11.5. *La pubblicazione* online *di dati personali riferiti ai dipendenti*

In più occasioni (v. anche par. 4.4) il Garante è stato chiamato a pronunciarsi sulla pubblicazione *online*, sui siti istituzionali degli enti pubblici ovvero nell'ambito delle sezioni dedicate all'albo pretorio, di dati, atti o provvedimenti contenenti dati personali (anche sensibili) riferiti a lavoratori o a partecipanti a concorsi e prove selettive.

Occupandosi della lamentata pubblicazione sul sito web di un'azienda per i servizi sanitari di un provvedimento con il quale veniva assunta la determinazione di recedere da un contratto individuale di lavoro, il Garante ha affermato che la determinazione aziendale, suscettibile di pubblicazione in base alla disciplina di settore, era stata tuttavia diffusa sul web nella versione integrale – che riportava, senza alcuna necessità, "in chiaro" l'identità del dipendente –, in violazione dei principi di pertinenza e non eccedenza nel trattamento dei dati personali di cui all'art. 11, comma 1, lett. *d*), del Codice (provv. 1° agosto 2013, n. 382, doc. web n. 2578588; nello stesso senso si è peraltro di recente pronunciata, su una decisione dell'Autorità, Cass. civ., sez. I, 20 luglio 2012, n. 12726 – confermando provv. 9 dicembre 2003, doc. web n. 1054649 – che aveva ritenuto illecita la diffusione da parte di un Comune delle generalità di un proprio dipendente nell'avviso pubblico di convocazione del consiglio comunale nel quale avrebbe formato oggetto di discussione una procedura esecutiva che lo riguardava). Sempre in tale caso, dagli accertamenti effettuati attraverso il motore di ricerca dell'albo aziendale *online* era altresì emerso che, inserendo gli estremi identificativi dell'interessato, una volta rimossa la delibera dal sito, persisteva comunque la possibilità di risalire all'"oggetto" della stessa contenente espressa indicazione del nominativo dell'*ex* dipendente. Pertanto, anche con riguardo a tale secondo profilo, l'Autorità ha dichiarato illecito il trattamento posto in essere dall'azienda e vietato l'ulteriore diffusione delle informazioni riferite all'interessato, atteso che, per il periodo eccedente i 15 giorni previsti dalla disciplina di settore, si era determinata una diffusione illecita di dati personali (artt. 11, comma 1, lett. *a*) e 19 comma 3, del Codice). Come più volte ribadito dal Garante, infatti, trascorsi i periodi di tempo specificatamente individuati dalla disciplina di settore, i dati devono essere rimossi dal web o privati degli elementi identificativi degli interessati (sul punto cfr. par. 5.2, richiamato dal par. 6.B linee guida in materia di trattamento di dati personali contenuti anche in atti e documenti amministrativi, effettuato da soggetti pubblici per finalità di pubblicazione e diffusione sul web, provv. 2 marzo 2011, n. 88, doc. web n. 1793203).

In altri casi ha formato oggetto di segnalazione la pubblicazione, sui siti web istituzionali di istituti scolastici nonché di altri uffici periferici del Ministero dell'istruzione dell'università e della ricerca, di graduatorie relative al personale docente ovvero al personale amministrativo tecnico ed ausiliario (cd. ATA) contenenti dati personali eccedenti e non pertinenti (quali codice fiscale, domicilio e recapiti telefonici degli interessati): in tali fattispecie, il Garante ha ritenuto illecita la diffusione dei dati eccedenti e non pertinenti rispetto alla finalità di pubblicità delle graduatorie (cfr. provv.ti 6 giugno 2013, n. 275, doc. web n. 2536184; n. 276, doc. web n. 2536409; n. 274, doc. web n. 2535862, in linea con le indicazioni dell'Autorità nelle linee guida del 3 marzo 2011, doc. web n. 1793203). Tale valutazione, peraltro, trova riscontro anche nell'indirizzo recepito dal Ministero dell'istruzione (peraltro interessato della vicenda) – dapprima con circolare del 7 marzo 2008 (prot. 45/dip./segr.) e, da ultimo, del 22 gennaio 2013 (prot. n. AOODGPER510 – Uff. III), diramate alle articolazioni territoriali concernenti la corretta messa a disposizione sul web dei dati personali detenuti dal Sistema informativo centrale del Ministero-SIDI –, anche in considerazione della presenza, all'interno delle citate graduatorie, di dati personali riferiti a un numero elevato di interessati.

In altro caso, concernente la diffusione mediante pubblicazione sul web, a far data dal 2010, di informazioni (segnatamente, l'elenco dei candidati ammessi alla prova scritta, all'esame orale e il diario delle prove), concernenti lo stato di disabilità di un segnalante e di altri partecipanti ad un concorso riservato ai disabili (ai sensi dell'art. 1, l. n. 68/1999, normativa concernente "il diritto al lavoro dei disabili"), l'Autorità, riservandosi di verificare con separato procedimento la sussistenza dei presupposti per le contestazioni delle sanzioni amministrative conseguenti all'illecito trattamento, ha vietato l'ulteriore diffusione su internet dei dati dei soggetti interessati contenuti nelle graduatorie (provv. 6 giugno 2013, n. 277, doc. web n. 2554965). Tanto, in base al divieto di diffusione dei dati idonei a rivelare lo stato di salute (art. 22, comma 8, del Codice) – la cui violazione è stata già stigmatizzata più volte dal Garante (cfr. par. 4.4) – quali le condizioni di invalidità, disabilità o handicap fisici e/o psichici (cfr. provv.ti 22 novembre 2012, doc. web n. 2194472; 29 novembre 2012, doc. web n. 2192671; 7 ottobre 2009, doc. web n. 1664456; 17 settembre 2009, doc. web n. 1658335; 25 giugno 2009, doc. web n. 1640102; 8 maggio 2008, doc. web n. 1521716; 18 gennaio 2007, doc. web n. 1382026; 27 febbraio 2002, doc. web n. 1063639).

12 Le attività economiche

12.1. *Il settore bancario*

Con provvedimento del 28 novembre 2013, n. 533 (doc. web n. 2801010), il Garante è tornato a pronunciarsi sul delicato tema del rapporto tra normativa antiriciclaggio e disciplina di protezione dei dati personali. Traendo spunto da una segnalazione – che aveva evidenziato, nell'ambito delle doverose verifiche effettuate da un ufficio postale ai sensi del d.lgs. n. 231/2007, l'espletamento di controlli su rapporti anche privati intrattenuti dall'interessato con Poste Italiane s.p.a., benché lo stesso operasse nella veste di mero esecutore materiale di un'operazione per conto di un Comune – l'Autorità ha ricordato come i controlli in materia di antiriciclaggio devono essere effettuati rispettando le garanzie previste dalla normativa sulla riservatezza ed essere proporzionati al profilo di rischio del cliente e alle caratteristiche dell'operazione da effettuare. Nel caso esaminato, il segnalante (già conosciuto dalla direttrice dell'ufficio postale) era stato incaricato di effettuare, in rappresentanza del Comune presso cui lavorava, l'acquisto, per poche migliaia di euro, di buoni lavoro da assegnare ad alcuni pensionari; in tale occasione, l'incaricata dell'ufficio postale, anziché limitarsi a identificarlo come semplice esecutore di un'operazione riconducibile all'ente locale, aveva effettuato una verifica nei suoi confronti volta ad analizzare anche i rapporti personali dal medesimo intrattenuti con la società. Nell'accogliere i rilievi formulati dall'istante, il Garante ha ritenuto illecito il trattamento effettuato da Poste Italiane s.p.a., avendo quest'ultima disatteso il principio dell'"approccio basato sul rischio" fissato dalla normativa vigente e svolto verifiche obiettivamente eccedenti e non giustificate dal basso "profilo di rischio" associabile all'interessato e al tipo di operazione richiesta. Il Garante ha quindi prescritto alla società di adottare, al di là del caso di specie, opportune misure formative e tecnico-organizzative in grado di prevenire operazioni di trattamento dei dati personali dei clienti che, nell'ambito dell'espletamento dei doverosi controlli richiesti dalla normativa in materia di antiriciclaggio, non siano conformi al criterio dell'"approccio basato sul rischio" fissato dall'art. 20, d.lgs. n. 231/2007.

A seguito del provvedimento n. 192 adottato dal Garante il 12 maggio 2011 in mareria di circolazione delle informazioni in ambito bancario e di tracciamento delle operazioni bancarie (in G.U. 3 giugno 2011, n. 127, doc. web n. 1813953) – con il quale l'Autorità ha prescritto adeguate misure volte a impedire accessi indebiti ai dati personali (informazioni bancarie) degli interessati –, è proseguita l'interlocuzione con l'Associazione bancaria italiana (Abi). Quest'ultima, infatti, unitamente a Poste Italiane s.p.a., ha presentato all'Autorità alcuni quesiti in merito all'implementazione delle misure prescritte nel provvedimento nonché una richiesta di differimento del termine per completare l'attuazione delle citate prescrizioni. All'esito dell'attività svolta, il Garante ha adottato il provvedimento n. 357 in data 18 luglio 2013 (doc. web n. 2573636), con il quale, nel rimettere ai titolari del trattamento la valutazione delle soluzioni organizzative più idonee per l'implementazione del sistema, ha fornito i chiarimenti richiesti, in particolare con riferimento all'ambito oggettivo e soggettivo di applicazione del provvedimento precedentemente adottato, accogliendo altresì la richiesta avanzata da Abi di differire l'applicazione del provvedimento, precedentemente fissata al 3 dicembre 2013, al 3 giugno 2014.

Alcune banche hanno presentato richieste di verifica preliminare per avvalersi della rilevazione delle impronte digitali per l'accesso dei clienti alle proprie cassette di sicurezza. Tale sistema avrebbe consentito ai clienti che avessero scelto di utilizzarlo, di potere accedere alle cassette di sicurezza, in modalità *self-service*, 24 ore su 24. La banca avrebbe offerto, quindi, ai propri clienti, due distinte modalità di accesso: quella con il sistema biometrico oppure quella con modalità tradizionali (*smartcard* e *pin*). Nel primo caso, il cliente avrebbe rilasciato l'impronta digitale, appoggiando il dito su un apposito lettore che avrebbe generato "un algoritmo matematico univoco ed irripetibile", memorizzato su una *smartcard* consegnata al cliente con il relativo *pin*, da utilizzare al momento dell'accesso. Non sarebbe stata prevista la conservazione dei dati biometrici raccolti, né da parte della banca, né in archivi centralizzati. Sul solco dei provvedimenti già adottati (cfr. provv. 13 settembre 2012, n. 242, doc. web n. 1927441 e provv. 18 ottobre 2012, n. 298, doc. web n. 2212554 richiamati nella Relazione 2012, p. 199), il Garante ha ribadito la liceità della finalità perseguita e la proporzionalità del trattamento dei dati personali, prescrivendo specifiche misure a garanzia degli interessati (cfr. provv. 14 febbraio 2013, n. 66, doc. web n. 2375735; provv. 19 settembre 2013, n. 106, doc. web n. 2710934). In particolare, oltre all'informativa che deve chiaramente indicare la possibilità per gli interessati di avvalersi del servizio relativo alle cassette di sicurezza con modalità alternative rispetto alla rilevazione dei loro dati biometrici, l'Autorità ha prescritto agli istituti di credito l'adozione di specifici accorgimenti, quali la designazione degli incaricati del trattamento, la conservazione di una descrizione scritta dell'intervento effettuato dall'installatore che attesti anche la conformità del sistema alle disposizioni del disciplinare tecnico (regola n. 25 dell'Allegato B al Codice) nonché la notifica al Garante del trattamento dei dati biometrici prima dell'inizio delle operazioni di trattamento (art. 37, comma 1, *lett. a)*, del Codice).

Sono infine pervenute segnalazioni e reclami concernenti la comunicazione a terzi di informazioni bancarie dei clienti da parte dei dipendenti in assenza del preventivo consenso degli interessati (art. 23 del Codice) e in mancanza di uno dei suoi equipollenti (art. 24). Al riguardo, quando tali comunicazioni sono risultate connesse ad indebiti accessi da parte di dipendenti, si è rinviato a quanto disposto con il citato provvedimento del 12 maggio 2011, precisando che, allo stato, il provvedimento non trova ancora completa attuazione per mancata decorrenza del termine fissato dal Garante per l'implementazione delle misure. A tale proposito, il Garante ha tuttavia ritenuto illecita la comunicazione ad un professionista di dati bancari riferiti ad un correntista (con il quale il primo aveva collaborato in passato e che lo aveva indirizzato presso la banca per richiedere un finanziamento), perché risultato sprovvisto di poteri rappresentativi ed in assenza del preventivo consenso dell'interessato (art. 23 del Codice) nonché di altro requisito equipollente (art. 24), in violazione del principio di liceità e correttezza di cui all'art. 11, comma 1, lett. *a)*, del Codice (cfr. provv. 18 dicembre 2013, n. 588, doc. web n. 2896472). Per tale motivo il Garante ha prescritto alla banca di adottare misure necessarie per assicurare che la comunicazione a terzi dei dati personali di coloro che entrino in contatto con l'istituto avvenga solo con il consenso degli interessati (art. 23 del Codice) o, in difetto, in presenza di uno dei presupposti equipollenti indicati dall'art. 24 del Codice, impartendo, a tal fine, anche adeguate istruzioni ai responsabili e agli incaricati del trattamento.

Infine, con provvedimento del 27 giugno 2013, n. 318 (doc. web n. 2577071), è stato dichiarato illecito il trattamento dei dati personali posto in essere da una banca che, nell'ambito di un procedimento giudiziario presso l'Arbitro bancario e finanziario (Abf), promosso nei suoi confronti da parte di alcuni clienti, non si era limitata a formulare eccezioni di rito o a contestare nel merito le argomentazioni poste dai ricorrenti a fondamento delle proprie pretese, ma aveva riportato fatti riferibili al pro-

curatore delle stesse parti, relative alla risoluzione dell'originario rapporto lavorativo tra la banca e lo stesso procuratore e alla successiva instaurazione di una vertenza dinanzi al giudice del lavoro. Al riguardo, il Garante ha ritenuto tali informazioni eccedenti rispetto alle concrete esigenze difensive della resistente, perché volte non tanto a dimostrare la eventuale scarsa attendibilità delle affermazioni rese dai ricorrenti, quanto a rendere un'immagine negativa, per fatti extraprocessuali e, comunque, estranei alla materia del contendere, del loro procuratore. Ciò ha comportato la violazione dell'art. 11 del comma 1, lett. *a*) e *d*), del Codice, con conseguente inutilizzabilità dei dati stessi (art. 11, comma 2).

Recupero crediti

Viste le numerosissime segnalazioni che sono continuate a pervenire, nonostante la vigenza del provvedimento generale adottato dal Garante il 30 novembre 2005 (doc. web n. 1213644), l'Autorità ha avviato un'attività istruttoria tesa a verificare non solo la liceità del trattamento dei dati personali posto in essere dalle società che svolgono, eventualmente in qualità di "responsabili del trattamento", le concrete attività di recupero crediti, ma anche in che termini le società creditrici, ove titolari, vigilino sull'operato delle predette.

All'esito degli accertamenti, il Garante ha adottato due provvedimenti, con i quali ha inibito l'uso di forme di comunicazione ritenute lesive della dignità dei debitori. Con il primo (cfr. provv. 11 aprile 2013, n. 181, doc. web n. 2497407), il Garante, nel ribadire i principi già affermati con il citato provvedimento del 2005, ha rilevato l'illiceità del comportamento della società incaricata di procedere al recupero del credito, la quale, nel tentativo di contattare la debitrice, aveva interloquito con il figlio e la nuora di costei, rendendoli edotti – in carenza di consenso dell'interessata – dell'esistenza di alcuni ratei di un finanziamento non pagati e del loro complessivo ammontare. Nella medesima fattispecie, il Garante, procedendo ad una attenta valutazione delle concrete attività svolte dall'appaltatore nella gestione del recupero crediti, anche sulla base dei compiti e delle responsabilità previste dallo specifico contratto di servizio, ha altresì riconosciuto che la qualifica di "titolare del trattamento", contrariamente a quanto stabilito nel contratto, poteva essere attribuita solo alla banca creditrice, risultando solo quest'ultima titolare del potere di assumere decisioni sulle finalità e modalità del trattamento svolto dalla società appaltatrice, di impartire istruzioni e direttive vincolanti, nonché di effettuare pregnanti controlli sull'operato della medesima.

Con il secondo provvedimento del 10 ottobre 2013, n. 445 (doc. web n. 2751860), invece, il Garante ha dichiarato illecito il trattamento dei dati personali effettuato a mezzo di "comunicazioni telefoniche preregistrate volte a sollecitare il pagamento", in quanto – come affermato dal provvedimento generale del 2005 – "suscettibile di rendere edotti soggetti diversi dal debitore della sua asserita condizione di inadempimento".

In particolare, l'Autorità, dando seguito ad una segnalazione concernente alcuni solleciti di pagamento preregistrati inviati da una banca, ha ritenuto che il sistema utilizzato non garantisse l'accertamento dell'identità di colui che rispondeva alla chiamata, né desse certezze circa il diritto di costui di venire a conoscenza delle informazioni inerenti la posizione debitoria dell'effettivo interessato. Detto sistema, infatti, limitandosi a rimettere all'interlocutore la sola facoltà di effettuare "una dichiarazione espressa di identificazione", non era idoneo ad assicurare che le informazioni veicolate attraverso le comunicazioni telefoniche preregistrate potessero essere ricevute dall'effettivo avente diritto (debitore o soggetti da costui autorizzati), con conseguente violazione non solo dei principi posti dalla disciplina sulla protezione dei dati personali, ma anche delle specifiche prescrizioni impartite dal Garante con il provvedimento generale del 2005. In tale occasione, comunque, il Garante ha precisato che l'utilizzo, a fini di recupero crediti, di un sistema basato su solleciti di pagamento preregistrati

non integra di per sé un trattamento illecito di dati, potendo essere utilizzato in presenza di idonei accorgimenti tecnici – basati anche su forme di autenticazione – tali da assicurare la ragionevole certezza che la presa di conoscenza delle informazioni oggetto di comunicazione avvenga solranto da parte di chi ne possa essere il legittimo destinatario (il debitore o terzi da lui autorizzati).

12.2. *Il settore assicurativo*

In attuazione del novellaro art. 135, d.lgs. n. 209/2005, il Garante è stato chiamato a rendere un parere (cfr. provv. 10 ottobre 2013, n. 441, doc. web n. 2725053) sullo schema di regolamento predisposto dall'Isrituro per la vigilanza sulle assicurazioni (Ivass) relativamente al funzionamento della "banca dati sinistri" e delle neocostituite "anagrafe testimoni" e "anagrafe danneggiati", funzionali a rendere più efficace la prevenzione e il contrasto alle frodi nel settore delle assicurazioni Rc auto. Al riguardo il Garante, pur condividendo, di massima, l'impostazione del testo sottoposto alla sua attenzione (principalmente orienrara a consentire accessi selettivi alle diverse tipologie di informazioni contenute nel proprio archivio informatico), ha tuttavia formulato alcune raccomandazioni all'Istituto, volte a rendere maggiormente aderenti ai dettami del Codice le adottande disposizioni regolamentari. In particolare, è stato suggerito all'Ivass di circoscrivere l'accesso alla banca dati per le sole finalità di prevenzione e contrasto dei fenomeni fraudolenri nel settore considerato, nonché di cancellare (previo riversamento su altro supporto informatico) i dati identificarivi degli interessati ivi memorizzati decorsi 5 anni dalla data di definizione dei sinistri.

Inoltre, nell'ottica di dare concreta attuazione ai principi di finalità e di trasparenza, il Garante ha raccomandato all'Ivass – benché quest'ultimo non sia a ciò tenuto, in base alle disposizioni vigenti – di dare evidenza dell'esistenza dei menzionati archivi (e dei connessi trattamenti di dari personali) a coloro chc, a vario titolo, possono trovarsi coinvolti in un sinistro, informando sinteticamente gli interessati già in occasione della compilazione del modulo di "Constatazione amichevole di incidente-denuncia di sinistro"; tale soluzione, infatti, potrebbe agevolare la conoscibilità di tali banche dati, accentuandone l'effetto dissuasivo in rapporto a possibili comportamenti fraudolenti.

Infine, con provvedimento del 10 gennaio 2013, n. 5 (doc. web n. 2367235), l'Autorità si è pronunciara sulla liceità della comunicazione a terzi (nel caso di specie, l'ex coniuge della segnalante), da parte di una società assicuratrice, di dati personali (polizza assicurativa e assegno bancario) di un soggetto assicuratò. L'Autorità, accertata l'assenza del consenso dell'interessaro (art. 23 del Codice) e l'inesistenza di un suo equipollente (art. 24 del Codice), ha dichiarato illecito il trattamento, prescrivendo alla società di adottare adeguate misure per sensibilizzare gli incaricati del trattamento all'osservanza delle regole in materia di trattamento dei dati personali e per garantire alla socierà una scrupolosa vigilanza sull'operato di costoro.

12.3. *Autonoleggio ed* event data recorder

A seguito di un'istanza di verifica preliminare formulata ai sensi dell'art. 17 del Codice, l'Autorità è stata nuovamente chiamata a valutare la liceità dei trattamenti connessi all'installazione, a bordo del parco veicoli in dotazione a una società di autonoleggio, di dispositivi satellitari multifunzione annoverabili tra i cd. *event data recorder*. Tali dispositivi, in grado di raccogliere e trasmettere a un apposito centro servizi numerose informazioni relative alle singole vetture (e indirettamente, ai relativi

conducenti), sarebbero stati utilizzati dalla società per garantire alcuni servizi (gestione di eventuali sinistri; ritrovamento di veicoli rubati; assistenza stradale; raccolta dati ed elaborazione statistica; consultazione "storica" degli automezzi; monitoraggio chilometri; diagnostica) solo in parte – secondo quanto sostenuto – comportanti un trattamento di dati personali. All'esito di una complessa istruttoria, l'Autorità ha ammesso i trattamenti oggetto dell'istanza (provv. 7 novembre 2013, n. 499, doc. web n. 2911484), ritenendoli conformi – ove effettuati nel rispetto delle modalità indicate – ai princìpi di liceità, necessità, finalità e proporzionalità (artt. 3 e 11 del Codice); tuttavia, sono state prescritte alla società alcune misure e accorgimenti volti ad assicurare una maggiore tutela degli interessati, sia sul piano dell'informativa da rendere a costoro, sia in relazione all'adozione di ulteriori e più stringenti misure di sicurezza, in grado di garantire l'autenticità, l'accuratezza e l'integrità delle informazioni rilevate dai dispositivi satellitari. L'Autorità ha precisato, inoltre, che i dati trattati per le suddette finalità non potranno essere utilizzati dalla società per profilare i conducenti, né per negare la stipula di nuovi contratti di autonoleggio.

12.4. *La videosorveglianza in ambito privato*

Nel corso dell'anno, il Garante si è pronunciato in relazione a numerose istanze di verifica preliminare (art. 17 del Codice) presentate da alcune società, sia al fine di essere autorizzate a conservare le immagini registrate per tempi superiori alla settimana, sia in vista dell'impiego di sistemi cd. intelligenti.

Con provvedimento del 7 febbraio 2013, n. 40 (doc. web n. 2305006), l'Autorità si è espressa in relazione ad un istanza di verifica preliminare presentata da una società che, operando nel settore dei trasporti e della logistica, si occupa di spedizioni nazionali ed internazionali, compresi i servizi doganali. La richiesta di autorizzazione per il prolungamento dei tempi di conservazione fino a 30 giorni delle immagini registrate presso il magazzino era stata giustificata non solo con l'esigenza di rafforzare il livello di tutela della merce stoccata, ma anche con quella di raggiungere uno *standard* di sicurezza più elevato, in linea con quanto previsto dal sistema di certificazione volontaria sulla qualità e sicurezza dei servizi legati al trasporto della merce, gestito dall'associazione internazionale "*Transported asset protection association*" (TAPA), *standard* di riferimento per gli operatori del settore.

L'Autorità, nel rilevare l'obbligo della società – già titolare della qualifica di "agente regolamentato" e di quella di "operatore economico autorizzato" – ad osservare stringenti norme poste da regolamenti comunitari e, in via amministrativa, dall'Ente nazionale per l'aviazione civile (Enac), ha autorizzato la conservazione delle immagini per il periodo richiesto per consentire l'accertamento, da parte dell'autorità giudiziaria, di eventuali illeciti, rilevando, al contempo, che lo *status* di "operatore economico autorizzato" impone alla società che lo abbia conseguito di comunicare alla dogana eventuali sospetti di reato relativi alle spedizioni trattate e di tenere a disposizione della stessa Autorità le spedizioni su cui si ritenga di dover effettuare dei controlli.

Analoga autorizzazione (provv. 6 giugno 2013, n. 278, doc. web n. 2544109) è stata rilasciata in sede di verifica preliminare ad una società che svolge attività di smistamento, distribuzione, consegna e ritiro pacchi e corrispondenza per conto di società di trasporto allo scopo di conservare per 30 giorni le immagini registrate presso il magazzino; ciò, non solo perché spesso non sarebbe stato possibile risalire con tempestività all'identificazione di un pacco mancante o recante qualche anomalia, ma anche in ragione dell'esigenza di rispondere alle istanze provenienti dagli stessi vettori che, imponendo "una tempistica specifica per la consegna della merce", avreb-

bero reso indispensabile "implementare stringenti misure di sicurezza lungo tutta la filiera al fine di garantire la celerità del servizio" e l'integrità delle spedizioni.

Con il provvedimento del 7 marzo 2013, n. 104 (doc. web n. 2340448), l'Autorità si è pronunciata su una richiesta di verifica preliminare (art. 17 del Codice) di un'azienda produttrice di carta moneta per la realizzazione di banconote, al fine di poter conservare per dodici mesi le immagini acquisite attraverso il sistema di videosorveglianza attualmente in uso. La richiesta è stata fondata sul fatto che la Banca Centrale Europea (BCE), titolare esclusivo del potere di autorizzare l'emissione di banconote in euro all'interno della Comunità, ha imposto ai produttori di banconote euro "accreditati" di conservare, per almeno dodici mesi, le immagini registrate dai sistemi di sorveglianza installati presso i siti produttivi; pertanto, quale "fabbricante" di carta moneta, la società ha dichiarato di essere soggetta alla procedura di "accreditamento di sicurezza" (richiesta dalla BCE) ed al rispetto delle "norme di sicurezza minima per la produzione, l'elaborazione, la custodia e il trasporto delle banconote, delle loro componenti, nonché dei relativi altri materiali e informazioni che necessitano di protezione".

L'Autorità, nel rilevare che la società richiedente, in quanto produttrice di carta per la realizzazione di banconote, è soggetta sia alla disciplina posta dalla decisione del 15 maggio 2008, sia a tutte le ulteriori regole periodicamente emanate dalla BCE – tra le quali quelle di sicurezza minime appositamente emanate nei confronti delle aziende in possesso di accreditamento di sicurezza per la produzione di banconote (cd. *Security rules and procedures for manufacturers of euro secure items*, in vigore dal 2 giugno 2008) che, tra l'altro, impongono che le immagini registrate dagli impianti di videosorveglianza installati presso i siti produttivi vengano conservate "per almeno 12 mesi" (v. art. 10, comma 4) – ha deciso di accogliere la richiesta di allungamento dei tempi di conservazione delle immagini, ritenendola conforme ai principi di non eccedenza e di proporzionalità stabiliti dall'art. 11, comma 1, lett. *d*) ed *e*), del Codice.

Il Garante si è espresso su un'istanza di verifica preliminare (art. 17 del Codice) presentata da una società che opera nel settore dei servizi per l'industria petrolifera *onshore* e *offshore*, in vista dell'installazione di un sistema di videosorveglianza cd. intelligente (perché provvisto di un *software* di "analisi della scena") volto a migliorare il livello di sicurezza del patrimonio aziendale e dei lavoratori presso le proprie sedi. Effettuata un'attenta ricognizione del quadro normativo (d.lgs. 11 aprile 2011, n. 61, attuativo della direttiva 2008/114/CE, che ha individuato nelle infrastrutture del settore energetico una potenziale criticità, anche di rilievo comunitario; decreto del Ministero dell'interno 1° dicembre 2010, n. 269, Allegato D, sez. III, punto 3.b.1, che definisce "obiettivi sensibili" le aziende pubbliche o private del settore energetico) e amministrativo (nota del Prefetto di Milano prot. n. 12b2/09007582 N.C. Div. Gab., all. C) del 15 giugno 2013, che ha rilevato, a fronte di un incremento qualitativo e quantitativo degli eventi pericolosi avvenuti nelle sedi della società, la necessità di dotare il sito produttivo di adeguati sistemi di protezione, comprensivi anche di impianti di videosorveglianza intelligente), ha ritenuto che le infrastrutture delle compagnie operanti nel settore energetico possano costituire concreti obiettivi per azioni di sabotaggio e di terrorismo, ammettendo, quindi, l'attivazione presso i siti della società – e a supporto dei dispositivi di ripresa già esistenti – del sistema di video-analisi oggetto dell'istanza, ritenuto in linea con i principi posti dagli artt. 3 e 11 del Codice (provv. 18 aprile 2013, n. 202, doc. web n. 2475774).

Inoltre, con il provvedimento n. 230 dell'8 maggio 2013 (doc. web n. 2433401), l'Autorità ha affrontato la questione della liceità del trattamento delle immagini dei minori iscritti presso un asilo nido che aveva installato un sistema di videosorveglianza dotato di *webcam*, in grado di consentire ai genitori di controllare i propri

figli durante il periodo di permanenza al nido. L'Autorità, condividendo i principi già affermati dal Gruppo Art. 29 ha ritenuto che l'acquisizione, anche a mezzo *web-cam*, di immagini relative a soggetti in età minore e la loro visione, via web, da parte di terzi muniti di specifiche credenziali di autenticazione, costituiscano operazioni di trattamento di dati personali alle quali deve essere rivolta particolare attenzione. Nel merito, l'Autorità ha ritenuto che le esigenze perseguite dall'asilo nido con l'installazione del sistema (sicurezza delle persone e del patrimonio aziendale; necessità di soddisfare le esigenze rappresentate dai genitori) non fossero sufficienti a ritenere l'installazione della *webcam* necessaria e proporzionata, sottolineando, al contempo, come detto sistema potesse porre in serio pericolo gli interessati, non sussistendo alcuna certezza del fatto che la visione dei genitori fosse limitata ai propri figli e, comunque, che restasse circoscritta ai soli soggetti muniti di credenziali d'accesso al sistema. Pertanto, l'Autorità ha dichiarato illecito il trattamento delle immagini dei minori iscritti presso l'asilo nido, effettuato mediante *webcam* posizionata all'interno dell'area didattica, perché in violazione dei principi di necessità e proporzionalità (artt. 3 e 11, comma 1, lett. *a*) e *d*), del Codice).

Successivamente, con provvedimento del 24 ottobre 2013, n. 467 (doc. web n. 2792798), l'Autorità si è pronunciata su un'istanza di verifica preliminare presentata da una società che opera nel segmento della progettazione e della realizzazione di *card* a banda magnetica e *smartcard* (con *microchip contact* e *contactless*), per il mercato bancario e per i settori *retail*, ID, trasporti e telefonia, curando, in alcuni casi, anche la "personalizzazione" dei supporti. La richiesta di autorizzazione per il prolungamento dei tempi di conservazione fino a 90 giorni delle immagini registrate presso l'azienda è stata giustificata – oltre che con le esigenze di tutela della proprietà aziendale, delle persone e dei dati dei clienti – con la necessità di rispettare i parametri fissati dai circuiti internazionali *MasterCard International* e *Visa International*, che impongono alle società certificate presso di loro l'osservanza di un più elevato *standard* di sicurezza durante l'intero processo di lavorazione.

L'Autorità ha accolto la richiesta – con riferimento alle sole immagini attinenti le aree esterne ai locali, quelle di ingresso e di uscita e le zone ritenute "sensibili" (*caveau*, magazzino, aree di produzione, di ricevimento e di spedizione), e purché la loro utilizzazione avvenisse nel rispetto delle procedure delineate dall'art. 4, l. n. 300/1970 nonché all'esclusivo fine dell'accertamento di eventuali illeciti e dell'individuazione, da parte dell'autorità giudiziaria, dei possibili responsabili –, tenendo conto non solo dell'ubicazione del sito, degli episodi criminosi già verificatisi e dell'estrema delicatezza dell'attività produttiva, comportante l'esigenza di proteggere i dati personali di enormi masse di clienti, ma anche della circostanza che le stesse organizzazioni sindacali si erano espresse favorevolmente, anche in vista dell'indispensabile adeguamento della società alle richieste provenienti dagli stessi enti certificatori.

L'Autorità, infine, si è espressa su una richiesta di verifica preliminare presentata da una società proprietaria di numerose sale da gioco in cui si svolge "attività di raccolta di gioco" a mezzo di apparecchiature videoterminali (VLT) e, contestualmente, di raccolta di denaro per conto dello Stato e/o del Concessionario della rete telematica dell'Amministrazione Autonoma dei Monopoli di Stato (AAMS), allo scopo di conservare per 15 giorni le immagini acquisite attraverso il sistema di videosorveglianza in uso, per salvaguardare il patrimonio aziendale da possibili atti illeciti facilitando l'accertamento di eventuali illeciti commessi da parte delle autorità competenti.

Appurato che la società non avrebbe potuto effettuare il controllo delle monete con cadenze inferiori a 10/15 giorni e, al contempo, che l'esame delle registrazioni per ragioni tecniche ed organizzative non avrebbe potuto concludersi nell'arco di soli sette giorni, l'Autorità ha accolto la richiesta, in quanto conforme ai principi di

necessità, proporzionalità, finalità e correttezza posti dagli artt. 3 e 11 del Codice, precisando che l'accesso alle immagini sarebbe potuto avvenire soltanto in caso di diretta rilevazione di illeciti – con l'osservanza di prestabilite modalità procedurali indicate nei provvedimenti autorizzatori rilasciati ai sensi dell'art. 4, comma 2, l. n. 300/1970 dalle Direzioni territoriali del lavoro competenti – o di richiesta proveniente dalle Forze dell'ordine o dall'autorità giudiziaria (provv. 18 dicembre 2013, n. 587, doc. web n. 2914191).

12.5. *La biometria*

In ragione della proliferazione di sistemi in grado, tra l'altro, di rilevare le caratteristiche dinamiche della firma autografa (ritmo; velocità; pressione; accelerazione; movimento) apposta dai clienti in occasione della sottoscrizione di atti o documenti, l'Autorità è stata chiamata a valutare, nell'ambito di una verifica preliminare presentata da una banca operante solo *online* e per il tramite di promotori finanziari, il trattamento di dati personali e biometrici connesso a un servizio di "firma grafometrica" offerto alla clientela (provv. 12 settembre 2013, n. 396, doc. web n. 2683533). Il sistema, che nell'ottica prospettata integrerebbe i requisiti previsti per la firma elettronica avanzata (d.P.C.M. 22 febbraio 2013), risulterebbe in grado di "sigillare" elettronicamente, all'interno del documento informatico sottoscritto dal cliente, i dati biometrici raccolti dai dispositivi (*tablet*) in dotazione ai promotori, sì da consentire *ex post*, ove richiesto dall'autorità giudiziaria, lo svolgimento di specifiche perizie calligrafiche sulla genuinità della sottoscrizione.

Nel valutare positivamente il trattamento – basato sul libero consenso degli interessati ed effettuato, oltre che nel rispetto dei principi di necessità e proporzionalità, per perseguire finalità lecite rese previamente note agli interessati (artt. 3, 11, 13 e 23 del Codice) –, l'Autorità ha evidenziato che la soluzione proposta (conforme anche agli *standard* ISO) poteva effettivamente contribuire – attraverso la garanzia di autenticità, non ripudio e integrità dei documenti sottoscritti elettronicamente – a conferire maggiore certezza nei rapporti giuridici intercorrenti con gli utenti; nondimeno, ha ritenuto opportuno indicare ulteriori misure a tutela degli interessati, considerato l'impiego "in mobilità" dei dispositivi e la loro possibile utilizzabilità per finalità (e in contesti) ulteriori rispetto a quelli considerati. In particolare, oltre all'adozione di idonee misure volte a ridurre i rischi di alterazione dei dispositivi e di installazione di *software* o applicazioni non autorizzati e potenzialmente pericolosi, è stato prescritto l'impiego di presidi tecnico-organizzativi in grado di assicurare la cancellazione "da remoto" delle informazioni in caso di loro smarrimento o sottrazione. Il Garante ha inoltre sottolineato la necessità che la banca preveda adeguate *policy* per la gestione di eventuali incidenti di sicurezza nell'ambito delle diverse fasi del processo di acquisizione della firma grafometrica.

13 Il trasferimento dei dati all'estero

Con riferimento ai flussi transfrontalieri di dati personali, l'attività del Garante si è caratterizzata sia sul versante delle autorizzazioni ai trasferimenti di dati personali verso Paesi terzi mediante norme vincolanti d'impresa (*Binding corporate rules* - BCR), sia sul piano delle autorizzazioni di carattere generale volte all'attuazione delle decisioni della Commissione europea sull'"adeguatezza" della normativa di protezione dei dati di Paesi non appartenenti all'UE.

In ordine al primo aspetto, è stato confermato il crescente interesse, da parte del settore privato (nella specie, società di carattere multinazionale), per l'utilizzo delle BCR quale strumento per il trasferimento intragruppo di dati personali verso Paesi terzi: relativamente elevato, infatti, è stato il numero di richieste di autorizzazione pervenute nel corso dell'anno (talune delle quali ancora in fase di verifica), il cui esame si è concluso con l'approvazione di sei autorizzazioni, rilasciate al termine di complesse istruttorie.

Nel verificare la conformità con l'ordinamento italiano del resto delle BCR approvato al termine della procedura europea di cooperazione (sulla base della procedura di mutua collaborazione cd. *Declaration on mutual recognition*), l'Autorità ha valutato la rispondenza, anche sul piano fattuale, tra gli impegni assunti dalle società istanti e i criteri stabiliti al riguardo dal Gruppo Art. 29, chiedendo alle stesse maggiori informazioni e, ove necessario, idonee rassicurazioni, soprattutto riguardo alla "clausola del terzo beneficiario", al regime di responsabilità, alla natura e alle finalità delle operazioni di trasferimento poste in essere nonché all'efficacia vincolante delle BCR.

Con riferimento a quest'ultimo aspetto, sono state considerate conformi ai principi sanciti dal Gruppo Art. 29 alcune BCR rese vincolanti attraverso strumenti diversi dal contratto plurilaterale, strumento che, invece, aveva caratterizzato le autorizzazioni rilasciate negli ultimi anni. In particolare, è stato valutato rispondente al requisito dell'efficacia vincolante l'obbligo contrattuale assunto dalle società del gruppo mediante la sottoscrizione di una dichiarazione unilaterale al rispetto delle BCR da parte della capogruppo e di un analogo impegno – contenuto in un apposito documento ("lettera di conferma") – assunto dalla società istante con sede in Italia (cfr. provv. 21 novembre 2013, n. 518, doc. web n. 2830367 e provv. 11 luglio 2013, n. 348, doc. web n. 2635057). Parimenti, è stata considerata idonea, in base al criterio dell'efficacia vincolante, l'impegno sottoscritto da tutte le società facenti parte del gruppo a conformarsi ai principi delle "*policy*" (tra cui anche la "*policy*" BCR) approvate dal consiglio di amministrazione della capogruppo (provv. 30 ottobre 2013, n. 485, doc. web n. 2909094); infine, è stata riconosciuta l'efficacia vincolante dell'impegno assunto in un contratto quadro – sottoscritto da tutte le società del gruppo in qualità di importatori e, al contempo, di esportatori di dati personali, individuante le regole per la stipulazione di successivi contratti aventi ad oggetto il trasferimento transfrontaliero di dati personali – tra le società del gruppo medesimo e contenenti clausole analoghe a quelle dell'accordo quadro (provv. 27 giugno 2013, n. 313, doc. web n. 2576345).

In materia di "clausola di responsabilità" sono stati valutati con particolare attenzione i sistemi di assunzione delle responsabilità in caso di violazione delle BCR diversi da quelli previsti dai documenti del Gruppo Art. 29 ma parimenti idonei ad assicu-

rare una adeguata tutela all'interessato. In particolare, sono stati giudicati positivamente i regimi di ripartizione della responsabilità nei confronti dei singoli esportatori situati in area UE, che consentono all'interessato di rivolgersi, in caso di violazione delle BCR, innanzi alla giurisdizione dello Stato in cui ha sede il soggetto esportatore dei dati (provv. 27 giugno 2013, n. 313 cit.).

In merito alla "clausola del terzo beneficiario", l'Autorità ha posto particolare attenzione sull'esigenza di ottenere, da parte della società istante, idonee rassicurazioni con riguardo alla circostanza che tale clausola, qualora di dubbia formulazione, venga interpretata conformemente a quanto previsto al riguardo dal Gruppo Art. 29 (provv. 20 giugno 2013, n. 302, doc. web n. 2550152); infine, quanto alle caratteristiche dei trasferimenti effettivamente posti in essere, sono state richieste specifiche informazioni volte a precisare l'ambito di applicazione dell'autorizzazione, con puntuale indicazione della tipologia dei dati trasferiti e delle finalità del trasferimento, di regola raggruppate in relazione alle singole categorie di interessati i cui dati sono coinvolti nel trasferimento (provv. 14 marzo 2013, n. 124, doc. web n. 2406306).

Il 2013 si è caratterizzato anche per l'adozione di due autorizzazioni di carattere generale volte a recepire, nell'ordinamento italiano, le decisioni della Commissione europea in merito all'adeguatezza delle normative di protezione dei dati personali della Nuova Zelanda (provv. 14 marzo 2013, n. 123, in G.U. 3 aprile 2013, n. 78, doc. web n. 2343701) e della Repubblica orientale dell'Uruguay (provv. 14 marzo 2013, n. 122 in G.U. 3 aprile 2013, n. 78, doc. web n. 2343793). È stato così ulteriormente ampliato il numero di Paesi non appartenenti all'Unione europea nei confronti dei quali è possibile trasferire dati personali senza l'adempimento di ulteriori formalità (quali quelle previste dagli artt. 43-44 del Codice).

Infine, l'Autorità ha fornito chiarimenti sia con riferimento alle modalità concrete di sottoscrizione delle clausole contrattuali tipo (in particolare, riguardo al nuovo testo adottato dalla Commissione europea n. 2010/87/UE, di recente recepimento da parte del Garante: v. Relazione 2012, p. 208), sia con riferimento all'ambito di applicazione ed alle modalità interpretative delle deroghe previste dall'art. 43 del Codice, in particolare per quanto riguarda il requisito del consenso dell'interessato e quello dell'adempimento di un obbligo di legge.

14 Le libere professioni

14.1. *L'attività forense e investigativa*

Campo di applicazione del Codice

Continuano a manifestarsi gli effetti della novella di cui all'art. 40, comma 2, lett. *a*), d.l. 6 dicembre 2011, n. 201, convertito, con modificazioni, dalla l. 22 dicembre 2011, n. 214, che ha ristretto la nozione di "dato personale" alle informazioni relative esclusivamente a persona fisica (cfr. l'art. 4, comma 1, lett. *b*), del Codice, nel testo attualmente vigente), così escludendo dalla nozione di "interessato" le persone giuridiche. In particolare, la segnalazione di una società che paventava l'illecito e dannoso trattamento di alcuni dati riservati nell'ambito di un giudizio è stata archiviata, in quanto non più riconducibile alla protezione dei dati personali (nota 9 settembre 2013).

Comunicazione di dati a terzi

L'Autorità ha ricevuto una segnalazione con la quale l'interessato ha lamentato l'invio da parte di un avvocato presso il suo indirizzo di lavoro di una lettera concernente questioni personali tra l'interessato e l'assistita dell'avvocato. Il legale ha precisato che la lettera era contenuta in una busta sigillata indirizzata personalmente all'interessato presso l'indirizzo di residenza, e che tale busta era stata a sua volta inserita all'interno del plico inviato all'indirizzo di lavoro dello stesso. L'Autorità ha rilevato che nella vicenda non sono emersi gli estremi di una violazione della disciplina in materia di protezione dei dati personali, in quanto l'avvocato ha adottato opportuni accorgimenti per evitare che la lettera potesse venire a conoscenza di soggetti terzi (nota 12 aprile 2013).

Produzione di documenti in giudizio

Con riferimento alla produzione documentale in sede giudiziaria, il Garante ha confermato che spetta al Giudice adito, ove ritualmente richiesto, la competenza a valutare la liceità del trattamento dei dati personali. Infatti, l'art. 160, comma 6, del Codice stabilisce che la validità, l'efficacia e l'utilizzabilità di atti, documenti e provvedimenti nel procedimento giudiziario basati sul trattamento di dati personali, ancorché non conforme a disposizioni di legge o di regolamento, restano disciplinate dalle pertinenti disposizioni processuali nella materia civile e penale (note 22 aprile, 23 aprile, 23 ottobre e 30 aprile 2013).

Con riferimento ad una segnalazione relativa al trattamento di dati personali da parte di un avvocato nella fase propedeutica all'istaurazione di un giudizio, il Garanre ha ricordato che il trattamento effettuato per far valere o difendere un diritto in sede giudiziaria non richiede né l'informativa all'interessato (art. 13, comma 5, lett. *b*), del Codice), né il suo consenso (art. 24, comma 1, lett. *f*), del Codice) e che l'esigenza di far valere o difendere un diritto non comporta la necessità che tra le parti interessate sia in corso un procedimento giudiziale. Infatti, il paragrafo 5, punto *b*), del codice di deontologia e di buona condotta per i trattamenti di dati personali effettuati per svolgere investigazioni difensive (provv. 6 novembre 2008, doc. web n. 1565171) precisa che il consenso dell'interessato non occorre sia per i dati trattati nel corso di un procedimento, anche in sede amministrativa, di arbitrato o di conciliazione, sia nella fase propedeutica all'instaurazione di un eventuale giudizio, sia nella fase successiva alla risoluzione giudiziale o stragiudiziale della lite (nota 9 luglio 2013).

Accesso per finalità di difesa a dati detenuti da terzi

L'Autorità ha 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 un diritto dei loro clienti in sede giudiziaria.

In un caso, un avvocato ha rappresentato l'interesse ad ottenere in un giudizio di separazione fra coniugi un certificato del casellario giudiziale relativo al coniuge della sua assistita, ricorrendo una delle ipotesi di cui all'art. 3, l. n. 898/1970. Al riguardo, il Garante ha evidenziato che la disciplina in materia di protezione dei dati personali, pur esonerando dal fornire l'informativa all'interessato e acquisirne il consenso anche chi intende raccogliere "per far valere o difendere un diritto in sede giudiziaria" dati personali detenuti da un altro soggetto, non obbliga il soggetto destinatario dell'istanza a fornire i dati richiesti. Il destinatario della richiesta resta invece tenuto, in qualità di titolare del trattamento, a valutare la liceità di rilasciare informazioni concernenti l'interessato, alla luce della disciplina in materia di protezione dei dati personali e della specifica normativa di settore, costituita nella specie dal d.P.R. n. 313/2002 (nota 11 marzo 2013).

Similmente in un'altra vicenda, un avvocato ha lamentato il riscontro negativo fornito dal gestore di un portale web alla richiesta di conoscere, per la tutela degli interessi del proprio assistito, i dati riguardanti un utente del portale. L'Ufficio ha evidenziato che il trattamento per far valere o difendere un diritto in sede giudiziaria esonera dagli adempimenti relativi all'informativa e al consenso, ma deve essere tenuto distinto dal trattamento consistente nella comunicazione di dati personali, detenuti dal titolare sulla base di disposizioni legislative e/o contrattuali, a chi manifesti la necessità di acquisirli per la suddetta finalità. Il Codice non pone a carico dei titolari del trattamento alcun obbligo a comunicare, ancorché a soggetti qualificati, i dati personali richiesti, costituendo ciò una facoltà, che per essere esercitata deve comunque tener conto delle garanzie che l'ordinamento giuridico appresta agli interessati. In particolare, come già evidenziato dal Garante (cfr. provv. 23 maggio 2001, doc. web n. 39821), il titolare, oltre a valutare l'effettiva necessità della comunicazione ai fini dell'esercizio del diritto di difesa, deve verificare che la natura dei dati, il contesto in cui essi sono trattati e, in particolare, il rapporto giuridico che lega il titolare medesimo all'interessato permetta di esercitare tale facoltà senza violare obblighi nascenti dalla legge o da un rapporto contrattuale (nota 5 settembre 2013).

Accesso ad atti delle pp.aa. per svolgere indagini difensive

Un avvocato ha presentato un'istanza di autorizzazione per il trattamento dei dati sensibili relativi allo stato di salute di una signora, a seguito della condanna in primo grado del suo assistito per reati asseritamente commessi nei confronti della medesima, al fine di far valere, in sede d'appello, la non colpevolezza del proprio assistito. L'Ufficio ha premesso che l'autorizzazione, richiesta dall'art. 26 del Codice, è stata già rilasciata dal Garante con l'autorizzazione generale n. 4/2012 al trattamento dei dati sensibili da parte dei liberi professionisti (doc. web n. 2159250). In particolare, l'autorizzazione stabilisce che il trattamento dei dati sensibili può essere effettuato, tra l'altro, ai fini dello svolgimento da parte del difensore delle investigazioni difensive di cui alla l. 7 dicembre 2000, n. 397 o, comunque, per far valere o difendere un diritto in sede giudiziaria, fermo restando che qualora i dati siano idonei a rivelare lo stato di salute e la vita sessuale, il diritto da far valere o difendere deve essere di rango pari a quello dell'interessato, ovvero consistente in un diritto della personalità o in un altro diritto o libertà fondamentale e inviolabile (punto 3). Con riferimento al caso di specie, si è, peraltro, rappresentato che il codice di procedura penale stabilisce che, ai fini delle indagini difensive, il difensore può chiedere i documenti in possesso di una p.a. (nella specie, un'azienda ospedaliera pubblica) e di estrarne copia a sue spese (art. 391-*quater*, commi 1 e 2, c.p.p.). In caso di rifiuto trovano applicazione gli artt. 367 e 368 c.p.p., i quali prevedono uno specifico mezzo di tutela giurisdizionale, nel cui ambito

gli organi giudiziari sono tenuti a valutare la richiesta anche sotto il profilo del rispetto dei principi di protezione dei dati personali, con specifico riferimento all'art. 71 del Codice. L'Ufficio ha dichiarato, pertanto, la propria incompetenza sulla vicenda (nota 29 aprile 2013).

Trattamento per fini esclusivamente personali

Un'interessata ha lamentato una violazione della disciplina in materia di tutela dei dati personali da parte di un avvocato che – nel corso del procedimento disciplinare a suo carico dinanzi a un Consiglio dell'Ordine (rispetto al quale l'interessata assumeva la veste di esponente) – aveva prodotto querele ed esposti presentati da una signora nei confronti dell'interessata, a dire di questa non attinenti all'oggetto del procedimento disciplinare.

L'Autorità, dopo avere osservato che le querele e gli esposti non possono essere considerati dati giudiziari, come definiti dall'art. 4, comma 1, lett. *e*), del Codice, in quanto non costituiscono di per sé dati idonei a rivelare la qualità di imputato o di indagato ai sensi degli artt. 60 e 61 c.p.p., ha rilevato che il trattamento era stato effettuato dall'avvocato per fini esclusivamente personali, qual è nella specie la propria difesa nel procedimento disciplinare, e che i dati personali oggetto del trattamento non erano stati destinati ad una comunicazione sistematica o alla diffusione (tale non essendo il deposito degli stessi nel procedimento disciplinare). Da ciò deriva che il trattamento in questione non è soggetto all'ambito applicativo del Codice, in conformità a quanto previsto dall'art. 5, comma 3, del Codice medesimo (cfr. par. 16.3). L'Ufficio ha altresì evidenziato che spetta all'organo presso il quale è avvenuto il deposito (nella specie, il Consiglio dell'Ordine degli avvocati) valutare la validità, l'efficacia e l'utilizzabilità degli atti in questione con riferimento al procedimento disciplinare in corso (nota 18 giugno 2013).

Un'interessata ha, altresì, lamentato una violazione del diritto alla tutela dei dati personali dei suoi pazienti da parte di una dottoressa che aveva prodotto in una causa civile degli estratti di alcune cartelle cliniche dell'archivio dell'interessata e un contratto di lavoro subordinato intercorrente tra l'interessata e una propria assistita. Anche in tale caso l'Autorità ha rilevato che il trattamento contestato era stato effettuato dalla professionista per fini esclusivamente personali, qual è nella specie la propria difesa in un procedimento giudiziario, e che i dati non erano stati destinati ad una comunicazione sistematica o alla diffusione, tale non essendo il deposito degli stessi in un procedimento giudiziario. Da ciò è derivato che il trattamento in questione non è soggetto all'ambito applicativo del Codice, in conformità a quanto previsto dall'art. 5, comma 3, del Codice medesimo (nota 18 giugno 2013).

15 Il registro dei trattamenti

Come noto, in attuazione dell'art. 154, comma 1, del Codice, il Garante cura la tenuta *online* del Registro dei trattamenti, formato sulla base delle notificazioni ricevute effettuabili esclusivamente attraverso una procedura telematica – semplificata nei contenuti con provvedimento del 22 ottobre 2008 (doc. web n. 1571196) e rispetto alla quale viene assicurata assistenza sia mediante un servizio di messaggistica automatica, sia grazie al supporto tecnico-amministrativo dell'Ufficio – la cui consultazione – consentita a chiunque e gratuita (art. 37, comma 4, del Codice) – ha luogo attraverso l'accesso ad una sezione del sito web dell'Autorità denominata "servizi *online*". L'obbligo di notificazione al Garante, ossia di comunicare in via preventiva l'intenzione di procedere al trattamento o di modificarne o cessarne uno in corso, sorge in capo al titolare del trattamento dei dati personali ove ricorra uno dei casi previsti dall'art. 37 del Codice e non si versi in una delle ipotesi di esonero individuate dall'Autorità con proprie deliberazioni (v. Relazione 2004, p. 109; provv. 31 marzo 2004, doc. web n. 852561; nota 23 aprile 2004, doc. web n. 993385; nota 26 aprile 2004, doc. web n. 996680; provv. 24 giugno 2011, doc. web n. 1823225).

Nel 2013 gli utenti hanno consultato il Registro con una media giornaliera di oltre 70 accessi e punte superiori ai 200 e, con riguardo al numero delle notificazioni presentate, si rileva un significativo incremento rispetto all'anno precedente; deve altresì segnalarsi l'incremento del numero delle cessazioni (cfr. sez. IV, tab. 1 e 13). Il 57% dei notificanti ha la propria sede nel nord del Paese (cfr. sez. IV, tab. 14).

Quanto all'andamento, nel primo e nel secondo trimestre dell'anno si registra un incremento delle notificazioni rispetto ai corrispondenti trimestri del 2012. Nella seconda metà del 2013 si verifica poi un forte incremento del numero delle notificazioni rispetto ai corrispondenti ultimi due trimestri del 2012, con una tendenza alla crescita che risulta confermata nel mese di gennaio 2014, che ha visto il maggior numero di notificazioni dal 2007 con riguardo al mese di gennaio e, in termini assoluti, è aumentato anche il numero delle cessazioni.

I dati percentuali relativi alla tipologia dei trattamenti notificati nel 2013 confermano nel loro insieme, con alcuni scostamenti, le tendenze del periodo 2004-2012: i trattamenti volti a definire il profilo e la personalità dell'interessato tramite l'ausilio di strumenti elettronici, in incremento (29%); quelli di dati idonei a rivelare lo stato di salute e la vita sessuale (22%) e quelli relativi al rischio sulla solvibilità economica, alla situazione patrimoniale, al corretto adempimento di obbligazioni (19%), coprono da soli il 70% di tutti i trattamenti notificati. Si registra, inoltre, in tale contesto anche una crescita delle notificazioni relative a trattamenti di dati biometrici e una diminuzione di quelle relative a trattamenti di dati genetici (cfr. sez. IV, tab. 15).

Anche nel 2013 le notificazioni presentate direttamente dai titolari hanno superato in numero assoluto quelle presentate tramite intermediario.

Si conferma, infine, come già prospettato lo scorso anno, che la disciplina della materia potrebbe costituire oggetto di modifiche nell'ambito della proposta, presentata dalla Commissione europea il 25 gennaio 2012, di un regolamento generale sulla protezione dei dati personali destinato a sostituire la direttiva 95/46/CE.