esclusivamente tramite la Banca dati nazionale dei contratti pubblici (Bdncp), istituita presso l'Avcp medesima. Tale atto è volto ad individuare i dati da inserire nella Bdncp al fine di consentire alle stazioni appaltanti/enti aggiudicatori di verificare il possesso dei requisiti degli operatori economici per l'affidamento dei contratti pubblici; a istituire il nuovo sistema *AVCPass* (*Authority Virtual Company Passport*), finalizzato alla verifica *online* dei requisiti attraverso la Bdncp, dotato di apposite aree dedicate ad operatori economici e a stazioni appaltanti/enti aggiudicatori; a stabilire i termini e le regole tecniche per l'acquisizione, l'aggiornamento e la consultazione dei predetti dati.

Il testo tiene conto delle indicazioni fornite all'Avcp dall'Ufficio del Garante, riguardanti in particolare, le modalità di realizzazione dei flussi informativi previsti nell'ambito del sistema *AVCPass*, la definizione di misure di sicurezza idonee a garantire i rischi di accessi non autorizzati e di trattamenti non consentiti o non conformi alle finalità della raccolta.

Il parere favorevole del Garante è stato, infine, condizionato all'esplicitazione del tempo di conservazione dei dati relativi agli accessi e alle operazioni compiute nel sistema (parere 19 dicembre 2012 [doc. web n. 2171106]).

4.9. L'ATTIVITÀ GIUDIZIARIA

Sicurezza nelle intercettazioni

Con delibera del 13 settembre 2012 il Garante ha avviato gli accertamenti volti a verificare l'idoneità delle misure di sicurezza adottate in relazione ai trattamenti di dati svolti presso le procure della Repubblica, anche tramite la polizia giudiziaria o soggetti terzi, nell'ambito delle attività di intercettazione di conversazioni o comunicazioni, effettuate per ragioni di giustizia, nonché preventive (artt. 266 e ss. c.p.p.; art. 226 disp. att. c.p.p.).

Al fine di individuare modalità operative e di cooperazione più efficaci il Garante, in una prima fase, ha inoltrato una preliminare richiesta di informazioni volta ad acquisire da alcune procure di medie dimensioni, dislocate in diverse aree del territorio nazionale e che hanno sede presso capoluoghi di provincia, elementi conoscitivi utili all'espletamento dei successivi accertamenti da svolgere *in loco*.

Le procure interpellate hanno fornito le informazioni richieste, che sono all'esame dell'Autorità.

Pubblicità dei dati nei procedimenti di espropriazione forzata

Anche nel 2012 sono pervenute segnalazioni relative al regime di pubblicità nell'ambito dei procedimenti di espropriazione forzata introdotto dalla riforma del processo esecutivo che prevede la pubblicazione in appositi siti internet di copia dell'ordinanza del giudice che dispone sulla vendita forzata e della relazione di stima dei beni da espropriare (d.l. 14 marzo 2005, n. 35, convertito, con modificazioni, dalla l. 14 maggio 2005, n. 80).

Al riguardo con due segnalazioni veniva lamentata la pubblicazione, sui siti istituzionali di due tribunali, di avvisi d'asta che recavano, tra le altre informazioni, i nominativi delle persone intestatarie dell'immobile oggetto della vendita nonché, nel primo caso, diverse immagini nelle quali erano riconoscibili i soggetti esecutati e, nel secondo, il nome del defunto coniuge di una delle persone soggette ad esecuzione.

Svolte le necessarie verifiche, l'Autorità ha rappresentato ai presidenti dei tribunali che, negli avvisi di vendita, dev'essere omessa l'indicazione del debitore (art. 490, comma 3, c.p.c., come modificato dall'art. 174, comma 9, del Codice) e, con riferimento ai documenti generalmente allegati agli avvisi d'asta, ha ribadito che anche i trattamenti di dati personali effettuati per motivi di giustizia sono assoggettati ai princìpi sanciti dall'art. 11 del Codice, fra i quali il principio di pertinenza e non eccedenza (comma 1, lett. *d)*).

Alla richiesta di fornire riscontro in ordine alle determinazioni adottate, nel primo caso il giudice delegato ai fallimenti ha disposto che la società incaricata della pubblicazione degli avvisi d'asta sul sito del tribunale provvedesse all'oscuramento di tutti i dati personali identificativi relativi a soggetti a vario titolo coinvolti nelle procedure esecutive individuali e concorsuali presenti negli atti pubblicati *online* e ha altresì disposto l'oscuramento di tutti i dati personali relativi ai segnalanti. La società destinataria del provvedimento ha ottemperato al disposto dandone avviso al giudice delegato e al Garante.

Nel secondo caso il presidente del tribunale ha rappresentato che l'associazione notarile per le procedure esecutive ha predisposto che i professionisti che redigono gli avvisi di vendita forniscano al soggetto addetto alla pubblicità documenti già privi di ogni dato non pertinente. La società responsabile per la pubblicazione in internet ha confermato che l'avviso d'asta oggetto della segnalazione non era più reperibile in rete (note 2 dicembre 2011 e 27 settembre 2012).

Competenza in materia di trattamento dei dati di parlamentari da parte di un organo delle Camere

Alcuni parlamentari avevano presentato al Garante un reclamo nei confronti del Presidente del Consiglio di giurisdizione della Camera dei deputati che, durante una conferenza stampa che aveva avuto vasta eco sui mezzi di informazione, aveva rivelato i nomi dei deputati ed *ex* deputati che avevano presentato ricorso avverso una deliberazione dell'Ufficio di Presidenza della Camera che aveva introdotto norme restrittive del loro trattamento previdenziale.

Il Garante ha dichiarato inammissibili i reclami in quanto il Consiglio di giurisdizione, quale organo della Camera dei deputati, è espressione del potere di autodichia degli organi costituzionali, disciplinato dai relativi regolamenti, nell'ambito della sfera di autonomia riservata loro dalla Costituzione (art. 64, primo comma). In ragione di tale autonomia, il Codice prevede che i trattamenti di dati personali effettuati dagli organi costituzionali sono disciplinati dai medesimi organi in conformità ai rispettivi ordinamenti (art. 22, comma 12) e la deliberazione n. 208 del 26 ottobre 2004 dell'Ufficio di Presidenza della Camera, recante la "Normativa in tema di protezione dei dati personali", stabilisce che, in tale materia "*si applicano le norme relative alla tutela dinanzi agli organi di giurisdizione interna della Camera dei deputati*" (art. 4). Trattandosi di atti di autonomia normativa adottati dal Parlamento ai sensi dell'art. 64, primo comma, della Costituzione, i regolamenti sono sottratti ad ogni sindacato da parte di qualsiasi altro potere dello Stato (cfr. Corte cost., sentenza n. 154 del 1985; Corte europea dei diritti dell'uomo, *Affaire Savino et autres c. Italie;* sentenza del 28 aprile 2009; Cass. civ., sez. unite, sentenza n. 11019/2004) (nota 3 aprile 2012).

Contenuto del decreto di giudizio immediato *ex* art. 456 c.p.p.

È stato sottoposto all'Autorità un quesito in ordine alla conformità alla disciplina del Codice dell'inserimento del domicilio della persona offesa nei decreti di disposizione del giudizio immediato nei confronti dell'imputato, di cui all'art. 456 c.p.p.. Il Garante ha ricordato che in base alla normativa applicabile (art. 52 del Codice e art. 456 c.p.p.) l'indirizzo della persona offesa, ancorché non formalmente indicato quale requisito del decreto di fissazione del giudizio immediato, costituisce tuttavia un'informazione essenziale ai fini della necessaria notificazione del provvedimento, salvo il caso in cui la parte abbia un difensore (domiciliatario *ex lege*). La questione appare peraltro rivestire una rilevanza formale, in quanto sia il difensore dell'imputato -che può svolgere indagini difensive ai sensi degli

artt. 391-*bis* e ss. c.p.p.- sia lo stesso imputato personalmente, hanno il diritto di prendere visione di tutti gli atti del fascicolo delle indagini, dove sono riportate le generalità complete e l'indirizzo anche della persona offesa; pertanto, omettere l'indirizzo nella copia del decreto che viene notificata all'imputato e al suo difensore appare una precauzione sostanzialmente inutile, a fronte dei diritti e delle garanzie di difesa (nota 30 novembre 2012).

Astensione dall'incarico di un consulente tecnico d'ufficio

In ordine ad un presunto trattamento illecito dei dati personali effettuato da un consulente tecnico d'ufficio nella comunicazione al magistrato dei motivi di astensione dall'incarico, che il segnalante riteneva lesiva della propria riservatezza e dannosa per la propria posizione processuale, il Garante ha ritenuto legittima tale comunicazione, in quanto il consulente che intende astenersi deve farne denuncia o istanza al magistrato che gli ha conferito l'incarico, perché si valuti se ricorra un giusto motivo di astensione (art. 63 c.p.c., 192 disp. att. c.p.c.) (nota 8 ottobre 2012).

Banca di dati sanitari ed attività dell'autorità giudiziaria

Una procura della Repubblica ha posto al Garante un interessante quesito riguardante la fattibilità di un protocollo da stipularsi tra la procura stessa e alcuni enti pubblici competenti, a vario titolo, in materia sanitaria, per favorire l'emersione delle patologie oncologiche aventi un nesso con l'esposizione lavorativa, attraverso l'inserimento in una banca dati condivisa delle informazioni in possesso degli enti firmatari -quali generalità del malato, patologia, attività lavorativa prestata, mansioni svolte- ai fini dell'eventuale promozione, da parte dell'autorità giudiziaria, di procedimenti penali tesi all'accertamento di responsabilità penali.

Il Garante, pur apprezzando lo scopo dell'iniziativa, ha rilevato che appare dubbio che i trattamenti svolti per ragioni di giustizia, come normativamente definiti, comprendano l'acquisizione ed il monitoraggio preventivo e generalizzato dei dati personali di tutti i lavoratori affetti dalle malattie croniche dalle caratteristiche eziologiche sopra precisate, al fine di individuare eventuali ipotesi delittuose. Del resto, il Codice prevede che l'autorità giudiziaria possa acquisire atti e documenti da soggetti pubblici, anche per via telematica, solo in conformità alle vigenti disposizioni processuali (art. 48 del Codice), ma il protocollo non individua un'idonea base normativa, che non potrebbe rinvenirsi nella disciplina sui poteri di accertamento dei reati da parte del pubblico ministero che non legittimano un flusso indiscriminato di dati, soltanto alcuni dei quali potrebbero costituire *notitiae criminis*.

Secondo la giurisprudenza di legittimità, inoltre è da escludere che possano essere promosse indagini preliminari non già sulla base di una notizia di reato, ma al fine di eventualmente acquisirla, con indagini a tappeto e in forma indiscriminata, dirette ad accertare se eventualmente ipotetici reati sono stati commessi (Cass., sez. terza, sentenza n. 3261/1999).

D'altro canto, poiché il trattamento -quindi, anche la comunicazione- di dati sensibili da parte di soggetti pubblici è consentito solo se autorizzato da espressa disposizione di legge (art. 20 del Codice), gli enti partecipanti al progetto non possono conferire tali dati per autonoma e volontaria determinazione, non avendo la piena ed incondizionata disponibilità dei dati detenuti *ratione officii* essendo, invece, necessaria una specifica norma di legge -come nel caso del "Sistema informativo nazionale per la prevenzione nei luoghi di lavoro", previsto e disciplinato dall'art. 8 del d.lgs. 9 aprile 2008, n. 81- o una autorizzazione del Garante (nota 12 dicembre 2012).

Ordini di esibizione dell'autorità giudiziaria

Con riferimento al quesito di un istituto pubblico in relazione alle richieste inoltrate dall'autorità giudiziaria ai sensi dell'art 256 c.p.p. di esibizione o sequestro di dati coperti dal segreto statistico, il Garante ha rappresentato che in base al Codice (art. 108) il trattamento di dati personali effettuato per scopi statistici da parte di soggetti che fanno parte del Sistema statistico nazionale, resta disciplinato, oltre che dal codice di deontologia e di buona condotta (provv. 16 giugno 2004 [doc. web n. 1556635]), dal d.lgs. 6 settembre 1989, n. 322 il quale detta, tra l'altro, disposizioni per la tutela del segreto statistico e indica anche i dati che non sono coperti dal segreto (art. 9).

Spetta pertanto all'istituto verificare se i dati oggetto della richiesta dell'autorità giudiziaria rientrano tra quelli coperti dal segreto statistico, attenendosi, in quest'ultimo caso, a quanto prevede l'art. 256 c.p.p. (nota 9 febbraio 2012).

Richiesta del giudice civile di accesso ai tabulati telefonici

Un tribunale ha chiesto al Garante di esprimersi sulla legittimità del rifiuto, opposto da alcune società telefoniche, all'ordine di esibizione dei tabulati telefonici emanato, ai sensi dell'art. 210 c.p.c., nell'ambito di una controversia civile.

Il Garante ha ricordato che i dati relativi al traffico telefonico non più necessari ai fini della trasmissione della comunicazione elettronica sono cancellati o resi anonimi dal fornitore del servizio, al quale è consentito il trattamento a fini di fatturazione per un periodo non

superiore a sei mesi, salva l'ulteriore conservazione necessaria per effetto di una contestazione anche in sede giudiziale. Al di fuori di tali ipotesi, i dati relativi al traffico telefonico sono conservati dal fornitore per ventiquattro mesi dalla data della comunicazione, solo per finalità di accertamento e repressione di reati (art. 132 del Codice, commi 1 e 3), non per richieste formulate nell'ambito di una controversia civile, amministrativa e contabile (in tal senso v. provvedimento generale sulla sicurezza dei dati di traffico telefonico e telematico del 17 gennaio 2008 [doc. web n. 1482111]).

Pertanto, il diniego opposto dalle società telefoniche all'ordine dell'autorità giudiziaria *ex* art. 210 c.p.c., è apparso legittimo, poiché l'ostensione di tali dati in sede civile è ammessa solo in controversie attinenti alla fatturazione del servizio (nota 31 ottobre 2012).

4.9.1. L'informatica giuridica

Linee-guida per la diffusione dei provvedimenti giudiziari

Le "Linee-guida in materia di trattamento di dati personali nella riproduzione di provvedimenti giurisdizionali per finalità di informazione giuridica", adottate dal Garante con delibera del 2 dicembre 2010 (in G.U. 4 gennaio 2011, n. 2 [doc. web n. 1774813]), prevedono che l'anonimizzazione del provvedimento giudiziario in caso di riproduzione per finalità di informazione giuridica, mediante oscuramento delle generalità e di ogni altro elemento in grado di identificare l'interessato, 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).

Al riguardo sono pervenuti all'attenzione dell'Autorità casi di cittadini che non avevano chiesto l'anonimizzazione della sentenza nel corso del giudizio, come previsto dall'art. 52 del Codice.

Con una segnalazione è stata lamentata la pubblicazione, sul sito internet di un ministero, di una sentenza concernente un procedimento giudiziale in cui era stato coinvolto il segnalante, successivamente indicizzata da un motore di ricerca.

Benché già prima della segnalazione il ministero avesse proceduto, su istanza dell'interessato -presentata oltre i termini di cui all'art. 52 del Codice-, ad anonimizzare la sentenza, la stessa risultava ancora associata al segnalante, digitando il suo nominativo nel motore di ricerca.

Il Garante ha in primo luogo rilevato che l'interessato non aveva presentato all'autorità giudiziaria l'istanza di anonimizzazione della sentenza prima che fosse definito il relativo grado di giudizio, sicché nessuna responsabilità per la pubblicazione integrale del provvedimento poteva attribuirsi al ministero né al motore di ricerca, che si limita ad offrire ospitalità sui propri *server* a siti internet gestiti dai relativi titolari in piena autonomia quale "*mero fornitore del servizio di fruizione della rete ... e assolvendo ad un'attività di mero trasporto delle informazioni*" (Cass. civ., sentenza n. 5525/2012; Trib. di Milano, ordinanza 24 marzo 2011).

Il gestore del motore di ricerca, su richiesta dell'Autorità, ha comunque eliminato la copia *cache* relativa alla pagina web oggetto della segnalazione (nota 27 aprile 2012).

In un altro caso l'interessato, lamentando la facile reperibilità in internet di una sentenza penale di condanna emessa nei suoi confronti, completa dei suoi dati identificativi e di informazioni di natura giudiziaria, aveva chiesto di evitare che il proprio nominativo potesse essere utilizzato come chiave di ricerca nei motori presenti in rete, tenuto conto del disagio creato nell'ambito della propria vita personale e professionale dalla facile reperibilità della sentenza.

Il Garante ha sottoposto la vicenda all'attenzione dell'organo giudicante, che accogliendo la richiesta dell'Autorità ha proceduto all'oscuramento della sentenza (nota 18 novembre 2011).

4.9.2. Notificazioni di atti e comunicazioni

Nel 2012 sono pervenute tre sole segnalazioni circa le modalità di notificazione di atti giudiziari in modo non conforme alle prescrizioni del Codice.

Notificazioni di atti giudiziari non a mani proprie

In un caso è stata lamentata la notificazione di un provvedimento giudiziario effettuata dall'ufficio notifiche del tribunale mediante consegna, in assenza dell'interessato, a mani del figlio convivente in plico non sigillato.

Al riguardo il Garante ha ricordato all'ufficio notifiche che l'art. 174 del Codice, nel modificare alcuni articoli dei codici di rito, ha previsto, ove la notifica non possa essere eseguita nelle mani proprie del destinatario, l'inserimento di copia dell'atto in busta chiusa e

sigillata su cui viene apposto il solo numero cronologico della notificazione, dandone atto nella relazione in calce all'originale e alla copia dell'atto stesso.

Il Garante ha quindi richiamato l'ufficio notifiche al rispetto di tali norme, a tutela della riservatezza dei destinatari degli atti (nota 2 aprile 2012).

Notificazioni di atti giudiziari presso il luogo di lavoro

Un cittadino ha lamentato che un agente della Guardia di finanza, al suo rifiuto di ricevere presso il suo luogo di lavoro la notificazione di un provvedimento giudiziario alla presenza dei colleghi dell'interessato, aveva telefonato ai propri superiori per chiedere consigli. Al riguardo l'Autorità non ha ravvisato violazioni della disciplina in materia di protezione dei dati personali, in quanto l'art. 139 c.p.c. prevede espressamente la notificazione di atti giudiziari anche sul luogo di lavoro del destinatario e, nel caso di specie, l'agente si era limitato a chiedere informazioni sulla corretta procedura da seguire, senza divulgare il contenuto dell'atto a terzi (nota 28 agosto 2012).

Con riferimento alla notifica di atti giudiziari mediante fax sul luogo di lavoro, il Garante, nel ricordare anche in questo caso che è ammessa la notificazione di atti sul luogo di lavoro (artt. 138 e 139 c.p.c.) (v. anche provv. 22 ottobre 1998 [doc. web n. 1104097]), ha altresì rilevato che il vigente codice di procedura civile contempla esplicitamente anche l'utilizzo del fax (art. 250 c.p.c., come modificato dall'art. 2, comma 3, d.l. 14 marzo 2005, n. 35, convertito, con modificazioni, con l. 14 maggio 2005, n. 80) (nota 29 febbraio 2012).

5. La sanità

5.1. I trattamenti per fini di cura della salute

Nel 2012 l'Autorità ha continuato ad occuparsi dei trattamenti dei dati sanitari effettuati da soggetti pubblici e privati per finalità di prevenzione, diagnosi, cura e riabilitazione dell'interessato.

A seguito di alcune segnalazioni, l'Autorità è intervenuta in due casi in cui sia un ambulatorio per la cura di patologie cardiovascolari sia una struttura sanitaria specializzata nella cura di malattie neurologiche avevano inviato a numerosi indirizzi di posta elettronica, visibili a tutti i destinatari, una e-mail riguardante proposte terapeutiche e scelte organizzative degli ambulatori stessi. In tal modo, i destinatari della e-mail erano venuti a conoscenza dei nominativi di tutti gli altri pazienti. A seguito dell'intervento del Garante, le aziende sanitarie hanno curato un adeguato addestramento del personale per evitare il ripetersi di tali incidenti. L'Autorità ha, tuttavia, avviato un procedimento sanzionatorio nei confronti delle aziende sanitarie per la comunicazione a terzi di dati idonei a rivelare lo stato di salute degli interessati senza il loro consenso (note 23 febbraio e 13 novembre 2012).

A seguito di un'altra segnalazione, l'Autorità ha ricordato ad un ospedale lombardo che in caso di accesso da parte del paziente alla cartella clinica, redatta con grafia illeggibile, la stessa deve essere trascritta in modo che le informazioni sanitarie risultino chiare per il malato, essendo la leggibilità la prima condizione per la piena comprensione dei dati personali che riguardano l'interessato (nota 2 febbraio 2012).

L'Autorità è stata chiamata anche ad esprimersi in merito alla possibilità di videoregistrare il parto a cura del marito/convivente.

Al riguardo, il Garante ha ribadito che la videoripresa, da parte di un familiare o di una persona di fiducia, della partoriente che vi si sottoponga volontariamente configura un trattamento di dati per fini esclusivamente personali come tale non soggetto alla disciplina del Codice. Tale esclusione opera esclusivamente nel caso in cui i dati in tal modo raccolti non siano destinati ad una comunicazione sistematica o alla diffusione e siano trattati in ambito familiare o amicale, ferma restando l'autonomia organizzativa della struttura sanitaria

in merito alla facoltà di ammettere i familiari o persone di fiducia del paziente durante lo svolgimento della prestazione sanitaria, nel rispetto di eventuali manifestazioni di volontà contrarie espresse dagli operatori sanitari presenti (nota 2 febbraio 2012).

Nel 2012 l'Autorità è inoltre intervenuta per ricordare al personale medico che deve trattare i dati personali dei pazienti per le sole finalità istituzionali proprie della struttura sanitaria in cui opera e non anche per ulteriori finalità, quali quelle di informare i pazienti circa i recapiti dello studio presso il quale viene svolta attività professionale privata (nota 2 febbraio 2012).

Limiti ancora più stringenti devono ravvisarsi per l'attività di propaganda elettorale a favore di candidati interni alla struttura sanitaria o da questi sostenuti. Il personale medico delle strutture sanitarie non può, infatti, utilizzare per fini elettorali indirizzari o altri dati personali raccolti per fini di cura della salute dell'interessato (nota 13 dicembre 2012).

A seguito di alcune notizie stampa l'Autorità è inoltre intervenuta nei confronti di una società operante in ambito sanitario che dichiarava di essere "*L'unico ente di certificazione riconosciuto (...) dal Garante della privacy per la verifica della conformità dei medical file alle disposizioni contenute nella normativa di settore*". Al riguardo, il Garante ha precisato che attualmente la disciplina in materia di protezione dei dati personali non prevede meccanismi di certificazione, sigilli o marchi di protezione dei dati e spetta solo all'Autorità verificare il rispetto della disciplina in materia di protezione dei dati personali, prescrivendo, se del caso le misure necessarie. L'Autorità ha, pertanto, invitato la società a non lasciar intendere che il suo operato sia autorizzato o riconosciuto dal Garante, nonché a chiedere alla testata giornalistica che aveva riportato la notizia di dare conto di tali precisazioni (nota 21 dicembre 2012).

Tra i diversi casi esaminati merita di essere menzionato uno assai delicato, sotto il profilo della tutela dei dati sensibili, riguardante un sistema di monitoraggio a distanza tramite "etichette intelligenti" (*Rfid*), che in campo sanitario si prestano a molteplici usi, ad esempio per tracciare le sacche di sangue o gli strumenti utilizzati nelle sale operatorie, ovvero per raccogliere dati clinici di pazienti al fine di consentire il controllo a distanza di alcune funzioni vitali (provv. 29 novembre 2012 [doc. web n. 2276103]).

Alcune di queste applicazioni combinano poi l'utilizzo della tecnologia *Rfid* con le tecniche di impianto di *microchip* sottocutaneo su individui.

Il caso trae origine dalla richiesta di una società francese, produttrice di apparecchiature medicali, e di un'azienda ospedaliera volta a valutare la conformità al Codice dei trattamenti di dati effettuati tramite un sistema di monitoraggio remoto di pazienti portatori di defibrillatori cardiaci impiantabili attivi. Il sistema utilizza le etichette intelligenti, inserite nel defibrillatore impiantato sotto la cute del paziente, per consentire agli operatori sanitari di verificare i dati registrati dal dispositivo cardiaco, controllando eventuali anomalie ed effettuando la defibrillazione, ove necessaria, evitando così al paziente la tradizionale visita ospedaliera.

In particolare, le etichette trasmettono i dati registrati dal defibrillatore ad un *monitor* installato a casa del paziente in modalità *wireless*; i dati sono poi trasferiti dal *monitor* al *server* centrale della società attraverso la linea telefonica o *GRPS* per essere consultabili dai medici dell'ospedale via web.

Al riguardo, in considerazione della delicatezza dei dati trattati, è emersa l'esigenza di incrementare il livello di sicurezza delle misure e degli accorgimenti posti in essere, al fine di ridurre i rischi connessi al trattamento dei dati clinici dei pazienti.

L'Autorità ha rilevato -tra l'altro- che la società, per alcune attività di assistenza tecnica, manutenzione e sicurezza del sistema si avvale di operatori esterni in subappalto che possono accedere ai dati clinici dei pazienti. Ha pertanto stabilito che la società designata dall'ospedale responsabile del trattamento può avvalersi per tali attività di terzi subappaltatori -sottoposti ai medesimi obblighi a cui è vincolata la società fornitrice- soltanto previo accordo con l'ospedale. La società deve inoltre inviare all'ospedale i contratti conclusi con i terzi e tenere un elenco aggiornato di tali contratti. Le operazioni di trattamento devono essere registrate e conservate per un periodo di tempo non inferiore a sei mesi. Per evitare che i dati possano essere utilizzati al di fuori del contesto clinico, è stata inoltre prescritta l'adozione di procedure informatiche volte a evitare la copia massiva di dati dal *server* centrale, predisponendo opportuni *alert* in presenza di anomalie.

Qualora i dati registrati dal sistema vengano messi a disposizione di professionisti non

appartenenti alla struttura sanitaria, questi, quali titolari autonomi del trattamento, sono obbligati a raccogliere preventivamente il consenso specifico ed espresso del paziente.

Il paziente inoltre deve poter ottenere in modo agevole la disattivazione del sistema di monitoraggio, con modalità delle quali deve essere data chiara evidenza nel modello di informativa.

L'ospedale deve poi essere tempestivamente informato degli interventi effettuati dal fornitore del servizio o dagli operatori esterni che rendano indispensabile accedere ai dati clinici dei pazienti per esclusive necessità di operatività e di sicurezza del sistema. In particolare, occorre tenere traccia degli utenti abilitati che hanno avuto accesso al servizio e delle altre operazioni eventualmente effettuate anche per consentire all'interessato di controllare i propri dati personali. Tali informazioni devono essere infatti fornite al paziente su sua richiesta.

Le persone autorizzate presso la struttura sanitaria ad accedere al sistema e quelle a vario titolo coinvolte nella manutenzione e nella sicurezza del servizio di monitoraggio devono infine essere adeguatamente istruite sulle funzionalità del sistema e sulle corrette modalità di utilizzo, specie in relazione agli aspetti concernenti la protezione dei dati personali dei pazienti.

5.1.1. L'informativa e il consenso al trattamento dei dati sanitari

Nel 2012 l'Autorità ha ricevuto numerose segnalazioni in merito ai modelli di informativa e di consenso utilizzati in ambito sanitario da parte di strutture pubbliche e private.

In tale ambito il Garante ha prescritto ad una struttura sanitaria privata romana, che aveva fornito prestazioni mediche gratuite nell'ambito di una campagna di prevenzione, di informare correttamente i pazienti sull'uso dei dati, nonché di raccogliere un consenso specifico per ogni tipo di trattamento effettuato (ad es., finalità di cura, comunicazioni a case farmaceutiche), di riformulare i modelli di informativa e consenso per conformarli alla normativa di settore indicando i trattamenti di dati indispensabili all'erogazione della prestazione medica e quelli invece facoltativi (ad es., per finalità di ricerca scientifica, offerta di altri servizi, campagne di prevenzione) ed evidenziando che il mancato consenso per questi ultimi non impedisce di usufruire della prestazione medica richiesta. Il Garante, infine, ha

prescritto alla società di utilizzare i dati finora raccolti esclusivamente per l'esecuzione delle prestazioni sanitarie richieste e per gli adempimenti di legge (es. contabili, fiscali), vietando il loro trattamento per altri tipi di finalità (quali marketing, eventuali comunicazioni a case farmaceutiche) (provv. 9 febbraio 2012 [doc. web n. 1875016]).

Analogamente, ad uno studio radiologico è stato prescritto di modificare i modelli utilizzati per l'informativa ed il consenso, evidenziando per quali dati il conferimento risulti obbligatorio e per quali, invece, facoltativo in relazione alle diverse finalità perseguite, poiché, salvi i casi di emergenza sanitaria, il mancato conferimento dei dati richiesti per le finalità di cura della salute (ivi comprese quelle amministrative a queste strettamente correlate), rende impossibile all'interessato l'accesso alla prestazione sanitaria, mentre il mancato consenso al trattamento dei dati per altre finalità eventualmente perseguite (ad es., ricerca scientifica o invio di referti al medico curante) non deve impedire l'accesso alla prestazione stessa (provv. 15 marzo 2012 [doc. web n. 1893708]).

In termini per vari aspetti simili, è stato fatto presente che qualora il titolare del trattamento intenda effettuare una comunicazione di dati personali a soggetti terzi (ad es., compagnie assicuratrici) non prevista dalla legge, è necessario acquisire uno specifico consenso dell'interessato e specificare nell'informativa se la comunicazione abbia ad oggetto anche dati idonei a rivelare lo stato di salute dell'interessato. In ogni caso, devono essere comunicati a terzi i soli dati indispensabili preferendo, ove possibile, la trasmissione di dati anonimi. A seguito dell'intervento del Garante l'azienda ha provveduto ad inviare un idoneo modello di informativa -attualmente in uso nei rapporti con i pazienti- che risolve le criticità riscontrate dall'Ufficio (nota 13 novembre 2012).

Sono anche state formulate osservazioni sui modelli di informativa e di consenso utilizzati da una azienda ospedaliera torinese con particolare riguardo alla circostanza che il consenso dell'interessato deve essere acquisito dalle aziende sanitarie pubbliche soltanto per il perseguimento delle finalità di cura della salute dell'interessato, e non anche per il trattamento di dati sensibili per finalità di carattere amministrativo, che deve essere conforme alle prescrizioni dello schema tipo di regolamento adottato dalla Conferenza delle regioni e delle province autonome su cui il Garante ha espresso parere favorevole (prov. 26 luglio 2012

[doc. web n. 1915390]; cfr. *infra* par. 5.2.). L'azienda ha conseguentemente modificato i modelli di informativa e consenso (nota 15 novembre 2012).

L'Ufficio è stato chiamato poi a fornire chiarimenti in merito all'obbligatorietà dell'acquisizione del consenso dell'interessato nel caso di trattamenti sanitari iniziati in epoca antecedente alla data di entrata in vigore della normativa in materia di protezione di dati personali. Una struttura sanitaria infatti aveva preso in cura il segnalante nel 1996 avendo poi acquisito il suo consenso al trattamento dei dati sanitari solo nel 2010. Al riguardo, l'Autorità ha ricordato, in base alle norme applicabili (art. 41, comma 1, l. n. 675/1996), che il consenso al trattamento dei dati del segnalante doveva essere acquisito dal primo luglio 2003, sicché il trattamento effettuato sino a quella data deve considerarsi illecito (nota 13 dicembre 2012).

5.1.2. Il fascicolo sanitario elettronico e i dossier sanitari

Già nel 2009 il Garante aveva adottato le "Linee-guida in tema di fascicolo sanitario elettronico (fse) e di *dossier* sanitario"(provv. 16 luglio 2009 [doc. web n. 1634116]) per rispondere, da un lato, alla mancanza a livello nazionale di una normativa quadro, dall'altro, al monito rivolto in sede europea dal Gruppo Art. 29 sulla necessità di individuare specifiche cautele per il trattamento dei dati personali nell'ambito di progetti di sanità elettronica.

Recentemente, con il d.l. 18 ottobre 2012, n. 179 ("Ulteriori misure urgenti per la crescita del Paese") convertito dalla l. 17 dicembre 2012, n. 221, è stata fornita una definizione di fascicolo sanitario elettronico corrispondente a quella elaborata dall'Autorità, individuando quale presupposto legittimante per il suo utilizzo il consenso dell'interessato, così come indicato dal Garante nelle predette linee-guida.

La citata normativa prevede che con decreto del Ministro della salute e del Ministro delegato per l'innovazione tecnologica, acquisito il parere del Garante, dovranno essere stabiliti -tra l'altro- i contenuti del fse, i sistemi di codifica dei dati, le garanzie e le misure di sicurezza da adottare nel trattamento dei dati personali nel rispetto dei diritti dell'assistito, le modalità e i livelli diversificati di accesso al fse. Nel gennaio del 2013 l'Autorità è stata invitata a partecipare al tavolo di lavoro istituito presso il Ministero della salute per l'elaborazione di tale schema di decreto.

Nel 2012, da un accertamento ispettivo, è emerso che le strutture sanitarie pubbliche del Friuli Venezia Giulia utilizzavano un *dossier* sanitario strutturato in modo tale da consentire a tutti i medici -inserendo *username* e *password*- di accedere ai referti di qualsiasi persona avesse effettuato in passato un esame clinico presso le diverse strutture sanitarie della Regione, indipendentemente dalla circostanza che il paziente fosse in cura presso il medico che effettuava il suddetto accesso.

Il Garante, rilevata l'illiceità del trattamento in ragione anche della mancanza di informativa e consenso, ha prescritto, in particolare, che i documenti sanitari attualmente utilizzati attraverso il *dossier* sanitario restino disponibili solo al professionista o alla struttura interna al titolare che li ha redatti (es. informazioni relative a un ricovero utilizzabili dal reparto di degenza) nonché per eventuali conservazioni per obbligo di legge, con l'adozione di idonei accorgimenti anche tecnici, affinché i medesimi documenti sanitari non siano più condivisi con altri professionisti che curino l'interessato presso altri reparti, fino al momento in cui lo stesso esprima uno specifico consenso.

Il Garante ha, inoltre, prescritto a tali strutture sanitarie di mettere in atto, entro un breve periodo, specifici accorgimenti che consentano ai soli professionisti sanitari che hanno in quel momento in cura il paziente (che abbia già manifestato un consenso informato alla costituzione del *dossier*) di accedere al suo *dossier* sanitario per il tempo in cui si articola il percorso di cura (provv. 10 gennaio 2013 [doc. web n. 2284708]).

5.1.3. I referti

L'Autorità è stata chiamata più volte ad intervenire in merito alla possibilità di comunicare le informazioni relative allo stato di salute degli assistiti, ai loro parenti e familiari senza aver acquisito prima uno specifico consenso.

In tali occasioni il Garante ha ribadito che per comunicare dati sensibili per fini di cura a soggetti diversi dall'interessato, in assenza di una disposizione normativa, si dovrà richiedere uno specifico consenso informato a quest'ultimo. Nel caso in cui l'interessato stesso sia incapace di intendere o volere, il consenso deve essere manifestato da parte del legale rappresentante (nota 11 dicembre 2012).

Da notizie stampa l'Ufficio ha appreso la vicenda che in un ospedale in provincia di Milano ad un paziente era stato consegnato al posto del suo referto quello di un altro paziente. Il Garante, sulla base dei riscontri richiesti all'ospedale, ha evidenziato l'illiceità della consegna del referto avviando un procedimento sanzionatorio e prescrivendo all'ospedale di fornire agli incaricati del trattamento dati apposite istruzioni affinché la consegna dei referti avvenga previa verifica dell'identità dell'interessato, o del soggetto da questo delegato, con consegna a quest'ultimo in busta chiusa (provv. 1° marzo 2012 [doc. web n. 1893694]). L'esigenza che informazioni sullo stato di salute siano consegnate a terzi incaricati sulla base di delega scritta, mediante busta chiusa, è stata ribadita anche successivamente. Tale misura non occorre invece nella consegna diretta all'interessato (note 15 novembre e 19 dicembre 2012).

In un altro caso, una paziente di una azienda sanitaria del nord Italia lamentava l'avvenuto invio del referto relativo all'esame istologico dei campioni di tessuto abortivo ad essa prelevati all'indirizzo di residenza del padre. Dalla documentazione agli atti è emerso che la paziente non aveva mai fornito tale indirizzo come recapito presso il quale ricevere comunicazioni da parte dell'azienda sanitaria. Nei confronti di questa è stato pertanto avviato un procedimento sanzionatorio per trattamento illecito di dati personali (nota 27 aprile 2012).

L'esigenza che le informazioni sullo stato di salute siano comunicate all'interessato solo per il tramite di un medico o di un altro esercente le professioni sanitarie che, nello svolgimento dei propri compiti, intrattenga rapporti diretti con il paziente e che gli esiti di esami clinici effettuati siano accompagnati dall'indicazione della disponibilità del medico a fornire ulteriori indicazioni a richiesta è stata richiamata con nota del 6 settembre 2012 .

In relazione alla notizia apparsa su alcuni organi di stampa relativa all'avvenuta installazione presso un'azienda sanitaria toscana di un "totem" a disposizione dei pazienti per la stampa dei referti, il Garante ha ricordato in particolare che devono essere adottate soluzioni, quali la previsione di distanze di cortesia, tali da prevenire l'indebita conoscenza da parte di terzi di informazioni idonee a rivelare lo stato di salute dell'interessato (nota 11 maggio 2012).