1.3. GIORNALISMO

Il bilanciamento tra la libertà di espressione e le esigenze di protezione dei dati personali ha caratterizzato le deliberazioni in materia di attività giornalistica ed informazione *online.*

Immagini relative all'arresto di persone indagate

Con riferimento ad una trasmissione televisiva che dava conto di indagini coordinate da una Direzione antimafia, il Garante ha vietato l'ulteriore diffusione delle immagini delle persone indagate ritratte all'interno delle proprie abitazioni private -anche attraverso l'utilizzo di cd. "primi piani"- nel momento delicatissimo dell'arresto, ritenendo travalicati i limiti posti dall'ordinamento all'esercizio del diritto di cronaca, in particolare il principio di tutela della dignità della persona e il principio di essenzialità dell'informazione rispetto a fatti di interesse pubblico (provv. 18 maggio 2012 [doc. web n. 1900914]).

Trattamento eccedente dell'immagine di dipendenti pubblici

Due provvedimenti, adottati su reclamo degli interessati, hanno riguardato casi in cui le immagini riconoscibili di dipendenti pubblici (non inquadrabili nella categoria delle cd. "persone note"), che svolgevano i propri compiti in un'aula parlamentare, erano state pubblicate, rispettivamente, su un quotidiano nazionale e diffuse da un servizio televisivo.

Nel primo caso l'Autorità ha ritenuto legittima la pubblicazione delle immagini, lecitamente raccolte, finalizzata alla individuazione visiva degli appartenenti a categorie professionali il cui trattamento giuridico ed economico è oggetto di un dibattito pubblico (provv. 15 novembre 2012 [doc. web n. 2247923]).

Nel secondo, è stata invece ritenuta illegittima la pubblicazione -anche in ragione delle tecniche di ripresa utilizzate- di immagini individualizzate del reclamante, presentato quasi come "emblema" di un'intera categoria. Non è stato tuttavia adottato alcun provvedimento inibitorio, considerata la spontanea decisione del titolare del trattamento di rimuovere dal sito e dai propri archivi le predette immagini (provv. 15 novembre 2012 [doc. web n. 2185342]).

Correttezza del trattamento e aggiornamento di notizie

Anche a seguito della sentenza della Corte di Cassazione n. 5525/2012 sul cd. "diritto all'oblio", la quale ha evidenziato l'esigenza di dar conto dei successivi sviluppi di una vicenda oggetto di informazione poiché "*altrimenti la notizia, originariamente completa e vera, diviene non aggiornata risultando quindi parziale e non esatta, e pertanto sostanzialmente non vera*", il Garante ha accolto due ricorsi che richiedevano di aggiornare, sulla base di sviluppi avvenuti *medio tempore*, articoli (già deindicizzati) presenti sul sito di un'importante testata

giornalistica. In particolare è stato prescritto all'editore di segnalare -ad es. con un'annotazione a margine dei singoli articoli- l'esistenza dello "sviluppo" della notizia, in modo da assicurare da un lato, all'interessato, il rispetto della propria attuale identità personale, e dall'altro, ad ogni lettore, un'informazione attendibile e completa (provv.ti 20 dicembre 2012 [doc. web n. 2286432] e 24 gennaio 2013 [doc. web n. 2286820]).

Procedimento di ricorso e organi costituzionali

Per alcuni profili connessa alla precedente è la problematica relativa alla disponibilità in rete della documentazione dell'attività svolta dalle Camere nelle legislature repubblicane comprendente una massa di dati personali spesso delicati, anche quando non sensibili. Al riguardo, in più occasioni, persone citate in atti parlamentari hanno chiesto di sottrarre i dati in parola all'azione dei motori di ricerca, ovvero di integrare notizie inesatte o incomplete. Gli organi parlamentari, pur richiamando la piena autonomia e insindacabilità nell'esercizio delle funzioni e delle prerogative parlamentari, nel 2012 hanno in particolare invocato il disposto dell'art. 8, comma 2, lettera *c)*, del Codice, che preclude l'utilizzo dello strumento del ricorso nei confronti dei trattamenti svolti da Commissioni parlamentari d'inchiesta.

Il Garante, nel condividere tale impostazione, e ritenendo pertanto inammissibile un ricorso in materia (provv. 19 luglio 2012 [doc. web n. 2065905]), non ha però cessato di ricercare un equilibrio più avanzato, anche alla luce della pur limitata giurisprudenza di merito (v. Trib. Civ. di Roma, 1ª sez., sentenza 19 gennaio 2012). Da qui uno scambio di note fra il Presidente della Camera dei deputati e il Presidente dell'Autorità allo scopo di promuovere ulteriori approfondimenti, volti ad individuare misure (quali la deindicizzazione dei testi) idonee ad evitare che, attraverso la pubblicazione *online* di atti parlamentari, si possano ledere diritti e libertà fondamentali.

1.4. SANITÀ

In questa materia si segnalano due deliberazioni di carattere generale, riguardanti principalmente la "gestione" dei dati da parte delle amministrazioni competenti.

Regolamento sul trattamento di dati sensibili da parte delle regioni

Più in dettaglio, il Garante ha espresso parere favorevole sullo schema tipo di regolamento per il trattamento di dati sensibili e giudiziari da parte di regioni, province autonome ed aziende sanitarie, volto a garantire un più ampio quadro di tutele rispetto ai flussi crescenti di

dati scambiati tra le pubbliche amministrazioni, anche per monitorare il buon andamento dell'attività amministrativa.

Nell'esprimere il parere, l'Autorità ha chiesto che lo schema venga integrato con specifiche garanzie, in particolare prevedendo la codificazione dei dati acquisiti dalle regioni ai fini di monitoraggio e valutazione dei trattamenti sanitari erogati, per evitare l'identificazione diretta del soggetto interessato. Le regioni e le province autonome che intendono aggiornare, sulla base del nuovo schema tipo, i propri atti regolamentari sono tenute a recepire le indicazioni formulate dal Garante nel parere.

Nello stesso atto l'Autorità ha espresso le sue valutazioni sul decreto del Ministero della salute concernente il sistema di sorveglianza delle nuove diagnosi di infezioni da HIV, richiamato dallo schema tipo e viziato per violazione di legge, in quanto emanato senza il previsto parere del Garante (v. art. 154, comma 4, del Codice).

Al riguardo, l'Autorità ha precisato che i trattamenti di dati sensibili possono essere effettuati nell'ambito delle attività amministrative correlate alla sorveglianza epidemiologica dei casi di infezione da HIV, nel rispetto delle specifiche cautele che saranno individuate dal Ministero, in collaborazione con l'Autorità, nel quadro di un percorso collaborativo che il Ministero intende avviare ai fini della revisione del decreto e dell'acquisizione del previsto parere.

Per quanto riguarda i nuovi flussi di dati tra i medici prescrittori e il Ministero dell'economia e delle finanze (Mef), per il monitoraggio della spesa sanitaria, è stata infine rilevata l'esigenza di modificare il protocollo, adottato previo parere dell'Autorità, con cui sono individuati sia i dati in possesso del Mef che possono essere trasmessi al Ministero della salute e alle regioni, sia le modalità di tale trasmissione (comma 10, dell'art. 50 del d.l. 20 settembre 2003, n. 269 (convertito dalla l. 24 novembre 2003, n. 326). Ciò, al fine di estendere le cautele previste dal protocollo per i flussi di dati relativi alle prescrizioni di farmaci e alle prestazioni specialistiche ai nuovi flussi originati dai medici prescrittori (provv. 26 luglio 2012 [doc. web n. 1915390]).

Registro dei tumori del Veneto

Di ambito più circoscritto, ma su materia che presenta profili di estrema delicatezza, il parere rilasciato alla Regione Veneto sullo schema di regolamento recante norme per il

funzionamento del Registro dei tumori (provv. 13 settembre 2012 [doc. web n. 1927415]) in attuazione della l.r. 16 febbraio 2010 n. 11, che prevede l'istituzione di diversi registri di interesse sanitario.

Il regolamento individua il titolare del trattamento dei dati contenuti nel Registro, gli scopi perseguiti nell'ambito della più ampia finalità di ricerca scientifica, i tipi di dati sensibili trattati, i soggetti tenuti ad alimentare il Registro, nonché l'ambito di comunicazione e di diffusione dei dati ivi contenuti (v. art. 18, comma 2, della l.r. n. 11/2010 cit. e artt. 20 e 98 del Codice).

Le osservazioni dell'Ufficio hanno riguardato, in particolare, il rispetto del principio di indispensabilità nel trattamento dei dati, anche con riferimento alla loro conservazione; l'esigenza di utilizzare codici identificativi per tutelare l'identità e la riservatezza dei malati; le cautele per comunicare i dati ai registri tumori di altre regioni, le modalità per dare l'informativa agli interessati, la specificazione di misure organizzative e di accorgimenti tecnici idonei a garantire un adeguato livello di sicurezza dei dati, tra le quali l'obbligo, per il personale incaricato di trattarli, di rispettare regole di condotta analoghe al segreto professionale, anche quando non sia a ciò tenuto per legge.

1.5. COMUNICAZIONI E RETI TELEMATICHE

Di diretta derivazione comunitaria, l'attività in questo settore si caratterizza per atti di rilievo generale.

Schema di d.lgs. di attuazione della Direttiva n. 2009/136/CE

In primo luogo si menziona il parere espresso su richiesta del Ministro dello sviluppo economico e delle infrastrutture e trasporti, sullo schema di d.lgs. n. 69/2012, recante, tra l'altro, modifiche al Codice, in attuazione della Direttiva n. 2009/136/CE, in materia di reti e di servizi di comunicazione elettronica (provv. 29 marzo 2012 [doc. web n. 1893400]).

In estrema sintesi, tra le più rilevanti innovazioni si segnala la disciplina del *data breach*, o violazione di dati personali, che comporta anche accidentalmente la perdita, la modifica o la rivelazione non autorizzata di dati trattati nella fornitura di un servizio di comunicazione elettronica.

In relazione ai *cookie* (i piccoli *file* di testo che i siti visitati dall'utente inviano al suo *browser* per essere poi ritrasmessi agli stessi siti alla successiva visita del medesimo utente), il

testo prevede modalità semplificate per l'espressione del consenso dell'interessato, sulla base di un'informativa a sua volta semplificata.

Nell'esprimere parere favorevole, il Garante ha tra l'altro rilevato, in forma di osservazione (poi recepita nel testo definitivo), l'esigenza di garantire -in merito alla nuova disciplina della raccolta di informazioni nei riguardi dell'abbonato e dell'utente *ex* art. 122 del Codice- l'effettività del diritto dell'interessato ad essere informato in ordine agli scopi del trattamento, se del caso con modalità opportunamente semplificate. Inoltre, è stato suggerito di chiarire che il d.l. n. 201/2011 convertito, con modificazioni, dalla l. n. 214 del 2011 (cd. "salva Italia"), nell'escludere persone giuridiche, enti o associazioni dall'ambito di applicazione del Codice, non ha modificato la definizione di "abbonato" contenuta nel Codice, che risulterebbe perciò -ad avviso del Garante- tuttora applicabile tanto alle persone fisiche quanto a quelle giuridiche.

Non essendo stato accolto tale suggerimento il Garante, con provvedimento di natura interpretativa, ha chiarito che i predetti soggetti continuano a non poter essere contattati se iscritti nel Registro delle opposizioni, né possono ricevere, senza consenso specifico per la finalità promozionale, telefonate automatizzate con messaggi preregistrati, e-mail, fax, sms, mms (provv. 20 settembre 2012 [doc. web n. 2094932]).

Linee-guida sulla comunicazione delle violazioni di dati personali

Gli adempimenti da effettuarsi in occasione di un *data breach* sono poi stati disciplinati in dettaglio nelle linee-guida recanti prescrizioni nei confronti dei fornitori, con particolare riguardo: all'individuazione dei soggetti obbligati a effettuare la comunicazione della violazione; alle circostanze in cui sussiste tale obbligo; all'avviso da dare agli utenti; alle misure di sicurezza tecniche e organizzative da adottare. In particolare, è stato chiarito che sono tenuti a comunicare i *data breach* esclusivamente i fornitori di servizi telefonici e di accesso a internet, e non le reti aziendali, gli internet *point*, i motori di ricerca, i siti internet che diffondono contenuti (provv. 26 luglio 2012, in G.U. 7 agosto 2012, n. 183 [doc. web n. 1915485]).

Informativa relativa ai *cookie* - consultazione pubblica

Come accennato, la disciplina relativa all'uso dei cd. "*cookie*" e degli altri strumenti analoghi (quali *web beacon/web bug, clear* GIF), è stata modificata, a seguito dell'attuazione della Direttiva n. 2009/136/CE ad opera del d.lgs. 28 maggio 2012, n. 69.

In particolare, l'archiviazione delle informazioni nell'apparecchio terminale di un utente o l'accesso a informazioni già archiviate, è consentito se l'interessato ha espresso il suo consenso sulla base di un'informativa semplificata, anche tramite specifiche configurazioni di programmi informatici o di dispositivi di facile e chiara utilizzabilità (v. nuovo testo art. 122 Codice).

Per individuare le modalità semplificate con cui rendere l'informativa *online* sull'utilizzo dei suindicati dispositivi, il Garante ha avviato una consultazione pubblica (provv. 22 novembre 2012, in G.U. 19 dicembre 2012, n. 295 [doc. web n. 2139697]).

1.6. LAVORO

In materia di lavoro la casistica è principalmente relativa a singoli trattamenti, spesso in relazione a segnalazioni degli interessati.

Protocollo informatico

In particolare, in un caso l'Autorità ha chiarito che le informazioni relative ai dipendenti acquisite nel protocollo informatico devono essere accessibili al solo personale specificamente incaricato di tali trattamenti e non alla generalità indifferenziata degli utenti dei servizi di protocollo. Nella vicenda oggetto di accertamenti un ampio numero di dipendenti poteva venire a conoscenza di dati personali di colleghi (quali permessi accordati in base alla l. n. 104/1992, permessi studio, ovvero contestazioni disciplinari), indipendentemente dalle mansioni svolte.

È stato pertanto prescritto, in particolare, di limitare la visibilità degli atti relativi al personale ai soli dipendenti incaricati del loro trattamento (provv. 11 ottobre 2012 [doc. web n. 2097560]).

Impiego di sistemi di videosorveglianza

In un altro caso, a seguito degli accertamenti effettuati presso un *call center*, il Garante ha vietato il trattamento dei dati rilevati mediante un sistema di videosorveglianza in grado di captare anche le conversazioni dei dipendenti (provv. 4 ottobre 2012 [doc. web n. 2066968]), effettuato peraltro in violazione dell'art. 4, l. n. 300/1970. Provvedimenti di analogo contenuto sono stati adottati in presenza di trattamenti effettuati mediante sistemi di videosorveglianza presso un hotel (provv. 25 ottobre 2012 [doc. web n. 2212826]) e un esercizio commerciale (provv. 25 ottobre 2012 [doc. web n. 2212623]), in assenza delle garanzie dettate dall'art. 4, l. n. 300/1970.

In altra fattispecie il Garante ha dichiarato l'illiceità e disposto il blocco del trattamento effettuato dal sistema di videosorveglianza, installato per finalità antitaccheggio presso un esercizio commerciale, mediante una telecamera che riprendeva anche l'area nella quale è posta l'apparecchiatura per la rilevazione delle presenze dei lavoratori (provv. 17 gennaio 2013 [doc. web n. 2291893]).

È stata anche ritenuta inidonea l'informativa fornita agli interessati (pur nelle forme semplificate indicate dall'Autorità nel provvedimento generale dell'8 aprile 2010 [doc. web n. 1712680]) ed è stata altresì riscontrata la possibilità di accedere alle immagini registrate con modalità diverse da quelle stabilite nell'accordo con le rappresentanze sindacali (in violazione dei princìpi di liceità e correttezza nel trattamento).

Un ulteriore profilo di illiceità del trattamento è stato rilevato nella circostanza che il personale incaricato di visionare le immagini per le menzionate finalità antitaccheggio, appartenente a società diversa dal titolare del trattamento, è risultato privo della licenza prefettizia richiesta dalla normativa di settore (art. 134, r.d. 18 giugno 1931, n. 773 (Tulps)), come confermato peraltro dal consolidato indirizzo interpretativo della giurisprudenza di legittimità secondo cui "*ogni forma di attività imprenditoriale di vigilanza e custodia di beni per conto terzi esige la licenza del prefetto, indipendentemente dalle modalità operative con le quali viene espletata*" (cfr. Cass. pen., sez. III, 3 dicembre 2010, n. 1821, con ulteriori richiami).

Installazione di un sistema di registrazione di immagini su veicolo di trasporto locale

Nell'ambito di una verifica preliminare presentata ai sensi dell'art. 17 del Codice, il Garante ha invece ritenuto lecita, da parte di una concessionaria del servizio di trasporto pubblico locale, l'installazione di un dispositivo sul parabrezza delle vetture, che consente di registrare e -al verificarsi di predeterminate "anomalie"- conservare, immagini relative sia all'interno che all'esterno del veicolo. Le finalità perseguite dalla società (salvaguardia del patrimonio aziendale nonché ricostruzione della dinamica di eventuali sinistri in vista della tutela dei diritti in giudizio) e le concrete modalità di trattamento dei dati (esclusione dell'immagine del conducente dall'angolo di ripresa, offuscamento dei volti di soggetti terzi non coinvolti negli eventi) sono state infatti ritenute conformi ai princìpi di necessità nonché di pertinenza e non eccedenza (artt. 3 e 11, comma 1, lett. *d)*, del Codice). Sono state invece ritenute eccedenti, rispetto alle finalità rappresentate, la raccolta e conservazione -pure prospettata dalla società- di registrazioni della

voce delle persone a bordo del veicolo, anche alla luce della sua possibile rilevanza penale (cfr. artt. 617, 617-*bis* e 623-*bis* c.p.) (provv. 29 novembre 2012 [doc. web n. 2257616]).

Operatori di un *call center* e controlli di qualità

L'Autorità ha altresì effettuato accertamenti in relazione sia alla registrazione e al riascolto delle telefonate degli operatori di un *call center* gestito da una cooperativa, sia al monitoraggio della condotta tenuta dagli stessi operatori mediante l'analisi del numero e della durata delle conversazioni.

Al riguardo, poiché la registrazione ed il riascolto delle comunicazioni consentono il controllo a distanza dell'attività dei lavoratori, il Garante ha rilevato che il mancato assolvimento degli adempimenti previsti dall'art. 4, comma 2, l. n. 300/1970 (fatto salvo dall'art. 114 del Codice) riverbera i propri effetti anche sulle operazioni di trattamento, le quali risultavano perciò in violazione dell'art. 11, comma 1, lett. *a)*, del Codice. Analoga la valutazione sul monitoraggio delle conversazioni di ciascun operatore telefonico in base al loro numero o durata, non essendo stati posti in essere gli adempimenti previsti dal cit. art. 4 (provv. 1° agosto 2012 [doc. web n. 1923325]; in materia provv. 9 febbraio 2011 [doc. web n. 1797032]).

Rilevazione dati biometrici per controllo delle presenze dei dipendenti

Sempre in sede di verifica preliminare è stata esaminata l'istanza di un comune, per l'installazione di un sistema di rilevazione biometrica delle presenze dei dipendenti, basato sulla lettura delle impronte digitali, volta ad impedire usi impropri del *badge*. Il Garante ha ritenuto non conforme ai princìpi di necessità, pertinenza e non eccedenza (in relazione agli artt. 3, 11, comma 1, lett. *d*), del Codice) il trattamento, poiché l'ente locale non aveva comprovato l'insufficienza delle ordinarie modalità di controllo, in alternativa ai più invasivi sistemi biometrici (provv. 31 gennaio 2013 [doc. web n. 2304669].

Trattamento di dati sensibili riferiti ai partecipanti ad una manifestazione sindacale

È stato altresì ritenuto illecito il trattamento, da parte di una casa circondariale, dei nominativi del personale di polizia penitenziaria che aveva preso parte ad una manifestazione sindacale (provv. 29 novembre 2012 [doc. web n. 2192643]).

Il trattamento, pur se (in astratto) consentito ai fini di un eventuale procedimento disciplinare, non risultava in concreto lecito, poiché la mera indizione e partecipazione ad una manifestazione sindacale non configura alcun illecito, alla luce della fondamentale libertà di riunione riconosciuta dall'art. 17 della Costituzione nonché dalla normativa di settore (v. art. 19, l. n. 395/1990 recante l'ordinamento del Corpo di polizia penitenziaria).

È stato pertanto prescritto alla casa circondariale -che si è tempestivamente conformata- il divieto di trattare ulteriormente i nominativi dei partecipanti alla manifestazione, nonché di portare a conoscenza dei soggetti, cui eventualmente i dati fossero stati comunicati, in particolare, l'inutilizzabilità dei dati stessi (provv. 29 novembre 2012 [doc. web n. 2192643]).

Consegna di comunicazioni ai lavoratori

In più di una circostanza, l'Autorità è stata chiamata a pronunciarsi in relazione alla notifica a mano di comunicazioni contenenti dati personali del lavoratore: tali sono stati considerati dal Garante anche i dati quantitativi e qualitativi riferiti allo svolgimento delle attività professionali che, nella fattispecie considerata, pur facendo complessivamente capo ad un'unità organizzativa, rientravano comunque nelle attribuzioni della reclamante (che ne era responsabile) (provv. 18 ottobre 2012 [doc. web n. 2174351]). Tale valutazione in merito alla nozione di dato personale è peraltro conforme a quella del Gruppo Art. 29 (Parere n. 4/2007, adottato il 20 giugno 2007 - WP 136, p. 6 e ss. [doc. web. n. 1607426]).

Da un altro caso è emerso con chiarezza che l'interesse del titolare del trattamento -specie riguardo ad atti dalla cui ricezione decorrono particolari effetti- a formare la prova dell'avvenuta ricezione mediante sottoscrizione del destinatario su copia degli atti, richiede l'adozione di adeguate cautele, tra le quali l'individuazione dell'incaricato in una persona già a conoscenza del contenuto per ragioni di ufficio. Si trattava della notifica di determinazioni aventi ad oggetto l'irrogazione di sanzioni disciplinari ad un lavoratore da parte del proprio superiore gerarchico (provv. 18 ottobre 2012 [doc. web n. 2174582]).

Accordo tra la Repubblica italiana e lo Stato di Israele sulla previdenza sociale

Connesso con la materia del lavoro è il parere espresso, su richiesta del Ministero degli affari esteri, su uno schema di d.d.l. recante la ratifica ed esecuzione di un accordo con lo Stato di Israele che, per garantire ai cittadini italiani ivi trasferitisi una pensione in linea con i contributi versati in Italia, prevede una comunicazione di dati da parte del Ministero del lavoro e delle politiche sociali ad altro soggetto straniero (e viceversa).

In proposito occorre tenere presente che il trasferimento di dati personali verso Paesi terzi può avvenire, tra l'altro, in base alle decisioni con le quali la Commissione europea constata che il Paese terzo garantisce un adeguato livello di protezione dei dati personali (art. 44, comma 1, lett. *b)*, del Codice).

Al riguardo, la decisione della Commissione europea del 31 gennaio 2011 n. 2011/61/UE ha ritenuto adeguato il livello di protezione assicurato nello Stato d'Israele -come definito ai sensi del diritto internazionale- ai trattamenti automatizzati, ai quali soli si applica la legge israeliana sulla protezione della vita privata (considerando n. 9 della citata Decisione). Il Garante aveva quindi autorizzato i trasferimenti di dati verso lo Stato d'Israele, in conformità alla suddetta Decisione (provv. 20 gennaio 2012 [doc. web n. 1868817]) ed ha conseguentemente espresso parere favorevole sul testo del d.d.l. (provv. 25 ottobre 2012 [doc. web n. 2185056]).

1.7. DIRITTI DELL'INTERESSATO E CORRETTEZZA DEL TRATTAMENTO

Si segnalano, ancora, tre casi che evidenziano profili di protezione di situazioni giuridiche soggettive in relazione a trattamenti posti in essere da soggetti pubblici.

Adozione ed attestazioni di stato civile

Attiene ad un delicatissimo ambito della sfera familiare il caso di una persona che contestava ad un comune di aver rilasciato a un avvocato, che agiva privo di delega per conto di alcuni parenti dell'interessato, la copia integrale del suo atto di nascita recante le informazioni sul provvedimento giudiziario riguardante la sua adozione.

L'Autorità ha al riguardo evidenziato che qualunque attestazione di stato civile riferita all'adottato può essere rilasciata solo con l'indicazione del nuovo cognome e con l'esclusione di qualsiasi riferimento alla paternità e alla maternità del minore, poiché indicazioni sul rapporto di adozione possono essere fornite solo su espressa autorizzazione dell'autorità giudiziaria (artt. 26, comma 4, e 28, comma 2, l. 4 maggio 1983, n. 184; artt. 106 e 107, commi 1 e 2, lett. *b*), d.P.R. 3 novembre 2000, n. 396; art. 177, comma 3, del Codice).

È stato quindi vietato ai parenti dell'interessato l'ulteriore utilizzo delle predette informazioni sull'adozione e prescritto al comune di fornire al personale di stato civile adeguate istruzioni per evitare ulteriori violazioni in materia (provv. 8 novembre 2012 [doc. web n. 2187244]).

Rettificazione di sesso su certificazioni di laurea

Riguarda la protezione della sfera personalissima il caso nel quale uno studente laureato ha chiesto chiarimenti sulla possibilità di ottenere, a seguito dell'avvenuta rettificazione di attribuzione di sesso, un nuovo diploma di laurea, indicante solo i nuovi dati anagrafici. Contestualmente, l'università ha rappresentato al Garante la propria intenzione di rilasciare tale secondo diploma, senza dar conto delle ragioni della ristampa. Questa soluzione è

apparsa all'Autorità idonea a tutelare la dignità degli interessati e il loro diritto a vedere correttamente rappresentata la loro attuale identità sessuale. Il Garante ha pertanto prescritto a tutte le università, nell'ambito della loro autonomia -fermi restando gli obblighi di conservazione dell'atto originario- l'adozione di idonei accorgimenti, affinché non siano riportate nella relativa documentazione elementi idonei a rivelare l'avvenuta rettificazione di attribuzione di sesso (provv. 15 novembre 2012 [doc. web n. 2121695]).

Punti patente

Si segnala ancora l'istanza di un cittadino, che lamentava la mancata registrazione, presso l'Anagrafe nazionale degli abilitati alla guida, della totalità delle annotazioni, comportanti variazione del punteggio della patente (decurtazioni e attribuzioni di punti).

Dalla documentazione prodotta è emerso che la comunicazione effettuata dal Ministero delle infrastrutture e dei trasporti non conteneva talune variazioni di punteggio, che non erano annotate neppure nell'estratto conto dei punti, consultabile nel portale di servizi di *e-government* del Dipartimento trasporti del Ministero, in contrasto con la disciplina di settore e con la regola secondo la quale le informazioni personali -anche quelle contenute in banche dati pubbliche- devono essere trattate secondo correttezza, esatte e, se necessario, aggiornate (art. 11, comma 1, lett. *a), c), d),* del Codice).

Il Garante ha pertanto prescritto al Ministero che le comunicazioni agli interessati (anche nel caso di consultazione diretta del cd. "portale dell'automobilista") contengano i dati relativi alla totalità delle variazioni, comprese quelle effettuate in modo automatizzato, di attribuzione di punti (*bonus*) e successiva decurtazione per illegittima attribuzione e, anche per quanto riguarda gli eventi passati, che, qualora l'interessato ne faccia specifica richiesta, sia assicurata la conoscibilità, nel dettaglio e cronologicamente, dei dati concernenti la totalità delle variazioni (provv. 24 gennaio 2013 [doc. web n. 2256617]).

1.8. PROGRAMMA STATISTICO NAZIONALE 2011-2013

Nel 2012 su richiesta dell'Istat, l'Autorità si è espressa in relazione al trattamento di dati personali inseriti per la prima volta nel Programma statistico nazionale (Psn) 2011-2013, Aggiornamento 2013, e alle modifiche apportate ai prospetti identificativi di lavori statistici, già inclusi nel precedente Programma 2011-2013 e nel relativo Aggiornamento 2012-2013 (parere 9 febbraio 2012 [doc. web n. 1876517]).

In primo luogo, il Garante ha preso atto del mancato adeguamento alle modifiche normative che hanno sottratto all'ambito di applicazione della disciplina in materia di protezione dati le informazioni relative a persone giuridiche, enti e associazioni. Sul punto l'Autorità ha raccomandato, in vista della redazione del Psn 2014-2016, di prestare particolare attenzione ai lavori statistici che, pur concernendo prevalentemente persone giuridiche, possono comportare il trattamento di dati personali riferiti a persone fisiche (quali le attività professionali svolte in forma individuale).

Inoltre sono state evidenziate specifiche criticità con riferimento agli studi progettuali del Ministero del lavoro e delle politiche sociali che prevedono, in particolare, la trasmissione al sistema informativo dell'Inps di informazioni trattate a fini amministrativi dai comuni, corredate di dati identificativi diretti e di informazioni molto delicate, relative anche allo stato di salute e alla vita sessuale dei minori.

Al riguardo, l'Autorità ha, tra l'altro, evidenziato che i dati personali trattati a fini statistici non possono essere utilizzati per scopi di altra natura e che il trattamento dei dati sensibili e giudiziari in parola non è previsto allo stato da alcuna norma di legge che individui i tipi di dati e le operazioni eseguibili, condizionando pertanto il parere favorevole sul Psn 2011-2013, Aggiornamento 2013, all'eliminazione dallo stesso dei predetti studi progettuali (parere 20 settembre 2012 [doc. web n. 2069239]).

1.9. PROPAGANDA ELETTORALE

In prossimità delle elezioni amministrative del 2012 e delle politiche del 2013 con due provvedimenti sono stati previsti speciali casi di esonero temporaneo dall'informativa per partiti, movimenti politici, sostenitori e singoli candidati, individuando le corrette modalità in base alle quali tali soggetti possono utilizzare a fini di propaganda elettorale i dati dei cittadini (provv.ti 5 aprile 2012 [doc. web n. 1885765] e 10 gennaio 2013 [doc. web n. 2181429]).

È stato così ricordato, in particolare, che possono essere usati senza il consenso dei cittadini i dati contenuti nelle liste elettorali detenute dai comuni, nell'elenco degli elettori residenti all'estero, o in altre fonti documentali detenute da soggetti pubblici accessibili a

chiunque, nonché i dati di iscritti ed aderenti e quelli raccolti nel quadro di relazioni interpersonali con cittadini ed elettori.

Il consenso è necessario segnatamente per utilizzare i dati raccolti su internet, per contattare gli abbonati presenti negli elenchi telefonici e per l'utilizzo di particolari modalità di comunicazione elettronica (quali sms, e-mail, telefonate preregistrate). È altresì necessario per l'uso dei dati di simpatizzanti o persone già contattate per singole iniziative politiche (ad es., *referendum*, proposte di legge, raccolte di firme).

Non sono invece utilizzabili, tra gli altri, gli archivi dello stato civile, l'Anagrafe dei residenti, indirizzi raccolti dai soggetti pubblici per svolgere attività e compiti istituzionali. Non possono essere usate neppure le liste elettorali di sezione già utilizzate nei seggi, recanti l'indicazione dei non votanti.

Trascorse le date indicate nei suddetti provvedimenti i soggetti che utilizzano i dati per esclusivi fini di selezione di candidati alle elezioni, di propaganda elettorale e di comunicazione politica possono continuare a trattare i dati personali solo informando gli interessati entro i termini indicati nei provvedimenti stessi.

Si segnala, infine che, nell'ambito delle consultazioni tenutesi nel 2012 per l'individuazione del candidato della coalizione di centro-sinistra alla Presidenza del Consiglio dei ministri (cd. "primarie"), l'Autorità ha esaminato alcuni profili problematici sollevati da un comitato e da alcuni privati cittadini in merito ad alcune disposizioni del relativo regolamento, che richiedeva la sottoscrizione di un "pubblico appello" e l'iscrizione in un apposito "albo", con connessa possibile diffusione di dati sensibili dei partecipanti alle citate consultazioni (provv. 31 ottobre 2012 [doc. web n. 2079275]).

Il Garante, richiamata la natura sensibile dei dati, ha ribadito l'esigenza di attenersi ai princìpi posti dagli artt. 3 e 11 del Codice, invitando altresì il Comitato della coalizione (nella dichiarata veste di titolare del trattamento) ad evitare forme di diffusione dei dati e ad adottare adeguate misure per la sicurezza dei medesimi, ed ha rinviato, per la disciplina dei profili non espressamente considerati, alle disposizioni dell'autorizzazione generale n. 3/2011, sul trattamento dei dati sensibili da parte di associazioni e fondazioni (provv. 24 giugno 2011 [doc. web n. 1822585]).

2. QUADRO NORMATIVO IN MATERIA DI PROTEZIONE DEI DATI PERSONALI

2.1. LE GARANZIE PREVISTE NEL CODICE E ALCUNI RECENTI INTERVENTI MODIFICATIVI

L'applicazione -anche in sede giurisdizionale e amministrativa- del Codice ne ha dimostrato l'assoluta rilevanza in chiave di garanzia dei diritti fondamentali della persona rispetto al trattamento di dati che la riguardano.

L'evoluzione del quadro normativo europeo ha imposto, però, l'adeguamento del Codice ai nuovi princìpi introdotti a livello sovranazionale, in particolare nel settore delle comunicazioni elettroniche (Direttiva n. 2009/136/CE).

Ulteriori, circoscritte modifiche sono ascrivibili ad un provvedimento d'urgenza del Governo (d.l. 9 febbraio 2012, n. 5 convertito, con modificazioni, dalla l. 4 aprile 2012, n. 35) emanato per esigenze di "semplificazione" di taluni adempimenti in materia di sicurezza dei dati e di "copertura normativa" al trattamento di dati giudiziari nel settore della prevenzione e del contrasto dei fenomeni di criminalità organizzata.

Di seguito si illustrano brevemente e partitamente le cennate modifiche.

2.1.1. Modifiche in materia di comunicazioni elettroniche

Le più rilevanti innovazioni alla disciplina in materia di protezione dati sono state introdotte, principalmente sotto forma di novella alle disposizioni del Codice, dal d.lgs. 28 maggio 2012, n. 69, adottato in attuazione delle Direttive n. 2009/136/CE, in materia di trattamento dei dati personali e tutela della vita privata nel settore delle comunicazioni elettroniche, e n. 2009/140/CE in materia di reti e servizi di comunicazione elettronica (art. 9, l. 15 dicembre 2011, n. 217 - legge comunitaria 2010).

Alla stesura del decreto è stato chiamato a collaborare, in via informale, il Garante che ha poi espresso, su richiesta del Governo, motivato parere, fornendo indicazioni per assicurare il rispetto del quadro normativo europeo e nazionale in materia di protezione dati (cfr. *infra* par. 3.1.).

Le disposizioni del decreto legislativo, nel dare attuazione al rinnovato quadro europeo (la citata Direttiva n. 2009/136/CE ha modificato la precedente Direttiva n. 2002/58/CE in

materia, cui il Governo aveva dato attuazione proprio con il d.lgs. n. 196/2003, recante il Codice), introducono significative modifiche al Codice, rispetto ai trattamenti effettuati da fornitori di servizi di comunicazioni elettroniche (Titolo X).

Tra le novità più importanti si segnalano l'introduzione della "violazione di dati personali" (*data breach*), intesa come *"violazione degli obblighi di sicurezza del trattamento che comporta, anche accidentalmente, la distruzione, la perdita, la modifica, la rivelazione non autorizzata o l'accesso ai dati personali trasmessi, memorizzati o comunque elaborati nel contesto della fornitura di un servizio di comunicazione accessibile al pubblico"* (art. 4, comma 3, lett. g-*bis*, del Codice), e gli adempimenti del fornitore del servizio di comunicazione elettronica in caso di violazione dati personali (art. 32-*bis* del Codice). Tali adempimenti consistono, essenzialmente, nella comunicazione dell'evento al Garante, al fine di consentirgli l'esercizio dei propri poteri a tutela degli interessati. Inoltre, qualora l'illecito rischi di "*arrecare pregiudizio ai dati personali o alla vita privata di un contraente o di altra persona*", il fornitore è tenuto a fornire idonea comunicazione anche a tali soggetti.

La nuova fattispecie è incentrata sul pregiudizio alla riservatezza dell'interessato, determinatosi -anche accidentalmente- per una "violazione degli obblighi di sicurezza" nell'ambito della fornitura di un servizio di comunicazione elettronica e nel conseguente onere informativo a carico del fornitore verso il Garante e verso i soggetti interessati. Tuttavia, ai descritti adempimenti non è tenuto il fornitore in grado di dimostrare di aver adottato misure di protezione tali da rendere i dati inintelligibili a chi non sia autorizzato ad accedervi, in virtù di una presunzione relativa di inoffensività della violazione in tali ipotesi. L'inadempimento ai suddetti obblighi realizza un illecito amministrativo punito con sanzioni pecuniarie, differenziate nel *quantum* in ragione della rilevanza dell'obbligo inadempiuto (nuovo art. 162-*ter* del Codice).

Gli adempimenti da effettuarsi in occasione del verificarsi di un *data breach* sono stati poi disciplinati nel dettaglio dalle linee-guida del Garante approvate il 26 luglio 2012 e sottoposte a consultazione pubblica [doc. web n. 1915485].

Altre novità di rilievo riguardano alcune definizioni già recate dal Codice (il *nomen* "abbonato" viene sostituito con "contraente"), la disciplina dell'archiviazione delle informazioni nel terminale del contraente, con particolare riferimento ai cd. "*cookie*" (art. 122), le

misure di sicurezza e procedure a cura dei fornitori di servizi di comunicazione elettronica (artt. 32 e 132-*bis*) e, infine, l'adeguamento dell'impianto sanzionatorio, con il nuovo art. 162-*ter* concernente "la violazione di dati personali", già citato.

Particolarmente interessante è la nuova disciplina della archiviazione delle informazioni nell'apparecchio terminale dell'abbonato (ora "contraente") e dell'utente, nonché dell'accesso a informazioni già archiviate (cd. "*cookie*"). Il decreto, nel modificare l'art. 122 del Codice, pur confermando l'importanza di una scelta consapevole degli utenti della rete e quindi di un loro consenso libero e informato al trattamento dei propri dati personali (cd. "*opt-in*"), ha previsto forme semplificate di informativa e modalità "agevolate" di espressione del consenso stesso.

Nell'esprimere parere favorevole, il Garante ha rilevato, tra l'altro, in forma di osservazione (poi recepita nel testo definitivo del decreto), l'esigenza di garantire l'effettività del diritto dell'interessato ad essere informato in ordine agli scopi del trattamento, a tal fine eliminando la clausola limitativa ("in quanto applicabile") nel rinvio all'art. 13 del Codice contenuta nello schema di decreto. Il Garante ha rilevato infatti come il diritto dell'abbonato e dell'utente ad essere informati ai sensi dell'art. 13 deve essere assicurato nella sua pienezza, a prescindere da ogni valutazione di "applicabilità" o di compatibilità. Interpretando tuttavia le esigenze di semplificazione connesse al contesto di riferimento, il Garante ha suggerito di fare riferimento a forme semplificate di informativa, che agevolino l'adempimento di tale obbligo da parte dei fornitori di servizi di comunicazione elettronica.

Il Garante ha, inoltre, sottolineato l'opportunità di delineare con chiarezza il quadro normativo riferibile alla figura dell'abbonato-persona giuridica nel contesto dei trattamenti disciplinati dal Titolo X del Codice (connessi alla fornitura di servizi di comunicazione elettronica). Il d.l. n. 201 del 2011, convertito, con modificazioni, dalla l. n. 214/2011 (cd. "decreto salva Italia"), nell'escludere persone giuridiche, enti o associazioni dalla sfera dei soggetti di diritto ai fini della protezione dati non ha, infatti, modificato le disposizioni del predetto Titolo X del Codice dedicate al trattamento di dati connesso alla fornitura di servizi di comunicazioni elettronica e, in particolare, in ossequio al quadro normativo europeo, non ha modificato l'oggetto della definizione di "abbonato" pure contenuta nel Codice, che risulta perciò tuttora applicabile tanto alle persone fisiche quanto a quelle giuridiche.