione di condomini (doc. web n. 1297626), e cioè che la conoscibilità delle informazioni concernenti i partecipanti alla compagine condominiale deve restare impregiudicata qualora ciò sia conforme alla disciplina civilistica o comunque sia prevista in base ad altre norme presenti nell'ordinamento, purché sussistano i relativi presupposti fissati dalla legge.

In occasione di un ulteriore quesito sul tema, l'Autorità ha fatto nuovamente presente che non si ravvisa alcuno specifico obbligo a carico del condomino di allegare documenti a riprova della veridicità delle informazioni rese ai fini della costituzione del citato registro di anagrafe da parte dell'amministratore di condominio. Si è, in particolare, puntualizzato che la trasmissione all'amministratore da parte del condomino della copia autentica del titolo che determina il trasferimento del diritto di proprietà prevista dall'art. 63 disp. att. c.c. concerne, espressamente, l'ipotesi in cui viene effettuata dallo stesso un'operazione di compravendita e pertanto non riguarda propriamente la tenuta del registro dell'anagrafe condominiale da parte dell'amministratore, se non eventualmente in un'ottica di successivo aggiornamento dello stesso. La *ratio* di tale disposizione normativa, non riguarda quindi la specifica disciplina inerente la realizzazione del registro dell'anagrafe condominiale di cui all'art. 1130 c.c., ma è piuttosto volta a soddisfare l'esigenza di sollevare il proprietario dell'immobile, che cede il diritto sull'unità immobiliare a terzi, dall'obbligo di contribuzione delle spese condominiali dal momento in cui il suddetto trasferimento viene reso noto al condominio (nota 16 dicembre 2015).

17 Il trasferimento dei dati all'estero

Con riguardo al tema dei trasferimenti transfrontalieri di dati personali, l'attività del Garante si è innanzitutto concentrata, come già verificatosi in passato, sulle numerose istanze volte al rilascio di autorizzazioni al trasferimento di dati verso Paesi terzi tramite le cd. *Binding corporate rules* (Bcr). È ormai evidente il crescente interesse e il diffuso utilizzo da parte del settore privato delle Bcr quale strumento privilegiato per il trasferimento di dati personali verso Paesi terzi effettuato nell'ambito di gruppi di imprese. Stante il cospicuo numero di autorizzazioni rese nel corso degli anni, l'Autorità, nel periodo di riferimento, ha effettuato alcuni accertamenti d'ufficio volti a verificare l'effettiva adozione, nonché la corretta applicazione, da parte delle imprese facenti parte dei gruppi e operanti sul territorio nazionale, di tali strumenti di trasferimento di dati all'estero.

Per quanto concerne le istanze pervenute nel 2015 ed inerenti l'impiego delle Bcr (per lo più, aventi ad oggetto il trasferimento di dati relativi a dipendenti, clienti e fornitori), sono state avviate istruttorie complesse che si sono concluse con l'approvazione di 5 autorizzazioni rilasciate dal Garante a conclusione di un *iter* nel corso del quale è stata verificata la conformità del testo delle Bcr – approvato al termine delle procedure europee tutte di mutuo riconoscimento –, con l'ordinamento italiano e con alcuni dei principali criteri stabiliti in materia dal Gruppo Art. 29 (cfr. provv.ti 2 aprile 2015 n. 197, doc. web n. 4003088; 13 maggio 2015 n. 290, doc. web n. 4167370; 10 settembre 2015 n. 470, doc. web n. 4362580; 22 ottobre 2015 n. 551, doc. web n. 4589496; 5 novembre 2015 n. 575, doc. web n. 4587199). Tali istruttorie sono state condotte alla stregua delle verifiche poste in essere negli anni precedenti in relazione ad analoghe istanze (cfr. Relazione 2014, p. 126, con particolare riguardo ai casi, oggetto di analisi anche nel periodo di riferimento, di Bcr consistenti esclusivamente in dichiarazioni unilaterali rilasciate dalla società capogruppo o in semplici *privacy policy*).

Il 2015 – come sopra evidenziato – si è caratterizzato anche per le indagini effettuate *in loco* nei confronti di alcune società italiane operanti sia nel settore manifatturiero, sia in quello della gestione dei pagamenti alle quali, nel corso degli anni 2001-2013, il Garante ha rilasciato le autorizzazioni nazionali per consentire l'utilizzo da parte delle stesse delle Bcr.

Tali indagini hanno evidenziato, in termini generali, alcune discrasie tra quanto dichiarato dalle società italiane in sede di richiesta di autorizzazione nazionale e quanto effettivamente posto in essere dalle stesse al proprio interno. Da una parte, infatti, è emerso che alcune delle società coinvolte negli accertamenti non effettuano, in realtà, alcun trasferimento di dati personali nell'ambito del gruppo e quindi non si avvalgono, in concreto, dello strumento delle Bcr (pur richiesto ed ottenuto); dall'altra, si è potuto rilevare che in taluni casi le società, nel porre in essere i trasferimenti di dati all'estero, non sembrano avere autonomi poteri decisionali in ordine alle iniziative da intraprendere all'interno della propria struttura organizzativa per poter realizzare in concreto quanto stabilito in materia di Bcr.

L'Autorità nel verificare, nel corso dei citati accertamenti, la sussistenza o meno dei singoli requisiti previsti in materia di Bcr, ha comunque potuto rilevare alcune criticità; ciò, in particolare, con riferimento al rispetto del principio di trasparenza

17

di cui al punto 5.7. del WP 74, nonché in materia di previsione di programmi di *audit*, così come indicato al punto 5.2. del WP 74. Ha pertanto fornito, all'esito delle verifiche condotte, alcune prescrizioni alle società interessate dai controlli, invitando le stesse ad adoperarsi per assicurare a tutti gli interessati una agevole individuazione e consultazione delle Bcr ponendo, ad esempio, i documenti che le compongono in un medesimo riquadro del sito e comunque differenziandole dal contesto delle ulteriori *policy* in materia di *privacy* presenti sui siti web delle società, nonché a prevedere e realizzare al proprio interno i programmi di *audit* come indicato dal Gruppo Art. 29. A fronte di tali richieste, le società hanno provveduto a porre in essere gli opportuni accorgimenti all'interno delle proprie strutture organizzative per garantire una effettiva e corretta applicazione dei princìpi contenuti nelle Bcr che erano già state oggetto di autorizzazione.

Sotto altro profilo, l'atrenzione del Garante è stata anche rivolta all'importante novità rappresentata dalla sentenza 6 ottobre 2015 con cui la CGUE si è pronunciata in ordine alla causa C-362/14, Maximillian Schrems vs. Data Protection Commissioner, dichiarando invalida la decisione della Commissione europea 26 luglio 2000 n. 2000/520/CE con la quale era stato ritenuto adeguato il livello di protezione dei dati personali garantito dagli Stati Uniti d'America nel contesto del cd. regime di *Safe Harbor*. Considerato il forte impatto di tale pronuncia sul complesso scenario relativo ai flussi dei dati transfrontalieri che coinvolgono l'Unione europea e gli Stati Uniti d'America, la questione è divenuta oggetto di un'attenta valutazione da parte dei Garanti europei riuniti nel Gruppo Art. 29 che hanno formulato alcune preliminari osservazioni in merito agli effetti della menzionata decisione sui trasferimenti dei dati effettuati dal territorio dell'Unione europea verso gli Stati Uniti d'America e alle future iniziative che gli stessi intendono intraprendere al fine di disciplinare adeguatamente tale tipologia di flussi transfrontalieri. In tale scenario, l'Autorità è intervenuta, con riferimento all'ambito nazionale, disponendo con provvedimento 22 ottobre 2015, n. 564 (doc. web n. 4396484) la caducazione dell'autorizzazione, resa il 10 ottobre 2001 sulla base della menzionata decisione della Commissione dichiarata invalida e volta a consentire i trasferimenti di dati personali dal territorio nazionale verso organizzazioni aventi sede negli Stati Uniti e operanti nel rispetto dei princìpi del *Safe Harbor* (doc. web n. 30939).

Stante il rilievo delle novirà menzionate, anche al fine di contribuire alla menzionata attività di approfondimento attualmente in corso a livello europeo e di sensibilizzare i soggetti coinvolti da tali trasferimenti, l'Autorità ha assunto l'iniziativa di inviare alle principali associazioni di categoria operanti nel settore industriale e commerciale una richiesta di informazioni sia per comprendere la portata nazionale del fenomeno in questione sia per conoscere eventuali iniziative e misure già adottate per consentire la prosecuzione dei trasferimenti di dati nel rispetto del quadro normativo esistente (art. 44 del Codice) (cfr. par. 22.3).

18 Il registro dei trattamenti

18.1. *La notificazione*

La notificazione è una dichiarazione con la quale un titolare (sia soggetto pubblico che privato) rende nota l'effettuazione di un determinato trattamento di dati personali (specificando una serie di informazioni obbligatorie) affinché, attraverso l'inserimento nel registro dei trattamenti, tali informazioni vengano rese pubbliche. Essa è validamente effettuata solo se è trasmessa per via telematica utilizzando il modello predisposto in ottemperanza alle istruzioni pubblicate sul sito, anche per quanto riguarda le modalità di sottoscrizione con firma digitale e di conferma del ricevimento della notificazione.

Le notificazioni sono inserite in un registro pubblico liberamente e gratuitamente consultabile *online* tramite il sito dell'Autorità, da cui chiunque può acquisire notizie e utilizzarle per le finalità di applicazione della disciplina in materia di protezione dei dati personali (ad es., per esercitare il diritto di accesso ai dati o gli altri diritti riconosciuti dal Codice). La notificazione del trattamento deve essere presentata al Garante prima dell'inizio del trattamento, una sola volta, indipendentemente dal numero delle operazioni e della durata del trattamento da effettuare e può anche riguardare uno o più trattamenti con finalità correlate. Una nuova notificazione è richiesta solo prima che cessi definitivamente l'attività di trattamento oppure quando si renda necessario modificare alcuno degli elementi in essa contenuti. I titolari hanno l'onere di mantenere aggiornato il registro comunicando le eventuali variazioni (quali, il cambio di sede o la denominazione della società) o la cessazione del trattamento (ad es., in occasione della cessazione dell'impresa). Nel caso in cui una pluralità di soggetti autonomi esercitano congiuntamente un potere decisionale sulle finalità e sulle modalità di un trattamento di dati personali in modo tale che si realizzi una vera e propria "contitolarità", ciascuno di essi è tenuto ad effettuare un'autonoma notificazione, nella quale indicherà anche tutti gli altri contitolari.

Le norme del Codice da tenere in considerazione quando si deve valutare la necessità di procedere a questo adempimento sono: l'art. 37 (Notificazione del trattamento) e l'art. 38 (Modalità di notificazione), per la parte sostanziale, l'art. 163 (Omessa o incompleta notificazione) e l'art. 168 (Falsità nelle dichiarazioni e notificazioni al Garante), per la parte sanzionatoria.

Occorre inoltre tenere presente che i provvedimenti di esonero dall'obbligo di notificazione o di chiarimento adottati dal Garante sono pubblicati, insieme alle istruzioni, nella sezione del sito www.garanteprivacy.it denominata "Notificazione e Registro dei trattamenti", raggiungibile dalla *home page* cliccando il *link* "servizi *online*".

18.2. *L'evoluzione della notificazione nel 2015*

Il Garante fornisce quotidianamente supporto a tutti i soggetti che notificano i trattamenti sul registro per agevolare la corretta conclusione delle procedure e chiarire eventuali dubbi sui tratramenti che necessitano di essere notificati. Al fine di ottimizzare il riscontro alle numerose richieste di chiarimenti che quotidianamente

pervengono al Garante tramite telefono o posta eletttronica, in merito alle necessità e modalità di notificazione, nonché allo scopo di agevolare il corretto e tempestivo adempimento di tale obbligo da parte dei titolari del trattamento, nel corso dell'anno è stato predisposto un documento esplicativo riportante le risposte alle domande più frequenti (cd. FAQ) finalizzato ad agevolare l'interfaccia verso l'utenza su aspetti, sia di natura tecnica che di merito, legati alla procedura di notificazione. Ad esempio, si consideri che nell'anno 2015 sono pervenute circa 1.200 richieste di chiarimento telefoniche e circa 600 tramite posta elettronica. La definitiva pubblicazione delle FAQ, oltre a fornire un servizio più celere agli utenti, consentirà, la liberazione di risorse interne da destinare ad attività più specifiche, quali, ad esempio, quelle relative ai controlli.

Nel 2015 è proseguita l'attività di controllo, sia nei confronti dei titolari iscritti nel Registro sia nei confronti di quelli che effettuano trattamenti oggetto di notificazione ma che non risultano presenti nel Registro; tale attività è stata effettuata anche mediante ispezioni *in loco*, nell'ambito della programmazione ispettiva di cui si è dato conto al par. 21.1. In particolare, dai controlli effettuati nel corso dell'anno sono emersi 44 casi di omessa o incompleta notificazione del trattamento e sono state contestate le relative violazioni ai titolari del trattamento. La maggior parte delle violazioni è stata riscontrata con riferimento al trattamento di dati che indicano la posizione geografica di persone od oggetti mediante una rete di comunicazione elettronica (art. 37, comma 1, lett. *a*) del Codice), principalmente nell'ambito del rapporto di lavoro dipendente, nel corso di un ciclo di ispezioni condotto nei confronti di alcune società di trasporti sul territorio nazionale. In rali circostanze, sono state contestate 15 violazioni per omessa notificazione ed effettuate 5 denunce in relazione alle violazioni penali riscontrate in merito agli obblighi previsti dallo Statuto dei lavoratori.

Di pari rilievo sono state le violazioni riscontrate con riferimento al trattamento di dati idonei a rivelare lo stato di salute e la vita sessuale, trattati a fini di procreazione assistita, nonché quello relativo alla prestazione di servizi sanitari per via telematica (art. 37, comma 1, lett. *b*) del Codice). Relativamente a tali trattamenti, infatti, l'Ufficio ha condotto un ciclo di ispezioni nei confronti di alcuni laboratori di analisi, dalle cui risultanze sono emerse, in particolare, 8 violazioni per l'omessa notificazione di tali trattamenti ed ulteriori 12 violazioni connesse all'incompleta norificazione; l'Ufficio ha quindi adottato i relativi atti di contestazione nei confronti dei titolari del trattamento coinvolti.

L'Ufficio ha inoltre provveduto, in ragione della numerosità delle violazioni riscontrate, ad inoltrare alle principali associazioni di categoria di rale settore, una nota volta a richiedere l'intervento delle stesse per stimolare presso i propri iscritti una verifica del corretto adempimento degli obblighi in materia di prorezione dei dati personali. In tale contesto è stato anche richiamato, quanto disposto dal Garante con il provvedimento 19 novembre 2009, recante "Linee guida in tema di referti *online*" (doc. web n. 1679033), evidenziando la necessità dell'adozione di specifiche misure di sicurezza per l'effettuazione di rale tipologia di trattamenti di dari personali. Le misure di sicurezza segnalate, difatti, appaiono necessarie al fine di prevenire possibili pregiudizi ai diritti degli assistiti, con riferimento ai trattamenti dei loro dati personali sensibili e genetici, in relazione alla fornitura di servizi di consultazione *online* dei referti o di trasmissione degli stessi per posta elerronica.

In tutti i casi sopra indicati, quindi, sono stati avviati i procedimenti per l'applicazione della sanzione prevista dall'art. 163 del Codice che prevede una pena pecuniaria da 20.000 a 120.000 euro.

Anche in ragione delle sopra esposte attività ispettive, delle numerose violazioni

contestate ai titolari e del conseguente adempimento da parte degli stessi e degli altri operatori del settore, si evidenzia che nell'anno 2015 il Registro dei trattamenti ha conseguito un picco nel numero di notificazioni pervenute. Infatti le stesse sono risultate pari a 2.622 nell'anno 2015, a fronte di una media pari a circa 1.300 notificazioni annue nell'ultimo quinquennio. Inoltre è possibile osservare come il dato relativo al 2015 sia il più elevato dell'intera serie storica delle notificazioni, fatta eccezione per l'anno 2004, anno di costituzione del Registro dei trattamenti (in cui furono effettuate più di 10.000 notificazioni) (cfr. sez. IV, tab. 12 e 14).

A tale risultato ha contribuito anche l'adozione del provvedimento generale relativo ai *cookie* (provv. 8 maggio 2014, n. 229, doc. web n. 3118884), che ha reso più evidenti ad una vasta platea di titolari gli obblighi connessi ad alcuni tipi di trattamento, come ad esempio quello relativo alla cd. profilazione degli interessati (art. 37, comma 1, lett. *d*) del Codice).

Tuttavia, anche a fronte della maggiore attenzione riscontrata rispetto a tale obbligo, occorre osservare che nella società odierna, in cui la dinamicità del trattamento dei dati passa attraverso semplici interazioni degli utenti con *app* e dispositivi interconnessi (*Internet of Things*), la staticità della notificazione appare sempre più inadeguata a garantire efficacemente i diritti degli interessati.

In questo senso quindi, nel nuovo regolamento europeo, la cui pubblicazione è prevista sulla GUUE del 4 maggio 2016, si supererà la logica della notificazione a vantaggio di nuovi strumenti più effettivi quali ad esempio l'introduzione di una nuova figura, il cd. *data protection officer* (definito nella traduzione italiana in maniera un po' infelice, Responsabile della protezione dei dati) al quale saranno affidati compiti sostanziali, per assicurare il rispetto della normativa in materia di *privacy* da parte della società o ente nell'ambito del quale viene designato. Sarà affidato a questo nuovo soggetto, dorato di una specifica professionalità nel settore della protezione dei dati personali, il ruolo di "presidio avanzato" del rispetto dei principi e degli adempimenti in materia nonché di interlocutore ed elemento di connessione tra il titolare del trattamento e l'Autorità.

19 La trattazione dei ricorsi

19.1. *I profili generali*

Il numero delle decisioni adottate nel 2015 (307) è stato pressoché uguale all'anno precedente (306) e le aree tematiche oggetto di trattazione corrispondono grosso modo a quelle sulle quali da diversi anni si concentrano la maggior parte delle questioni sottoposte al Garante in sede di ricorso.

Uno sguardo più approfondito, che tenga conto non solo del contenuto delle richieste formulate, ma anche delle ragioni sostanziali alla base dei singoli procedimenti, permette di cogliere la frequente connessione delle vicende esaminate alle varie sfaccettature della crisi economica e sociale tutt'ora in atto. Ne sono testimonianza i numerosi ricorsi nei confronti di istituti di credito e società finanziarie spesso volti ad assicurare in tempi rapidi la possibilità di ricostruire il quadro completo dei rapporti bancari riconducibili ad una persona, ad una società, o ad un defunto (art. 9, comma 3, del Codice). L'art. 7 del Codice è utilizzato come strumento per ricostruire l'assetto e l'evoluzione dei patrimoni e dei rapporti bancari personali, familiari, imprenditoriali, nonché il punto di pattenza per contestare le condizioni conrrattuali con il sistema creditizio o, più in dertaglio, per verificare la congruità dei tassi d'interesse praticati. Più spesso il diritto di accesso riconosciuto dal menzionato art. 7 costituisce lo strumento indispensabile per verificare la liceità del trattamento nell'ampio settore della centralizzazione dei rischi di credito e in quello, ancora più esteso, delle banche dati che forniscono informazioni commerciali sulle persone ovvero sulla correttezza e tempestività nell'onorare le scadenze dei pagamenti e, più in generale, sulla loro affidabilità economica. Al riguardo è importante sottolineare l'adozione da parte del Garante del codice di deontologia e buona condotta per il trattamento dei dati personali effettuato a fini di informazione commerciale (provv. 17 settembre 2015, n. 479, doc. web n. 4298343), promosso dall'Autorità e redarto unitamente a vatie associazioni di categoria imprenditoriali e di consumatori e volto a regolare un settore particolarmente importante per il corretto funzionamento del mercato (cfr. par. 13.4).

Le valutazioni economiche, finanziarie e patrimoniali effettuate dalle società specializzate in questo settore infatti sono in grado di segnalare prevenrivamente eventuali rischi relativi a soggetti in affari.

Il Garante, inrervenendo nel corso degli anni, a seguito di numerosi ricorsi, aveva infatti più volte sottolineato che il non corretto utilizzo di banche dati e strumenti di analisi così invasivi può arrecare seri danni alla dignità e tiservatezza delle persone coinvolte, pertanto nel "nuovo codice" si è cercato di coniugare esigenze di semplificazione degli adempimenti cui sono tenute le società di informazioni commerciali con il diritto alla ptotezione dei dati personali dei soggetti coinvolti, e quindi di declinare al meglio quel bilanciamento fra la libertà di iniziativa economica privata e sicurezza, dignità e libertà individuale. Non è un caso, quindi, che ormai da anni il Garante sia diventato un punto di riferimento in questa matetia grazie anche agli orientamenti espressi in relazione, in particolare, all'amplissimo settore dei trattamenti svolti presso i sistemi di informazioni creditizie, la Centrale dei rischi della Banca d'Italia, la Centtale d'allarme interbancaria.

19

19.2. *I dati statistici*

Per ciò che concerne la tipologia delle decisioni, si conferma nel periodo di riferimento l'alta percentuale di decisioni di non luogo a provvedere (60%), cioè di procedimenti conclusisi con il soddisfacimento, nel corso dell'istruttoria, delle richieste degli interessati/ricorrenti. Tale dato testimonia l'utilità e l'efficacia di questa specifica forma di tutela, la cui funzione principale è quella di favorire la composizione delle controversie direttamente tra l'interessato e il titolare del trattamento. Tale obiettivo viene perseguito assicurando, da un lato, che i diritti tutelati dall'art. 7 del Codice siano esercitati con richieste mirate e chiare e dall'altro che il riscontro del titolare sia tempestivo e pertinente.

Posto che l'attivazione del ricorso dinanzi all'Autorità è passaggio necessariamente successivo rispetto alla proposizione di un apposito interpello rivolto previamente al soggetto detentore dei dati, unica eccezione, i cui limiti sono stati ben delineati dalla giurisprudenza del Garante, è costituita dal comma 1, art. 146 del Codice, vale a dire quando attendere i tempi previsti dall'interpello preventivo potrebbe provocare un pregiudizio imminente ed irreparabile.

Sul piano della tipologia delle decisioni va comunque sottolineato un incremento dei casi di accoglimento (totale o parziale) delle richieste dei ricorrenti (15%). In aumento è anche la percentuale delle decisioni dichiarate inammissibili – ivi comprese quelle per mancata regolarizzazione ai sensi dell'art. 148, comma 2, del Codice - (11%), mentre rimane invariata la percentuale delle decisioni dichiarate infondate (14%) (cfr. sez. IV, tab. 4).

Non meno significativo è il dato relativo alle principali caregorie di titolari del trattamento, sia pubblici che privati: in primo luogo gli editori (anche televisivi), le banche e società finanziarie, le società di informazioni commerciali, le Amministrazioni pubbliche e concessionari di servizi pubblici, i fornitori telefonici e telematici, le compagnie di assicurazione, le strutture sanitarie pubbliche e private, gli amministratori condominiali, i liberi professionisti, i datori di lavoro pubblici e privati (cfr. sez. IV, tab. 5).

Tale casistica riflette le difficoltà occupazionali e i profili di criticità del settore lavoristico ed evidenzia la configurazione di un "nuovo" contenzioso (messo in risalto anche nella precedente Relazione) rispetto all'utilizzo delle moderne tecnologie e la ricerca del delicato equilibrio fra tutela della riservatezza dei singoli e le esigenze organizzative del datore di lavoro.

19.3. *La casistica più significativa*

Nel 2015, risulta consolidata la tendenza, già rilevata come tale negli anni precedenti, di un aumento dei ricorsi in materia di lavoro, legati in particolar modo alla fase patologica ovvero alla cessazione del rapporto. Tali fattispecie si sono per lo più contraddistinte per l'utilizzo, da parte del datore di lavoro, di dati personali del dipendente connessi allo svolgimento dell'attività lavorativa, con particolare riguardo a quelli relativi alle comunicazioni avvenute tramite *account* di posta elettronica aziendale contenente il nome e cognome del dipendente stesso.

In tale ambito meritano una particolare attenzione, tra gli altri, alcuni casi che, pur avendo come base comune l'affermato indebito utilizzo, per finalità di controllo, da parte del datore di lavoro dei dispositivi assegnati al dipendente per lo svolgimento della propria attività lavorativa, presentavano elementi specifici ed ulteriori.

Tra questi il ricorso proposto da un avvocato legato da un rapporto di collaborazione ad uno studio legale associato rispetto al quale, pur potendosi ravvisare alcuni

19

tratti tipici del rapporto di lavoro dipendente (quali la suddivisione interna del lavoro per aree di competenza, la gestione centralizzara delle incombenze amministrative, l'utilizzo di strumenti lavorativi dello studio con assegnazione di *account* di posta elettronica facenti capo allo studio stesso, seppur individualizzati mediante l'utilizzo del nome e cognome dell'utente), vi erano comunque elementi di divetsità dati dal fatto che ciascun collaboratore godeva anche di un margine di autonomia nella gestione della propria attività. Il ricorrente ha, in particolare, lamentato l'illegittimo perdurante utilizzo da parte dello studio resisrente, per il tempo successivo al venir meno del rapporto di collaborazione tra le parti, dell'*account* di posta elettronica al medesimo assegnato e contenente i suoi dati identificativi, eccependo peraltro che gli sarebbe stato altresì impedito di accedere ai dati contenuti nel predetto *account*. Lo studio resistente ha precisato che nel proprio disciplinare interno, facente parte del complessivo assetto contrattuale tra quest'ultimo e i propri collaboratori, qualsiasi indirizzo di posta elettronica deve risultare composto dal nome e cognome dell'assegnatario seguito dall'indicazione dello studio e qualificabile come strumento di lavoro di proprietà del datore del lavoro. L'Autorità, facendo applicazione dei princìpi generali contenuti nel provvedimento 1° marzo 2007, Linee guida del Garante per posta elettronica e internet (n. 13, doc. web n. 1387522), ha accolto il ricorso (provv. 5 marzo 2015, n. 136, doc. web n. 3985524) ordinando allo studio legale resistente la disattivazione dell'*account* di posta elettronica contenente i dati identificativi del ricorrente con contestuale utilizzo di un risponditore automatico volto ad avvisare gli utenti dell'avvenuta disattivazione, indicando altresì un indirizzo di posta elettronica aziendale alternativo cui inviare i messaggi attinenti l'attività svolta dallo studio. L'Autorità ha altresì disposto la sospensione immediata di qualunque procedura atta a consentire, in assenza dell'interessato, la consultazione del contenuto dei messaggi, già pervenuti o che sarebbero potuti pervenire sino all'attuazione del provvedimento. Al ricorrente è stato inoltre garantito l'accesso al contenuto dei predetti messaggi al fine di individuare quelli aventi carattere privato o che, pur collegati alla sfera professionale, fossero relativi a rapporti che, in base all'accordo raggiunto tra le parti al termine della collaborazione, continuassero ad essere curati dal medesimo e di poter così verificare l'avvenuta successiva cancellazione dei predetti messaggi da parte del titolare del trattamento.

Altro caso singolare, sempre in ambito lavoristico, è stato quello di una dipendente, licenziata per affermata condotta infedele la quale ha lamentato l'illecita acquisizione da parte del datore di lavoro delle conversazioni avvenute con alcuni clienti e/o fornitori dell'azienda presso cui era impiegata mediante l'utilizzo di Skype, in parte avvenute al di fuori del luogo di lavoro e alla base del predetto licenziamento. Il datore di lavoro, per sua stessa ammissione, aveva provveduto ad installare sul computer assegnato alla dipendente un *software* in grado di visualizzare sia le conversazioni effettuate dalla ricorrente dalla propria postazione, sia quelle avvenute successivamente all'uscita dall'azienda da un computer collocato presso la propria abitazione. Tale condotta è stata riconosciuta dall'Autorità in contrasto con i princìpi posti dalle citate Linee guida del 1° marzo 2007, con le disposizioni più generalmente poste dall'ordinamento a tutela della segretezza delle comunicazioni (v. art. 15 Cost. e artt. 616 ss. c.p.), nonché con la stessa *policy* aziendale adottata a riguardo dal titolare del trattamento e specificamente approvata negli stessi termini dalla competente Direzione territoriale del lavoro. Il ricorso è stato pertanto accolto (provv. 4 giugno 2015, n. 345, doc. web n. 4211000), disponendo per il datore di lavoro il divieto di trattare ulteriormente i dati illecitamente acquisiti, prevedendone la sola conservazione ai fini dell'eventuale acquisizione da parte dell'autorità giudiziaria. Occorre infatti tener presente che il contenuto delle comunicazioni di tipo

elettronico e/o telematico sono assistite da garanzie di segretezza, tutelate anche a livello costituzionale, dirette a consentire, anche in ambito lavorativo, l'esplicazione della persona umana e dunque ad impedire, in attuazione dei princìpi di necessità, correttezza, pertinenza e non eccedenza, un'interferenza ingiustificata sui diritti e sulle libertà fondamentali di lavoratori, come pure di soggetti esterni che ricevono o inviano comunicazioni elettroniche di natura personale. Ciò vale, a maggior ragione, con riferimento a conversazioni che avvengano al di fuori del contesto lavorativo, come verificatosi nel caso di specie.

Da ultimo si riporta il caso significativo di un addetto alla biglietteria presso una compagnia di navigazione, il cui datore di lavoro avrebbe utilizzato i dati registrati dalle telecamere di sorveglianza nell'ambito del procedimento disciplinare e del successivo licenziamento per giusta causa. Il ricorrente ha chiesto il blocco e la cancellazione dei dati per essere stati illecitamente acquisiti, utilizzati e comunque conservati per un periodo superiore a quello consentito dalla legge. Nel corso del procedimento la società resistente ha precisato che l'installazione delle telecamere a circuito chiuso presso le biglietterie è volta ad elevare lo *standard* di sicurezza nelle biglietterie, potenzialmente esposte a rischi connessi alla costante detenzione di denaro contante, nonché ad assicurare agli addetti la possibilità di riscontri oggettivi rispetto a reclami della clientela. Inoltre, la compagnia ha ammesso di aver conservato le immagini registrate per un periodo di novanta giorni, e quindi per un periodo superiore al termine di conservazione previsto dal provvedimento del Garante in materia di videosorveglianza dell'8 aprile 2010 (doc. web n. 1712680), senza aver previamente ottenuto un provvedimento, in sede di verifica preliminare ai sensi dell'art. 17 del Codice, di autorizzazione alla conservazione delle immagini per un tempo più lungo di quello consentito dalla legge. L'Autorità ha pertanto accolto il ricorso disponendo, quale misura a tutela dei diritti dell'interessato, il divieto per la società resistente di trattare ulteriormente i dati personali del ricorrente, salva la loro conservazione per esclusiva finalità di tutela dei diritti in sede giudiziaria.

Anche nel 2015 numerosi sono stati i ricorsi (50) riguardanti richieste di deindicizzazione dal motore di ricerca Google di notizie riportanti dati non più di interesse pubblico. Com'è noto con la sentenza CGUE (C-131/12, 13 maggio 2013) la Corte ha riconosciuto la società statunitense titolare del trattamento dei dati personali che appaiono nell'elenco dei risultati del suo motore di ricerca, riconoscendo il diritto all'interessato di rivolgersi al gestore del motore di ricerca al fine di ottenere la deindicizzazione dei risultati ottenuti. Di fronte al diniego di Google gli utenti italiani possono rivolgersi in appello al Garante o all'autorità giudiziaria.

Una opportunità, quella del ricorso al Garante, sfruttata finora da un esiguo numero di persone di fronte alle migliaia di istanze rigettate dalla società di Mountain View. In circa un terzo dei casi definiti, il Garante ha accolto le richieste degli interessati ordinando a Google la rimozione dei *link* a pagine presenti sul web che riportavano dati personali ritenuti non più di interesse pubblico, informazioni spesso eccedenti, riferite anche a persone estranee alla vicenda giudiziaria narrata, o lesive della sfera privata. In tutti gli altri casi, invece, l'Autorità ha respinto le richieste ritenendo che la posizione di Google fosse corretta, risultando prevalente l'interesse pubblico ad accedere alle informazioni tramite motori di ricerca. Si trattava, infatti, in prevalenza, di vicende processuali di sicuro interesse pubblico, anche a livello locale, spesso recenti o per le quali non erano ancora stati esperiti tutti i gradi di giudizio. I dati personali riportati, tra l'altro, risultavano trattati nel rispetto del principio di essenzialità dell'informazione.

20 Il contenzioso giurisdizionale

20.1. *Considerazioni generali*

Come riferito in precedenti Relazioni, il d.lgs. n. 150/2011 con l'art. 34 ha abrogato l'art. 152 del Codice – con l'eccezione del comma 1 – dettando all'art. 10 nuove regole procedurali concernenti le controversie in materia di applicazione delle disposizioni del Codice. In particolare, l'art. 34 ha abrogato il comma 7 dell'art. 152, che prevedeva esplicitamente l'obbligo della notifica al Garante dei ricorsi proposti direttamente davanti all'autorità giudiziaria, non coinvolgenti le pronunce dell'Autorità.

Tale abrogazione continua a far sentire i suoi effetti negativi sul numero delle notifiche relative a tale tipologia di giudizi, che in alcuni casi l'autorità giudiziaria ha continuato a ritenere necessarie: a fronte dei 32 ricorsi notificati nel 2013 e dei 31 nel 2014, nel 2015 sono stati notificati, e da questa trattati, 19 ricorsi.

Attesa l'accertata validità di tale strumento a disposizione degli interessati, volto alla tutela giurisdizionale del diritto alla protezione dei dati personali in alternativa al ricorso presentato in sede amministrativa al Garante, assume sempre maggiore rilevanza l'obbligo – purtroppo non sempre puntualmente adempiuto per le cancellerie di trasmettere al Garante copia dei provvedimenti emessi dall'autorità giudiziaria in relazione a quanto previsto dal Codice o in materia di criminalità informatica (art. 154, comma 6).

Tale obbligo, unitamente alle notifiche dei ricorsi proposti direttamente davanti al giudice che l'autorità giudiziaria riterrà di effettuare, potrà consentire all'Autorità di continuare ad avere conoscenza dell'evoluzione della giurisprudenza in materia di protezione dei dati personali e di segnalare al Parlamento e al Governo degli interventi normativi necessari per la tutela dei diritti degli interessati (come previsto dall'art. 154, comma 1, lett. *f*), del Codice).

20.2. *I profili procedurali*

In tema di giurisdizione, il Tribunale di Bologna, pronunciandosi su una questione relativa al contributo spese per l'esercizio dei diritti previsti dall'art. 7 del Codice di cui nel seguito si dà conto più in dettaglio – ha ribadito che gli artt. 151 e 152 del Codice non lasciano margini a dubbi circa la volontà del legislatore di attribuire l'intera materia alla cognizione dell'A.G.O. senza eccezioni di sorta (26 gennaio 2015, n. 2841).

Vi è stata, inoltre, una pronuncia del Tribunale di Tivoli che si è dichiarato incompetente in favore del Tribunale di Milano, per il trattamento effettuato da una testata giornalistica ivi avente sede, ai sensi dell'art. 10, comma 2, d.lgs. n. 150/2001 come richiamato dall'art. 152 e ss. del Codice, che prevede la competenza esclusiva del tribunale del luogo in cui ha residenza il titolare del trattamento dei dati (13 marzo 2015, n. 620).

In altro caso la Corte di Cassazione ha annullato una sentenza di primo grado del Tribunale di Latina riguardante l'impugnazione di un'ordinanza ingiunzione