lare attenzione è stata posta alle tecniche di anonimizzazione ed alle modalità di aggregazione dei dati personali contenuti nella banca dati che l'Inps deve fornire a Ministero del lavoro e delle politiche sociali, regioni e province autonome, comuni e altri enti pubblici responsabili della programmazione di prestazioni e di servizi sociali e socio-sanitari ed al Mef-Dipartimento della Ragioneria (art. 4, commi 4, 5 e 6). In particolare, sono state individuati specifici livelli di aggregazione (su base territoriale) e cadenze temporali (annuale) per la comunicazione dei dati al Mef per finalità di monitoraggio con l'adozione di ogni opportuna cautela al fine di impedire l'identificazione di singoli interessati. È stata, inoltre, puntualmente descritta la tecnica di anonimizzazione dei dati che l'Inps deve fornire al Ministrero del lavoro e delle politiche sociali, regioni, province autonome, comuni e altri enti pubblici responsabili della programmazione di prestazioni e di servizi sociali e socio-sanitari per finalità di monitoraggio, programmazione nonché per elaborazioni a fini statistici, di ricerca e di studio. Tale procedura prevede, in particolare, che a ciascuna posizione venga associato un codice numerico avente natura causale e non progressiva, senza alcun riferimento ai dati oggetto di trattamento, creato appositamente per anonimizzare i dati in questione e non conservato dall'Inps. Anche in questo caso sono stati previsti valori soglia per le variabili di osservazione, in modo da non trasmettere le posizioni per le quali si potrebbe risalire all'individuazione del soggetto ed è stato precisato che l'Inps fornirà le predette informazioni con riferimento ad una finestta temporale non superiore a tte anni, facendo esplicito divieto di diffondere le informazioni ricevute. Gli enti erogatori possono inviare i dati relativi alle prestazioni sociali agevolate o facendo un invio massivo tramite *upload* di un *file* ovvero ttamite acquisizione interattiva attraverso l'inserimento manuale su una web *form*. Al riguardo, con specifico riferimento alla trasmissione dei dati tramite cooperazione applicativa, è stato specificato, coerentemente con le indicazioni emerse nella fase istruttoria, che viene fatto uso di modelli *advanced* di porta di dominio. Le comunicazioni avvengono in modalità *https* e la verifica degli accessi viene basata sulla mutua autenticazione.

È stato previsto, inoltre, che gli accessi ai servizi *online* sono consentiti solo ad operatori espressamente autorizzati da parte dell'ente, dotati di credenziali personali e non cedibili, tramite l'uso di postazioni di lavoro connesse alla rete IP dell'ente. Al riguardo, l'Inps ha imposto agli enti che accedono alla banca dati in parola di individuare ogni misura atta a garantire che l'accesso avvenga da postazioni specificamente autorizzate inoltre ha esplicitamente previsto il ricorso, per l'accesso ai servizi *online*, all'infrastruttura Spid. Al fine di evitate la duplicazione delle informazioni raccolte nella banca dati, sono stati previsti sistemi di tracciamento, *auditing* e notifica attraverso i quali l'Istituto può verificare la frequenza e la numerosità delle posizioni interrogate ed, eventualmente, sospendere l'accesso dell'utenza del soggetto che risulta aver raggiunto determinate soglie di attenzione. L'Inps ha precisato infine che i dati delle prestazioni sociali agevolate verranno conservati per un periodo di cinque anni oltre il quale saranno archiviati e conservati con i sistemi di *back up* dell'Istituto e, salve le ipotesi previste dalle legge, non saranno accessibili da soggetti terzi.

Il Garante ha reso parere favorevole sullo schema di decreto direttoriale dell'Inps recante il disciplinare tecnico conrenente le "Misure di sicurezza per il trattamento dei dati personali di cui al d.m. 10 gennaio 2013 - attuazione della sperimentazione della nuova carta acquisti - modalità di trasmissione dei dati tra l'Inps e i comuni, livelli e modalità di accesso selettivo ai dati, tracciabilità degli accessi e termini di conservazione dei relativi dati" (provv. 12 marzo 2015, n. 143, doc. web n. 3863732) (art. 11, comma 2, d.m. 10 gennaio 2013).

L'art. 60, d.l. 9 febbraio 2012, n. 5, convertito con modificazioni in l. 4 aprile 2012, n. 35 ha previsto che venga avviata una sperimentazione, nei comuni con più di 250.000 abitanti, volta a favorire la diffusione della carta acquisti tra le fasce di popolazione in condizione di maggiore bisogno (art. 81, comma 32, d.l. 25 giugno 2008, n. 112, convertito, con modificazioni, dalla l. 6 agosto 2008, n. 133) ed ha affidato ad un decreto del Ministro del lavoro e delle politiche sociali, adottato di concerto con il Mef, la definizione delle disposizioni per l'attuazione della sperimentazione della nuova carta acquisti (d.m. 10 gennaio 2013, sul quale il Garante ha fornito il proprio parere di competenza in data 6 dicembre 2012, n. 395, doc. web n. 2216848). Il citato decreto prevede che il cd. soggetto attuatore (Inps) adotti un provvedimento concernente le misure di sicurezza per i trattamenti dei dati personali previsti dal decreto, le modalità di trasmissione dei dati tra lo stesso ed i comuni, i livelli e le modalità di accesso selettivo ai dati, la tracciabilità degli accessi e i termini di conservazione dei relativi dati, su conforme parere del Garante, entro tre mesi dall'entrata in vigore del decreto stesso (art. 11, comma 2). Lo schema di decreto presentato è risultato conforme alle numerose indicazione fornite dall'Ufficio ai competenti uffici dell'Istituto nel corso di contatti, anche informali.

4.10. *L'attività giudiziaria*

Sicurezza nelle intercettazioni

Con provvedimento 25 giugno 2015, n. 375 (doc. web n. 4120817) l'Autorità è nuovamente intervenuta sulla delicata materia delle misure di sicurezza nelle attività di intercettazione da parte delle Procure della Repubblica, con riferimento alle prescrizioni oggetto del provvedimenro 18 luglio 2013, n. 356 (doc. web n. 2551507) i cui termini per l'adempimento erano già stati differiti con provvedimento 26 giugno 2014, n. 322 (doc. web n. 3235971).

Al riguardo, sulla base sia della documentazione trasmessa dal Ministero della giustizia sul monitoraggio dello stato di attuazione delle misure, sia degli approfondimenti svolti presso il Ministero da un tavolo di lavoro a carattere interistituzionale, si è riconosciuto il carattere prioritario alle criticità riguardanti le misure informatiche, di più immediato ed incisivo impatto sulla sicurezza dei trattamenti.

Pertanto si è provveduto nuovamente a differire i termini per l'adempimento di alcune misure informatiche, con riserva di valutare successivamente se l'attuazione di tali misure, e delle altre che siano poste in essere, anche alla luce dell'evoluzione tecnologica, consenta di supetare le prescrizioni di tipo strutturale imposte con il provvedimento del 2013, il cui termine di attuazione è stato, pertanto, sospeso.

Pubblicazione di sentenze a fini di informazione giuridica

È pervenuta a questa Autorità una segnalazione con cui si è lamentata la facile reperibilità in internet di un'ordinanza giudiziaria, recante i dati identificativi, dati sensibili e informazioni di natura sanitaria relativi all'interessato. Al riguardo l'Autorità, nel rappresenrare che l'interessato non si era potuto avvalere della facoltà di richiedere l'anonimizzazione dell'ordinanza non essendosi costituito in giudizio (cfr. art. 52, comma 1, del Codice e le Linee guida in materia di trattamento di dati personali nella riproduzione di provvedimenti giurisdizionali per finalità di informazione giuridica adottate il 2 dicembre 2010, doc. web n. 1774813), ha invitato il Tribunale amministrativo che aveva adottato l'ordinanza a valutare l'opporrunità di anonimizzazione disposta d'ufficio oppure, in alrernativa, l'adozione di accorgimenti tecnici idonei ad evitare l'indicizzazione nei motori di ricerca dell'ordinanza pubblicata sul sito isriruzionale (nota 16 marzo 2015). Il Tribunale ha provveduto

ad oscurare il nome dell'interessato.

Anche nel 2015 sono pervenute all'Autorità 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. 14 maggio 2005, n. 80), 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. Al riguardo, con una segnalazione veniva lamentata la pubblicazione sul sito istituzionale di un Tribunale di avvisi d'asta che recavano, tra le altre informazioni, i nominativi delle parti debitrici. L'Autorità, pur verificando che allo stato attuale gli avvisi non contenevano dati personali relativi agli interessati, ha richiamato l'attenzione del Presidente del Tribunale ove si svolgevano le procedure sulla necessità di applicare la vigente normativa in materia di esecuzioni immobiliari conformemente alla normativa in materia di protezione dei dati personali e alle vigenti prescrizioni di cui agli artt. 174, comma 9, del Codice e 490, comma 3, c.p.c. al fine di assicurare la piena tutela dei diritti dei debitori sottoposti all'esecuzione. L'Autorità ha ricordato, in particolare, di avere già invitato, con provvedimento 7 febbraio 2008 (doc. web n. 1490838) gli uffici giudiziari e i professionisti delegati alle operazioni di vendita nelle esecuzioni immobiliari ad omettere, conformemente a quanto prescritto dagli artt. 174, comma 9, del Codice e 490, comma 3, c.p.c., l'indicazione del debitore e di eventuali terzi estranei alla procedura dagli avvisi d'asta, estendendo tale omissione anche alla documentazione allegata ai predetti avvisi (nota 2 febbraio 2015).

Pubblicità dei dati nei procedimenti di espropriazione forzata

Con riferimento alla produzione documentale in sede giudiziaria, il Garante, nel ricordare preliminarmente che l'art. 24, comma 1, lett. *f*), del Codice consente il trattamento di dati personali senza consenso laddove il trattamento sia indispensabile per far valere o difendere un diritto in sede giudiziaria, ha confermato che spetta al giudice adito, ove ritualmente richiesto, la competenza a valutare la liceità del trattamento dei dati personali. Infatti, l'art. 160, comma 6, del Codice srabilisce che la validità, l'efficacia e l'utilizzabilità di atti, documenti e provvedimenti nel procedimento giudiziario basati sul trattamento di dati personali, ancorché non conforme a disposizioni di legge o di regolamento, restano disciplinate dalle pertinenti disposizioni processuali nella materia civile e penale (note 10 aprile, 13 e 14 maggio, 1° giugno, 8 luglio, 16 ottobre e 6 novembre 2015). L'art. 160, comma 6, del Codice è stato richiamato dall'Autorità con riferimento ad altre segnalazioni relative a trattamenti di dati personali nel corso di procedimento giudiziario (note 6 e 27 novembre 2015).

Produzione di documenti in giudizio

Con riferimento ad altre segnalazioni con cui si lamentava la notifica di atti giudiziari a soggetti estranei alle relative procedure giudiziarie, il Garante ha fatto presente che, trattandosi di atti inerenti al giudizio civile, la loro valutazione spetta al giudice adito ai sensi dell'art. 160, comma 6, del Codice. In un caso, l'Autorità ha tuttavia rappresentato che, laddove l'interessato ritenga che l'atto giudiziario, in quanto notificato ad estranei, si caratterizzi per il suo contenuto lesivo e si collochi al di fuori di un trattamento per finalità di giustizia, può valutare se sia utilizzabile l'interpello di cui all'art. 8 del Codice per far valere nei confronti del titolare del trattamento il diritto alla cancellazione dei dati trattati in violazione di legge ai sensi dell'art. 7, comma 3 lett. *b*) (nota 27 novembre 2015).

Notificazioni di atti giudiziari a soggetti estranei alle procedure

In un altro caso, invece, essendo stata interessata altresì la Procura della Repubblica, l'Autorità ha affermato che l'impossibilità di interferire con l'attività dell'autorità giudiziaria, dotata di poteri di accertamento ben più penetranti di quelli spettanti al Garante, e la necessità di rispettare i diritti dei soggetti coinvolti (quali, in ipotesi, la facoltà di non rendere dichiarazioni, *ex* art. 64 c.p.p.), rendono,

nei fatti, inattuabili gli accertamenti da parte di questa Autorità, indispensabili per assumere le determinazioni di competenza. Del resto, le verifiche che spettano a questa Autorità possono risultare condizionate anche all'esito dell'esposto, quanto meno in ordine all'accertamento dei fatti. Ove perdurasse l'interesse alle determinazioni dell'Autorità, si è chiesto pertanto all'interessato di dare notizia dell'esito del procedimento civile e della querela dallo stesso presentato, per consentire di valutare se residuino margini per le decisioni di competenza dell'Autorità medesima (nota 21 aprile 2015).

Anche con riferimento ad altre segnalazioni, che sono state oggetto di esposti e querele alla Procura della Repubblica, l'Autorità ha sottolineato, tra l'altro, l'impossibilità di interferite con l'attività dell'autorità giudiziaria (nota 10 aprile, 1° giugno, 16 ottobre e 6 novembre 2015).

Acquisizione del certificato penale e comunicazioni di dati giudiziari

A seguito di una segnalazione, l'Autorità si è occupata di alcuni trattamenti di dati giudiziari effettuati da un Tribunale in modo non conforme a quanto sancito dal Codice. In particolare, è stato rilevato che l'acquisizione del certificato penale relativo al segnalante da parte del Tribunale, presso il quale il medesimo segnalante rivestiva il ruolo di assistente amministrativo, sarebbe avvenuta impropriamente "per ragioni di giustizia" *ex* art. 21, d.P.R. 313/2002, mentre appariva correttamenre riferibile alla previsione di cui all'art. 28, d.P.R. 313/2002. Si accertava, altresì, l'avvenuta comunicazione, non in conformità al Codice, dei dati giudiziari relativi al segnalante da parte del Tribunale alla Procura della Repubblica, nonché al Consiglio della magistratura militare. Ciò in quanto il trattamento di dati giudiziati da parte di soggetti pubblici deve essere autorizzato da espressa disposizione di legge o provvedimento del Garante che specifichino le finalità di rilevante interesse pubblico del trattamento, i tipi di dati trattati e di operazioni eseguibili (art. 21 del Codice), che invece nel caso di specie mancavano. Ciò considerato non si sono, tuttavia, ravvisati gli estremi per l'adozione di un provvedimento da parte dell'Autorità, avendo tali condotte esaurito i loro effetti, restando comunque salva la facoltà per l'interessato di adire l'autorità giudiziaria ordinaria per il risarcimento di eventuali danni subiti (nota 25 agosto 2015).

5 La sanità

5.1. *I trattamenti per fini di cura*

Continuano a pervenire numerose segnalazioni in merito al mancato rispetto delle disposizioni in materia di tutela dei dati personali da parte di strutture sanitarie pubbliche e private nell'erogazione dei servizi di diagnosi, cura e riabilitazione degli assistiti.

A seguito della segnalazione di un cittadino, l'Ufficio ha verificato che sul sito web di un'Asl era possibile consultare i dati anagrafici degli assistiti che si erano registrati sullo stesso per usufruire dei servizi *online*. In particolare, inserendo parte di un nome o di un cognome, si potevano consultare le relative schede anagrafiche nelle quali erano riportati la residenza, il codice fiscale e il numero di telefono degli assistiti ed era, inoltre, possibile modificare tali dati nonché cancellare l'*account*. Il Garante ha, così, vietato la diffusione dei dati personali degli assistiti registrati sul portale dell'azienda, rilevando l'illiceità del trattamento effettuato e ha ricordato alle pp.aa. che offrono servizi in rete di adottare idonee misure di sicurezza tali da ridurre al minimo i rischi di accesso non autorizzato o di trattamenti di dati non consentiti (provv. 17 dicembre 2015, n. 665, doc. web n. 4630534). Sebbene l'azienda abbia prontamente adempiuto, bloccando l'accesso indiscriminato ai dati, l'Autorità si è, comunque, riservata di approfondire il caso e ha al contempo avviato un autonomo procedimento sanzionatorio per le violazioni riscontrate.

In altri casi l'Ufficio è intervenuto in relazione ad iniziative promosse dalle aziende sanitarie che prevedevano il trattamento dei dati sulla salute degli assistiti. In un caso, due aziende sanitarie avevano manifestato l'intenzione di implementare un nuovo servizio consistente nel rendere automaticamente disponibili agli organi di stampa le informazioni sugli interventi effettuati dalla Centrale operativa 118 attraverso un collegamento telematico con i sistemi informativi aziendali. Al riguardo, l'Ufficio ha evidenziato i significativi profili di criticità connessi all'automatica messa a disposizione degli organi di stampa dei dati sanitari rilevati negli interventi in emergenza di tutti i pazienti a prescindere dalla rilevanza pubblica della notizia. A seguito dell'intervento dell'Ufficio le aziende sanitarie hanno modificato il progetto non consentendo il collegamento telematico tra gli applicativi in uso presso i servizi del 118 e gli organi di stampa (nota 20 aprile 2015).

Ulteriori chiarimenti sono stati resi nei confronti dei medici di medicina generale con riferimento alle cautele da adottare nella consegna delle ricette o di altri certificati medici qualora – su richiesta dell'interessato – la suddetta documentazione non sia consegnata direttamente ma, ad esempio, da un farmacista indicato dallo stesso interessato. In tali casi è indispensabile che il documento sia contenuto all'interno di una busta chiusa. Qualora l'interessato intenda far ritirare la suddetta documentazione da parte di un terzo (ad es., un parente o un convivente) è necessario che quest'ultimo, al momento del ritiro, esibisca una delega scritta (nota 23 febbraio 2015).

L'Ufficio è intervenuto in merito all'abbandono di documentazione clinica presso locali in disuso di strutture sanitarie dando avvio a un procedimento sanzionatorio per mancata adozione delle misure di sicurezza (nota 5 novembre 2015).

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

Sono pervenute numerose segnalazioni nelle quali i pazienti lamentano di non aver manifestato il proprio consenso al trattamento dei dati sanitari e di non aver ricevuto alcuna informativa in merito all'utilizzo degli stessi o di aver ricevuto al riguardo informazioni insufficienti o lacunose. Le maggiori criticità riscontrate nelle istruttorie hanno riguardato modelli di informativa e consenso nei quali non venivano evidenziati i trattamenti di dati indispensabili all'erogazione della prestazione medica rispetto a quelli facoltativi (ad es., per finalità di ricerca scientifica, offerta di altri servizi, campagne di prevenzione). L'omissione di tale specificazione non consentiva al paziente di comprendere le conseguenze del mancato conferimento del consenso con specifico riferimento alla possibilità di usufruire della prestazione medica richiesta.

A seguito degli interventi dell'Ufficio numerose strutture sanitarie hanno modificato i propri modelli di informativa e di consenso. L'Autorità ha, tuttavia, avviato un procedimento sanzionatorio nei confronti delle predette strutture (note 23 febbraio e 20 maggio 2015).

In relazione all'incremento dei servizi riconducibili alla sanità digitale e alla necessità di regolamentare tale settore, il Garante ha accolto l'invito del Ministero della salute partecipando, già dal mese di luglio, al tavolo di lavoro interistituzionale sulla *m-Health* e sulle *apps* in ambito medico cui partecipa, tra gli altri, il Ministero dello sviluppo economico, l'Istituto superiore di sanità, l'AgID, l'Aifa e l'Università Tor Vergata. Particolare attenzione sarà data all'aspetto dell'informativa e all'acquisizione del relativo consenso.

5.1.2. Il Fascicolo sanitario elettronico e i dossier *sanitari*

Nel periodo di riferimento è stato adottato il primo dei decreti attuativi del Fascicolo sanitario elettronico (di seguito Fse). Con il d.P.C.M. 29 settembre 2015, n. 178 sono stati, infatti, definiti i contenuti del Fse, le responsabilità e i compiti dei soggetti coinvolti, le garanzie e le misure di sicurezza da adottare nel trattamento dei dati personali, le modalità e i livelli diversificati di accesso in relazione alle specifiche finalità, i criteri di interoperabilità, nonché i contenuti informativi e le codifiche del profilo sanitario sintetico e del referto di laboratorio, individuati quali primi contenuti da attivare a livello nazionale.

Su tale decreto l'Autorità aveva espresso parere favorevole nel 2014 (n. 261, doc. web n. 3230826). Lo schema di decreto, elaborato nell'ambito di un tavolo di lavoro istituito presso il Ministero della salute cui ha partecipato l'Ufficio fin dalla sua costituzione nel gennaio 2013, prevede, in particolare, che il paziente sia informato chiaramente e possa decidere con consapevolezza se dare il consenso all'alimentazione del Fse, e in caso positivo, decidere se dare anche il consenso per finalità di cura (in mancanza del quale il fascicolo potrà essere utilizzato solo per finalità di monitoraggio, programmazione e ricerca, con le dovute garanzie di anonimato).

Con riferimento ai trattamenti di dati personali effettuati attraverso il *dossier* sanitario, l'Autorità ha inteso diramare le Linee guida in materia di *dossier* sanitario, al fine di definire un quadro di riferimento unitario per il corretto trattamento dei dati raccolti nei *dossier*, già istituiti o che si intendono istituire, da parte di strutture sanitarie pubbliche e private (provv. 4 giugno 2015, n. 331, doc. web n. 4084632).

Le numerose istruttorie poste in essere negli anni precedenti avevano fatto emergere la necessità di fornire alcuni chiarimenti soprattutto in merito ai principali adempimenti previsti. Affinché i *dossier* sanitari utilizzati presso le strutture sanitarie rappresentino uno strumento di ausilio nei processi di diagnosi e cura dei pazienti, è necessario che gli stessi siano realizzati in maniera da garantire la certezza

dell'origine, la correttezza dei dati e l'accessibilità degli stessi solo da parte di soggetti legittimati. Il provvedimento del Garante stabilisce, in particolare, che ai pazienti deve essere consentito di scegliere, in piena libertà, se far costituire o meno il *dossier* sanitario. In assenza del consenso il medico avrà a disposizione solo le informazioni rese in quel momento dal paziente o in precedenti prestazioni fornite dallo stesso professionista. La mancanza del consenso non deve incidere minimamente sulla possibilità di accedere alle cure mediche richieste. Per poter inserire nel *dossier* informazioni particolarmente delicate (infezioni HIV, interventi di interruzione volontaria della gravidanza, dati relativi ad atti di violenza sessuale o pedofilia) sarà necessario un consenso specifico.

Per consentire al paziente di scegliere in maniera libera e consapevole, la struttura dovrà informarlo in modo chiaro, indicando in particolare, chi avrà accesso ai suoi dati e che tipo di operazioni potrà compiere. Ne deriva, quindi, che nell'informativa al *dossier* deve essere sottolineata l'intenzione da parte del titolare del trattamento di costituire un insieme di informazioni riguardanti l'interessato quanto più complete, che possano documentare parte della sua storia sanitaria attraverso un sistema integrato da parte del personale sanitario che lo avrà in cura; allo stesso tempo l'interessato deve essere informato che, in caso di mancato consenso al trattamento dei dati personali mediante *dossier*, non vedrà preclusa la possibilità di accesso alle cure richieste.

La struttura sanitaria inoltre, dovrà garantire al paziente l'esercizio dei diritti riconosciuti dal Codice (accesso ai dati, integrazione, rettifica, etc.) e la conoscenza del reparto, della data e dell'orario in cui è avvenuta la consultazione del suo *dossier*. Molte delle segnalazioni pervenute al Garante lamentavano accessi al *dossier* sanitario avvenuti per scopi personali (curiosità, cause giudiziarie tra le parti, etc.) o per fini commerciali da parte di personale amministrativo o di personale sanitario che non era mai stato coinvolto nel processo di cura dell'interessato. Tali casi hanno messo in risalto i rischi di accesso non autorizzato e hanno portato l'Autorità a prevedere che l'interessato possa chiedere al titolare del trattamento quali siano stati gli accessi al proprio *dossier*, con l'indicazione del reparto/struttura e della data e dell'ora dell'accesso.

Al paziente dovrà essere, inoltre, garantita la possibilità di oscurare alcuni dati o documenti sanitari che non intende far confluire nel *dossier* mediante il sistema dell'"oscuramento dell'oscuramento" ovvero con modalità tali da non rendere palese la menzionata decisione a chi legittimamente accede ai dati.

Considerata la particolare delicatezza del *dossier* il Garante ha prescritto l'adozione di elevate misure di sicurezza. I dati sulla salute dovranno essere separati dagli altri dati personali e dovranno essere individuati criteri per la cifratura dei dati sensibili. L'accesso al *dossier* sarà consentito solo al personale sanitario coinvolto nella cura. Ogni accesso e ogni operazione effettuata, anche la semplice consultazione, saranno tracciati e registrati automaticamente in appositi *file* di *log* che la struttura dovrà conservare per almeno 24 mesi.

Eventuali violazioni di dati o incidenti informatici dovranno essere comunicati all'Autorità, entro quarantotto ore dalla conoscenza del fatto, attraverso un modulo predisposto dal Garante all'indirizzo: databreach.dossier@pec.gpdp.it.

Alla fine del 2015, dopo l'adozione delle suddette Linee guida l'Autorità è intervenuta con riferimento al tratramento dei dati effettuato tramite il *dossier* sanitario da parte di un'Asl (provv. 22 ottobre 2015, n. 550, doc. web n. 4449114).

Le irregolarità emerse nel corso di un accertamento ispettivo riguardavano il modello di informativa e la mancanza del consenso del paziente per la costituzione del *dossier* sanitario. Il sistema informativo aziendale era poi strutturato in modo tale che l'operatore sanitario potesse effettuare ricerche non solo con riferimento ai pro-

pri pazienti, ma anche a soggetti che non aveva in cura ma che avevano sostenuto un esame clinico presso l'azienda.

Ciò premesso il Garante ha prescritto all'Asl di regolare gli accessi al sistema informativo aziendale, rendendo consultabili i documenti sanitari del paziente contenuti nel *dossier* solo da parte del professionista che lo ha in cura, nonché di integrare il modello dell'informativa in uso, specificando, tra l'altro, i diritti dell'interessato e le modalità attraverso le quali è possibile revocare il consenso ed oscurare uno o più eventi clinici.

L'Ufficio ha, inoltre, in corso ulteriori attività istruttorie in merito alla presunta violazione della disciplina il materia di protezione dei dati personali che si sarebbe verificata a seguito di accessi abusivi al *dossier* sanitario di un paziente da parte di professionisti sanitari che non lo avevano in cura. In uno dei casi in esame tale consultazione sarebbe stata possibile simulando un accesso in emergenza del paziente, in altri casi mediante un accesso diretto al *dossier* in quanto il sistema informativo è risultato privo di meccanismi di profilazione degli utenti.

In un altro caso, con riferimento al *dossier* sanitario utilizzato nell'ambito di un sistema informativo integrato tra i vari servizi di neuropsichiatria infantile regionali, l'Ufficio ha riscontrato alcune criticità in merito alle modalità di condivisione dei dati tra i vari servizi, con particolare riferimento alla circostanza che nella maggior parte dei casi il paziente veniva effettivamente seguito da un solo servizio di neuropsichiatria. A seguito dell'intervento dell'Ufficio, il sistema è stato modificato non consentendo più la possibilità di condivisione dei dati clinici dei minori a livello regionale (nota 21 dicembre 2015).

5.1.3. I referti e la documentazione sanitaria

Nel 2015 vi è stato un incremento delle segnalazioni relative alla consegna di documentazione sanitaria a soggetti diversi dall'interessato sprovvisti di delega. In molti dei casi esaminati la consegna di referti, lettere di dimissione ospedaliera o cartelle cliniche è avvenuta per errore umano dettato dal mancato rispetto delle disposizioni dettate dalla struttura sanitaria in occasione del ritiro della documentazione medica.

Le fattispecie esaminate hanno riguardato, in particolare, informazioni sanitarie riferite a soggetti terzi contenute nella documentazione consegnata all'interessato e la consegna di referti a soggetti non muniti di delega.

Nei casi segnalati, nei confronti dei quali è stato aperto un procedimento amministrativo sanzionatorio, le strutture sanitarie interessate hanno intrapreso azioni correttive nel processo di consegna dei referti, migliorando le procedure di archiviazione della documentazione medica e realizzando una maggiore formazione del personale coinvolto (note 15 gennaio, 9 aprile, 28 luglio e 21 dicembre 2015).

Merita particolare attenzione quanto segnalato da un paziente che aveva ricevuto dalla struttura sanitaria presso la quale si era recato per alcune analisi cliniche le credenziali di accesso al servizio di ritiro dei referti *online* relative alla prestazione erogata in favore di un altro paziente (nota 16 dicembre 2015).

Analogamente, l'Autorità è intervenuta in merito alla consegna in busta aperta presso una farmacia comunale dei referti relativi alle analisi di laboratorio eseguiti presso un'Asl locale. Anche in tal caso, dopo l'intervento dell'Ufficio, sono state predisposte azioni migliorative nonché calendarizzata un'attività formativa nei confronti di tutto il personale dei vari *front office* (nota 4 settembre 2015).

Richieste su delega dell'autorità giudiziaria

Una unità sanitaria locale ha posto al Garante un quesito sulla condotta da assumere a fronte delle richieste di fornire documentazione relativa ad un paziente della struttura, da parte della polizia giudiziaria su delega dell'autorità giudiziaria, Il Garante, considerato che la menzionata attività risulta ricompresa nella previsione

dell'art. 47 del Codice secondo cui, in caso di trattamento di dati personali effettuato – per ragioni di giustizia – presso uffici giudiziari alcune disposizioni del Codice non si applicano, ha rilevato che la normativa in materia di tutela della riservatezza dei dati personali non osta all'esercizio dei poteri di polizia giudiziaria disciplinati dal c.p.p. Spetta, tuttavia, all'Asl valutare se, nel caso di specie, l'ostensione di quanto richiesto sia impedita dal segreto professionale (richiamato nel Codice dall'art. 83), in ipotesi opponibile all'autorità giudiziaria procedente ai sensi e per gli effetti dell'art. 256 c.p.p., sull'applicazione del quale il Garante non ha competenza. Circa i requisititi delle richieste di documentazione, il Garante ha altresì precisato che, purché siano chiari la fonte ed il contenuto dei poteri esercitati, i trattamenti effettuati dalla polizia giudiziaria per attività di indagine o su delega dell'autorità giudiziaria non richiedono una compiuta informativa, comprensiva di tutti gli elementi indicati nell'art. 13 del Codice; del resto, alcune informazioni potrebbero essere non ostensibili, in considerazione di eventuali esigenze di segreto investigativo (329 c.p.p.), la cui violazione è sanzionata penalmente (art. 326 c.p.) (nota del 16 ottobre 2015).

5.1.4. La tutela della dignità della persona

Anche nel 2015 l'Autorità ha prestato particolare attenzione riguardo al trattamento dei dati personali delle donne che decidono di partorire in anonimato con specifico riferimento alla tutela della loro dignità e riservatezza (art. 30, comma 1, d.P.R. n. 396/2000). Sono pervenute, infatti, molte richieste di chiarimenti e alcune segnalazioni in merito al trattamento dei dati personali delle madri che al momento del parto si sono avvalse del diritto di non essere nominate, con particolare riferimento agli effetti della sentenza della Corte costituzionale del 18 novembre 2013, n. 278 sul quadro normativo vigente. Più precisamente, è stato segnalato che talune agenzie di servizi, presumendo l'immediata esecutività della suddetta sentenza, hanno avviato iniziative commerciali per la ricerca delle origini biologiche dei figli nati da donne che si sono avvalse del diritto di partorire in anonimato. In altri casi, sono state più genericamente rappresentate all'Autorità talune iniziative di organi giudiziari, attivati su istanza del figlio biologico, volte a contattare la madre che aveva scelto di non essere nominata nella dichiarazione di nascita.

Al riguardo, l'Autorità ha avviato alcune attività istruttorie nei confronti di strutture sanitarie e agenzie di servizi, anche mediante accertamenti ispettivi, che non hanno evidenziato specifiche criticità relativamente al trattamento dei dati personali in questione. In materia si evidenzia che il Garante ha già inviato una lettera al Presidente della Commissione giustizia della Camera dei deputati in merito alle proposte di legge in materia di anonimato materno, con particolare riferimento alle disposizioni in materia di accesso del figlio adottato non riconosciuto alla nascita, alle informazioni sulle proprie origini e sulla propria identità (segnalazione del 25 settembre 2014). In tale circostanza è stato evidenziato come la sentenza della Corte costituzionale non abbia scalfito il diritto alla riservatezza delle madri che al momento del parto si sono avvalse del diritto di non essere nominate, non avendo la pronuncia interessato il menzionato art. 30, d.P.R. n. 396/2000 ed avendo, al contrario, la Corte ribadito la necessità di proteggere in termini rigorosi il diritto all'anonimato delle donne "attraverso un procedimento, stabilito dalla legge, che assicuri la massima riservatezza" delle stesse. Solo un organico intervento del legislatore può assicurare che il diritto dei figli a conoscere le proprie origini biologiche non vada a completo detrimento della riservatezza delle donne.

Tutele alla conoscibilità dei dati sanitari

Con specifico riferimento alle segnalazioni pervenute in ordine al mancato rispetto delle misure poste a tutela della riservatezza e della dignità della persona nell'erogazione della prestazione sanitaria e nello svolgimento delle attività amministra-

tive a questa connesse, l'Ufficio ha richiamato le strutture segnalate all'adozione di soluzioni tali da prevenire, durante i colloqui, l'indebita conoscenza da parte di terzi di informazioni idonee a rivelare lo stato di salute, prevedendo, ad esempio, apposite distanze di cortesia, tenendo conto dell'eventuale uso di apparati vocali o di barriere (note 28 luglio e 1° ottobre 2015).

In altri casi, l'Ufficio è intervenuto in merito ai certificati rilasciati dagli organismi sanitari ai pazienti affinché questi ultimi possano produrli a terzi per fini amministrativi (ad es., al datore di lavoro per giustificare l'assenza dal lavoro). Tali certificati non devono contenere informazioni in grado di far risalire allo stato di salute dell'interessato: sono rali l'indicazione della struttura o del reparto presso cui ha ricevuto le cure, oppure il timbro recante la specializzazione dell'operatore sanitario che vi abbia provveduto (note 6 maggio e 4 novembre 2015).

Tutte le strutture sanitarie interessare dalle attività istruttorie dell'Ufficio hanno modificato i modelli di certificazione in uso, rendendoli rispettosi delle disposizioni sopra richiamate.

Merita particolare attenzione l'attività svolta con riferimento alla diffusione di immagini ed informazioni relative all'anamnesi e alla diagnosi dei pazienti di un pronto soccorso pubblicate da un medico ivi operante sul *social network Twitter*.

Le immagini pubblicate, sebbene lesive della dignità umana, non sono risultate riferibili a persone identificate o identificabile; i fatti sono srati denunciati alla Procura della Repubblica.

L'Autorità si è occupata della somministtazione e distribuzione dei presìdi sanitari presso le aziende sanitarie locali. Gli interventi hanno riguardato in particolare la necessità che le ditte aggiudicatarie della distribuzione dei suddetti presìdi siano designate responsabili del trattamento ed abbiano ricevuto idonee istruzioni in ordine al trattamento dei dati personali dei pazienti. Questi ultimi, inoltre, devono essere debitamente informati in merito alle caratteristiche del trattamento dei dati sanitari raccolti in occasione della valutazione e della scelta del presidio sanitario (nota 31 luglio 2015). In alcuni casi, a seguito dell'attività istruttoria, è stato aperto un procedimento sanzionatorio nei confronti della struttura sanitaria.

5.1.5. Il trattamento di dati personali concernente l'accertamento dell'infezione da HIV

Continuano a pervenire segnalazioni in merito al mancato rispetto delle misure a tutela della dignità e della riservatezza dei malati di HIV in occasione dell'erogazione di prestazioni sanitarie.

Al riguardo l'Ufficio ha ricordato che la l. 5 giugno 1990, n. 135 "Programma di interventi urgenti per la prevenzione e la lotta contro l'Aids", ha previsto specifiche disposizioni per la protezione del contagio professionale da HIV nelle strutture sanitarie ed assistenziali pubbliche e private, che sono state attuate con il d.m. 28 settembre 1990. In particolare, in considerazione dell'impossibilità "di identificare con certezza tutti i pazienti con infezione da HIV", il legislatore ha previsto alcune "precauzioni finalizzate alla protezione dal contagio [...], nei confronti della generalità delle persone assistite" (cfr. premesse del cit. d.m.). L'Ufficio ha, pertanto, richiamato il provvedimento 12 novembre 2009 (doc. web n. 1686068) in cui ha individuato specifiche garanzie per la raccolta d'informazioni sullo stato di sieropositività dei pazienti da parte degli esercenti le professioni sanitarie, che devono essere tenute in considerazione da tali soggetti nello svolgimento delle proprie attività professionali. In tale provvedimento il Garante ha vietato agli esercenti le professioni sanitarie di raccogliere l'informazione circa l'eventuale stato di sieropositività in fase di accettazione di ogni paziente che si rivolge a questi per la prima volta, indipen-

dentemente dal tipo di intervento clinico o dal piano terapeutico da eseguire, fermo restando che tale dato anamnestico può essere legittimamente raccolto, previo consenso informato dell'interessato, da parte del medico curante nell'ambito del processo di cura (nota 23 febbraio 2015).

In merito al rilascio del codice di esenzione dalla partecipazione al costo per le prestazioni di assistenza sanitaria previsto per le infezioni da HIV l'Autorità ha continuato a collaborare con il Ministero della salute e l'Istituto superiore di sanità, al fine di individuare idonee cautele volte a non far evincere in modo immediato l'esistenza di un'infezione da HIV dalla documentazione amministrativa necessaria all'erogazione della prestazione sanitaria da parte del Ssn. In tal senso, l'Autorità ha condiviso una lodevole iniziativa del Ministero della salute volta a far conoscere a tutti gli Assessorati della sanità delle regioni e province autonome l'esperienza della Regione Toscana relativa all'introduzione di procedure per il riconoscimento dell'esenzione più rispettose della disciplina in materia di protezione dei dati personali (note 5 marzo e 28 luglio 2015).

In occasione di alcune istruttorie l'Ufficio ha inoltre ricordato a diverse strutture sanitarie che la normativa in materia di prevenzione e lotta contro l'Aids non prevede l'anonimato del *test* per accertare l'infezione dell'HIV ma, impone precise cautele in relazione al trattamento del dato relativo all'avvenuto accertamento dell'infezione. La rilevazione statistica dell'infezione da HIV deve essere, infatti, effettuata con modalità tali che non consentano l'identificazione della persona e analogamente le analisi di accertamento di infezione da HIV nell'ambito di programmi epidemiologici è consentita soltanto su campioni di sangue resi anonimi (art. 5, l. n. 135/1990) (nota 6 febbraio 2015).

5.2. *I trattamenti di dati sanitari per fini amministrativi*

L'Autorità ha continuato ha fornire la propria collaborazione istituzionale nei confronti delle amministrazioni operanti nel settore sanitario con riferimento ai trattamenti di dati personali effettuati per finalità amministrative correlate alla cura anche con riferimento allo schema tipo aggiornato di regolamento per il trattamento dei dati sensibili e giudiziari che possono essere raccolti e utilizzati da regioni, province autonome, aziende sanitarie locali e altre strutture sanitarie facenti parte del Servizio sanitario regionale nell'ambito dello svolgimento delle relative funzioni istituzionali.

Una complessa attività istruttoria è stata inoltre svolta con riferimento ai trattamenti di dati personali effettuati dai centri unici di prenotazione (cup) delle aziende sanitarie.

In un caso l'Ufficio, a seguito di una segnalazione, ha riscontrato notevoli criticità in merito alla tipologia dei dati consultabili dagli operatori cup. In particolare gli operatori erano in grado di visualizzare informazioni relative alle prestazioni sanitarie già erogare e ai passati ricoveri del soggetto che stava usufruendo del servizio di prenotazione. Il sistema cup, inoltre, non forniva agli interessati una idonea informativa in merito al trattamento dei dati personali. Ulteriore criticità riscontrata riguardava la possibilità di accesso al sistema da parte di un numero elevato di soggetti non sempre deputati alla prenotazione delle prestazioni sanitarie pubbliche. A seguito del riscontro le aziende interessate hanno, tuttavia, prontamente modificato il sistema di prenotazione superando le predette criticità. Ulteriori attività istruttorie relative al trattamento dei dati personali effettuato dai cup sono attualmente in corso con particolare riferimento al coinvolgimento di società private delegate dalle strutture sanitarie all'attività di prenotazione telefonica delle prestazioni sanitarie.

L'Ufficio ha ricevuto numerose richieste di chiarimenti in merito alle modalità di consegna del promemoria della ricetta dematerializzata all'assistito con particolare riferimento alla possibilità di utilizzare modalità alternative a quella cartacea. Come è noto, la dematerializzazione della ricetta medica per le prescrizioni a carico del Ssn è stata introdotta con decreto del Mef del 2 novembre 2011. Il medico, a prescrizione avvenuta, rilascia all'assistito il promemoria della ricetta dematerializzata provvisto di numero ricetta elettronica (nre) e codice di autenticazione dell'avvenuta transazione. L'art. 1, comma 4, d.m. richiamato prevede che "il medico prescrittore rilascia all'assistito il promemoria cartaceo della ricetta elettronica secondo il modello riportato nel disciplinare tecnico Allegato 2. Su richiesta dell'assistito, tale promemoria può essere trasmesso tramite i canali alternativi di cui all'Allegato 1". Il menzionato decreto, dopo aver disciplinato le modalità dell'invio telematico dei dati della prescrizione al Sac (Sistema di accoglienza centrale), precisa che "porranno essere resi disponibili ulteriori canali per accedere ai servizi di cui al presente disciplinare erogati dal Sac, in modo particolare per la fruizione del promemoria da parte degli assistiti" (art. 3.5.1.) "attraverso il sito del Ministero dell'economia e delle finanze (www.sistemats.it)" (art. 4.1.).

Allo stato le modalità alternative alla stampa del promemoria cartaceo non sono state ancora individuate, tuttavia l'Autorità ha manifestato la propria disponibilità ad avviare un confronto con le amministrazioni istituzionali deputate ad intervenire in tale materia, al fine garantire che il trattamento dei dati personali degli assistiti avvenga nel rispetto della dignità e della riservatezza dell'interessato (note 2 ottobre 2015).

Con riferimento al trattamento dei dati personali effetruato nell'ambito dello svolgimenro delle funzioni amministrative nel settore sanitario, un importante intervento del Garante ha riguardato la trasmissione telematica delle certificazioni mediche legate alla gravidanza all'Inps. Il Garante ha infatti chiesto maggiori tutele a garanzia delle lavoratrici madri nel parere espresso su uno schema di decreto interministeriale elaborato dal Ministero del lavoro e delle politiche sociali che detta le modalità tecniche per la predisposizione e l'invio all'Inps dei certificati medici di gravidanza, interruzione della gravidanza e parto (provv. 4 giugno 2015, n. 334, doc. web n. 4130998).

Lo schema di decreto, che ha recepito molte delle indicazioni fornite dall'Ufficio nel corso di incontri avuti con le amministrazioni interessate, presenta ancora dei profili che devono essere ulteriormente perfezionati. Secondo l'Autorità lo schema deve essere integrato prevedendo che l'invio telematico dei certificati, come stabilito dalla normativa, non sia automatico, ma avvenga su richiesta della lavoratrice per consentirle di potersi avvalere dei diritti che l'ordinamento le riconosce (inrerruzione della gravidanza, non riconoscimento del figlio, parto in anonimato). Occorre, infatri, scongiurare il rischio che si instauri la prassi dell'invio automatico dei certificati senza verificare che la donna sia una lavoratrice e che voglia avvalersi dei benefici erogati dall'Inps. Nello schema inoltre, deve essere inserita una specifica disposizione che preveda l'adozione di idonee misure di sicurezza a protezione dei dari. Particolare attenzione poi, deve essere, riservata ai dati che possono essere inclusi nei certificati, evitando per esempio le diciture che possono risultare generiche o ambigue o che possono arrecare lesioni alla riservatezza delle lavoratrici.

Ulteriori modifiche richieste dal Garante riguardano il perfezionamento dello schema per evitare che il datore di lavoro venga a sapere informazioni che non deve conoscere quali l'individuazione, anche per categorie, delle strutrure sanitarie competenti all'invio dei certificati.

Procreazione medicalmente assistita

All'esito dell'esame di alcune segnalazioni, l'Ufficio è intervenuto in merito alla procreazione medicalmente assistita (di seguito pma) e, in particolare, sulle modalità di raccolta, da parte del Centro nazionale trapianti (di seguito Cnt), di dati ana-

grafici e sanitari, riferiti ai donatori di gameti destinati alla fecondazione eterologa presso le strutture sanitarie autorizzate al prelievo e al trattamento di cellule riproduttive (quali il codice fiscale, il luogo e la data di nascita, la nazionalità di origine, la cittadinanza, la provincia di residenza, lo stato civile, il titolo di studio, la condizione professionale e la posizione professionale dei donatori).

La raccolta dei dati in questione era stata disposta in attuazione della legge istitutiva del Registro nazionale dei donatori di cellule riproduttive per la fecondazione eterologa che è volto a garantire la tracciabilità del percorso delle cellule riproduttive dal donatore al nato e viceversa, nonché il conteggio dei nati generati dalle cellule riproduttive di un medesimo donatore. Queste disposizioni prevedono, inoltre, che, in attesa della piena operatività del Registro nazionale informatizzato nel quale saranno registrati tutti i soggetti ammessi alla donazione, mediante l'attribuzione di un codice identificativo ad ogni donatore – i dati riferiti ai donatori di gameti siano comunicati al Cnt "in modalità cartacea, salvaguardando comunque l'anonimato dei donatori" (art. 1, comma 298, l. 23 dicembre 2014, n. 190).

Nell'ambito di diverse interlocuzioni intercorse con il Cnt, l'Ufficio ha contribuito a individuare le misure di sicurezza necessarie e le garanzie adeguate a tutelare l'anonimato dei donatori nella fase transitoria di raccolta delle informazioni in modalità cartacea. All'esito di tale attività, il Centro ha, infatti, rivisto e modificato le procedure utilizzate per la raccolta dei dati personali dei donatori di gameti, al fine di conformarle ai principi e alle regole in materia di protezione dei dati personali.

In particolare, nella trasmissione dei dati al Cnt, sarà utilizzato dai centri di pma un codice identificativo, generato da un algoritmo di cifratura, in modo da non consentire di ricondurre i dati ricevuti alle persone cui questi si riferiscono e da permettere soltanto ai centri di identificare i donatori, qualora ne emerga la necessità per motivi di tutela della salute del donatore o dei nati. Inoltre, dalla scheda cartacea di raccolta dei dati, saranno espunte le informazioni che identificano in chiaro i donatori, mentre i dati riferiti ai donatori e ai nati, destinati a essere memorizzati nel Registro, saranno associati al predetto codice identificativo (nota 10 novembre 2015).

Registri tumori

In risposta a un quesito riguardante la liceità della trasmissione a un'Asl, che ne aveva fatto richiesta, dei dati sanitari, riferiti ad alcuni esami clinici effettuati da pazienti oncologici per l'implementazione del registro tumori aziendale, l'Ufficio ha chiarito, che qualora una struttura sanitaria intenda comunicare dati attinenti alla salute a soggetti diversi dall'interessato per finalità di carattere amministrativo, correlate ad attività di tutela della salute, tale operazione è consentita, solo se autorizzata da espressa disposizione legislativa o regolamentare che specifichi i tipi di dati che possono essere trattati e di operazioni eseguibili, nonché persegua una delle finalità di rilevante interesse pubblico individuate dalla legge (artt. 20 e 85 o 98 del Codice) (nota 23 ottobre 2015).

Pertanto, in questi casi, occorre fare riferimento alle previsioni (normative) regionali di settore eventualmente adottate, anche in attuazione del quadro di garanzie introdotto dalla normativa nazionale in materia di sistemi di sorveglianza e registri di patologia (cfr. art. 12, commi 10 ss., d.l 18 ottobre 2012, n. 179 conv., con modificazioni dalla l. 17 dicembre 2012, n. 221 e provv. 23 luglio 2015, n. 435, doc. web n. 4252386). Altrimenti la predetta verifica dovrà essere effettuata alla luce del regolamento sul trattamento dei dati sensibili e giudiziari di competenza delle aziende sanitarie, che la regione avrebbe dovuto adottare in conformità allo schema tipo su cui il Garante ha espresso il proprio parere favorevole il 26 luglio 2012 (provv. n. 220, doc. web n. 1915390, cfr. in particolare, la scheda n. 39 dell'allegato B al cit. schema tipo).

Sempre con riferimento ai registri di patologia, è proseguita l'attività di collaborazione dell'Ufficio con talune Regioni che sono in procinto di disciplinare con proprio atto regolamentare i trattamenti di dati sensibili e, in particolare, di quelli attinenti alla salute, connessi alla tenuta e al funzionamento di registri di patologia su base regionale, quali, ad esempio, quelli dei tumori (nota 8 settembre 2015).

5.2.1. L'attività consultiva sugli atti regolamentari e amministrativi del Ministero della salute

Nell'ambito dell'attività consultiva obbligatoria concernente gli atti regolamentari e amministrativi suscettibili di incidere sulla protezione dei dati personali, il Garante ha espresso, inoltre, il proprio parere su diversi decreti del Ministero della salute riguardanti temi di grande rilevanza, che coinvolgono il trattamento di dati sulla salute, raccolti in ambito sanitario in maniera sistematica e tenuti in grandi banche dati o registri a copertura nazionale o regionale, oppure idonei a rivelare lo stato di salute dei donatori di organi e di coloro che li ricevono o ancora trattati per la diagnosi precoce, in età neonatale, di malattie metaboliche ereditarie, ivi comprese quelle genetiche (cfr. par. 3.4.1).

Interconnessione dei sistemi informativi sanitari

In questo quadro, l'Autorità si è espressa su uno schema di regolamento del Ministero della salute sulle procedure per l'interconnessione a livello nazionale dei sistemi informativi su base individuale del Ssn, anche quando gestiti da diverse amministrazioni dello Stato (provv. 19 marzo 2015, n. 162, doc. web n. 3869889).

La materia è particolarmente rilevante in quanto la prevista interconnessione comporta la raccolta centralizzata, nell'ambito del Nuovo sistema informativo sanitario (Nsis), di una notevole quantità di informazioni personali degli assistiti, particolarmente delicate, trattandosi di dati sensibili idonei specialmente a rivelare, anche nel dettaglio, lo stato di salute.

Il complesso delle informazioni, che confluiranno nel nuovo sistema centralizzato, su base individuale, ma in forma codificata, consentirà al Ministero, alle regioni e alle province autonome di valutare gli esiti delle prestazioni assistenziali, di monitorare i livelli essenziali e uniformi di assistenza e di programmare l'attività sanitaria (v. art. 15, comma 25-*bis*, d.l. 6 luglio 2012, n. 95, convertito, con modificazioni, dalla l. 7 agosto 2012, n. 135). I sistemi informativi coinvolti nelle procedure di interconnessione sono quelli del Ministero della salute previsti nell'ambito del Nsis (ad es., ticoveti, assistenza domiciliare, schede di dimissioni ospedaliere, vaccinazioni, etc.), il sistema informativo Tessera sanitaria del Ministero dell'economia e delle finanze (riguardo alle prestazioni di specialistica ambulatoriale e di assistenza farmaceutica convenzionata), nonché i sistemi informativi sanitari delle regioni e delle province autonome (limitatamente ai dati raccolti nell'ambito dei flussi del Nsis).

Per consentire l'interconnessione a livello nazionale, nell'ambito del Nsis, dei sistemi informativi sopra menzionati, lo schema di regolamento definisce le procedure per l'anonimizzazione dei dati individuali presenti nei flussi informativi del Ssn, prevedendo l'assegnazione a ciascun assistito di un codice univoco a livello nazionale, in sostituzione del codice fiscale, che non consente alcuna correlazione immediata con i dati anagrafici dell'interessato, in modo da tutelare la sua identità nel procedimento di elaborazione dei dati (art. 35, d.lgs. 23 giugno 2011, n. 118).

Lo schema di regolamento, su cui il Garante si è pronunciato con un parere favorevole condizionato, è stato elaborato dal Ministero della salute a seguito di una complessa attività, che ha coinvolto anche l'Autorità attraverso riunioni e interlocuzioni, volte a innalzare i livelli di protezione prospettati per i dati sanitari e ad indicare misure e caurele per la loro messa in sicurezza.

Le indicazioni dell'Ufficio hanno riguardato, in particolare: la definizione di procedure e modalità del trattamento in grado di assicurare adeguate garanzie a tutela della riservatezza degli assistiti, specie con riferimento al sistema informativo delle schede di dimissione ospedaliera (Sdo), per il quale sussistono particolari esigenze che richiedono un'applicazione graduale del sistema di codifica univoco previsto a livello nazionale; la precisazione dei limiti e delle modalità di accesso alle informazioni rese disponibili dal sistema Nsis, secondo un approccio selettivo e coerente con i princìpi di necessità e di indispensabilità; la razionalizzazione e l'implementazione delle misure a protezione dei dati e dei sistemi, al fine di garantire un livello di sicurezza adeguato al volume significativo e all'estrema delicatezza dei dati trattati (ad es., è stato previsto il ricorso a strumenti di autenticazione forte degli utenti per i trattamenti che prevedono l'accesso a dati sanitari riferiti a singoli individui).

Schede di dimissione ospedaliera

L'Autorità si è poi espressa su un altro schema di decreto del Ministero della salute che regola l'adeguamento della disciplina riguardante i flussi informativi dei pazienti dimessi dagli istituti di ricovero pubblici e privati (d.m. 27 ottobre 2000, n. 380) alle esigenze di monitoraggio, valutazione e pianificazione della programmazione sanitaria. Tale adeguamento trae origine anche dagli orientamenti definiti al riguardo dalla normativa dell'Unione europea che sono stati recepiti nel nostro ordinamento con il d.lgs. 4 marzo 2014, n. 38 (v. direttiva 2011/24/UE, concernente l'applicazione dei diritti dei pazienti relativi all'assistenza sanitaria transfrontaliera e direttiva 2012/52/UE, comportante misure destinate ad agevolare il riconoscimento delle ricette mediche emesse in un altro Stato membro).

Sebbene il decreto abbia recepito talune delle osservazioni e dei rilievi formulati dall'Autorità all'esito di un tavolo tecnico con il Ministero, il Garante ha sottolineato l'esigenza di apportare al testo ulteriori perfezionamenti. Ciò, in ragione della complessità della materia e delle implicazioni riguardanti il trattamento dei dati sanitari degli assistiti e, in misura minore, di quelli giudiziari, nonché dello stretto collegamento delle previsioni del decreto con lo schema di regolamento sull'interconnessione dei sistemi informativi appena citato.

L'intervento dell'Autorità, ha consentito, tra l'altro, di estendere (a regime) al flusso informativo delle Sdo le cautele relative all'utilizzo di un codice univoco nazionale dell'assistito, previste dallo schema di regolamento sull'interconnessione dei sistemi informativi nell'ambito del Nsis, in attuazione dell'art. 35, d.lgs. n 118/2011 (la cui entrata in vigore è successiva al d.m. n. 380/2000). Tale disposizione, infatti, prevede l'anonimizzazione dei dati individuali presenti nei flussi informativi della sanità, proprio per esigenze di protezione dei dati personali, senza peraltro contemplare alcuna deroga per il flusso informativo Sdo (cfr. art. 11, comma 4, d.lgs. n. 38/2014 laddove richiama l'osservanza dell'art. 15, comma 25-*bis*, d.l. n. 95/2012).

Nel parere, inoltre, il Garante ha chiesto al Ministero di modificare le previsioni del decreto che disponevano la raccolta in chiaro nelle Sdo dei dati identificativi dei chirurghi e degli anestesisti degli interventi principali e secondari, prevedendo l'adozione di accorgimenti e misure volte sostituire il codice fiscale degli interessati con un codice univoco a livello nazionale, in analogia a quanto previsto per il trattamento del codice identificativo dei pazienti.

All'esito delle risultanze istruttorie e alla luce di una lettura del quadro normativo vigente correttamente orientata al rispetto della direttiva 95/46/CE (richiamata peraltro dalla stessa direttiva 2011/24/UE), non è emersa infatti la necessità per gli uffici del Ministero di trattare i codici fiscali dei professionisti (dai quali si possono facilmente identificare gli interessati) per monitorare e valutare gli esiti degli interventi sanitari la definizione degli *standard* di qualità, l'efficacia ed efficienza, non-

ché per monitorare il rischio clinico previsto dall'art. 11, comma 4, d.lgs. n. 38/2014 e dalla normativa europea che quest'ultima previsione intende attuare. Infine, l'Autorità ha richiamato l'attenzione del Ministero sulla necessità di limitare la raccolta dei dati contenuti nelle Sdo a quelli strettamente indispensabili, tenendo in considerazione l'esigenza che i dati oggetto di trasmissione siano conformi a quelli contenuti negli altri flussi previsti nell'ambito del Nsis, (si fa riferimento in particolare alle informazioni riferite alla data di nascita completa e al comune di nascita del paziente che non sono contemplate nei flussi informativi previsti nell'ambito del Nsis).

Per quanto riguarda invece le misure di sicurezza, in analogia a quanto previsto nello schema di regolamento sull'interconnessione dei sistemi informativi, è stato richiesto di ricorrere a strumenti di autenticazione forte per gli utenti del sistema che effettuano trattamenti particolarmente delicati, nonché di circoscrivere i casi in cui è consentito a questi ultimi di accedere ai dati sanitari riferiti a singoli pazienti dimessi dagli istituti di ricovero (provv. 26 marzo 2015, n. 178, doc. web n. 3878687).

Sistemi di sorveglianza e registri

Sempre in tema di sistemi informativi sanitari, il Garante ha reso il parere su uno schema di d.P.C.M. riguardante i sistemi di sorveglianza e i registri, ai sensi dell'art. 12, comma 11, d.l. 18 ottobre 2012, n. 179, convertito con modificazioni dalla l. 17 dicembre 2012, n. 221 (provv. 23 luglio 2015, n. 435, doc. web n. 4252386).

Lo schema in questione, individua i sistemi di sorveglianza e i registri di mortalità, di tumori e di altre patologie, "di rilevanza nazionale e regionale", quelli "già disciplinati dalla normativa vigenre a livello nazionale" e quelli "di rilevanza esclusivamente regionale" precisandone le finalità, in aderenza con il dettato normativo sopra richiamato (segnatamente prevenzione, diagnosi, cura e riabilitazione, programmazione sanitaria, verifica della qualità delle cure, valutazione dell'assistenza sanitaria e ricerca scientifica in ambito medico, biomedico ed epidemiologico; cfr. art. 12, comma 10, d.l. n. 179/2012).

Sulla base del quadro notmativo vigente sopra richiamato, la definizione delle garanzie per il trattamento dei dati personali contenuti nei predetti sistemi e registri è demandata ad un regolamento da adottarsi su proposta del Presidente del Consiglio dei ministti, acquisito il parere del Garante, in conformità alle disposizioni di cui agli artt. 20, 22, e 154 del Codice (cfr. art. 13, comma 2, d.l. 21 giugno 2013, n. 69, convertito dalla l. 9 agosto 2013, n. 98 e art. 12, comma 13, d.l. n. 179/2012). Poiché non è risultato che tale atto sia stato adottato, l'Autorità ha innanzitutto richiamato l'attenzione sulla necessità che il predetto regolamento venga predisposto quanto prima al fine di rendere leciti e rispettosi di adeguate cautele i trattamenti di dati sensibili effettuati in tale ambito.

In ragione della particolare delicatezza della materia (art. 94 del Codice) al fine di registrare e caratterizzare tutti i casi di rischio per la salute di una particolare malattia o di una condizione di salure rilevante in una popolazione definita, il Garante ha condizionato il proprio parere favorevole al recepimento di una serie di indicazioni volte a rendere conforme il testo del regolamento alla disciplina in materia di protezione dei dati personali.

Tali osservazioni hanno riguardato, in parricolare, la verifica dell'idoneità dei presupposti legittimanti l'utilizzo a fini di cura dei dati contenuti nei sistemi di sorveglianza e nei registti, al fine di scongiurate trattamenti illeciti di dati e un utilizzo improprio degli archivi in questione (quasi fossero fascicoli sanitari elettronici accessibili, però, in assenza delle specifiche cautele previste per questi ultimi; cfr. art. 12, commi 1-7, d. l. n. 179/2012). Al riguardo, va tenuto in considerazione, infatti, che il trattamento di dati sulla salute per le predette finalità può essere legittimamente effettuato soltanto da organismi sanitari e da esercenti la professione sanitaria, nel