

Nel caso di un altro comune che intendeva trasmettere ad una società di rilevazione dei consumi idrici i dati personali contenuti nelle banche dati anagrafiche, dei contribuenti TARSU/TIA e ICI, nonché il catasto terreni e fabbricati, è stato fatto presente che la comunicazione di dati personali da parte dei soggetti pubblici a privati è regolata da un distinto e più stringente quadro normativo (art. 19, comma 3, del Codice) (*Nota* 10 dicembre 2010).

In un altro caso, al comune che aveva chiesto chiarimenti in ordine alla legittimità del rifiuto opposto da un altro comune a una richiesta volta a conoscere determinate informazioni riguardanti una propria dipendente, è stato fatto presente che non risulta sindacabile da parte del Garante il diniego opposto dall'amministrazione interpellata in materia di accesso agli atti amministrativi né il diniego fondato sul combinato disposto degli artt. 19, comma 2, e 39 del Codice (*Nota* 11 giugno 2010).

3.8. L'ATTIVITÀ GIUDIZIARIA

Anche nel 2010 sono pervenute segnalazioni relative al regime di pubblicità nell'ambito dei procedimenti di espropriazione forzata introdotto dalla riforma del processo esecutivo (d.l. 14 marzo 2005, n. 35, convertito, con modificazioni, dalla l. 1° maggio 2005, n. 80), che prevede la pubblicazione, in appositi siti Internet, di copia dell'ordinanza del giudice che dispone sulla vendita forzata, nonché della relazione di stima dei beni da espropriare.

Pubblicità dei dati
nei procedimenti
di espropriazione
forzata

In riscontro a tali segnalazioni, l'Autorità ha richiamato il *provvedimento* 7 febbraio 2008 ([doc. *web* n. 1490838]; v. *Relazione* 2007, p. 55) con il quale ha indicato all'autorità giudiziaria e ai professionisti incaricati delle vendite l'esigenza di omettere nelle copie pubblicate sia dell'avviso di vendita, sia delle ordinanze e delle relazioni di stima, le generalità e ogni altro dato personale idoneo a rivelare l'identità del debitore e di eventuali soggetti terzi non previsto dalla legge e comunque non pertinente rispetto alla procedura in corso.

In un caso particolare l'interessato, di età avanzata, ha lamentato che la pubblicazione in Internet della consulenza tecnica d'ufficio riguardante una procedura esecutiva a lui relativa consentiva la sua agevole identificazione, in quanto non erano stati oscurati il luogo e la data di nascita del medesimo, unica persona nata in quel comune in quel giorno. Nel caso di specie l'Autorità, dopo aver verificato l'esattezza delle indicazioni contenute

nella segnalazione, ha ritenuto che, nonostante fosse stato omesso il nominativo dell'interessato, le informazioni pubblicate in chiaro nella consulenza tecnica ne consentissero effettivamente l'agevole identificazione. Tenuto conto delle peculiari circostanze della fattispecie, ha quindi invitato il giudice dell'esecuzione a disporre l'integrale oscuramento delle informazioni relative al segnalante (*Nota* 20 luglio 2010).

È pervenuta una segnalazione anche con riferimento alla pubblicazione su un quotidiano di un avviso recante i nominativi delle persone proprietarie di immobili confinanti con quello oggetto della procedura esecutiva. Nel riscontrare la segnalazione l'Autorità, ricordato il contenuto del *provvedimento* 7 febbraio 2008, ha provveduto a richiamare l'attenzione del giudice dell'esecuzione sul necessario rispetto dei principi posti a tutela della riservatezza sia dei soggetti coinvolti in procedimenti esecutivi, sia di eventuali soggetti terzi (*Nota* 5 maggio 2010).

In entrambi i casi le autorità giudiziarie hanno provveduto all'oscuramento delle informazioni oggetto delle segnalazioni.

3.8.1. L'informatica giuridica

Linee-guida per
la diffusione dei
provvedimenti
giudiziari

A seguito di numerosi quesiti e segnalazioni, e dopo avere un'ampia consultazione con gli operatori e gli editori del settore, il Garante ha adottato, in data 2 dicembre 2010, le *“Linee-guida in materia di trattamento di dati personali nella riproduzione di provvedimenti giurisdizionali per finalità di informazione giuridica”* ([doc. web n. 1774813], in *G.U.* 4 gennaio 2011, n. 2).

Le linee-guida attengono esclusivamente alla pubblicazione delle sentenze e dei provvedimenti giurisdizionali su riviste giuridiche, *cd-rom*, *dvd*, siti istituzionali, a fini di informazione giuridica. Non incidono, quindi, sulle norme processuali, quali quelle in materia di copie originali delle sentenze e degli altri provvedimenti giurisdizionali, o del loro deposito nelle cancellerie giudiziarie, e non riguardano l'attività giornalistica, che è oggetto di specifiche disposizioni (art. 136 ss. del Codice; *“Codice di deontologia relativo al trattamento dei dati personali nell'esercizio dell'attività giornalistica”*, adottato dal Garante il 29 luglio 1998, in *G.U.* 3 agosto 1998, n. 179).

Con la *deliberazione*, viene prescritto l'obbligo di oscurare, sempre e in ogni caso, i dati dei minori e delle parti nei procedimenti che hanno ad oggetto i rapporti di famiglia e lo stato delle persone (ad es., controversie in materia di matrimonio, filiazione, adozione, abusi familiari, richieste di rettificazione di sesso), anche quando il giudizio si riferisca ad aspetti patrimoniali o economici. Devono, inoltre, essere omessi i dati relativi ad altre persone dai quali possa desumersi, anche indirettamente, l'identità dei soggetti tutelati. I dati devono essere oscurati non solo nei provvedimenti riprodotti per esteso, ma anche in quelli diffusi sotto forma di massima o contenuti in un elenco.

Al di fuori dei casi sopra indicati, nei quali la tutela opera *ope legis*, qualunque interessato (ad es., le parti in un giudizio civile o l'imputato in un processo penale, o anche un testimone o un consulente), può rivolgere un'istanza al giudice, prima della conclusione del processo, per chiedere che, in caso di riproduzione del provvedimento per finalità di informazione giuridica, siano oscurati le generalità e ogni altro elemento in grado di identificarlo. L'istanza deve indicare i "*motivi legittimi*" che la giustificano: ad es., la delicatezza del caso o la particolare natura dei dati contenuti nel provvedimento (stato di salute, vita sessuale). Se l'istanza è accolta si appone una annotazione sull'originale della sentenza.

L'anonimizzazione del provvedimento giudiziario può essere disposta dal giudice anche d'ufficio, nei casi in cui la diffusione di informazioni particolarmente delicate possa arrecare conseguenze negative alla vita di relazione o sociale dell'interessato (ad es., in ambito familiare o lavorativo).

Viene rilevato, infine, che non spetta all'ufficio giudiziario, ma a chi riceve la copia dei provvedimenti con l'annotazione che dispone l'oscuramento delle generalità provvedere in tal senso ove intenda riprodurli o diffonderli, anche sotto forma di massima, per finalità di informazione giuridica.

3.8.2. *Trattamento di dati negli uffici giudiziari*

Con *provvedimento* 3 dicembre 2009, a seguito di una segnalazione ricevuta, il Garante ha deliberato di effettuare, ai sensi dell'art. 160 del Codice, gli accertamenti necessari a

Accertamenti presso il Consiglio di Stato e il TAR del Lazio

verificare l'attuazione e l'idoneità delle misure di sicurezza adottate in relazione ai trattamenti di dati personali effettuati per ragioni di giustizia, ai sensi dell'art. 47, comma 2, del Codice, presso il Consiglio di Stato e il Tribunale amministrativo regionale del Lazio [doc. *web* n. 1753845].

Dalle verifiche svolte, pur in un generale quadro di rispetto delle regole, sono emerse alcune criticità. Il Garante ha pertanto prescritto alcune misure volte a rafforzare le misure di sicurezza a protezione dei dati trattati dai due uffici giudiziari sia in via informatica, sia in forma cartacea (*Prov. 23 settembre 2010* [doc. *web* n. 1753845]).

Sotto il primo profilo, particolare attenzione è stata posta alla messa in sicurezza del Nuovo sistema informativo della giustizia amministrativa (NSIGA), che gestisce i documenti e i processi lavorativi dell'intero sistema, costituito dal Consiglio di Stato e dai ventinove Tribunali amministrativi regionali.

Deve essere in particolare garantito che per le comunicazioni gestite da NSIGA fra le sedi del sistema giudiziario amministrativo e per gli accessi dei magistrati a NSIGA da postazioni esterne agli uffici –la *cd. "scrivania del magistrato"*– sia adottato un protocollo che cifri i dati in transito. Tutte le operazioni compiute su NSIGA dai magistrati e dal personale amministrativo devono essere tracciate, compresi gli accessi in sola lettura e non solo le operazioni di scrittura. Devono, inoltre, essere adottate delle *policy* che specifichino agli utenti di non utilizzare *password* banali per accedere a NSIGA (ad es., contenenti il nome stesso dell'utente).

Infine, l'accesso alla sala *server* e alla sala dove sono collocati i gruppi di continuità deve essere registrato (tramite *log*) e consentito solo con *badge* nominativi. I locali, inoltre, devono essere costantemente monitorati, eventualmente anche attraverso un impianto di videosorveglianza interno.

Quanto al trattamento in via cartacea, il Consiglio di Stato deve custodire i fascicoli processuali in armadi tutti dotati di serratura e il TAR del Lazio deve collocare i fascicoli dell'archivio in locali chiusi e controllati.

Sia il Consiglio di Stato che il TAR del Lazio hanno comunicato di aver già posto in essere gran parte delle misure indicate.

Sono giunti al Garante alcuni quesiti posti da uffici giudiziari in materia di accesso ad atti concernenti i processi. In un caso, una testata televisiva giornalistica aveva chiesto di accedere agli atti di un processo penale, al fine di utilizzare il materiale nell'ambito di un programma avente ad oggetto vicende giudiziarie. In un altro caso, un avvocato privo di mandato difensivo aveva chiesto di prendere visione dei ruoli di udienza.

Nel fornire riscontro, l'Autorità ha in primo luogo ricordato che la normativa in materia di protezione dei dati personali non ha innovato o modificato la disciplina relativa alla conoscenza degli esiti e dei calendari dei processi —come alla visione e al rilascio di estratti e di copie di atti giudiziari, alla pubblicità delle udienze e alla consultazione dei registri relativi ai procedimenti giudiziari— che rimane assoggettata alle pertinenti disposizioni processuali (art. 51 del Codice). Si tratta di attività che integrano trattamenti svolti “*per ragioni di giustizia*” (art. 47, comma 2, del Codice), che vengono svolte sotto il controllo dell'autorità giudiziaria e nel rispetto delle norme di settore. La decisione in ordine all'accesso deve essere quindi ricavata nel quadro del regime di pubblicità attribuito agli atti dalle norme processuali.

In secondo luogo, l'Autorità ha, peraltro, rilevato che anche a tali trattamenti si applicano i principi posti dall'art. 11 del Codice, in base ai quali l'accesso ai dati personali può essere consentito solo previa verifica dell'esistenza di uno scopo determinato, esplicito e legittimo (comma 1, lett. *b*)) e relativamente alle sole informazioni pertinenti e non eccedenti rispetto allo scopo medesimo (comma 1, lett. *d*)).

In caso di decisione favorevole a consentire l'accesso, il Garante ha, infine, invitato l'autorità giudiziaria a valutare attentamente la possibilità di raggiungere gli scopi perseguiti dal soggetto richiedente sulla base di soli dati anonimi, mediante preventiva omissione di informazioni atte a consentire l'identificazione dei soggetti coinvolti nei giudizi (*Note* 5 gennaio e 21 gennaio 2011).

3.8.3. *Notificazioni di atti e comunicazioni*

Come negli anni precedenti, il Garante è intervenuto in numerose occasioni per assicurare l'adozione di procedure idonee a tutelare la riservatezza delle persone alle quali

vengono notificati atti giudiziari, verbali di contravvenzione, avvisi fiscali o altri atti amministrativi (art. 174 del Codice).

In particolare, con riferimento alle notificazioni di atti tributari, l'Ufficio ha ricordato che sulla busta devono essere leggibili solo le informazioni necessarie all'invio della comunicazione al destinatario (art. 11, comma 1, del Codice) (*Nota* 28 aprile 2010).

In un'altra occasione è stato evidenziato che la notificazione deve essere effettuata in busta sigillata solo se la consegna non possa avvenire nelle mani proprie del destinatario al quale l'atto può essere notificato, ancorché aperto, per il tramite del messo comunale. Con particolare riferimento all'accessibilità del contenuto del documento da parte degli addetti al protocollo e del messo comunale, si è precisato che essi, in qualità di dipendenti pubblici ovvero incaricati di pubblico servizio, sono tenuti al segreto d'ufficio (art. 15 del d.P.R. 20 gennaio 1957, n. 3) (*Nota* 13 maggio 2010).

4. LA SANITÀ

4.1. IL TRATTAMENTO DI DATI IDONEI A RIVELARE LO STATO DI SALUTE

4.1.1. I trattamenti per fini di cura della salute

Anche nel 2010, l'Autorità ha richiamato l'attenzione dei titolari del trattamento operanti in ambito sanitario sulla necessità di fornire l'informativa e di acquisire il consenso per il trattamento dei dati personali nell'ambito del rapporto medico paziente.

Al riguardo sono stati forniti chiarimenti in ordine alle modalità di acquisizione del consenso di minori detenuti temporaneamente nei centri di prima accoglienza, in caso di assenza di chi ne esercita legalmente la potestà genitoriale; è stato in particolare evidenziato che è possibile acquisire il consenso, in tale caso, da un prossimo congiunto, da un familiare, da un convivente o, in loro assenza, dal responsabile della struttura presso cui dimora (art. 82, comma 2, lett. *a*), del Codice) (*Nota* 30 settembre 2010).

Merita altresì menzione una segnalazione circa l'illegittima acquisizione, da parte del coniuge del segnalante, di alcuni scritti contenuti in un diario, successivamente consegnati ad un medico specialista per la redazione di un parere sullo stato di salute del segnalante, poi prodotto nel giudizio di separazione.

In merito è stato rappresentato che la validità, l'efficacia e l'utilizzabilità in giudizio di atti, basati sul trattamento di dati non conforme alle norme vigenti restano disciplinate dalle pertinenti disposizioni processuali (art. 160, comma 6, del Codice; cfr. *Prov. 23 settembre 2010* [doc. *web* n. 1756065]) e che resta salva la facoltà della persona interessata di far valere le proprie pretese risarcitorie, ove ne ricorrano i presupposti, davanti all'autorità giudiziaria ordinaria (art. 15 del Codice) (*Nota* 22 ottobre 2010).

4.1.1.1. Le linee-guida in tema di fascicolo sanitario elettronico (FSE) e di dossier sanitario

Una regione ha sottoposto al Garante uno schema di regolamento in materia di fascicolo sanitario elettronico e di *dossier* sanitario elettronico.

Al riguardo, l'Ufficio ha ricordato che, in base alle “*Linee-guida in tema di fascicolo sanitario elettronico (FSE) e di dossier sanitario*” (*Prov. 16 luglio 2009* [doc. *web*

n. 1634116]), i trattamenti di dati personali effettuati attraverso il FSE devono essere resi noti al Garante mediante una apposita comunicazione da effettuarsi secondo il modello adottato dall'Autorità con specifico *provvedimento* (*Prov. 16 luglio 2009 [doc. web n. 1633793]*), da parte delle strutture coordinatrici delle iniziative di FSE e, in via residuale, in caso di assenza di tale struttura, dai singoli titolari del trattamento coinvolti.

La suddetta comunicazione non deve essere effettuata nel caso di *dossier* sanitari e dall'invio di tali comunicazioni non può desumersi alcuna approvazione implicita da parte dell'Autorità delle iniziative comunicate (*Nota 26 luglio 2010*).

Ad oggi risultano pervenute 44 comunicazioni, delle quali solo 6 effettivamente riconducibili al FSE, mentre le altre non dovevano essere inviate in quanto relative ad altri trattamenti (ad es., *dossier* sanitari; condivisione da parte di più strutture solo di alcuni dati clinici del paziente e non della sua intera storia clinica; flussi di dati per finalità amministrative correlate alla cura; flussi di dati tra aziende sanitarie e medici di medicina generale; trattamenti effettuati da farmacie nell'ambito della somministrazione di farmaci).

4.1.1.2. Consultazione online dei referti medici

È stato chiesto dal Ministero della salute il previsto parere al Garante su uno schema di decreto di attuazione delle disposizioni che hanno definito nuovi compiti e funzioni assistenziali per le farmacie pubbliche e private convenzionate con il servizio sanitario nazionale (art. 1, comma 2, lett. *f*), d.lgs. 3 ottobre 2009, n. 153), tra cui la prenotazione di prestazioni ambulatoriali presso le strutture accreditate, i relativi pagamenti, ed il ritiro dei referti. Lo schema di decreto ha sostanzialmente recepito le indicazioni rese dall'Autorità per garantire un più elevato *standard* di tutela del diritto alla protezione dei dati personali. Tuttavia, è stata evidenziata l'esigenza che al momento del ritiro del referto da parte degli assistiti presso le farmacie, l'operatore acceda al referto stesso solo per consegnarlo all'interessato, e che sia impedita la creazione di banche dati di referti digitali presso la farmacia (*Parere 19 gennaio 2011 [doc. web n. 1787887]*).

Nell'ambito dello stesso parere è stata altresì rappresentata l'esigenza di individuare adeguati tempi di conservazione dei referti (art. 11, comma 1, lett. *e*), del Codice) e che

gli operatori della farmacia, individuati quali incaricati del trattamento dei dati nell'ambito del sistema CUP (centro unificato di prenotazione), non tenuti per legge al segreto professionale, siano sottoposti a regole di condotta analoghe al segreto professionale, come già previsto in ambito sanitario (art. 83, comma 2, lett. *i*), del Codice).

4.1.2. I trattamenti per fini amministrativi

In diverse occasioni, l'Ufficio ha ricordato alle strutture sanitarie che per perseguire finalità amministrative correlate alle finalità di cura non devono acquisire il consenso dell'interessato, ma rispettare i limiti e le garanzie individuate nei regolamenti regionali adottati in conformità allo schema-tipo di regolamento per i trattamenti dei dati sensibili e giudiziari di competenza delle regioni e di altri enti, su cui il Garante ha espresso parere favorevole (*Prov. 13 aprile 2006 [doc. web n. 1272225]*).

Da parte di più enti, anche alla luce delle numerose modifiche normative sopravvenute, è stata manifestata l'esigenza di revisionare il predetto schema-tipo di regolamento, ed a tal fine, l'Ufficio, che ha condiviso tale necessità, partecipa ad un tavolo di lavoro interregionale all'uopo istituito.

Tra i casi di maggior rilievo affrontati, si evidenziano talune segnalazioni relative al trattamento da parte di un comune, di dati idonei a rivelare lo stato di salute di cittadini, contenuti in prescrizioni mediche di farmaci svizzeri e in documenti relativi alla avvenuta dispensazione di tali farmaci.

Il comune, nel fornire riscontro alla richiesta di informazioni dell'Ufficio, aveva documentato di essere stato legittimato al trattamento, in quanto designato responsabile del trattamento di dati personali da parte della azienda sanitaria, sicché l'istruttoria preliminare si è conclusa senza specifici provvedimenti del Garante (v. artt. 11, comma 1, lett. *d*) e 13, comma 4, del regolamento del Garante n. 1/2007) (*Note 15 dicembre 2010*) (v. anche il parere favorevole del Garante sullo schema-tipo di regolamento per il trattamento dei dati sensibili e giudiziari effettuato dai comuni *Prov. 21 settembre 2005 [doc. web n. 1170239]*).

Nel riscontrare, infine, talune osservazioni sullo svolgimento di attività connesse al servizio CUP, da parte di detenuti di una casa di reclusione, l'Ufficio ha confermato che, se designati

incaricati del trattamento, i detenuti possono legittimamente trattare dati personali di cui l'azienda sanitaria è titolare per lo svolgimento delle sue funzioni istituzionali. Gli incaricati del trattamento devono operare sotto la diretta autorità del titolare o del responsabile e attenersi alle istruzioni loro impartite (art. 30 del Codice) (*Nota* 1 luglio 2010).

4.1.3. Il trattamento di dati personali in occasione dell'accertamento dell'infezione da HIV

L'Autorità ha nuovamente affrontato la questione relativa alla comunicazione, adottando un *provvedimento* di divieto di comunicazione dei dati relativi ai risultati degli accertamenti diagnostici diretti o indiretti per l'infezione da *HIV*, a persona diversa dall'interessato.

In particolare, un cittadino aveva lamentato di essere stato informato del suo stato di sieropositività dal medico di famiglia, il quale ne aveva avuto notizia da un medico operante presso la casa di cura ove erano state effettuate le analisi per l'accertamento dell'infezione da *HIV*.

Al riguardo, considerato l'obbligo di comunicare i risultati di tali esami esclusivamente alla persona cui essi sono riferiti (art. 5, comma 4, l. 5 giugno 1990, n. 135), il Garante ha vietato non solo alla casa di cura, ma anche al medico di famiglia del segnalante che aveva indebitamente avuto notizia dei risultati, la comunicazione dei predetti dati a persona diversa dall'interessato (*Prov. 27* maggio 2010 [doc. *web* n. 1738383]).

In relazione ad un quesito presentato da un ordine dei medici, in ordine alla raccolta di dati personali relativi allo stato di sieropositività dei pazienti che si rivolgono per la prima volta ad uno studio medico, l'Ufficio ha chiarito che quanto prescritto nei *provvedimenti* 12 novembre 2009 [doc. *web* nn. 1686068 e 1673588] non ha in alcun modo inteso impedire la raccolta di dati anamnestici del paziente. Nei citati provvedimenti, infatti, l'Autorità ha espressamente evidenziato che la doverosa raccolta da parte del medico di un'anamnesi dettagliata non può impedire all'interessato di scegliere, in modo informato —e quindi consapevole— di non comunicare al medico alcune informazioni sanitarie che lo riguardano, ivi compresa la sua eventuale sieropositività, senza perciò subire alcun pregiudizio sulla possibilità di usufruire delle prestazioni sanitarie richieste

(cfr. par. n. 3, linee-guida in tema di fascicolo sanitario elettronico (FSE) e di *dossier* sanitario - *Prov. 16* luglio 2009 [doc. *web* n. 1634116]).

Nella medesima occasione è stato, inoltre, puntualizzato che contrasta con i principi di pertinenza e non eccedenza dei dati rispetto alle finalità di cura dell'interessato, la raccolta di informazioni sull'eventuale stato sieropositività di ogni paziente che si rivolge per la prima volta allo studio medico, effettuata in fase di accettazione, indipendentemente dal tipo di intervento clinico o dal piano terapeutico che lo stesso deve eseguire (ad es., trattamento di igiene orale professionale, ablazione del tartaro, *rx* ortopantomica). Tali informazioni –previo consenso informato del paziente– possono infatti essere raccolte solo se necessarie in funzione del tipo di intervento sanitario o di piano terapeutico.

Sempre con riferimento ai dati relativi all'accertamento dell'infezione da *HIV*, l'Ufficio ha, altresì, avviato una istruttoria a seguito di una notizia stampa, in ordine allo svolgimento di indagini sanitarie volte ad accertare l'esistenza dell'infezione da *HIV*, tra i dipendenti di una azienda sanitaria, chiedendo ogni elemento di valutazione in ordine a quanto riportato nell'articolo, specie con riferimento al rispetto delle specifiche disposizioni contenute nella l. n. 135/1990 (*Nota* 30 novembre 2010).

4.1.4. Le strutture sanitarie e la tutela della dignità delle persone

Come già avvenuto nel corso degli ultimi anni, il Garante ha richiamato al rispetto delle misure previste dal Codice a tutela della dignità della persona in ambito sanitario (art. 83), numerosi organismi sanitari pubblici e privati, che hanno di conseguenza modificato le modalità di erogazione previste per la fornitura delle prestazioni e dei servizi sanitari.

Si menziona in proposito una segnalazione effettuata durante un servizio giornalistico televisivo, dalla quale era emerso che un ospedale sardo non aveva rispettato, in particolare, la dignità e la riservatezza di una paziente in stato comatoso.

Al riguardo, l'Ufficio ha richiamato al rispetto della dignità dei pazienti sottoposti a trattamenti medici invasivi, o nei cui confronti è comunque doverosa una specifica attenzione (v. punto 3, lett. *a*), del *Prov. generale* 9 novembre 2005 [doc. *web* n. 1191411] sul rispetto della dignità degli interessati nelle strutture sanitarie) (*Nota* 10 maggio 2010).

L'ospedale ha comunicato di aver previsto idonee misure, anche di tipo organizzativo, volte a progettare gli spazi disponibili, in modo da renderli più rispettosi dei diritti dei malati.

È stato, inoltre, segnalato che la prenotazione di prestazioni sanitarie e il pagamento del *ticket* presso il centro unificato di prenotazione (CUP) di un ospedale umbro venivano effettuati con modalità tali da consentire la conoscenza di dati sensibili degli interessati da parte di altri soggetti a causa della mancanza di appropriate distanze di cortesia.

Interpellato sul punto, l'ospedale ha comunicato di aver posto in essere taluni accorgimenti idonei a garantire la riservatezza degli interessati, tra i quali la predisposizione di apposite distanze di cortesia per coloro che effettuano la prenotazione di prestazioni sanitarie, e la previsione di specifiche modalità per informare i terzi legittimati sulla dislocazione dei degenti nei reparti (art. 83, comma 2, lett. *c*) e *d*), del Codice; punto 3, lett. *b*), del cit. *provvedimento*) (Nota 12 marzo 2010).

Anche un servizio di igiene e sanità pubblica, richiamato dal Garante in ordine alla necessità di adottare misure idonee a garantire la riservatezza di una minore, in occasione delle chiamate per effettuare la vaccinazione ed acquisire il consenso informato dei genitori, ha comunicato di voler istituire una procedura di chiamata alfanumerica al momento dell'accettazione (Nota 7 dicembre 2010).

In relazione ad una segnalazione relativa alla "*poca attenzione*" posta nella conservazione delle cartelle cliniche dei pazienti, in una casa di cura pugliese, l'Ufficio ha rappresentato alla menzionata struttura sanitaria che il titolare del trattamento deve adottare procedure idonee a garantire la custodia di atti e documenti in archivi ad accesso selezionato (art. 35 del Codice) e che qualora gli atti o i documenti contengano dati personali sensibili, gli stessi devono essere controllati e custoditi dagli incaricati durante lo svolgimento dei relativi compiti fino alla loro restituzione, in maniera che agli stessi non possano accedere persone prive di autorizzazione (punto 28 del Disciplinare tecnico Allegato B. al Codice).

Essendo emerso dall'istruttoria preliminare, in particolare, che il trattamento dei dati contenuti in taluni referti radiologici non era conforme alle misure minime di sicurezza

prescritte dal Codice (artt. 33-36 del Codice e Allegato B. al Codice), la casa di cura ha assicurato di aver provveduto a garantire la custodia di atti e documenti in archivi ad accesso selezionato, in particolare, sistemando i citati referti in appositi armadi chiusi e custoditi da personale sanitario (*Nota* 23 novembre 2010).

Sulla base di una notizia di stampa, relativa ad un policlinico all'interno del quale, presso taluni cassonetti per la raccolta dei rifiuti era stata abbandonata documentazione clinica, unitamente a documenti contabili riguardanti pazienti della struttura, l'Ufficio ha riscontrato, la non conformità del trattamento alle misure minime di sicurezza prescritte dal Codice (artt. 33-36 del Codice e Allegato B. al Codice) (*Nota* 13 dicembre 2010).

In un'altra segnalazione si lamentava la comunicazione, ad un familiare che ne aveva fatto richiesta, dei nominativi di tutti i soggetti residenti presso una casa di riposo che erano stati trasportati presso gli ospedali della zona per visite e accertamenti sanitari, e non soltanto del singolo parente.

Nel riscontrare le specifiche richieste di chiarimenti dell'Ufficio, la casa di riposo si è impegnata, qualora si ripresentasse una simile richiesta, a fornire dati anonimi, per quel che riguarda i soggetti diversi dal familiare, in modo da evitare la ripetizione della condotta lamentata.

Alla luce delle idonee assicurazioni fornite, non sono stati adottati specifici provvedimenti da parte del Garante (art. 11, comma 1, lett. *d*) e 13, comma 4, del regolamento n. 1/2007) (*Nota* 11 giugno 2010).

Su un altro piano, merita particolare attenzione un parere reso alla Presidenza del Consiglio dei ministri-Commissione per l'accesso ai documenti amministrativi.

Nella vicenda un genitore, avendo trovato nella camera della figlia sedicenne una confezione di un farmaco contraccettivo già utilizzato, aveva chiesto all'azienda sanitaria di zona di accedere ai documenti sanitari più recenti della minore per assicurarsi, a suo dire, che il farmaco fosse stato prescritto da personale medico.

Nel parere, l'Autorità ha condiviso quanto affermato dalla Commissione secondo la quale, in base alla l. 22 maggio 1978, n. 194, i minori possono rivolgersi alle aziende ospedaliere e ai consultori senza che i genitori ne siano informati in quanto, l'obiettivo

della norma è quello di garantire l'anonimato dei minorenni che non vogliano o non possano mettere al corrente i propri genitori, ed evitare che le minori possano rivolgersi clandestinamente a soggetti privi della necessaria affidabilità, serietà e professionalità invece che a strutture sanitarie autorizzate, in grado di assicurare le necessarie garanzie (*Parere* 17 novembre 2010 [doc. web n. 1769451]).

4.1.5. La ricerca scientifica

Nel corso dell'anno l'Autorità ha in più di un caso autorizzato il trattamento di dati relativi allo stato di salute degli interessati, in mancanza del loro consenso, a fini di ricerca scientifica in campo medico ed epidemiologico (art. 110 del Codice). Le autorizzazioni sono state accordate in ragione della rilevanza degli scopi scientifici perseguiti, nonché delle difficoltà, rappresentate nei diversi casi, di informare i pazienti per acquisire il loro consenso, trattandosi di studi retrospettivi relativi a cospicui campioni di interessati, spesso irreperibili.

In tutti i casi è stato autorizzato il trattamento delle sole informazioni indispensabili per lo svolgimento degli studi, e sono state individuate le precauzioni nel curare ed incrementare il livello di sicurezza del trattamento dei dati in conformità alle “*Linee-guida per i trattamenti di dati personali nell'ambito delle sperimentazioni cliniche di medicinali*” (*Prov. 24 luglio 2008* [doc. web n. 1533155]).

Più in dettaglio, con un *provvedimento* (27 aprile 2010 [doc. web n. 1722683]) un'università francese è stata autorizzata ad accedere alla documentazione medico-clinica di un campione di circa 3.000 pazienti italiani con insufficienza epatica acuta, per uno studio retrospettivo di farmacoepidemiologia che coinvolgeva i centri trapianti di 7 Paesi europei, volto ad individuare i potenziali rischi per la salute derivanti da farmaci antinfiammatori contenenti una determinata sostanza attiva.

Lo studio era stato raccomandato dall'Agenzia europea per i medicinali, ed alla sua realizzazione era stato subordinato, dalla Commissione europea, il mantenimento delle autorizzazioni all'immissione in commercio (cfr. art. 133 d.lgs. del 24 aprile 2006, n. 219).

Il *provvedimento* di autorizzazione ha però prescritto che, qualora i pazienti dovessero

tornare a rivolgersi ai centri trapianti, dovranno essere informati sul trattamento dei loro dati e dovrà essere richiesto il loro eventuale consenso.

Un'altra autorizzazione (*Prov. 16 settembre 2010 [doc. web n. 1753153]*) è stata rilasciata ad una casa farmaceutica, promotrice di uno studio clinico sul tumore alla mammella, ad un'azienda ospedaliera, quale centro di ricerca coordinatore, e ad altri 48 centri di cura, per accedere alla documentazione medico-clinica di un campione di 1.000 pazienti curate presso gli stessi centri, in assenza del consenso al trattamento dei dati di coloro che, al momento dell'arruolamento, risultassero irreperibili o decedute, a seguito di apposite verifiche effettuate dal personale medico dei centri partecipanti.

Lo studio, prevedeva di raccogliere retrospettivamente i dati clinici delle pazienti che avevano iniziato il trattamento nel 2007, quando alcuni farmaci non erano in uso, per confrontarli con quelli delle pazienti sottoposte nel 2009-2010 alle nuove terapie in esame.

L'autorizzazione prevede che i nominativi delle donne, siano trattati esclusivamente dai centri di cura preposti, nella sola fase di individuazione del campione e di raccolta dei dati sanitari dalle cartelle cliniche, mentre nelle fasi successive dello studio, a partire dalla registrazione dei dati, questi siano sostituiti con un codice identificativo univoco associato ai singoli centri. Una volta concluso lo studio, i dati raccolti vanno trasformati in forma anonima.

Per garantire, a partire dalla fase di registrazione dei dati, la loro protezione dai rischi di accesso non autorizzato o di trattamento non consentito, è stato indicato anche il ricorso a tecnologie crittografiche. Inoltre, con riferimento al *database* centralizzato per l'archiviazione dei dati dello studio devono essere previsti sistemi di *audit log* in grado di garantire la loro inalterabilità, al fine di assicurare il controllo degli accessi al *database* e il rilevamento di eventuali anomalie.

Un'altra autorizzazione è stata rilasciata all'Istituto superiore di sanità, per il trattamento dei dati personali riguardanti le donazioni effettuate e le trasfusioni ricevute da soggetti segnalati al Registro della malattia di *Creutzfeldt-Jacob* e sindromi correlate, per uno studio epidemiologico retrospettivo sul rischio di trasmissione della forma sporadica della malattia attraverso le trasfusioni di sangue o di suoi derivati. Lo studio prevede, in

particolare, di raccogliere i dati personali e sanitari dei donatori di sangue a pazienti inseriti nel Registro, nonché dei riceventi trasfusioni dai medesimi pazienti presso i centri di coordinamento regionale sangue e le strutture trasfusionali periferiche, tramite la collaborazione del Centro nazionale sangue, nonché presso le aziende sanitarie di residenza degli interessati.

In particolare, l'Istituto aveva evidenziato l'impossibilità, per motivi etici, di informare i donatori o i trasfusi di soggetti segnalati al Registro della malattia di *Creutzfeldt-Jacob* e sindromi correlate, in quanto ciò li avrebbe portati a conoscenza del rischio di sviluppare in futuro la stessa malattia incurabile e fatale, rischio peraltro non ancora accertato e che lo studio mirava proprio a definire e a quantificare.

Nell'autorizzazione, il Garante ha rilevato che, per le sue caratteristiche, lo studio non avrebbe potuto essere realizzato mediante il trattamento di dati anonimi, né senza l'identificazione, anche temporanea, degli interessati (*Prov. 4 novembre 2010 [doc. web n. 1767796]*).

Sempre nel corso dell'anno, in applicazione dell'art. 105, comma 4, del Codice e dell'art. 6, comma 4, del codice deontologico per i trattamenti di dati personali per scopi statistici e scientifici, sono state individuate le modalità per l'informativa, da parte dell'Istituto superiore di sanità, in collaborazione con il Ministero della difesa, da rendere per la realizzazione del Progetto di sorveglianza epidemiologica dei tumori nella popolazione militare impegnata in Bosnia-Herzegovina e nel Kosovo —ove è stato fatto uso di uranio impoverito— incluso nel programma nazionale per la ricerca sanitaria di cui all'art. 12-*bis* del d.lgs. n. 502/1992. Il progetto prevede la realizzazione di due studi retrospettivi volti a verificare la mortalità e l'incidenza di tumori nei membri di due coorti formate dai militari inviati in missione nei medesimi territori dal 1995 al 2004 e da un campione di carabinieri, mai impegnati in teatri operativi all'estero.

Ritenendo che il conferimento dell'informativa a ciascun interessato, ai sensi dell'art. 13 del Codice, avrebbe richiesto uno sforzo sproporzionato rispetto al diritto tutelato, il Ministero della difesa ha quindi informato l'Autorità di voler pubblicare l'informativa su due quotidiani di diffusione nazionale, sui siti Internet del Ministero della difesa, delle