interessati sui diversi aspetti connessi alla protezione dei dati personali, ivi compresi quelli relativi alla sicurezza nonché sui presupposti di legittimità dei trattamenti dei dati biometrici. Si è così stabilito che, con particolare riguardo ai casi di:

- autenticazione informatica, le caratteristiche biometriche dell'impronta digitale o dell'emissione vocale di una persona possono essere utilizzate come credenziali di autenticazione per l'accesso a banche dati e sistemi informatici. Tale trattamento può essere effettuato anche senza il consenso dell'utente;
- controllo di accesso fisico ad aree "sensibili" e utilizzo di apparati e macchinari pericolosi, le caratteristiche dell'impronta digitale o della topografia della mano potranno essere trattate per consentire l'accesso ad aree e locali ritenuti "sensibili" oppure per consentire l'utilizzo di apparati e macchinari pericolosi ai soli soggetti qualificati. Tale trattamento può essere realizzato anche senza il consenso dell'utente;
- sottoscrizione di documenti informatici, l'analisi dei dati biometrici associati all'apposizione a mano libera di una firma autografa potrà essere utilizzata per la firma elettronica avanzata. Questa modalità è però consentita solo con il consenso degli interessati, consenso non necessario invece in ambito pubblico, se devono essere perseguite specifiche finalità istituzionali. Dovranno comunque essere resi disponibili sistemi alternativi (cartacei o digitali) di sottoscrizione, che non comportino l'utilizzo di dati biometrici;
- utilizzo per scopi cd. facilitativi, l'impronta digitale e la topografia della mano potranno essere utilizzate anche per consentire l'accesso fisico di utenti ad aree fisiche in ambito pubblico (es. biblioteche) o privato (es. aree aeroportuali riservate). Anche in questo caso l'utilizzo è consentito solo con il consenso degli interessati. Dovranno comunque essere previste modalità alternative per l'erogazione del servizio per chi rifiuta di far utilizzare i propri dati biometrici.

Ogni sistema di rilevazione dovrà essere configurato in modo tale da raccogliere un numero limitato di informazioni (principio di minimizzazione) e previa adozione delle numerose misure di sicurezza individuate dal Garante (ad es., quella che obbliga a cifrare il riferimento biometrico con tecniche crittografiche, con una lunghezza delle chiavi adeguata alla dimensione e al ciclo di vita dei dati). Anche al fine di prevenire eventuali furti di identità biometrica, tutte le violazioni dei dati o gli incidenti informatici (*data breach*) che possano avere un impatto significativo sui sistemi biometrici o sui dati personali custoditi, dovranno essere comunicati da chi detiene i dati al Garante entro 24 ore dalla scoperta, così da consentire di adottare opportuni interventi a tutela delle persone interessate. A tal fine è stato predisposto un modulo che consente di semplificare il predetto adempimento. Sono esclusi dalle modalità semplificate individuate nel provvedimento del Garante i trattamenti che prevedono la realizzazione di archivi biometrici centralizzati, per i quali continuerà ad essere obbligatorio richiedere una verifica preliminare. Rimane in vigore anche l'obbligo di notificazione al Garante per i trattamenti non esplicitamente esclusi dal provvedimento, come quelli effettuati da esercenti le professioni sanitarie e da avvocati.

# 16 Il trattamento dei dati nel condominio

A seguito dell'entrata in vigore, nel giugno del 2013, della legge 11 dicembre 2012, n. 220, recante modifiche alla disciplina del condominio negli edifici, cittadini e associazioni di categoria hanno sottoposto all'Autorità diversi quesiti circa l'esatta interpretazione di alcune delle nuove norme ivi contenute; ciò con particolare riferimento alle disposizioni di cui agli artt. 1129, comma 7, c.c. in ordine alla previsione di un conto corrente intestato al condominio e all'art. 1130, comma 1, punto 6, c.c. relativo all'obbligo di tenuta da parte dell'amministratore del cd. registro di anagrafe condominiale.

Al riguardo, il Garante ha chiarito che il condomino non è tenuto a fornire alcuna prova documentale delle informazioni rese all'amministratore per la costituzione del predetto registro di anagrafe condominiale; su altro fronte, può invece chiedere all'amministratore copia integrale, senza oscuramenti, degli atti e dei documenti bancari relativi al conto corrente intestato al condominio.

In ordine al primo aspetto, l'Autorità ha ribadito che l'amministratore può trattare solo informazioni pertinenti e non eccedenti rispetto alle finalità da perseguire. Al fine di adempiere correttamente al nuovo obbligo sancito dalla riforma, l'amministratore può, quindi, legittimamente acquisire le informazioni che consentono di identificare e contattare i singoli partecipanti al condominio – siano essi proprietari, usufruttuari, conduttori o comodatari delle unità immobiliari – richiedendo, come stabilito dalla norma, le cd. generalità, comprensive del codice fiscale, della residenza o del domicilio. Può chiedere, inoltre, le informazioni volte ad individuare catastalmente le singole unità immobiliari (cd. estremi di identificazione catastale), ossia: la sezione urbana, il foglio, la particella, il subalterno e il comune. Per quanto concerne poi le informazioni relative alle condizioni di sicurezza, con l'entrata in vigore del cd. decreto destinazione Italia (d.l. 23 dicembre 2013, n. 145), i condòmini non dovranno più fornire alcuna informazione sulla propria unità immobiliare, perché i dati da raccogliere riguardano ora solo le parti comuni dell'edificio.

A riprova della veridicità delle informazioni rese, il condomino non è però tenuto, perché risulterebbe eccedente, ad allegare alcuna eventuale ulteriore documentazione (ad es., l'atto di compravendita in cui sono riportati i dati).

Con riferimento alla novità introdotta dal legislatore nell'art. 1130 c.c., l'Autorità ha evidenziato (nota 31 marzo 2014) che, a seguito della riforma, deve essere aperto e utilizzato dall'amministratore un conto condominiale, al quale ciascun condomino, seppur per il tramite dello stesso amministratore, può accedere. In particolare, il Garante ha chiarito che nonostante il conto sia intestato alla compagine condominiale nella sua complessità, i singoli condòmini sono titolari di una posizione giuridica che consente loro di verificare la destinazione dei propri esborsi e l'operato dell'amministratore mediante l'accesso in forma integrale ai relativi estratti conto bancari o postali. Tale principio, già sancito in linea generale dal Garante nelle Linee guida in ambito bancario (provv. 25 ottobre 2007, doc. web n. 1457247), comporta infatti il diritto di ottenere "copia di atti o documenti bancari" senza alcuna limitazione, neanche nelle forme di un parziale oscuramento, anche se contengono dati personali di terzi. Nel confermare l'attualità dei principi già stabiliti da questa Autorità in passato in materia di trattamento di dati personali e di amministrazione

di condomini con il provvedimento generale del 18 maggio 2006 (doc. web n. 1297626), si è colta l'occasione anche per ribadire che resta fermo in capo alla stessa compagine condominiale (nella qualità di titolare del trattamento) – di regola per il tramite dell'amministratore (nell'eventuale veste di responsabile del trattamento) –, l'obbligo di adottare le idonee misure di sicurezza atte a prevenire illecite comunicazioni e diffusioni di dati personali raccolti anche ai fini della tenuta del predetto registro, tutto ciò ai sensi e per gli effetti degli artt. 31 e ss. del Codice (cfr. provv. 18 maggio 2006, punto 3.3).

Nell'ambito delle istruttorie aperte dall'Autorità, il Garante è stato inoltre chiamato (provv. 19 giugno 2014, n. 314, doc. web n. 3275910 e provv. 30 ottobre 2014, n. 482, doc. web n. 3658161) a definire alcune controversie inerenti il tema della divulgazione dei dati personali nell'ambito delle attività connesse all'amministrazione dei condomìni. Ciò con specifico riferimento al trattamento di dati personali effettuato da amministratori che hanno inviato solleciti di pagamento o comunque attestazioni di uno stato di morosità dell'inquilino a terzi (in un caso al datore di lavoro mediante l'invio ad un indirizzo *e-mail* accessibile da chiunque sul posto di lavoro, in un altro ad un'agenzia di intermediazione immobiliare coinvolta nella vendita di un immobile sito nel relativo condominio), anziché allo stesso inquilino personalmente. L'Autorità, in ambedue i casi, è intervenuta accertando l'avvenuto trattamento di dati in modo non conforme alla legge. Il Garante ha altresì prescritto agli amministratori coinvolti in dette vicende di adottare le misure necessarie in grado di assicurare effettivamente il rispetto delle regole poste dal Codice a tutela della comunicazione di dati personali a terzi e di impartire adeguate istruzioni in merito al personale in servizio presso gli studi ove gli stessi operano.

# 17 Le libere professioni

## 17.1. *L'attività forense e investigativa*

**Trattamento dei dati da parte di investigatori privati**

Nel valutare una segnalazione, l'Autorità ha chiarito gli ambiti di legittimità delle investigazioni private finalizzate ad acquisire elementi di prova nell'ambito delle controversie civili per quanto riguarda l'obbligo di fornire all'interessato l'informativa di cui all'art. 13 del Codice (nota 19 maggio 2014). Nella specie, l'attività investigativa era volta ad acquisire elementi relativi alla capacità economica dell'interessato, di professione medico, ed era stata commissionata dalla moglie in relazione ad una causa di separazione giudiziale. Un collaboratore dell'investigatore, per comprovare il maggior reddito dell'interessato rispetto alle risultanze della documentazione fiscale, si era recato in incognito – ossia, senza fornire alcuna informativa in merito all'attività investigativa in corso – presso lo studio del medico, con il pretesto di sottoporsi ad una visita clinica, a seguito della quale riportava l'informazione che il medico non aveva rilasciato la ricevuta fiscale; il collaboratore effettuava altresì, clandestinamente, riprese fotografiche del professionista al fine della sua sicura identificazione.

Il titolare dell'agenzia investigativa aveva giustificato la mancata informativa all'interessato invocando l'art. 13, comma 5, lett. *b*), del Codice, in quanto i dati del segnalante erano trattati esclusivamente per far valere o difendere un diritto in sede giudiziaria, per il periodo strettamente necessario a tal fine. L'Autorità, invece, ha ritenuto illegittimo il trattamento in argomento, in quanto l'esenzione dall'obbligo di fornire l'informativa, prevista dal citato art. 13, comma 5, del Codice, opera solo con riferimento "alla disposizione di cui al comma 4" del medesimo articolo, relativa al caso in cui "i dati personali non sono raccolti presso l'interessato", mentre nel caso in esame i dati erano stati acquisiti direttamente presso l'interessato. Del resto, l'autorizzazione n. 6/2013 relativa al trattamento dei dati sensibili da parte degli investigatori privati (doc. web n. 2819019) testualmente prescrive che "l'interessato o la persona presso la quale sono raccolti i dati deve essere informata ai sensi dell'art. 13 del Codice, ponendo in particolare evidenza l'identità e la qualità professionale dell'investigatore, nonché la natura facoltativa del conferimento dei dati. Nel caso in cui i dati siano raccolti presso terzi, è necessario informare l'interessato e acquisire il suo consenso scritto (art. 13, commi 1, 4 e 5 e art. 26, comma 4, del Codice), solo se i dati sono trattati per un periodo superiore a quello strettamente necessario per esercitare il diritto in sede giudiziaria o per svolgere le investigazioni difensive [...]. Tale orientamento, espresso già in passato (provv. 19 febbraio 2002, doc. web n. 1063652), è condiviso anche dalla giurisprudenza (Trib. Bergamo, 31 luglio 2002, n. 4436 e Cass., 15 luglio 2005, n. 15076).

**Uso del fax**

Con riferimento all'uso, da parte di un avvocato, del fax per l'invio – nel caso di specie ritenuto di per sé legittimo – ad una società di comunicazioni contenenti dati personali di un dipendente della medesima, l'Autorità ha ricordato (nota 22 settembre 2014) che l'utilizzo del fax per comunicazioni giudiziarie è ben noto al vigente codice di procedura civile. In particolare, il Giudice può autorizzare il difensore a provvedere alle notificazioni degli atti giudiziari attraverso mezzi particolari (art. 151 c.p.c.), tra i quali è compreso il fax (cfr. Cass., Sez. lav., 21 luglio

2008, n. 20078); inoltre, l'art. 250 c.p.c. (come modificato dall'art. 2, comma 3, d.l. 14 marzo 2005, n. 35, convertito con modificazioni dalla l. 14 maggio 2005, n. 80) stabilisce che l'intimazione a comparire ai testimoni ammessi dal giudice istruttore può essere effettuata dal difensore attraverso l'invio di copia dell'atto mediante lettera raccomandata con avviso di ricevimento, a mezzo di telefax, oppure di posta elettronica, nel rispetto della normativa, anche regolamentare, concernente la sottoscrizione, la trasmissione e la ricezione dei documenti informatici e teletrasmessi. Inoltre, nel caso in esame, il Giudice aveva formalmente autorizzato la parte a procedere alla comunicazione degli atti, anziché alla notificazione. Né è valso a rendere illegittimo l'uso del *fax* la circostanza che tale mezzo di comunicazione, ove usato per trasmettere documenti ad organizzazioni complesse come una società, può determinare l'apprensione dei dati ivi contenuti da parte di persone non abilitate ad accedervi. Infatti, proprio in considerazione della necessità di assicurare la tutela della riservatezza dei dati personali anche nell'ambito delle strutture complesse, il Codice prescrive al titolare del trattamento di designare per iscritto gli incaricati del trattamento, i quali – e solo essi – possono effettuare le operazioni di trattamento dei dati, sotto l'autorità del titolare (o del responsabile), attenendosi alle istruzioni prescritte (art. 30 del Codice). Inoltre, il titolare del trattamento è tenuto ad adottare tutte le misure di sicurezza necessarie ad assicurare il corretto trattamento dei dati personali (art. 33 del Codice). Pertanto, è obbligo della società adottare le misure organizzative che assicurino che la conoscenza dei dati personali sia possibile solo per coloro che sono incaricati del loro trattamento. Peraltro, ferma la legittimità dell'invio della comunicazione a mezzo fax, l'Autorità ha richiamato l'attenzione delle parti a considerare l'opportunità, nel caso di eventuali ulteriori comunicazioni di tale natura, di utilizzare canali di comunicazione (quale la corrispondenza in busta chiusa) che consentano una maggiore tutela della riservatezza dei soggetti i cui dati personali sono contenuti nella documentazione trasmessa, anche tenendo conto delle particolari cautele introdotte dal Codice in materia di notifica di atti giudiziari.

**Obbligo di informativa del cliente da parte dell'avvocato**

In ordine all'obbligo di informativa che l'avvocato deve rendere al proprio cliente ai sensi dell'art. 13 del Codice, è stato sottoposto al Garante un caso in cui il legale, antecedentemente al primo appuntamento presso il suo studio, aveva acconsentito a ricevere via *e-mail* documentazione contenente dati personali, anche giudiziari, da un potenziale cliente. A seguito del mancato conferimento dell'incarico al legale ed alla richiesta di questo del compenso professionale per l'attività svolta sulla documentazione inviata, l'interessato lamentava di non avere ricevuto dall'avvocato l'informativa relativa al trattamento dei suoi dati personali. L'Autorità ha ritenuto illegittimo il trattamento dei dati personali effettuato dal professionista, in quanto l'informativa di cui all'art. 13 del Codice deve essere fornita all'interessato prima del trattamento dei suoi dati. È pur vero che prima dell'incontro presso lo studio legale i contatti tra le parti erano avvenuti solo attraverso posta elettronica e che fu l'interessato a proporre all'avvocato la trasmissione dei documenti contenenti i suoi dati giudiziari affinché quest'ultimo potesse valutarli ed esprimere "un parere con cognizione di causa" nel successivo incontro. Tuttavia, l'avvocato consentì espressamente, tramite *e-mail* inviata all'interessato, a tale trasmissione ed a trattare successivamente i dati ivi contenuti senza fornire all'interessato l'informativa dovuta. Ove il professionista avesse voluto ispirare la sua condotta al rispetto della disciplina sulla tutela dei dati personali, avrebbe dovuto previamente fornire all'interessato l'informativa di cui all'art. 13 del Codice, ad esempio con la *e-mail* con la quale acconsentiva a ricevere dal segnalante i suoi dati personali (nota 16 aprile 2014).

**Registrazione video e telefonica da parte di un avvocato degli incontri avvenuti con la clientela**

Un avvocato ha posto un quesito sulla possibilità di effettuare riprese degli incontri avuti con i clienti e di registrare le conversazioni telefoniche con essi intercorse, adducendo esigenze di natura probatoria nell'ipotesi di contestazioni relative all'espletamento del mandato e, in generale, di sicurezza e tutela del patrimonio e dei professionisti operanti nello studio. L'Ufficio ha richiamato le disposizioni più rilevanti del contesto normativo disciplinante la fattispecie in esame, precisando che deve aversi riguardo, quale criterio fondamentale per considerare i singoli casi dubbi, al principio generale di proporzionalità nel trattamento di dati, nel senso di pertinenza e non eccedenza dei dati ai sensi dell'art. 11 del Codice. In proposito, si è rilevato che tale principio induce a dubitare che la astratta eventualità di situazioni pregiudizievoli, esemplificate in termini del tutto generali ovvero con mero riferimento a fatti di cronaca, possa di per sé dimostrare che nel singolo caso ricorrono circostanze che giustificano le modalità del trattamento oggetto del quesito (nota 19 settembre 2014).

**Altre segnalazioni**

Pervengono frequentemente segnalazioni che ritengono non conformi al Codice condotte tenute da avvocati nei confronti dei propri clienti. Tuttavia l'Autorità ha rilevato che molti dei comportamenti segnalati non attengono alla disciplina dei dati personali (come nel caso del mancato deposito da parte di un avvocato dell'atto di rinuncia all'incarico professionale nel fascicolo di ufficio relativo alla controversia, ai sensi dell'art. 85 c.p.c., o in quello della mancata restituzione della documentazione ricevuta dalla parte assistita per l'espletamento del mandato, che è regolata dall'art. 42 del Codice deontologico forense), sì che la valutazione di detti comportamenti non rientra tra i compiti istituzionali dell'Autorità (cfr. note 15 ottobre e 7 novembre 2014).

# 18 Il trasferimento dei dati all'estero

La materia dei trasferimenti transfrontalieri di dati personali è stata oggetto di costante attenzione da parte del Garante sia in occasione dell'attiva partecipazione dell'Autorità ai lavori del Gruppo Art. 29, sia con riferimento, a livello nazionale, alle numerose istanze volte al rilascio di autorizzazioni al trasferimento di dati verso Paesi terzi tramite le cd. *Binding corporate rules* (Bcr).

Anche nel corso dell'anno di riferimento è stato confermato il crescente interesse da parte del settore privato (in particolare, delle società di carattere multinazionale) all'utilizzo delle Bcr quale strumento per il trasferimento infragruppo di dati personali (per lo più di quelli relativi ai clienti, dipendenti e fornitori delle società facenti parte del gruppo richiedente) verso Paesi terzi. Il numero di richieste di autorizzazione giunte è stato elevato e il relativo *iter* si è concluso con l'approvazione di nove autorizzazioni rilasciate dal Garante al termine di complesse istruttorie, ove è stata verificata la conformità del testo delle Bcr, approvato al termine delle procedure europee di mutuo riconoscimento, con l'ordinamento italiano e con alcuni dei principali criteri stabiliti in materia dal Gruppo Art. 29 (cfr., fra gli altri, provv. 23 gennaio 2014, n. 27, doc. web n. 3058168; provv. 15 maggio 2014, n. 246, doc. web n. 3233476; provv. 26 giugno 2014, n. 325, doc. web n. 3320773; provv. 9 ottobre 2014, n. 449, doc. web n. 3635086). Ma il 2014 si è caratterizzato soprattutto per l'esame da parte dell'Autorità di alcune Bcr consistenti, a differenza dei casi affrontati negli anni precedenti (ove erano generalmente previste soluzioni contrattuali: cfr. Relazione 2013, p. 123), esclusivamente da dichiarazioni unilaterali sottoscritte dalle società capogruppo o, in taluni casi, in semplici regole di condotta (cd. *privacy policy*). Trattandosi di fattispecie che presentano profili di più incerta qualificazione nell'ordinamento giuridico nazionale, il Garante, al fine di rilasciare le relative autorizzazioni, ha ritenuto opportuno effettuare maggiori approfondimenti oltre a quelli di regola condotti nell'ambito delle precedenti istruttorie. A tal fine l'Autorità ha preso in considerazione e reputato rilevanti specifici aspetti volti ad accertare la cd. "vincolatività interna" (ossia la garanzia dell'effettivo rispetto delle Bcr da parte dei membri del gruppo e del personale dipendente: cfr. WP 74, par. 3.3.1) concernenti: l'impegno della capogruppo e delle altre società del gruppo ad osservare i principi contenuti nelle Bcr stesse (ivi comprese le clausole di responsabilità e del terzo beneficiario); l'avvenuta approvazione delle Bcr ad opera del consiglio di amministrazione della capogruppo, da cui discende l'obbligo di osservanza delle stesse da parte di tutte le società e del personale dipendente del gruppo; la sussistenza del potere della capogruppo, in virtù della propria posizione di controllo, di richiedere alle altre società l'attuazione delle Bcr; la previsione, in caso di mancata osservanza delle Bcr, di un sistema di sanzioni disciplinari nei confronti del personale dipendente; la realizzazione all'interno delle società di un programma di controllo volto ad assicurare il raggiungimento degli obiettivi aziendali tra cui il rispetto delle politiche in materia di protezione dei dati.

Una volta accertati tali aspetti in sede di istruttoria, l'attenzione è stata poi rivolta all'ulteriore profilo della cd. vincolatività esterna (ossia la garanzia per l'interessato di veder soddisfatti i diritti a lui riconosciuti all'interno delle Bcr: cfr. in merito WP 74, par. 3.3.2). Al riguardo, nei relativi provvedimenti di autorizzazione (provv. 4 dicem-

bre 2014, nn. 560 e 561, doc. web nn. 3668394 e 3668436) è stato evidenziato come l'art. 44, comma 1, lett. *a*), del Codice – a seguito della modifica apportata al testo, anche in ragione della presentazione al Parlamento e al Governo di una specifica segnalazione in materia (cfr. segnalazione 8 novembre 2007, doc. web n. 1467485) –, riconosce ora espressamente il potere del Garante di autorizzare un trasferimento di dati personali verso Paesi terzi anche nel caso in cui tale trasferimento sia posto in essere tramite regole di condotta esistenti nell'ambito di società appartenenti ad un medesimo gruppo, purché le stesse presentino adeguate garanzie per i diritti dell'interessato. È stato pertanto ritenuto che in virtù di tale previsione normativa, le predette regole di condotta possano costituire un fatto idoneo a produrre effetti giuridicamente vincolanti nell'ordinamento nazionale, ai sensi dell'art. 1173 c.c.

Alla luce di tali valutazioni, l'Autorità ha reso alle società istanti le relative autorizzazioni, ribadendo al contempo che l'interessato, in base al diritto nazionale applicabile, può, in ogni caso, far valere i propri diritti nel territorio dello Stato anche in ordine all'inosservanza delle garanzie contenute nelle Bcr (art. 44, comma 1, lett. *a*), del Codice) e che il Garante, in virtù dei poteri attribuitigli dal Codice, ai sensi degli artt. 154 e 157, può svolgere in qualsiasi momento i necessari controlli sulla liceità e correttezza del trasferimento dei dati e, comunque, su ogni operazione di trattamento ad essi inerente, nonché adottare, se necessario, i provvedimenti previsti dalla normativa nazionale applicabile.

# 19 Il registro dei trattamenti

## 19.1. *La notificazione*

La notificazione è una dichiarazione con la quale un titolare del trattamento (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).

È importante tenere sempre in considerazione che la notificazione del trattamento deve essere presentata al Garante prima dell'inizio del trattamento, una sola volta, indipendentemente dal numero delle operazioni e dalla 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.

Sui titolari che hanno notificato un trattamento incombe l'onere di mantenere aggiornato il registro comunicando le eventuali variazioni (ad es. 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 gli altri contitolari.

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

Occorre inoltre tenere presente i provvedimenti di esonero dall'obbligo di notificazione o di chiarimento adottati dal Garante che sono tutti 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*".

## 19.2. *Il registro dei trattamenti a dieci anni dalla sua istituzione*

Nel 2014 il nuovo registro dei trattamenti, istituito con il Codice a decorrere dal 1° gennaio 2004, ha compiuto dieci anni: può quindi risultare interessante

verificare, al di là delle delle notificazioni effettuate nel 2014 (cfr. sez. IV, tab. 17), come sia cambiata la mappa dei trattamenti notificati al Garante.

Nel 2004 sono state effettuate n. 10.014 notificazioni al registro dei trattamenti, con la compilazione di n. 15.084 tabelle relative ai vari tipi di trattamento (una singola notificazione, ovviamente, può riguardare più tipologie di trattamento). Alla fine del 2014 erano invece presenti sul registro dei trattamenti n. 24.075 notificazioni, con n. 35.488 tabelle compilate (cfr. sez. IV, tab. 14).

Le varie tipologie di trattamenti notificati hanno avuto un andamento piuttosto variabile nel corso di questi dieci anni, come si può verificare dai dati analitici inerenti l'evoluzione su base annua delle varie tabelle compilate dai titolari del trattamento (cfr. sez. IV, tab. 12 e 13 e grafico 15).

Volendo però fotografare in maniera sintetica l'attuale distribuzione delle tipologie di trattamento presenti sul registro delle notificazioni alla fine del 2014, effettuando una comparazione con la situazione verificatasi all'avvio del nuovo registro nell'anno 2004 (cfr. sez. IV, tab. 16), è possibile osservare in particolare che:

- la notificazione di trattamenti di dati personali idonei a rivelare lo stato di salute e la vita sessuale (art. 37, comma 1, lett. *b*) ha registrato una riduzione dell'incidenza percentuale sul totale dei trattamenti, passando dal 24,3% del 2004 al 21,1% del 2014;
- la notificazione di trattamenti relativi alle "banche dati sulla solvibilità e le frodi" (art. 37, comma 1, lett. *f*) si è ridotta, passando da un'incidenza relativa del 21% nel 2004 al 18,5% del 2014;
- parallelamente, in questo decennio è aumentata in percentuale la notificazione di trattamenti relativi alla cd. "geolocalizzazione" (art. 37, comma 1, lett. *a*), passati da una percentuale del 7,7% nel 2004 al 9,9% nel 2014 e, soprattutto, si è registrata una crescita consistente nella notificazione dei trattamenti inerenti la cd. "profilazione" (art. 37, comma 1, lett. *d*), incrementatisi dal 23,7% del 2004 al 28,9% del 2014.
- per gli altri trattamenti di cui all'art. 37, l'incidenza relativa sul totale delle notificazioni non ha subito grossi scostamenti a tutto il 2014 rispetto alla situazione rilevata nell'anno 2004.

Sotto il profilo della natura pubblica o privata del titolare del trattamento, è possibile riscontrare che dal 2004 al 2014 è aumentata l'incidenza dei soggetti privati che hanno notificato trattamenti, rispetto ai soggetti pubblici. Infatti, dall'88% di titolari del trattamento privati che avevano notificato almeno una tipologia di trattamento alla fine del 2004, si è passati, alla fine dell'anno 2014, ad una percentuale del 91%, con un corrispondente decremento nella percentuale di soggetti pubblici (cfr. sez. IV, grafico 18).

Sotto un altro profilo, appare interessante notare, come peraltro prevedibile, che esistono alcune rilevanti differenze nelle tipologie di trattamenti notificate a seconda della natura pubblica o privata del titolare (cfr. sez. IV, grafico 19). Alla fine del 2014, infatti, la principale categoria di trattamenti notificata da titolari aventi natura pubblica ha riguardato i dati di cui all'art. 37, comma 1 lett. *b*), del Codice ("dati idonei a rivelare lo stato di salute e la vita sessuale [...]") – riepilogati nella tab. 4 del registro dei trattamenti – con una percentuale del 28% sul totale dei trattamenti notificati da soggetti pubblici al 31 dicembre 2014. Al secondo posto troviamo il trattamento di dati genetici (art. 37, comma 1, lett. *a*), del Codice – tab. 1 reg. trattamenti), con una percentuale del 17% circa e, al terzo posto, il 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 – tab. 3 reg. trattamenti), con una percentuale del 15%.

Per i soggetti privati, alla stessa data di rilevazione, la principale tipologia di trattamento notificata è risultata essere quella relativa alla cd. "profilazione" (art. 37, comma 1, lett. *d*), del Codice), con una percentuale del 31% circa, mentre i trattamenti di dati di cui alla tab. 4 del registro si classificano solo in seconda posizione con una percentuale del 20% sul totale, seguiti a loro volta dai trattamenti di dati relativi alle cd. "banche dati sulla solvibilità e le frodi" (art. 37, comma 1, lett. *f*), del Codice – tab. 8 reg. trattamenti), che rappresentano il 19% del totale.

In generale possiamo dire che l'adempimento "notificazione" così come reinterpretato nel 2003 dal Codice (limitato cioè solo ad alcune tipologie di trattamento) è un adempimento che ha avuto un certo impatto e una discreta diffusione.

Già nel 2005, il Gruppo Art. 29, nell'ambito di una propria riflessione sull'istituto della notificazione, aveva osservato che la notificazione conservava una particolare valenza soprattutto nei Paesi di recente adesione all'UE, laddove rivestiva una funzione general-preventiva di richiamo dell'attenzione sull'esistenza di particolari obblighi connessi alla legislazione sulla protezione dei dati (cfr. Relazione sull'obbligo di notifica da parte delle autorità di controllo nazionali, sull'utilizzo più appropriato di eccezioni e semplificazioni e sul ruolo degli incaricati per la protezione dei dati in ambito UE 18 gennaio 2005 - WP 106). In contesti nei quali, invece, la disciplina di protezione dei dati personali è più matura, tra i quali possiamo sicuramente annoverare l'Italia, esso invece tende ad essere considerato come un mero adempimento burocratico. 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, nella proposta di nuova regolamentazione europea in corso di approvazione si supererà la logica della notificazione a vantaggio di nuovi strumenti più effettivi, primo fra tutti l'introduzione della nuova figura del *data protection officer* (definito nella traduzione italiana, in maniera un po' infelice, "Responsabile della protezione dei dati") – i cui compiti sono ancora in corso di definizione –, "presidio avanzato" presso il titolare del trattamento del rispetto dei principi e degli adempimenti in materia nonché interlocutore ed elemento di connessione tra il titolare del trattamento e l'Autorità.

### 19.3. *L'attività di supporto per i titolari del trattamento e di controllo sul registro*

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 trattamenti che necessitano di essere notificati.

Nel 2014 è proseguita anche un'assidua 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, effettuata anche mediante ispezioni *in loco* (v. al riguardo quanto riportato al par. 22).

In particolare, dalle verifiche effettuate sono emersi 16 casi di omessa/ritardata notificazione del trattamento con riferimento, rispettivamente a: trattamenti di dati biometrici (5); trattamenti di dati genetici (3); trattamenti di dati idonei a rivelare lo stato di salute (4); trattamento di dati che indicano la posizione geografica di persone od oggetti mediante una rete di comunicazione elettronica (3); trattamenti di dati con finalità di profilazione.

In tutti questi casi 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.

# 20 La trattazione dei ricorsi

## 20.1. *I profili generali*

Racchiudendo in uno sguardo d'insieme l'esperienza pluriennale, nell'ambito dell'attività decisionale su ricorsi può dirsi essersi consolidata una "giurisprudenza" dell'Autorità che, in particolare su alcuni "filoni", costituisce ormai un sicuro riferimento, ben conosciuto da tutti i soggetti interessati e largamente sostenuto anche dai giudici aditi in sede di opposizione ai sensi dell'art. 152 del Codice.

Ciò spiega perché alcune tematiche, oggetto di ampio contenzioso in passato, occupino ormai uno spazio marginale. Basti pensare alle richieste di accesso ai dati personali di tipo valutativo, con particolare riguardo a quelli contenuti nelle perizie medico legali redatte in ambito assicurativo; il tema, oggetto di numerosi ricorsi negli anni precedenti, ha trovato oggi un suo assestamento, sia in relazione alle situazioni nelle quali la richiesta di accesso a tali dati è accolta (e quindi rapidamente soddisfatta), sia in riferimento ai pochi casi nei quali tale accesso è differito in ragione della presenza di legittime esigenze difensive e di tutela delle ragioni del titolare del trattamento (art. 8, comma 2, lett. *e*), del Codice). La valutazione della sussistenza di un effettivo pregiudizio deve essere fatta in concreto dal Garante, sulla base degli elementi forniti dal titolare del trattamento o comunque desumibili dagli atti, come avvenuto nel caso di un'azienda sanitaria che ha legittimamente invocato il differimento del diritto di accesso adducendo ragioni volte a non pregiudicare l'esercizio del proprio diritto di difesa nella fase precontenziosa che, in ragione delle iniziative già intraprese dall'interessata, risultava preludere all'instaurazione di una controversia giudiziaria (cfr. provv. 3 luglio 2014, n. 346, doc. web n. 3347884).

Se si guarda al numero complessivo di ricorsi pervenuti all'Autorità e all'insieme dei temi affrontati, si può parlare senz'altro di "incremento" e di "evoluzione" del carico di lavoro. In particolare, dall'esame del numero delle decisioni adottate (306) si evince che si tratta di un numero rilevante di procedimenti, che ha subito un notevole incremento (pari al 38%) rispetto all'anno precedente (222), mentre le tipologie principali dei procedimenti instaurati corrispondono grosso modo ad ambiti già familiari all'Autorità.

## 20.2. *Dati statistici*

Per ciò che concerne la tipologia delle decisioni, si conferma l'alto numero di decisioni di non luogo a provvedere (60% del totale), cioè di procedimenti conclusisi con il soddisfacimento, nel corso dell'istruttoria, delle richieste degli interessati/ricorrenti. Una percentuale così alta di procedimenti conclusisi velocemente e positivamente depone a favore dell'utilità e dell'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. Sul piano della tipologia delle decisioni va poi sottolineato un andamento costante per ciò che concerne i casi di accoglimento (totale o par-

ziale) delle richieste dei ricorrenti (9%). Costante è anche la percentuale delle decisioni dichiarate infondate (15%) o inammissibili (16%), categoria quest'ultima in cui rientrano anche i provvedimenti adottati per mancata regolarizzazione ai sensi dell'art. 148, comma 2, del Codice (cfr. sez. IV, tab. 4).

Non meno significativo è lo sguardo alle principali categorie di titolari del trattamento, sia pubblici che privati, tra i quali si caratterizzano alcune macro-categorie: in primo luogo banche e società finanziarie, a seguire gli operatori nel settore del *marketing*, i gestori di sistemi di informazioni creditizie come pure di altri archivi centralizzati relativi alla verifica della affidabilità delle imprese, i fornitori di servizi telefonici e telematici nonché le amministrazioni condominiali (cfr. sez. IV, tab. 5). A sottolineare l'attuale momento storico, sono i numerosi ricorsi concernenti il trattamento dati legato all'attività economica; va altresì rilevato il numero significativo di procedimenti attivati nei confronti dei datori di lavoro pubblici e privati. Tale dato riflette le difficoltà occupazionali e la crisi che sta attraversando il mondo del lavoro ed evidenzia il profilo del "nuovo" contenzioso rispetto all'utilizzo delle moderne tecnologie sul luogo di lavoro. Un aspetto di rilevante interesse in questo ambito è la necessità di garantire, in un'ottica di bilanciamento tra i contrapposti interessi, la tutela del diritto del dipendente alla segretezza delle proprie comunicazioni. Considerata infatti l'equivalenza tra la corrispondenza tradizionale e quella elettronica, occorre assicurare un elevato livello di tutela anche alle comunicazioni scambiate dal dipendente con soggetti esterni o interni alla struttura aziendale, tenuto conto del fatto che l'eventuale trattamento di tali dati implicherebbe un'operazione idonea a rendere conoscibili talune informazioni personali relative all'interessato. La necessità di tutela, particolarmente evidente laddove l'*account* di posta elettronica aziendale assegnato in dotazione al dipendente sia individualizzato, ovvero contenga il nome e cognome del medesimo, implica che l'eventuale trattamento dei dati riferiti a comunicazioni di posta elettronica inviate e ricevute dal dipendente presso il menzionato *account* sia tale da evitare un'interferenza ingiustificata sui diritti e sulle libertà fondamentali di lavoratori. Questa considerazione vale anche nell'ipotesi in cui, per qualunque causa, venga a cessare il rapporto di lavoro o di collaborazione tra le parti rendendo di fatto non più legittimamente utilizzabile dal datore di lavoro, né per inviare la posta in uscita né per ricevere quella in entrata, un *account* di posta elettronica aziendale riconducibile ad un soggetto che non fa più parte dell'organizzazione; tale circostanza rende altresì necessaria l'adozione di misure idonee ad informare i terzi estranei della disattivazione dell'indirizzo medesimo, con contestuale indicazione di un diverso indirizzo di posta elettronica aziendale cui inviare le comunicazioni attinenti la sfera lavorativa (cfr. provv. 27 novembre 2014, n. 551, doc. web n. 3718714).

Significativa anche la decisione del 17 luglio 2014, n. 370 (doc. web n. 3405174) con cui il Garante ha parzialmente accolto il ricorso di un alto dirigente di una società che, sospeso in via cautelare dal servizio per la ritenuta commissione di un grave illecito, era stato privato degli strumenti aziendali in dotazione (*pc, I-phone* e *I-pad*) con relativa disattivazione delle schede Sim e dell'*account* di posta elettronica al fine di effettuare verifiche e accertamenti sul corretto utilizzo degli stessi. Al riguardo, l'Autorità, pur ritenendo lecita l'attività di controllo svolta dalla società (che peraltro ha dichiarato che i controlli avrebbero riguardato esclusivamente l'indirizzo di posta elettronica aziendale), si è pronunciata favorevolmente nei confronti dell'istanza del ricorrente di poter accedere ai propri dati personali contenuti nella corrispondenza elettronica intrattenuta tramite il proprio *account* aziendale (salvo il differimento ai sensi dell'art. 8, comma 2, lett. *e*), del Codice, invocato dalla società resistente per i soli dati acquisiti nel corso delle verifiche esperite sull'*account* del ricorrente); ciò considerato che l'indirizzo di posta elettronica aziendale utilizzato

dal ricorrente era un indirizzo individualizzato recante nome e cognome dello stesso – e non un indirizzo condiviso tra più lavoratori – tale quindi da dover essere considerato dato personale, anche a prescindere dal contenuto della corrispondenza.

Ma la novità che emerge dalla comparazione dei dati con l'anno precedente è l'incremento (dal 10 al 14%) del numero dei ricorsi nei confronti degli editori, anche televisivi (in merito v. *infra* par. 20.3).

Si evidenziano, infine, casi ancora frequenti di ricorsi che vengono proposti da società commerciali ed enti vari, forse ignari del fatto che, a seguito delle modifiche normative intervenute alla fine del 2011 con riguardo alle nozioni di "interessato" e di "dato personale" (art. 4 del Codice), i soggetti diversi dalle persone fisiche sono stati privati della possibilità di utilizzare gli strumenti di tutela previsti dal Codice, qui con particolare riguardo all'esercizio del diritto d'accesso.

### 20.3. *La casistica più significativa*

Se, come accennato, abitualmente i ricorsi si incentrano su materie ormai note all'Autorità – si pensi all'ambito lavorativo, all'opposizione a trattamenti svolti per finalità promozionali, all'accesso a informazioni bancarie e finanziarie (anche per ricostruire posizioni contabili relative a persone defunte), ovvero alle istanze di cancellazione di posizioni "negative" da alcuni grandi archivi pubblici e privati (centrale dei rischi di Banca d'Italia, Archivio CAI, Sistemi di informazioni creditizie) –, merita qui soffermarsi su alcune decisioni adottate dal Garante con riguardo al trattamento dei dati per finalità giornalistiche, con un'attenzione speciale ai trattamenti svolti tramite i cd. archivi storici *online* dei principali quotidiani nonché ai trattamenti effettuati da parte dei motori di ricerca cd. generalisti.

**Trattamenti in ambito giornalistico**

Sta assumendo ormai una particolare rilevanza il filone delle richieste di deindicizzazione dai motori di ricerca cui si affiancano da ultimo le richieste di aggiornamento dei dati rivolte agli editori titolari degli archivi *online*. Questa ultima categoria di procedimenti, oggetto peraltro di recente intervento da parte della Corte di giustizia nel caso *Google Spain* (sulla quale v. il par. 23.3), conferma come attraverso lo strumento dei ricorsi pervengano all'attenzione dell'Autorità richieste di intervento sui temi più attuali.

La necessità di ricercare soluzioni tecniche idonee a garantire l'effettivo esercizio del diritto di rettifica e di aggiornamento delle notizie diffuse in rete è emersa da una pronuncia della Corte di Cassazione (n. 5525 del 5 aprile 2012) che ha espressamente riconosciuto il diritto all'aggiornamento e all'integrazione delle notizie lesive per l'interessato ove superate dagli eventi (come nel caso del soggetto noto alla cronaca giudiziaria per essere stato indagato ma di cui si taccia poi del tutto l'avvenuto proscioglimento o, in caso di condanna, l'intervenuta riabilitazione). Il richiamo agli sviluppi successivi rispetto alla notizia originaria consente, da un lato, di tutelare la dignità del soggetto leso e, dall'altro, di migliorare la stessa qualità dell'informazione, che risulta in tal modo esatta ed aggiornata.

Nel prevedere l'obbligo per il titolare di un archivio *online* di contestualizzare nel tempo le informazioni, la sentenza richiamata ha affermato che le necessarie integrazioni per aggiornare la notizia debbano avvenire "con modalità tecniche non modificative dell'originale", rimettendo in capo ai titolari la scelta in merito alle corrette modalità di attuazione.

Sul tema dell'aggiornamento delle notizie è utile analizzare l'orientamento interpretativo nel tempo assunto dal Garante: inizialmente, le richieste volte ad ottenere l'aggiornamento di notizie giudiziarie – specie se non indicizzate dai motori di

ricerca – non venivano accolte in quanto si ritenevano interventi modificativi del contenuto originario degli articoli che, nati come espressione di libera manifestazione del pensiero, venivano poi legittimamente conservati per finalità di documentazione all'interno di archivi. Questi ultimi, benché informatizzati, assolvendo la medesima funzione storica degli archivi cartacei, ben potevano pertanto contenere gli articoli pubblicati secondo il loro contenuto originario.

Con tali decisioni rese dall'Autorità, la tutela riconosciuta all'interessato consisteva nel non rendere più indicizzabili, dai motori di ricerca esterni al sito in cui l'archivio è contenuto, le sole pagine web contenenti gli articoli oggetto di contestazione. Le informazioni – anche se non aggiornate – restavano comunque reperibili direttamente nell'archivio storico del giornale.

In seguito alla menzionata sentenza della Corte di Cassazione n. 5525/2012, l'Autorità ha invece espressamente riconosciuto il diritto "ad ottenere l'aggiornamento/integrazione dei dati personali che lo riguardano quando eventi e sviluppi successivi (adeguatamente documentati) hanno modificato le situazioni oggetto di cronaca giornalistica (seppure a suo tempo corretta) incidendo significativamente sul profilo e l'immagine dell'interessato". Si è così prescritto all'editore titolare del trattamento, non solo di deindicizzare gli articoli non aggiornati, ma anche, e soprattutto, di predisporre nell'ambito dell'archivio storico *online* del quotidiano, un sistema idoneo a segnalare (ad es., a margine dei singoli articoli o in nota agli stessi) la sopravvenienza di nuovi elementi ed il loro contenuto (come nel caso di intervenuta definizione in via giudiziaria della vicenda) consentendone il rapido ed agevole accesso al lettore. Così la decisione di accoglimento parziale del ricorso contro una testata giornalistica nazionale a cui il Garante ha ordinato di predisporre, nell'ambito dell'archivio storico *online* del relativo quotidiano, un sistema di aggiornamento/integrazione degli articoli in questione idoneo a fornire ai lettori l'immediata visibilità degli sviluppi informativi facendo sì che gli stessi emergessero già nell'anteprima dell'articolo presente tra i risultati del motore di ricerca dell'archivio storico (provv. 9 gennaio 2014, n. 9, doc. web n. 3001832).

Un ulteriore passo in avanti si è registrato con una decisione dell'11 dicembre 2014, n. 604 (doc. web n. 3732971) che ha riconosciuto l'idoneità di una soluzione "tecnica" che rende effettivo l'aggiornamento di una notizia anche quando la stessa continua ad essere reperibile sui motori di ricerca generalisti. Nel caso in esame, il ricorrente aveva chiesto (tra l'altro) l'adozione di un sistema idoneo a segnalare l'esistenza del seguito della notizia in relazione ad un articolo del maggio 2013 – rinvenibile sul web associato al proprio nominativo – pubblicato su un quotidiano locale *online* e riferito ad una vicenda giudiziaria nella quale era stato coinvolto. Ed invero, il procedimento penale avviato nei suoi confronti (avviso di garanzia) e riportato dalla testata *online* si era concluso con l'adozione di un decreto di archiviazione per non aver commesso il fatto. Tale notizia era stata successivamente riportata in un articolo pubblicato nel novembre successivo dalla medesima testata ma della stessa non era fatta alcuna menzione nell'articolo originario.

In particolare, non si contestava la liceità della notizia come originariamente pubblicata (avviso di garanzia) quanto piuttosto la mancanza di un sistema idoneo ad informare il lettore di un seguito della stessa (archiviazione). Il ricorrente precisava inoltre che digitando soltanto il proprio nominativo era possibile rinvenire nel motore di ricerca entrambe le notizie, mentre utilizzando chiavi di ricerca diverse (come ad es., i nomi degli altri soggetti menzionati nell'articolo quali, ad es., altri indagati, l'avvocato o il consulente) i risultati riportavano esclusivamente l'articolo iniziale relativo all'indagine penale avviata (anche) nei suoi confronti. Pertanto, la notizia, originariamente corretta, se non aggiornata, risulta a distanza di tempo parziale e non esatta.

Nel corso dell'istruttoria l'editore resistente ha provveduto non soltanto ad inibire ai motori di ricerca l'accesso all'articolo attraverso la compilazione del *file* "*robots.txt*", ma ha apposto in calce all'articolo originario un *link* nel quale è possibile rinvenire la notizia dell'avvenuta archiviazione del procedimento penale a carico del ricorrente.

L'Autorità ha affrontato nel dicembre 2014, per la prima volta dopo la citata sentenza della Corte di giustizia nel caso Google Spain, le problematiche che coinvolgono ormai direttamente non soltanto gli editori-titolari dei quotidiani *online* ma anche, e soprattutto, i motori di ricerca che, sebbene non qualificabili come editori, sono comunque da considerarsi titolari del trattamento dei dati contenuti nei relativi indici e, in quanto stabiliti sul territorio di uno Stato membro, sono tenuti a rispettare le disposizioni nazionali in materia di protezione dei dati. Nel caso di specie (provv. 18 dicembre 2014, n. 618, doc. web n. 3736353), la richiesta formulata da un ricorrente volta alla deindicizzazione dell'indirizzo url che lo riguardava, rinvenibile attraverso Google, non è stata accolta dal momento che le notizie rinvenibili a tale indirizzo, pubblicate nel giugno 2014, erano assai recenti nonché di pubblico interesse, riguardando un'importante indagine giudiziaria. Nella medesima decisione, tuttavia, l'Autorità ha affrontato un profilo delicato riguardante le modalità con le quali i dati/informazioni riferiti ad un soggetto sono associati e, quindi, visualizzati dagli utenti nel cd. *snippet*. Come noto ogni risultato di ricerca è sostanzialmente composto da un titolo e da una descrizione, un *abstract* che riporta, in breve, le parole chiave utilizzate dall'utente nella stringa di ricerca – e che spesso sono rese più evidenti utilizzando una grafica particolare. Nel caso di specie, il ricorrente lamentava il fatto di aver rivestito una posizione marginale rispetto ai reati di usura ed estorsione menzionati nel titolo dell'articolo indicizzato dal motore di ricerca, mentre l'*abstract* associava espressamente il suo nominativo alle parole "misure cautelari" facendo così presumere – erroneamente – che lo stesso fosse stato sottoposto anche a misure restrittive della libertà personale. Il ricorrente ha pertanto fatto valere la pretesa a che l'*abstract* visualizzato sotto il titolo dell'articolo "non associ genericamente", per mezzo delle scansioni operate automaticamente dal motore di ricerca, il proprio nominativo alle notizie principali dell'articolo (riassunte nel titolo), indipendentemente dalla specifica narrazione dei fatti relativi all'interessato come riferiti. Il motore di ricerca ha provveduto a rimuovere integralmente lo *snippet* associato all'indirizzo *url* contenente l'articolo. L'aspetto più rilevante della decisione richiamata riguarda il fatto che l'Autorità ha ritenuto legittima la richiesta avanzata dal ricorrente affinché anche l'*abstract* visualizzato dalle ricerche effettuate non associ genericamente, per mezzo delle scansioni operate automaticamente dal motore di ricerca, il nominativo dell'interessato alle notizie principali contenute nell'articolo indicizzato e, dunque, indipendentemente dalla specifica narrazione dei fatti.

Appare evidente come il tema in esame, richieda un adeguamento costante, con particolare riferimento alle soluzioni tecniche necessarie a codificare ed implementare i principi giuridici.