Nel corso dell'attività di collaborazione sono stati esaminati i princìpi e le regole da applicare affinché il trattamento posto in essere risulti conforme al Codice: l'informativa ai sensi dell'art. 13 del Codice; l'acquisizione del consenso, rispetto al quale è applicabile la fattispecie di esonero previsto dall'art. 24, comma 1, lett. *a*), del Codice, considerato che il trattamento posto in essere è espressamente previsto da una specifica norma di legge; i tempi di conservazione non superiori a quelli necessari agli scopi per i quali sono stati raccolti e successivamente trattati (art. 11, comma 1, lett. *c*), del Codice). Tuttavia sono risultati ancora in fase di definizione specifici aspetti, tra cui l'individuazione dei dati personali oggetto di trattamento all'interno del sistema e delle informazioni concernenti eventuali inadempimenti contrattuali dei clienti. La definizione di tali contenuti avverrà con delibera del Collegio dell'Autorità per l'energia elettrica e il gas, a seguito di una consultazione pubblica avviata dalla stessa Autorità di settore, sicché il Garante, pur individuando misure ed accorgimenti affinché il trattamento sia effettuato in conformità al Codice, si è riservato di formulare un formale parere all'esito dell'elaborazione del documento finale (nota 2 maggio 2012).

14.4. VIDEOSORVEGLIANZA IN AMBITO PRIVATO

Nel corso dell'anno, il Garante si è pronunciato in relazione ad una serie di istanze di verifica preliminare (art. 17 del Codice) presentate da alcune società del settore privato per l'allungamento dei tempi di conservazione delle immagini registrate e con riferimento a sistemi cd. "intelligenti".

Con provvedimento del 12 gennaio 2012 [doc. web n. 1875004], l'Autorità si è pronunciata sulla richiesta (art. 17 del Codice) di attivazione di un impianto di video-sorveglianza cd. "intelligente", provvisto anche di un sistema di captazione audio, presso una centrale termoelettrica di interesse nazionale -stante la sua considerevole capacità produttiva- che era stata bersaglio, nel corso del tempo, di vari atti illeciti. La società stessa ha quindi scelto di dotarsi di un sistema di sorveglianza "intelligente", provvisto anche di un sistema di captazione audio, che garantisse una veloce identificazione di possibili intrusioni dall'esterno da parte di persone non autorizzate.

Il Garante ha ritenuto che l'impianto di videosorveglianza intelligente fosse conforme ai princìpi di pertinenza, non eccedenza e proporzionalità (v. artt. 3 e 11 del Codice) poiché l'ubicazione isolata del sito, la sua notevole estensione e la posizione dell'area al di fuori delle zone in cui le forze dell'ordine svolgono la routinaria attività di pattugliamento, giustificavano l'adozione di sistemi di sicurezza che, consentendo una rilevazione di possibili intrusioni in tempi estremamente brevi, risultassero effettivamente in grado di prevenire accessi non autorizzati alla struttura e, quindi, riducessero significativamente il rischio di atti in grado di provocare gravi disservizi.

Invece, con specifico riferimento al connesso sistema di captazione audio, l'Autorità ha ritenuto che lo stesso non fosse conforme al richiamato principio di proporzionalità, potendo determinare un'ulteriore e non giustificata riduzione della sfera di riservatezza di chiunque si trovasse a transitare in prossimità di un'area già abbondantemente monitorata, per finalità di sicurezza, con un modernissimo sistema di videosorveglianza.

Pertanto, è stata accolta la richiesta di verifica preliminare limitatamente alla sola attività di videosorveglianza e non per il sistema di captazione audio.

È stata altresì accolta, con provvedimento del 15 marzo 2012 [doc. web n. 1893742], in sede di verifica preliminare, l'istanza presentata da una società operante tra altro nei settori del petrolio, del gas naturale e della petrolchimica, volta all'istallazione di due sistemi di videosorveglianza cd. "intelligente" presso due suoi siti produttivi, per finalità connesse alla tutela del patrimonio aziendale e della sicurezza dei lavoratori.

In particolare, l'Autorità ha considerato sia che le situazioni di rischio erano state espressamente acclarate a più riprese dagli organi istituzionalmente preposti, sia la ridotta efficacia delle protezioni e dei sistemi di sicurezza esistenti ed ha perciò ritenuto giustificata l'attivazione di un sistema di video-analisi a supporto dei dispositivi di ripresa che, consentendo una rilevazione automatica delle intrusioni, risultasse effettivamente in grado di prevenire accessi non autorizzati alla struttura, forieri di grave pericolo per la sicurezza dei siti in questione e l'incolumità del personale ivi impiegato.

È stata invece respinta, in sede di verifica preliminare, l'istanza di conservare sino a novanta giorni le immagini del sistema di videosorveglianza di una società che opera nella persona-

lizzazione e postalizzazione di tessere magnetiche ed a microprocessore, per applicazioni di sicurezza e sanitarie (carte di credito e, più in generale, carte di identificazione).

La richiesta era stata giustificata non solo con l'esigenza di rafforzare il livello di tutela della proprietà aziendale e di sicurezza, ma anche con la necessità di osservare concretamente i parametri fissati dai circuiti internazionali *MasterCard International* e *Visa International,* presso i quali l'azienda risultava certificata per la produzione di carte di credito.

Il Garante ha in contrario osservato, da un lato, che le "prescrizioni" impartite dagli enti certificatori risultavano "derogabili" in presenza di "restrizioni legali" all'utilizzo di sistemi di videosorveglianza; dall'altro, che non si erano mai verificate in concreto condotte criminose (verosimilmente anche in ragione delle altre numerose misure di sicurezza già approntate).

L'Autorità ha peraltro ricordato il consolidato orientamento giurisprudenziale che riconosce al datore di lavoro la possibilità, nel rispetto delle garanzie previste dall'ordinamento (in particolare, gli artt. 2, 3 e 6 della l. n. 300/1970), di adibire a mansioni di vigilanza e tutela del patrimonio aziendale anche propri dipendenti, a mezzo dei quali poter controllare l'attività di altri lavoratori per accertare eventuali comportamenti fraudolenti estranei alla prestazione lavorativa e rilevanti sull'integrità del patrimonio aziendale (provv. 21 marzo 2012 [doc. web n. 1893723]).

Si riferisce, infine, di una richiesta di verifica preliminare inoltrata da una società che gestisce un importante complesso museale con sede in Venezia, per l'allungamento dei tempi di conservazione delle immagini registrate dal sistema di videosorveglianza -rispetto a quelli indicati nel provvedimento generale adottato dal Garante in materia (provv. 8 aprile 2010 [doc. web n. 1712680])- giustificato dal pericolo di furti e di atti vandalici, in molti casi rilevabili solo a distanza di tempo, cui sarebbero state esposte numerose opere di inestimabile valore custodite all'interno del museo.

A seguito di tale richiesta, il Garante ha ritenuto sussistente il rischio paventato, considerate le dimensioni delle sale d'esposizione e il numero delle opere esposte e dei visitatori; ha quindi accolto la richiesta di allungamento dei tempi di conservazione delle immagini sino a due settimane, con successiva cancellazione automatica delle stesse (provv. 8 marzo 2012 [doc. web n. 1891026]).

14.5. BIOMETRIA

A seguito di due distinte segnalazioni, l'Autorità è stata chiamata a pronunciarsi sulla liceità del trattamento di dati biometrici effettuato presso due centri sportivi per finalità di accesso alle relative strutture e di gestione dei servizi offerti (provv.ti 16 febbraio 2012 [doc. web n. 1894570] e 29 marzo 2012 [doc. web n. 1891999]). Dagli accertamenti ispettivi espletati è emerso come non fosse stato nemmeno acquisito un libero consenso degli interessati rispetto allo specifico trattamento dei dati biometrici con conseguente violazione degli artt. 11, comma 1, lett. *a)* e 23, del Codice. Peraltro, a fronte della indimostrata insufficienza o non attuabilità di eventuali misure alternative alla rilevazione del dato biometrico, il trattamento è risultato vieppiù sproporzionato (art. 11, comma 1, lett. *d)*, del Codice) in ragione delle prescelte modalità di configurazione del sistema, preordinato alla conservazione centralizzata dei *template* in luogo della loro memorizzazione su dispositivi affidati esclusivamente agli interessati. In un caso, poi, il trattamento dei dati biometrici, che interessava anche alcuni lavoratori, è risultato altresì in violazione delle prescrizioni contenute nel provvedimento generale recante le linee-guida in materia (provv. 23 novembre 2006 [doc. web n. 1364099]). L'Autorità ha quindi vietato, nei confronti dei rispettivi titolari, l'ulteriore trattamento dei dati biometrici degli utenti.

Il Garante ha invece ammesso il trattamento dei dati biometrici dei passeggeri connesso all'installazione, presso i *gate* presenti in aeroporto, di un sistema di rilevazione delle loro impronte digitali volto a coniugare le esigenze di rigoroso accertamento dell'identità degli interessati con quelle di semplificazione e velocizzazione delle operazioni di imbarco cd. "*fast-boarding*" (provv. 4 ottobre 2012 [doc. web n. 2059743]).

Il trattamento -basato sulla conversione del rilievo dattiloscopico in un *template* memorizzato, unitamente ai dati identificativi dell'interessato, su una *smartcard* posta nell'esclusiva disponibilità di quest'ultimo e leggibile, attraverso l'utilizzo di tecnologia *Rfid*, solamente dal dispositivo a ciò preposto cd. "*reader*"-, sarebbe stato effettuato nel rispetto di rigorose misure di sicurezza a garanzia degli interessati e su base esclusivamente volontaria, previa acquisizione del libero consenso informato degli interessati. L'Autorità, nel valutare positivamente l'iniziativa (anche in ragione dei rigidi protocolli di sicurezza in ambito

aeroportuale previsti dalla normativa di settore), ha ritenuto che il trattamento così configurato non fosse illecito né sproporzionato. Nondimeno, fermo restando l'obbligo di notifica del trattamento (artt. 37 e ss. del Codice) e il rispetto delle previste misure di sicurezza (in particolare, la regola 25 dell'Allegato B. al Codice), è stato prescritto alla società di indicare chiaramente, nell'informativa da rendere all'utenza, le finalità del trattamento e la natura del conferimento dei dati, nonché di adottare una serie di accorgimenti volti a ridurre ulteriormente l'utilizzo di dati personali nell'ambito del servizio offerto.

Inoltre, con riguardo a due distinte verifiche preliminari (ai sensi dell'art. 17 del Codice) richieste da alcuni istituti di credito e da una *certification authority*, l'Autorità ha valutato il trattamento connesso all'utilizzo, nell'ambito del più ampio servizio di sottoscrizione dei documenti con firma digitale, di sistemi di autenticazione basati sulla rilevazione dei dati biometrici degli utenti in occasione delle operazioni allo sportello (provv. 31 gennaio 2013 [doc. web n. 2304808]). Tali sistemi, preordinati alla raccolta delle caratteristiche "comportamentali" degli interessati attraverso l'analisi di alcuni parametri (quali velocità, pressione, accelerazione, inclinazione) desumibili dall'apposizione della loro firma autografa su *tablet* a ciò dedicati, avrebbero garantito -attraverso la comparazione dei *template* acquisiti di volta in volta allo sportello con lo *specimen* di firma generato in occasione della registrazione al servizio- il rigoroso riconoscimento degli utenti (in osservanza, tra l'altro, degli specifici obblighi gravanti sugli istituti di credito e sui soggetti certificatori), riducendo conseguentemente i rischi connessi ad eventuali pratiche fraudolente (quali il furto di identità).

Il Garante, nel richiamare i pareri resi in materia dal Gruppo Art. 29 (WP 80 - 1° agosto 2003 [doc. web n. 1609419]; WP 193 - 27 aprile 2012 [doc. web n. 2375294]), ha sottolineato come il trattamento dei dati biometrici degli utenti risultasse effettivamente rispondente, nei casi esaminati, alle esigenze di rigoroso riconoscimento evidenziate dagli istanti, oltre che funzionale al contrasto di eventuali fenomeni fraudolenti e allo snellimento delle operazioni allo sportello; tanto, muovendo dall'ulteriore presupposto che, in entrambi i casi considerati, il trattamento sarebbe stato effettuato previa acquisizione del consenso informato degli interessati. Inoltre, sono risultate adeguate le modalità di configurazione del sistema e di gestione dei dati prescelte dagli istanti, come pure le misure di sicurezza indicate

a tutela dei dati biometrici oggetto di trattamento (artt. 31 e ss. del Codice). L'Autorità ha tuttavia prescritto, in un caso, alcune misure e accorgimenti, con particolare riferimento all'informativa da rendere agli interessati (art. 13 del Codice), all'acquisizione del loro consenso (art. 23 del Codice), ai tempi di conservazione dei dati (art. 11, comma 1, lett. *e)*, del Codice) e, infine, alla modifica della notificazione del trattamento (provv. 31 gennaio 2013 [doc. web n. 2311886]).

15. IL TRASFERIMENTO DEI DATI ALL'ESTERO

Nel periodo di riferimento l'attività del Garante si è svolta su differenti piani. Innanzitutto è proseguita l'analisi delle molteplici richieste di autorizzazione pervenute in materia di *Binding corporate rules (Bcr)* (norme vincolanti di impresa) e delle decisioni adottate dalla Commissione europea sull'adeguatezza delle normative di protezione dei dati di alcuni Paesi terzi (decisione relativa alla Repubblica orientale dell'Uruguay del 21 agosto 2012 e alla Nuova Zelanda del 19 dicembre 2012).

Quanto alle istanze concernenti l'impiego delle *Bcr*, sono state avviate istruttorie complesse, tuttora in corso, concernenti operazioni di trasferimento all'estero di dati effettuate da importanti gruppi multinazionali operanti in diversi settori economici; tali istruttorie sono frutto di procedure poste in essere a livello europeo, per lo più nell'ambito del cd. "accordo di mutua collaborazione" (cfr. Relazione 2009 p.189).

Altrettanto intensa, poi, è stata l'attività in materia di *standard contractual clauses*, con particolare riferimento anche a quanto evidenziato dal Garante italiano -in occasione delle attività di approfondimento condotte dal Gruppo Art. 29 con il documento WP 176 del 12 luglio 2010- riguardo ad alcuni quesiti formulati in vista dell'entrata in vigore della decisione della Commissione europea del 5 febbraio 2010, n. 2010/87/UE.

Come già diffusamente descritto nelle precedenti Relazioni (v. Relazione 2009 p. 189 e Relazione 2010 p. 154) il Garante, con specifica autorizzazione (v. provv. 27 maggio 2010 [doc. web n. 1728496]), ha attuato nell'ordinamento italiano la Decisione della Commissione n. 2010/87/EU del 5 febbraio 2010, che ha sostituito il *set* di clausole contrattuali tipo "da titolare a responsabile" già esistente (Decisione della Commissione n. 2002/16/EC) con un nuovo schema che contiene una clausola cd. di "*subcontracting*", secondo cui l'importatore (in qualità di responsabile del trattamento) può affidare il trattamento (o una parte di esso) a un soggetto terzo (cd. "*sub-incaricato*"), che agisce anch'esso come responsabile.

A seguito di tale delibera, sono pervenuti a questa Autorità vari quesiti, di analogo tenore a quelli contenuti nel WP 176, volti a conoscere se sia possibile utilizzare il citato modello di

clausole contrattuali tipo anche nel caso in cui il responsabile, che affidi il trattamento ad un "*sub-incaricato*" ubicato in un Paese terzo che non assicuri un livello di protezione adeguato, sia stabilito nella Unione europea. Tali richieste sono state determinate dalla crescente diffusione di forme di affidamento di attività di trattamento a terzi (in particolare, a società di servizi, spesso stabilite nell'Unione europea) e dalla consequenziale esigenza del settore privato di disporre di strumenti comuni e di modalità uniformi da utilizzare nei casi in cui tale affidamento comporti un successivo trasferimento di dati personali verso Paesi terzi che non assicurino un livello di protezione adeguato.

Al riguardo, in questa prima fase, il Garante ha adottato un provvedimento (provv. 15 novembre 2012 [doc. web n. 2191156]) con il quale, tenuto conto di quanto previsto nel considerando 23 della citata Decisione n. 2010/87/UE e di quanto già accennato al riguardo nella menzionata autorizzazione dell'Autorità, ha prescritto al titolare del trattamento stabilito nel territorio dello Stato (esportatore) di conferire al responsabile stabilito nell'Unione europea che intenda affidare il trattamento dei dati ad un altro responsabile (importatore) stabilito nel Paese terzo che non assicuri un livello di protezione adeguato, un apposito mandato (ai sensi dell'art. 1704 c.c.), per la sottoscrizione delle clausole contrattuali tipo di cui all'allegato della Decisione della Commissione europea del 5 febbraio 2010, n. 87/2010/UE.

La scelta di tale strumento da parte dell'Autorità, che lascia intatta la facoltà del titolare del trattamento di chiedere al Garante una specifica autorizzazione per trasferire i dati personali (ai sensi dell'art. 44, comma 1, lett. *a*), del Codice), è frutto anche del recepimento delle osservazioni e dei suggerimenti resi in tal senso dal Gruppo Art. 29 il quale, tra le possibili soluzioni, aveva ipotizzato l'utilizzazione dello schema contrattuale del mandato.

Infine, di rilievo è stato l'esame condotto dall'Autorità in ordine a due istanze -di analogo contenuto- avanzate da due società aventi sede in Italia ed operanti nel settore dell'offerta di prodotti assicurativi di risparmio e di cd. "*employee benefits*", volte ad ottenere un'autorizzazione al trasferimento di dati personali verso altre società, anch'esse titolari del trattamento, situate negli Stati Uniti.

In particolare, le istanze avevano ad oggetto il trasferimento dei dati personali relativi al personale per il perseguimento non solo delle finalità connesse alla gestione della forza

lavoro, ma anche per comunicazioni ed emergenze, per il compimento di operazioni commerciali e per attività di *compliance*, monitoraggio e pianificazione integrata svolte ordinariamente dalle società.

Dopo una complessa istruttoria, volta a valutare se il cd. "contratto di trasferimento" utilizzato dalle suddette società per il trasferimento dei dati all'estero contenesse adeguate garanzie per i diritti degli interessati, l'Autorità ha rilasciato le autorizzazioni richieste, nei limiti delle modalità e delle finalità indicate nel suddetto "contratto", riservandosi di controllare la liceità e la correttezza dei trasferimenti dei dati e di adottare eventuali provvedimenti di blocco o di divieto di trasferimento (provv. 11 ottobre 2012 [doc. web n. 2111613]).

Per quanto riguarda la valutazione del Gruppo Art. 29 sull'adeguamento del livello di protezione dei dati personali nel Principato di Monaco, si fa rinvio al paragrafo 21.3..

16. LE LIBERE PROFESSIONI

16.1. ORDINI PROFESSIONALI

Il Garante ha fornito numerosi chiarimenti in ordine alle modalità di trattamento ed al regime di conoscibilità dei dati personali degli iscritti agli ordini professionali. In particolare, ad un ordine che aveva effettuato una comunicazione al Garante, ai sensi degli artt. 19, comma 2, e 39 del Codice, per poter trasmettere a diversi soggetti i provvedimenti disciplinari assunti a carico di un iscritto, l'Autorità ha precisato che gli ordini e i collegi professionali possono comunicare a terzi, e diffondere, anche mediante reti di comunicazione elettronica, i dati diversi da quelli sensibili e giudiziari, che, secondo le disposizioni di settore, devono essere inseriti nei rispettivi albi (cfr. artt. 18, 19 e 61 del Codice). L'Ufficio ha evidenziato che, nel rispetto dei princìpi di pertinenza, non eccedenza e proporzionalità dei dati, il Codice consente di menzionare l'esistenza di provvedimenti che dispongono la sospensione o che incidono sull'esercizio delle professione, purché il trattamento riguardi informazioni corrette, complete ed aggiornate (nota 22 agosto 2011).

In relazione ad un quesito circa il regime di conoscibilità dell'indirizzo di posta elettronica certificata degli avvocati iscritti all'albo, l'Ufficio, nel ribadire i presupposti suddetti, ha evidenziato che nell'albo degli avvocati deve essere indicato, oltre al codice fiscale, anche l'indirizzo di posta elettronica certificata (cfr. art. 16 r.d. 27 novembre 1933, n. 1578 e successive modificazioni, recante "Ordinamento delle professioni di avvocato e procuratore") (nota 23 maggio 2011).

È giunto inoltre all'Autorità un reclamo relativo ad un collegio professionale dei periti industriali che, nell'ambito della campagna elettorale per le elezioni di un organo consiliare, aveva diffuso sul proprio sito internet istituzionale dati giudiziari relativi al reclamante e ad altri professionisti, iscritti, per altro, ad un altro collegio. Al riguardo, l'Autorità ha ribadito che il collegio, quale soggetto pubblico, può trattare dati giudiziari solo sulla base di idonea previsione normativa (v. artt. 20 e 21 del Codice).

In tale quadro il Ministero della giustizia ha adottato, in conformità al parere espresso dal Garante il 7 dicembre 2006 [doc. web n. 1370395], lo schema tipo di regolamento per il

trattamento dei dati sensibili e giudiziari da parte degli organismi professionali sottoposti alla sua vigilanza che, con riferimento al trattamento dei dati sensibili e giudiziari "*indispensabili allo svolgimento delle elezioni e alla gestione dei componenti degli organi elettivi del Consiglio/collegio*", ammette la diffusione "*limitatamente ai risultati elettorali*" (scheda n. 4). Rilevata l'illiceità della predetta diffusione, l'Autorità ha quindi vietato al collegio professionale di diffondere ulteriormente i dati giudiziari contenuti nei predetti atti (artt. 143, comma 1, lett. *c)*, e 154, comma 1, lett. *d)*, del Codice). L'Ufficio ha, infine, disposto gli opportuni accertamenti per l'eventuale applicazione della sanzione amministrativa conseguente alla violazione del divieto di diffusione (art. 162, comma 2-*bis*, del Codice) (provv. 17 gennaio 2013 [doc. web n. 2315622]).

Un iscritto all'ordine dei commercialisti ha lamentato, da parte del relativo ordine, la pubblicazione sull'albo dell'indirizzo completo relativo alla residenza anagrafica di ogni singolo iscritto. Al riguardo, in base alla normativa di settore, il predetto albo deve contenere, per ogni iscritto, tra l'altro, "*il cognome, il nome, la data ed il luogo di nascita, la residenza e l'indirizzo (anche telematico se posseduto) degli studi professionali*" (art. 34 del d.lgs. 28 giugno 2005, n. 139). Per residenza deve necessariamente intendersi l'indirizzo completo di residenza anagrafica, rilevante sia ai fini dell'iscrizione e della permanenza nell'albo, anche in considerazione dei poteri di vigilanza disciplinare spettanti all'ordine, sia ai fini civilistici e processuali. Per tali ragioni, l'Ufficio ha ritenuto di non dover promuovere iniziative per l'adozione di specifici provvedimenti da parte del Collegio (nota 5 giugno 2012).

16.2. ORGANISMI DI MEDIAZIONE

Il d.lgs. 4 marzo 2010, n. 28 disciplina e configura come obbligatoria -in termini giudicati incostituzionali dalla Corte costituzionale con sentenza n. 272 del 6 dicembre 2012- la mediazione finalizzata alla conciliazione delle controversie civili e commerciali per chi intenda esercitare in giudizio un'azione nelle materie ivi previste. La mediazione è volta ad assistere due o più soggetti sia nella ricerca di un accordo amichevole per la composizione di una controversia, sia nella formulazione di una proposta per la risoluzione della stessa. Il procedimento è gestito da organismi di mediazione, costituiti da enti

pubblici o privati che, all'atto della presentazione della domanda di mediazione, designano un mediatore o più mediatori ausiliari.

L'Autorità è intervenuta al fine di assicurare che, nell'ambito di tale procedimento, siano rispettate tutte le garanzie previste dalla normativa di settore a tutela, in particolare, dei dati sensibili (si pensi, ad es., ai procedimenti inerenti il risarcimento del danno da responsabilità medica e da diffamazione) e giudiziari (quali i dati relativi a sentenze di condanna in base alle quali si può richiedere il risarcimento del danno) riferiti alle parti della mediazione e ad altri soggetti eventualmente coinvolti nel procedimento stesso.

In tale quadro e con specifico riferimento ai soggetti pubblici che intendano costituire un organismo di mediazione, con apposito provvedimento del Garante, in collaborazione con il Ministero della giustizia, sono stati identificati i tipi di dati che possono essere trattati e le operazioni eseguibili per il perseguimento della rilevante finalità di far valere il diritto di difesa (art. 71, comma 1, lett. *b),* del Codice; provv. 21 aprile 2011 [doc. web n. 1809039]). Gli enti pubblici che intendano costituire un organismo di mediazione, nell'adeguare il proprio regolamento per il trattamento dei dati sensibili e giudiziari -che ciascun soggetto pubblico deve avere adottato ai sensi dell'art. 20 del Codice- possono, quindi, avvalersi del documento allegato al predetto provvedimento, senza richiedere all'Autorità un parere specifico per poter trattare dati sensibili e giudiziari per l'attività degli organismi di mediazione (artt. 20, comma 2, e 21, comma 2, del Codice).

Nell'ipotesi in cui i suddetti organismi siano costituiti da soggetti privati, il Garante ha autorizzato il trattamento di dati sensibili delle parti coinvolte nell'attività di mediazione finalizzata alla conciliazione delle controversie civili e commerciali con un provvedimento di carattere generale, con il quale sono stati stabiliti i princìpi e le misure per il corretto trattamento di tali dati (provv. 21 aprile 2011 [doc. web n. 1808658]).

Gli organismi di mediazione pubblici e privati, il Ministero della giustizia e gli enti di formazione di cui all'art. 16, comma 5, del d.lgs. 4 marzo 2010, n. 28 e successive modificazioni e integrazioni, e all'art. 1, comma 1, lett. *n),* del d.m. n. 180/2010, sono stati autorizzati, inoltre, sempre con un provvedimento di natura generale, a trattare i dati giudiziari per la verifica dei requisiti di onorabilità di soci, associati, amministratori e

rappresentanti degli organismi di mediazione e degli enti di formazione di natura privata, nonché dei singoli mediatori (provv. 21 aprile 2011 [doc. web n. 1808676]).

I titolari dei trattamenti che rientrano nell'ambito di applicazione di entrambe le autorizzazioni generali -efficaci fino al 30 giugno 2012- e che intendano effettuare un trattamento di dati sensibili e/o giudiziari, conforme alle prescrizioni in esse contenute, non sono tenuti a presentare una specifica richiesta di autorizzazione a questa Autorità.

16.3. ATTIVITÀ FORENSE E INVESTIGATIVA

Nel corso del 2012 sono pervenute all'Autorità numerose segnalazioni relative al trattamento di dati personali nell'ambito dell'attività forense e investigativa, effettuato "*per far valere o difendere in sede giudiziaria un diritto*".

Utilizzo dei dati depositati in giudizio

Nel fornire riscontro a un quesito posto da un avvocato riguardante la legittimità dell'utilizzo di dati personali depositati dalla controparte in giudizio, il Garante ha chiarito che per lo svolgimento di indagini difensive di cui alla l. n. 397/2000 o, comunque, per far valere o difendere un diritto in sede giudiziaria (artt. 13, comma 5, lett. *b)* e 24, comma 1, lett. *f)*, del Codice), l'informativa all'interessato e il suo consenso non sono richiesti, sempre che i dati siano trattati esclusivamente per tali finalità e per il periodo strettamente necessario al loro perseguimento (nota 2 aprile 2012).

Comunicazione dei dati a terzi

A diversa conclusione il Garante è giunto riguardo a una segnalazione con cui l'interessata, parte in un procedimento giudiziale di separazione, aveva contestato la condotta dell'avvocato del coniuge per aver trasmesso ad una struttura alberghiera, insieme a una richiesta di informazioni concernente l'interessata e la figlia, anche la copia integrale del ricorso in appello, contenente dati sensibili dell'interessata medesima. Non risultando la comunicazione di dati necessaria a far valere o difendere un diritto in sede giudiziaria, l'Autorità ha ritenuto il trattamento non conforme agli artt. 13, comma 5, lett. *b)* e 24, comma 1, lett. *f)*, del Codice, avendo comportato una comunicazione di dati anche sensibili dell'interessata a soggetto non legittimato a conoscerli senza il consenso della medesima. Poiché il trattamento aveva ormai esaurito i suoi effetti, non è stato adottato alcun provvedimento prescrittivo o inibitorio ai sensi dell'art. 143, comma 1, del Codice (artt. 12, comma 4 e 14, comma 2, del Regolamento

n. 1/2007 del 14 dicembre 2007), salva la valutazione da parte dell'Autorità della ricorrenza di violazioni amministrative (nota 6 giugno 2012).

L'Autorità ha deciso in maniera analoga una segnalazione concernente il trattamento svolto dall'*ex* avvocato del segnalante, parte in un procedimento giudiziale di separazione, che aveva comunicato al legale del coniuge non solo la rinuncia al mandato, ma anche la notula delle prestazioni fornite al segnalante, in tal modo effettuando una comunicazione di dati personali a soggetto non legittimato a conoscerli senza il consenso dell'interessato (nota 19 settembre 2012).

In un'altra segnalazione l'interessato lamentava di aver ricevuto una raccomandata con avviso di ricevimento recante sulla busta anche il suo *status* di "fallito in proprio" e "legale rappresentante di una società fallita".

Il Garante ha ritenuto che l'indicazione dello *status* di fallito sulla busta risultasse eccedente (ai sensi dell'art. 11, lett. *d),* del Codice) rispetto alla finalità adottata dall'avvocato mittente di assicurare la presenza dell'interessato all'udienza fissata per l'approvazione del rendiconto di gestione, secondo quanto previsto dall'art. 116 della legge fallimentare e ha pertanto invitato il professionista a conformare pienamente le operazioni di trattamento alle disposizioni del Codice, evitando il ripetersi di episodi analoghi (nota 9 febbraio 2012).

In un altro caso, un pubblico dipendente aveva lamentato l'invio, da parte di un'avvocatura distrettuale dello Stato, di una sentenza di un Tar relativa ad una controversia tra il segnalante e l'amministrazione sua datrice di lavoro e contenente dati sensibili dell'istante, non all'ufficio territoriale dove l'esponente prestava servizio, bensì all'ufficio di una circoscrizione territoriale diversa. Nel fornire riscontro, il Garante ha rappresentato che la comunicazione dei dati sensibili effettuata ad un ufficio diverso da quello legittimato a conoscerli, risultava non conforme a quanto prescritto dall'art. 20 del Codice che ammette il trattamento dei dati sensibili da parte di soggetti pubblici.

Poiché il trattamento aveva ormai esaurito i suoi effetti, non si è proceduto all'adozione di un provvedimento prescrittivo o inibitorio ai sensi dell'art. 143, comma 1, del Codice (artt. 12, comma 4 e 14, comma 2, del Regolamento n. 1/2007 del 14 dicembre 2007), salva la valutazione da parte dell'Autorità della ricorrenza di violazioni amministrative (nota 22 marzo 2012).

Un interessato ha lamentato che l'avvocato della sua *ex* coniuge aveva inviato una diffida diretta nei suoi confronti, contenente informazioni riservate di carattere patrimoniale e familiare, al legale che lo aveva assistito nel corso del procedimento per la cessazione degli effetti civili del matrimonio, il cui mandato, a suo dire, si era esaurito con la definizione del procedimento.

Invitato a fornire chiarimenti, l'avvocato della donna, consapevole delle sanzioni penali previste in caso di inosservanza dell'art. 168 del Codice, ha dichiarato che l'intimazione aveva ad oggetto l'attuazione degli obblighi anche economici fissati dalla sentenza di divorzio e che il destinatario risultava essere ancora il legale di fiducia del segnalante. Sulla scorta anche della deliberazione del competente consiglio dell'ordine degli avvocati, che ha archiviato la segnalazione, l'Autorità non ha ravvisato violazioni della disciplina in materia di protezione dei dati personali (nota 5 ottobre 2012).

Diffusione di dati

È stata lamentata la divulgazione da parte di un avvocato, tramite pubblicazione su un sito internet, di un atto prodotto in giudizio dall'interessato e relativo ad un procedimento giudiziale in corso, riguardante anche l'avvocato suddetto. Dall'istruttoria è risultato che la pubblicazione rientrava tra i trattamenti finalizzati alla manifestazione del pensiero, che possono essere effettuati anche senza il consenso dell'interessato rispettando i limiti del diritto di cronaca e, in particolare, quello dell'essenzialità dell'informazione riguardo a fatti di interesse pubblico (art. 137, commi 2 e 3, del Codice). Il documento pubblicato riguardava, infatti, un giudizio che aveva assunto un rilevante interesse pubblico non solo nell'ambito professionale, essendo stato trattato anche da organi di stampa; e non era risultato violato il principio di essenzialità dell'informazione, in quanto l'atto pubblicato non conteneva dati o elementi da ritenersi non essenziali rispetto alla sottesa vicenda di pubblico interesse. Il Garante non ha, pertanto, ravvisato violazioni della disciplina in materia di protezione dei dati personali (nota 26 luglio 2012).

Accesso agli atti amministrativi

Con riferimento ad un quesito presentato da un avvocato relativamente alle modalità attraverso cui è consentito ottenere da un istituto pubblico notizie relative alla posizione lavorativa di un debitore di una sua assistita, il Garante ha ricordato che in tema di accesso agli atti amministrativi il Codice sancisce che i presupposti, le modalità, i limiti e la tutela

giurisdizionale in materia di accesso restano disciplinati dalla l. 7 agosto 1990, n. 241 (artt. 59 e 60 del Codice). Nel caso di specie, poiché l'istanza era stata respinta, il Garante ha evidenziato la possibilità di presentare ricorso al tribunale amministrativo regionale ovvero chiedere alla commissione per l'accesso ai documenti amministrativi di riesaminare la determinazione, come prescritto dall'art. 25 della l. n. 241/1990, salvi i poteri istruttori del giudice competente nella causa in corso (nota 17 ottobre 2012).

Accesso per finalità di difesa a dati detenuti da terzi

Il Garante ha in più occasioni chiarito la posizione dei soggetti che detengono per legge o per contratto dati personali di terzi rispetto a richieste di accesso presentate da avvocati o investigatori privati "*per far valere o difendere in sede giudiziaria un diritto*".

In un caso, l'interessata aveva posto all'attenzione dell'Autorità una richiesta di informazioni presentata ad una società di abbigliamento volta a conoscere, in particolare, se un debitore dell'interessata risultasse essere dipendente della società che forniva la vigilanza presso la detta società di abbigliamento. Al riguardo, il Garante ha evidenziato che la disciplina in materia di protezione dei dati personali, pur esonerando chi intende raccogliere dati personali presso terzi "*per far valere o difendere un diritto in sede giudiziaria*" dal fornire l'informativa all'interessato e acquisire il suo consenso (artt. 13, comma 5, lett. *b)* e art. 24, comma 1, lett. *f)*, del Codice), non pone a carico del soggetto destinatario della richiesta l'obbligo di fornire informazioni. Tale soggetto resta invece tenuto, in qualità di titolare del trattamento, a rispettare la disciplina in materia di protezione dei dati personali e a valutare l'opportunità e la liceità di rilasciare informazioni concernenti soggetti terzi (nota 13 febbraio 2012).

In un'analoga vicenda, un avvocato aveva contestato il rigetto, giustificato da motivi di *privacy*, delle richieste di informazioni presentate ad alcune compagnie telefoniche concernenti le intestazioni di numeri telefonici di utenze fisse e mobili relative ad atti d'indagine e procedimenti penali in corso. Anche in tale vicenda, è stato evidenziato che il Codice non pone a carico dei titolari del trattamento alcun obbligo a comunicare, ancorché a soggetti qualificati, i dati personali richiesti, trattandosi semmai di una facoltà da esercitare tenendo conto delle garanzie che l'ordinamento giuridico appresta per gli interessati. A tal fine, come chiarito nel provvedimento del 23 maggio 2001 [doc. web n. 39821] "*il titolare del trattamento, oltre a valutare l'effettiva necessità della comunicazione ai fini dell'esercizio del diritto*