di opposizione mediante l'iscrizione della numerazione della quale è intestatario in un registro pubblico delle opposizioni, del quale ha previsto l'istituzione. Peraltro si evidenzia che, con *provvedimento* generale del 25 giugno 2009 [doc. *web* n. 1629107] sono state dettate le regole per il corretto uso dei dati personali a fini di profilazione nel settore delle telecomunicazioni, essendo emerso, anche a seguito di numerose ispezioni, che i gestori telefonici, senza il consenso degli interessati, avevano assai spesso usato i dati dei loro clienti, per profilare tra l'altro le abitudini, conoscere le preferenze, analizzare le spese telefoniche di tali soggetti.

Il Garante ha ribadito, innanzitutto, che i dati non possono essere utilizzati per le menzionate finalità senza un'adeguata informativa e senza l'esplicito consenso degli interessati.

Tuttavia rispetto ai dati trattati in forma "aggregata", è stato previsto che i gestori telefonici possano anche chiedere una specifica verifica preliminare, indicando le modalità del trattamento che intendono effettuare. Nell'ambito di tale verifica il Garante potrà valutare, caso per caso, se consentire tali trattamenti senza l'esplicito consenso degli interessati. Anche in questa ipotesi tuttavia dovrà essere data sempre una adeguata informativa ai clienti.

Ai gestori che già svolgono questa attività è stato dato il termine del 30 settembre 2009 per regolarizzare i trattamenti, e chiedere al Garante la necessaria verifica. Le suddette regole sono applicabili alle attività di profilazione avviate dopo l'entrata in vigore del *provvedimento.*

A seguito di numerose segnalazioni, inoltre, il Garante ha per la prima volta vietato l'effettuazione di telefonate commerciali tramite un sistema che generava i numeri da contattare attraverso sequenze casuali, elaborate con criteri geografici (*Provv.* 3 dicembre 2009 [doc. *web* n. 1679436]).

L'Autorità ha al riguardo chiarito che anche il numero casualmente composto e chiamato telefonicamente deve considerarsi *"dato personale"*, in quanto ricollegabile, anche indirettamente, a una persona identificata o identificabile. Sicché, per utilizzare anche questo tipo di numerazione a fini commerciali è necessario il previo consenso dell'interessato.

L'Autorità si è inoltre occupata della *cd.* "ricerca inversa", ossia della possibilità, per i fornitori di servizi di informazione sugli elenchi, di comunicare, *online* o al telefono, i dati personali degli abbonati, ricercati in base al numero telefonico o ad altra informazione personale.

In materia, il Garante aveva stabilito in particolare che l'attivazione della funzione di "ricerca inversa" presuppone il consenso specifico degli interessati (*cfr. Provv.* 15 luglio 2004 [doc. *web* n. 1032381], Allegato I, punto 4.2.1) da raccogliere tramite il questionario contenuto nel modulo di informativa e raccolta del consenso di cui all'Allegato IV del *provvedimento* ora citato.

Successivamente con numerose istanze, alcuni fornitori di servizi di informazione sugli elenchi avevano chiesto di modificare tale disciplina poiché, in assenza di risposta al detto questionario, i dati personali degli abbonati già presenti nei vecchi elenchi erano stati inseriti automaticamente anche nei nuovi elenchi, ma, non essendo in passato stata chiesta agli stessi alcuna manifestazione di volontà in merito all'utilizzabilità dei loro dati nei servizi di ricerca inversa, tale funzione, in assenza di risposta, era stata generalmente intesa come inibita nei loro confronti.

Alla luce di ciò l'Autorità, con *provvedimento* 8 aprile 2010 successivamente pubblicato nella *Gazzetta Ufficiale* [doc. *web* n. 1713429] in un'ottica di semplificazione, ha disposto che, con esclusivo riferimento ai "vecchi" abbonati i cui dati erano già inseriti in un elenco pubblico alla data del 1° febbraio 2005, possa essere attivata a partire dal 1° gennaio 2011 - previa idonea informativa nella bolletta telefonica entro il 31 dicembre 2010 e sui siti *web* dei gestori entro il 31 maggio 2010 - la funzione di ricerca inversa anche senza il consenso espresso degli abbonati, salvo il rispetto di eventuali volontà contrarie comunicate dagli stessi al proprio operatore.

Di rilievo generale anche la decisione (*Provv.* 1° aprile 2010, successivamente pubblicato sulla *Gazzetta Ufficiale* [doc. *web* n. 1711492]) riguardante il *database* unico (Dbu) utilizzato per formare gli elenchi telefonici, basati su dati inseriti dai singoli operatori di telefonia in base al consenso espresso dai clienti (*cfr.* delibera Agcom 6 febbraio 2002, n. 36/02/CONS).

Gli operatori del settore, segnalando un significativo decremento delle utenze presenti nel Dbu in un arco di tempo relativamente breve, hanno ricondotto il fenomeno alla mancata compilazione, da parte dei clienti che cambiano operatore telefonico, del modulo per esprimere il consenso all'inserimento nel Dbu (di cui all'Allegato IV del *cit. provvedimento* 15 luglio 2004).

Al riguardo, nella *decisione* dell'aprile 2010 si è ricordato che, anche se l'interessato decide di conservare il numero telefonico - *number portability* (*Np*) - in caso di attivazione di una nuova utenza telefonica, anche mobile, il nuovo operatore è tenuto a sottoporgli il modulo di informativa e raccolta del consenso.

Tuttavia, poiché il numero telefonico non cambia e, quindi, restano invariati tutti gli elementi oggetto di pubblicazione negli elenchi, il Garante ha ritenuto che i clienti che modificano l'operatore con *Np* possano essere assimilati ai "vecchi" clienti di cui al *provvedimento* del 2004, ossia a quei soggetti i cui nominativi erano già presenti negli elenchi pubblicati prima dell'entrata in vigore del nuovo regime degli elenchi telefonici. Anche i predetti soggetti infatti hanno già espresso in passato al proprio operatore la volontà di inserimento nel Dbu e, conseguentemente, negli elenchi, dei dati personali che li riguardano.

Pertanto, per tale categoria di utenti, il nuovo operatore telefonico può mantenere invariate le opzioni scelte in passato, in assenza di risposta al questionario entro sessanta giorni dalla ricezione dello stesso, fermo restando che gli interessati possono manifestare in qualunque momento, al nuovo operatore, una diversa volontà.

1.1.6. Attività d'impresa

Il trattamento di dati all'interno dell'impresa o dei gruppi di impresa è stato oggetto nel 2009 di deliberazioni del Garante di rilievo generale.

Con *deliberazione* del 10 dicembre 2009 [doc. *web* n. 1693019] l'Autorità ha deciso di segnalare a Parlamento e Governo l'opportunità di un intervento normativo per disciplinare (in sintonia con il parere 1° febbraio 2006 del Gruppo Art. 29), i sistemi di segnalazione (*cd. "whistleblowing"*) di illeciti commessi da soggetti operanti a vario

titolo nell'organizzazione aziendale, nonché i profili di interferenza di tale fenomeno con la disciplina di protezione dei dati. Occorre al riguardo segnalare che altri ordinamenti, quali quello degli Stati Uniti e della Gran Bretagna, hanno già adottato provvedimenti legislativi in merito, prevedendo, tra l'altro, misure a protezione degli autori (in buona fede) delle segnalazioni.

L'Autorità ha evidenziato che manca nel nostro ordinamento una disciplina di carattere generale sulla liceità del trattamento di dati nell'ambito di tali sistemi di segnalazione, che pure potrebbero tutelare anche interessi di carattere generale "esterni" all'azienda, (*ad es.*, tutela della stabilità dei mercati finanziari, lotta alla corruzione, contrasto alla criminalità economica e finanziaria, tutela dei risparmiatori). Appaiono da disciplinare, con norma primaria, in particolare i profili relativi: all'individuazione dei soggetti operanti all'interno delle società che possono assumere la qualità di segnalanti, delle finalità che si intendono perseguire, delle fattispecie oggetto di possibile "denuncia" da parte dei segnalanti. Occorre chiarire la portata del diritto di accesso previsto dall'art. 7 del Codice da parte del soggetto al quale si riferisce la segnalazione (interessato), con riguardo ai dati identificativi dell'autore della segnalazione (denunciante), nonché l'eventuale ammissibilità dei trattamenti derivanti da segnalazioni anonime.

Con *deliberazione* 10 settembre 2009 (in *G.U.* 16 novembre 2009, n. 267 [doc. *web* n. 1664492]) l'Autorità ha affrontato la questione del coordinamento tra la normativa di protezione dei dati personali e la disciplina di settore in materia di antiriciclaggio (in ordine alla quale il Garante si era espresso con il *parere* del 25 luglio 2007 [doc. *web* n. 1431012]).

In proposito l'Autorità, ponderando gli interessi in gioco, ha deciso che i titolari del trattamento tenuti ad effettuare una segnalazione antiriciclaggio in conformità alla disciplina di settore (d.lgs. n. 231/2007) possono dare comunicazione dell'avvenuta segnalazione agli intermediari finanziari appartenenti al medesimo gruppo, senza che a tal fine sia necessario acquisire il consenso degli interessati (art. 24, comma 1, lett. *g*) del Codice). Inoltre, ai titolari del trattamento è stato prescritto (ai sensi degli artt. 143, comma 1, lett. *b*), e 154, comma 1, lett. *c*), del Codice) di fornire agli interessati

specifiche indicazioni anche sulla possibilità che le informazioni relative alle operazioni poste in essere dagli stessi interessati, ove queste siano ritenute "sospette" ai sensi dell'art. 41, comma 1, del d.lgs. 21 novembre 2007, n. 231, siano comunicate ad altri intermediari finanziari appartenenti al medesimo gruppo.

A seguito di richieste riguardanti operazioni di riassetto nel settore bancario, relative ad un numero estremamente elevato di soggetti interessati, il Garante ha individuato le modifiche che, nelle operazioni societarie di fusione o scissione, devono essere fornite rispetto all'informativa resa in precedenza dalla società scissa o dalle società partecipanti alla fusione (art. 154, comma 1, lett. *c*) e *h*), del Codice) (*Provv.* 8 aprile 2009 [doc. *web* n. 1609999]).

In sostanza, ha previsto che le società coinvolte nel processo di fusione o scissione informino tutti i soggetti interessati (clienti, lavoratori, fornitori, *ecc.*) su chi sia il titolare e il nuovo responsabile del trattamento dei dati personali in possesso dell'impresa, al quale potersi rivolgere per esercitare il diritto di accesso e tutti gli altri diritti previsti dal Codice.

Per semplificare gli adempimenti, l'Autorità ha deciso che in un primo tempo potrà essere fornita una comunicazione generale immediata, sui siti *web* delle società coinvolte, non appena definito il nuovo assetto societario. Alla prima occasione di contatto, poi, le società dovranno comunque inviare i nuovi riferimenti a tutti gli interessati.

Nel caso in cui le società risultanti dal processo di fusione o scissione effettuino trattamenti in cui è prevista la notificazione al Garante, tali aziende dovranno effettuare o integrare la notificazione secondo le procedure *standard* già previste dall'Autorità.

Con *deliberazioni* del 18 marzo 2010, nn. 18 e 19 [doc. *web* nn. 1708078 e 1709118] è stato determinato il contributo spese che i Sistemi di informazione creditizie (Sic) gestiti da Crif S.p.A., nonché *Experian information services*, Cts e Assilea, potranno richiedere - in qualità di titolari presso i quali *"si determina un notevole impiego di mezzi in relazione ... all'entità delle richieste"* - agli interessati in caso di esercizio dei diritti ai sensi dell'art. 7, commi 1 e 2, lett. *a*), *b*), *c*), del Codice, secondo quanto previsto dall'art. 10, commi 7 e 8, 1° cpv., del Codice, e in ottemperanza a quanto disposto dal Consiglio di Stato con sentenza n. 5198/09.

Nel merito è stato deciso, tra l'altro, che: tutte le volte in cui l'interessato richieda espressamente il riscontro attraverso l'invio a mezzo di posta elettronica, lo stesso dovrà essere reso a titolo gratuito; per le richieste successive alla prima, nell'arco di ciascun anno solare, formulate ai sensi dell' art. 7, commi 1 e 2, lett. *a*) e *b*), potrà essere richiesto un contributo spese commisurato ai costi effettivamente sostenuti e, comunque, non superiore a 7 euro (incluse le spese postali); qualora sia presentata una richiesta incompleta e per fornire un idoneo riscontro si renda indispensabile contattare l'interessato, il contributo spese non dovrà superare i costi effettivamente sostenuti e, in ogni caso, l'importo di 3 euro.

1.1.7. Protezione dei dati dei lavoratori dipendenti e dei collaboratori

Alcuni provvedimenti adottati dal Garante nel 2009 sul trattamento dei dati personali in ambito lavoristico - con particolare riferimento ai dati sulla salute dei dipendenti - evidenziano la duplice esigenza di rispettare i princìpi di pertinenza e non eccedenza dei dati trattati e di evitare improprie forme di circolazione delle informazioni, all'esterno, ma anche all'interno dell'ambito lavorativo.

Al riguardo, si cita il *provvedimento* con il quale il Garante ha intimato alla Provincia di Foggia il blocco dei dati sulla salute di una dipendente, la quale aveva segnalato la diffusione - attraverso il sito internet del menzionato ente locale presso il quale lavorava, nonché attraverso il motore di ricerca *Google* - di due determinazioni riguardanti la propria richiesta di riconoscimento dell'infermità da causa di servizio (*Provv.* 25 giugno 2009 [doc. *web* n. 1640102]). Uno dei documenti riportava, in particolare, accanto al nome e cognome della dipendente, la valutazione medico-legale relativa al tipo di infermità riscontrata, in violazione del divieto di diffusione di dati relativi alla salute (art. 2, comma 7, d.P.R. 29 ottobre 2001, n. 461 e tab. A, allegata al d.P.R. 30 dicembre 1981, n. 834; *v.* anche art. 6 decreto 12 febbraio 2004).

Con *provvedimento* 24 settembre 2009 [doc. *web* n. 1658058] è stato altresì disposto il blocco, nei confronti di una commissione medica di verifica del Ministero dell'economia e delle finanze, dei dati sensibili contenuti in un verbale di accertamento

di inidoneità all'impiego di un'insegnante. L'organo di accertamento aveva trasmesso copia integrale del verbale di visita; l'Autorità ha richiesto alla commissione medica di utilizzare un attestato riportante la sola valutazione medico-legale ai fini della comunicazione, alle amministrazioni di appartenenza dei lavoratori, dell'esito degli accertamenti sanitari di inidoneità al servizio o altre forme di inabilità non dipendenti da causa di servizio.

È stato ritenuto illecito anche il trattamento dei dati sanitari della docente posto in essere dall'amministrazione scolastica presso cui prestava servizio, in ragione dell'inutilizzabilità delle informazioni trattate in violazione della disciplina sulla protezione dei dati (artt. 11 e 22, commi 1, 3 e 5, del Codice; art. 5, l. n. 135/1990; artt. 4, 5 e 6, comma 8, d.P.R. n. 461/2001; *v.* anche punti 3.2 e 8.4 delle *"Linee-guida sul trattamento di dati dei lavoratori per la gestione del rapporto di lavoro in ambito pubblico"* (*Provv.* 14 giugno 2007 [doc. *web* n. 1417809]). L'amministrazione avrebbe dovuto limitarsi ad utilizzare la valutazione medico-legale, adottando ogni misura per l'ulteriore conservazione del documento idonea a limitarne rigorosamente la conoscibilità.

Con *provvedimento* 21 ottobre 2009 [doc. *web* n. 1689440] è stata ritenuta fondata la segnalazione di un militare cessato dal servizio per permanente inidoneità, il quale aveva contestato la liceità del trattamento dei suoi dati personali detenuti dall'ufficio del personale del Ministero della difesa, rappresentando che questo, avente competenze non sanitarie in materia di stato giuridico, avanzamento e contenzioso del personale militare, avesse indebitamente raccolto informazioni relative al suo stato di salute attraverso l'acquisizione di certificazioni e verbali di visita medica formati dagli organismi militari.

Nella specie, la documentazione medica trasmessa dalle commissioni mediche militari all'ufficio del personale era risultata contenere informazioni non necessarie per l'adozione dei provvedimenti di competenza in materia di stato giuridico e di avanzamento dei militari. Richiamando le indicazioni fornite nelle linee-guida in materia di trattamento di dati personali dei dipendenti pubblici, il Garante ha pertanto richiesto all'amministrazione di rendere conformi alla normativa sulla riservatezza le modalità di circolazione interna dei dati sulla salute del personale.

Nello stesso senso la *decisione* (2 ottobre 2009 [doc. *web* n. 1658119]), che ha ritenuto

fondato il reclamo con cui un dipendente aveva contestato l'indicazione del suo nome e della diagnosi, nel verbale della visita collegiale, trasmesso dalla commissione medica all'Ispettorato di sanità della marina militare, ai fini dell'attestazione dell'idoneità al servizio. La copia del verbale inviata all'ufficio del personale con la diagnosi *"sbarrata e omessa"* consentiva, seppur indirettamente, di risalire all'infezione Hiv, essendo questa l'unica patologia per la quale è prevista la "cancellazione" dai verbali di accertamento medico.

Ribadito che ai dipendenti sieropositivi deve essere assicurata garanzia assoluta di anonimato, il Garante, oltre a inibire l'uso dei dati del dipendente, ha ordinato al Ministero di conformare alla normativa sulla riservatezza la circolazione dei dati sanitari al suo interno e di informare i lavoratori chiaramente sull'obbligatorietà o meno di fornire dati sulla propria salute e sulle relative conseguenze nell'ambito degli accertamenti medico-legali ai fini dell'idoneità al servizio.

Si segnala infine il *provvedimento* 4 marzo 2010 [doc. *web* n. 1706464] con cui il Garante ha espresso parere favorevole in ordine a uno schema di regolamento interno del Ministero dell'ambiente e della tutela del territorio e del mare per l'utilizzo della posta elettronica e della rete internet, predisposto in attuazione delle linee-guida adottate dal Garante il 1° marzo 2007, in merito all'uso di internet e della posta elettronica sul luogo di lavoro.

1.1.8. Dati genetici e sanitari

Nel quadro del processo di ammodernamento della sanità pubblica e privata, dopo un'articolata procedura di consultazione pubblica (*cfr. Relazione 2008*, p. 17 e *Deliberazione* n. 8 del 5 marzo 2009, in *G.U.* 26 marzo 2009, n. 71 [doc. *web* n. 1598313]), e tenuto conto delle osservazioni formulate dal gruppo di lavoro costituito presso il Ministero del lavoro, della salute e delle politiche sociali sono state adottate, in attesa di un'adeguata legislazione in materia, le *"Linee-guida in tema di fascicolo sanitario elettronico (Fse) e di* dossier *sanitario"* (*Provv.* 16 luglio 2009, *G.U.* 3 agosto 2009, n. 178 [doc. *web* n. 1634116]).

Il *provvedimento* stabilisce, in particolare che il paziente deve poter scegliere, in piena libertà, se far costituire o meno un fascicolo sanitario elettronico, con tutte o solo alcune delle informazioni sanitarie che lo riguardano; deve poter manifestare un consenso autonomo e specifico, distinto da quello che si presta a fini di cura della salute; al paziente deve essere inoltre garantita la possibilità di *"oscurare"* la visibilità di alcuni eventi clinici, così come, in generale, egli può decidere di non informare il medico di alcuni eventi sanitari che lo riguardano. Un consenso specifico è richiesto per informazioni particolarmente delicate, quali quelle relative ad atti di violenza sessuale, pedofilia, allo stato di sieropositività, all'interruzione volontaria di gravidanza.

L'informativa, in termini chiari e dettagliati, deve indicare chi (medici di base, del reparto ove è ricoverato il paziente, farmacisti) ha accesso ai dati e che tipo di operazioni può compiere.

Il fascicolo sanitario elettronico potrà essere consultato dal paziente con modalità adeguate (*ad es.*, tramite *smart card*) e dal personale sanitario strettamente autorizzato, solo per finalità sanitarie, non invece da periti, compagnie di assicurazione, datori di lavoro.

Il paziente che non vuole aderire al Fse deve poter usufruire comunque delle prestazioni del Servizio sanitario nazionale.

Per garantire la sicurezza del trattamento gli accessi alle informazioni dovranno essere tracciabili e graduali e i dati sanitari dovranno essere protetti con misure di sicurezza che limitino il più possibile i rischi di abusi, furti e smarrimento.

Dopo una consultazione pubblica (avviata con *Deliberazione* 25 giugno 2009 [doc. *web* n. 1630271]), grazie alla quale sono state raccolte osservazioni formulate da professionisti sanitari, organismi rappresentativi ed associazioni di pazienti il Garante, con *provvedimento* 19 novembre 2009 [doc. *web* n. 1679033], ha altresì approvato le *"Linee-guida in tema di referti* online", che fissano rigorose misure a protezione dei dati sanitari dei pazienti che ricevono il referto via mail o "scaricano" gli esami clinici direttamente dal sito *web* della struttura sanitaria.

Anche in questo caso, come per il fascicolo sanitario elettronico, l'Autorità ha sostanzialmente svolto un ruolo di supplenza in attesa dell'adozione di una apposita normativa.

In sintesi, nel menzionato *provvedimento* è previsto che l'adesione al servizio sia facoltativa e che il referto elettronico non sostituisca quello cartaceo, che rimarrà comunque disponibile. Per chiedere il consenso dell'assistito occorre fornire una informativa chiara e trasparente che spieghi tutte le caratteristiche del servizio di *"refertazione online"*.

Il referto resterà a disposizione *online* per un massimo di quarantacinque giorni e dovrà essere accompagnato da un giudizio scritto e dalla disponibilità del medico a fornire ulteriori indicazioni su richiesta dell'interessato.

Le strutture sanitarie dovranno adottare importanti misure di sicurezza tecnologica (utilizzo di *standard* crittografici, sistemi di autenticazione "forte" convalida degli indirizzi e-mail con verifica *online*, uso di *password* per l'apertura del *file*) e, per offrire la possibilità di archiviare e continuare a consultare via *web* i referti, acquisire un autonomo consenso sulla base di un'ulteriore specifica informativa.

A conclusione dell'attività istruttoria, di cui si è riferito nella *Relazione 2008* (*cfr.* p. 75), è emerso che il controllo a fini tributari della natura e della qualità dei farmaci venduti, richiesto dalla legge, può essere effettuato attraverso l'utilizzo del "numero di autorizzazione all'immissione in commercio" (Aic) presente sulla confezione dei farmaci. Il codice alfanumerico, rilevabile anche mediante lettura ottica, consente, infatti, di identificare in modo univoco ogni singola confezione farmaceutica venduta.

Nel rispetto della normativa vigente, pertanto, il Garante ha prescritto che, a partire dal 1° gennaio 2010, lo scontrino fiscale rilasciato dalle farmacie per dedurre e detrarre la spesa sanitaria nella dichiarazione dei redditi riporti, in luogo dello specifico nome del farmaco acquistato, l'indicazione del codice alfanumerico posto sulla confezione di ogni medicinale (*Provv.* 29 aprile 2009 [doc. *web* n. 1611565]).

Nella *Relazione 2008*, p. 96, si è dato conto dell'avvio del processo di revisione dell'*autorizzazione* generale al trattamento dei dati genetici (*Provv.* 22 febbraio 2007 [doc. *web* n. 1389918]). All'esito della menzionata revisione il Garante, in data 12 dicembre 2009, ha approvato in via preliminare, ed inviato al Ministro della salute per il parere del Consiglio superiore di sanità, un nuovo schema di autorizzazione, che tiene conto dell'esperienza maturata e delle osservazioni di qualificati esperti,

con particolare riferimento all'aggiornamento delle definizioni utilizzate, ai trattamenti effettuati per la tutela della salute di familiari in assenza del consenso dell'interessato, alle ricerche scientifiche che coinvolgono soggetti vulnerabili senza comportare per loro alcun beneficio diretto, nonché alla comunicazione ai familiari dell'interessato di dati genetici indispensabili per evitare un grave pregiudizio per la loro salute.

In attesa della definizione della predetta procedura consultiva, l'efficacia della vigente *autorizzazione* generale è stata prorogata al 30 aprile 2010 (*Provv.* 22 dicembre 2009 [doc. *web* n. 1683067]) e potrà esserlo ulteriormente qualora l'*iter* previsto non si perfezioni nel frattempo.

Con un *provvedimento* generale del 12 novembre 2009 [doc. *web* n. 1686068], essendo emerso che diversi studi medici e dentistici raccoglievano informazioni sull'Hiv mediante la distribuzione di un questionario al momento dell'accettazione dei pazienti, sono stati indicati i princìpi ai quali devono attenersi i medici nella raccolta di informazioni sulla sieropositività.

In sintesi, l'Autorità ha stabilito che gli esercenti la professione sanitaria non possono raccogliere informazioni sulla sieropositività di ogni paziente che si rivolge per la prima volta allo studio medico, se ciò non è indispensabile per il tipo di intervento o terapia da eseguire, e comunque è al riguardo necessario il consenso dell'interessato. La raccolta di informazioni sull'Hiv fin dall'accettazione non può essere giustificata neanche dalla necessità di attivare specifiche misure di protezione per il contagio, che la normativa di settore prevede siano adottate nei confronti di ogni paziente, a prescindere dalla conoscenza dello stato di sieropositività. Infine, il medico che venga a conoscenza di un caso di Aids o di Hiv, oltre a rispettare specifici obblighi di segretezza e non discriminazione nei confronti del paziente, ha l'obbligo di adottare ogni misura individuata dal Codice per garantire la sicurezza dei dati sanitari.

Appare di interesse anche la *decisione*, adottata a seguito di ricorso, del 17 settembre 2009 [doc. *web* n. 1656642] relativa alla richiesta del convivente superstite di accedere alle informazioni contenute nella cartella clinica e nei referti diagnostici detenuti dalla struttura ospedaliera nella quale la *de cuius* era stata ricoverata ed era poi deceduta.

La richiesta è stata accolta, atteso che il convivente ha esercitato il diritto per disporre delle informazioni necessarie ad intraprendere le azioni giudiziarie volte a verificare eventuali inadempienze nelle prestazioni sanitarie rese dalla struttura ospedaliera.

La tematica del consenso è stata oggetto specifico dell'*autorizzazione* (*Provv.* 16 aprile 2009 [doc. *web* n. 1611936]) rilasciata ad un istituto di ricovero e cura a carattere scientifico per condurre, su circa ventimila pazienti affetti da patologie neoplastiche mammarie, uno studio epidemiologico retrospettivo volto all'individuazione del miglior trattamento del carcinoma mammario operabile.

Dall'istruttoria è emerso che lo studio, di durata limitata, non avrebbe potuto raggiungere i suoi scopi senza l'identificazione, anche temporanea, degli interessati e che il trattamento era limitato ai soli dati personali contenuti nelle cartelle cliniche di pazienti curati in precedenza dallo stesso istituto e conservate da questi a norma di legge. Ancora, l'istituto si era impegnato a raccogliere le manifestazioni di volontà di quegli assistiti che si sarebbero nuovamente recati presso la struttura per il *follow-up* e a non comunicare in alcun modo o diffondere le informazioni utilizzate per la ricerca.

L'iniziativa è stata autorizzata, anche in assenza del consenso informato dei pazienti, in ragione dello scopo scientifico perseguito, delle specifiche modalità di trattamento previste, nonché della limitata durata temporale dello studio, anche alla luce del codice di deontologia e buona condotta per i trattamenti di dati personali per scopi statistici e scientifici (art. 11, [doc. *web* n. 1038384]).

Nella *Relazione 2006*, p. 62, si è riferito del divieto di pubblicare, sul sito internet di una regione, le graduatorie per la concessione di contributi regionali indicanti, tra l'altro, le generalità e le motivazioni di esclusione dalle stesse di circa quattromilacinquecento soggetti disabili (*Provv.* 18 gennaio 2007 [doc. *web* n. 1382026]).

A seguito di una segnalazione l'Autorità, accertato che le suddette graduatorie, rimosse solo da alcune pagine, erano ancora presenti sul sito, ha vietato alla regione (*Provv.* 17 settembre 2009 [doc. *web* n. 1658335]) la diffusione, in particolare tramite il sito istituzionale, dei dati idonei a rivelare lo stato di salute degli interessati contenuti nei documenti relativi agli elenchi e alle graduatorie dei disabili.

Si segnala anche che il Garante, il 16 dicembre 2009 [doc. *web* n. 1689676] ha espresso *parere* favorevole, con osservazioni, in ordine a uno schema di disegno di legge governativo recante l'istituzione del registro nazionale e dei registri regionali degli impianti protesici mammari. L'Autorità, pur dichiarando di condividere le linee generali del disegno di legge e le finalità perseguite, ne ha tuttavia evidenziato talune criticità segnatamente sotto i profili dell'individuazione delle specifiche finalità perseguite con l'istituzione dei registri, delle categorie di dati oggetto di trattamento, nonché del regime di conoscibilità dei dati conservati nei registri ed ha suggerito al Governo l'adozione di misure idonee a soddisfare tali esigenze.

Si ricorda infine che in data 21 gennaio 2010 il Garante ha espresso *parere* favorevole [doc. *web* n. 1693904], con osservazioni volte ad evitare l'utilizzo di informazioni non indispensabili, in ordine a uno schema di decreto del Ministro per la pubblica amministrazione e l'innovazione, relativo alle modalità di assorbimento della tessera sanitaria nella carta nazionale dei servizi, cosicché le regioni possano distribuire un'unica *smart card* che assolva ad entrambe le funzioni e consenta l'accesso ai servizi erogati in rete, nel rispetto degli *standard* di sicurezza previsti dal Codice.

1.1.9. Videosorveglianza e biometria

Videosorveglianza

In materia di videosorveglianza si segnalano, da un lato, alcuni significativi provvedimenti diretti ad assicurare il rispetto del *provvedimento* generale del 29 aprile 2004 [doc. *web* n. 1003482], dall'altro, il provvedimento sulle nuove linee-guida.

Sul primo punto, si era rivolta all'Autorità la Soprintendenza speciale per il polo museale napoletano, alla quale il Comando dei Carabinieri-tutela patrimonio culturale nucleo di Napoli aveva chiesto di conservare per almeno trenta giorni le immagini raccolte tramite i sistemi di videosorveglianza installati presso alcuni musei della Regione Campania, maggiormente esposti al rischio della minaccia terroristica.

Per l'eccezionalità della situazione prospettata, considerato che la normativa di settore consente controlli continuativi tramite impianti audiovisivi per garantire la sicurezza dei beni culturali esposti o comunque raccolti e depositati nei musei statali

(art. 1, d.l. 14 novembre 1992, n. 433) e richiamando l'esigenza di rispettare i princìpi generali di liceità, necessità, proporzionalità e finalità affermati dal Codice (artt. 3, 11, comma 1, lett. *a*) e *d*) e 18, comma 2, del Codice e punto 2.1. del *provvedimento* aprile 2004), il Garante ha prescritto alla Soprintendenza, con *provvedimento* adottato ai sensi dell'art. 154, comma 1, lett. *c*), del Codice, di conservare le immagini raccolte presso alcuni siti museali della Regione Campania per un periodo di trenta giorni, fintantoché persiste la dichiarata eccezionale necessità (*Provv.* 12 marzo 2009 [doc. *web* n. 1605521]).

È altresì da menzionare l'approvazione (condizionata), in sede di verifica preliminare (art. 17 del Codice), di un apparato di videosorveglianza presso un istituto scolastico di Verona a salvaguardia del patrimonio scolastico, contro teppismo ed atti vandalici (*Provv.* 4 settembre 2009 [doc. *web* n. 1651744]).

In conformità al suddetto *provvedimento* del 2004, è stata prevista l'attivazione delle telecamere solo negli orari di chiusura degli istituti. Tuttavia, nel caso in cui l'attività didattica o ad essa strumentale all'interno della scuola coincida con l'orario di attivazione delle telecamere, è stata ritenuta necessaria la definizione, in accordo con il dirigente scolastico, degli orari di funzionamento delle telecamere.

Le telecamere possono riprendere esclusivamente le mura esterne, devono essere segnalate da appositi cartelli con visibilità anche notturna e la visualizzazione delle immagini è stata consentita solo a polizia e autorità giudiziaria.

Biometria

Sempre in sede di verifica preliminare (*Provv.* del 17 settembre 2009 [doc. *web* n. 1655708]), una società che svolge attività di vigilanza e sicurezza è stata autorizzata a trattare i dati biometrici dei dipendenti che accedono alle aree riservate ed esposte a rischio sicurezza degli aeroporti di Milano "Linate" e "Malpensa", Roma "Fiumicino", Venezia e Pisa. Nel progetto sottoposto alla verifica era previsto che i dati biometrici dei dipendenti, costituiti da caratteristiche tratte dall'impronta digitale, fossero memorizzati sotto forma di *template* ed in modalità cifrata, su un supporto (*smart card*) posto nell'esclusiva disponibilità del lavoratore. Il progetto escludeva comunque il controllo sull'orario di lavoro.

L'Autorità ha ritenuto proporzionati la raccolta e l'uso delle impronte digitali dei dipendenti in relazione agli accessi alle sole *"aree sterili"*, prescrivendo tuttavia

alla società di prevedere modalità alternative di accesso e identificazione e di fornire ai dipendenti un'apposita informativa sulla natura facoltativa del consenso al trattamento dei dati biometrici. La conservazione dei dati relativi agli accessi alle *"aree sterili"* è stata approvata per un tempo massimo di sette giorni.

Il nuovo provvedimento in materia di videosorveglianza

Anche in base al nuovo *provvedimento* generale dell'8 aprile 2010 in materia di videosorveglianza ([doc. *web* n. 1712680], in pubblicazione in *G.U.*), adottato previa consultazione del Ministero dell'interno, dell'Associazione nazionale comuni italiani e dell'Unione delle province d'Italia, l'Autorità ha ribadito, tra l'altro, che devono essere utilizzati solo dati anonimi quando le finalità del trattamento lo consentono e comunque unicamente immagini pertinenti e non eccedenti rispetto alle finalità perseguite.

Gli interessati devono essere resi edotti dell'esistenza di sistemi di videosorveglianza, anche attraverso il modello di informativa "minima" messo a disposizione nel *provvedimento* del 2004 *cit.* (art. 13, comma 3, del Codice). È stato, altresì, predisposto un nuovo modello semplificato per i titolari del trattamento che intendono attivare un collegamento diretto con le forze di polizia.

I sistemi che associano immagini a dati biometrici e quelli capaci di rilevare automaticamente comportamenti o eventi anomali e segnalarli devono essere sottoposti alla verifica preliminare, poiché comportano rischi specifici per i diritti e le libertà fondamentali.

Per quanto riguarda le misure di sicurezza l'Autorità ha disposto, tra l'altro, che: agli incaricati e responsabili del trattamento devono essere conferiti diversi livelli di visibilità e trattamento delle immagini, in relazione alle diverse competenze di ciascuno; occorre limitare le ipotesi di visione delle immagini raccolte e registrate e predisporre specifiche misure per la cancellazione delle immagini conservate nonché applicare tecniche crittografiche per la trasmissione di immagini da una rete pubblica o tramite connessioni *wireless.*

Fatte salve speciali esigenze di ulteriore conservazione in relazione alla chiusura di uffici o esercizi, o specifiche richieste a scopo investigativo delle autorità preposte, le immagini devono essere conservate al massimo per ventiquattro ore, dopo la loro rilevazione e solo per peculiari esigenze tecniche o per la particolare rischiosità

dell'attività del titolare del trattamento sino a una settimana.

Per i comuni, e solo per fini di tutela della sicurezza urbana, il termine massimo è di sette giorni, salvo eccezionali esigenze da sottoporre a una verifica preliminare del Garante.

L'informativa agli interessati è necessaria anche nei casi in cui i sindaci, quali ufficiali del Governo, o i comuni utilizzano sistemi di videosorveglianza in luoghi pubblici o aperti al pubblico per tutelare la sicurezza urbana.

La rilevazione di immagini tramite sistemi di videosorveglianza svolta da soggetti privati può avere legittimamente luogo previa acquisizione del consenso degli interessati o in presenza di un requisito equipollente (artt. 23 e 24 del Codice). A tal proposito, il provvedimento ha individuato i casi in cui, per la tutela di persone o di beni, la rilevazione di immagini può avvenire senza la previa acquisizione del consenso.

Per i *cd. "sistemi integrati di videosorveglianza"* tra soggetti diversi sono state previste specifiche garanzie per quei trattamenti che sono effettuati mediante: l'utilizzo, da parte di diversi e autonomi titolari del trattamento, delle stesse infrastrutture tecnologiche; il collegamento telematico di diversi titolari del trattamento ad un "centro" unico gestito da un soggetto terzo; il collegamento con le forze di polizia, anche nelle predette ipotesi.

Al riguardo, sono state prescritte alcune misure di sicurezza ulteriori quali l'adozione di sistemi per la registrazione degli accessi logici e delle operazioni compiute sulle immagini registrate e la separazione logica delle immagini registrate dai diversi titolari.

Con specifico riferimento ai sistemi di videosorveglianza integrati utilizzati dagli enti territoriali, inoltre, è stato stabilito che non possono essere tracciati gli spostamenti degli interessati e le immagini gestite da un unico centro devono essere trattate in forma differenziata.

Devono altresì essere sottoposti a verifica preliminare i sistemi integrati di videosorveglianza non rientranti nei modelli sopra descritti e per i quali non sia possibile adottare le misure e gli accorgimenti indicati nel provvedimento.

In considerazione del fatto che anche i dispositivi elettronici per la rilevazione di violazioni al codice della strada comportano un trattamento di dati personali, nel