Recenti Prog Med 2015; 106: 455-470

Utilizzo dei dati: aspetti legali ed etici

Gianluigi Ciacci

Riassunto. Gli esercenti le professioni sanitarie e gli organismi sanitari nello svolgimento della loro attività tipica compiono costantemente trattamenti di informazioni relative a persone fisiche, identificate o identificabili, anche indirettamente, e quindi di informazioni c.d. "personali". Conseguenza di ciò è l'applicazione della disciplina stabilita nel D.Lgs. 30 giugno 2003 n. 196, il Codice in materia di protezione dei dati personali, e integrata dalle pronunce dell'autorità demandata all'applicazione di questa complessa normativa, il Garante per la protezione dei dati personali: disciplina che a circa 12 anni dalla sua pubblicazione risulta essere ancora non completamente applicata, o comunque non in maniera corretta o con la dovuta attenzione. E, di conseguenza, portando spesso a non tutelare adeguatamente i dati personali oggetto di trattamento, e allo stesso tempo rendendo estremamente complessa a livello organizzativo la gestione degli stessi cercando di rispettare la legge: questo in particolare con riferimento alle più recenti realtà applicative nella sanità, anche caratterizzate dall'uso delle nuove tecnologie dell'informazione e della comunicazione, come per i registri clinici e il Fascicolo Sanitario Elettronico. Nel presente capitolo si evidenzia come, anche in presenza di attività di trattamento di dati personali in realtà di particolare delicatezza, e nello stesso tempo di grande rilevanza, sia possibile conciliare necessità di accesso e gestione delle informazioni con quelle di tutela dei soggetti cui tali informazioni si riferiscono. Possibilità che però è strettamente legata alla consapevolezza delle problematiche coinvolte, consapevolezza che a sua volta nasce dall'indispensabile conoscenza dei differenti aspetti della complessa normativa.

Parole chiave. Privacy, protezione dato personale, Garante, registri clinici.

Use of data: legal and ethical aspects

Summary. Health care professionals and organizations, in carrying out their activities, consistently handle information related to identified or identifiable (even indirectly) natural persons, therefore "personal data". The application of Legislative Decree 30 June 2003 n. 196 – the Code concerning the protection of personal data – as integrated by the pronunciations of the authority tasked with the application of such a complex legislation, the Authority for the Protection of Personal Data, consequently follows. The aforementioned legislation is seldom fully applied even 12 years after its publication, and even so not properly or with the adequate level of care. As a consequence, the data processed is often not adequately safeguarded, and compliance is hindered at an organisational level: this is particularly true with reference to the state of the art in medical technology, which is characterized by the utilization of ICT technologies such as the ones used with clinical registries and the Electronic Health Record. This chapter shows that, even when processing personal data that is of a sensitive nature, and at the same time of great importance, it is possible to reconcile the need to access and manage information with the protection of the individuals to whom such information refers to. This possibility is however closely linked to the awareness of the issues involved, awareness that in turn comes from an indispensable knowledge of the different aspects of that complex legislation.

Key words. Privacy, protection of personal data, Guarantor, clinical registries.

Privacy e sanità: peculiarità e problemi del trattamento dei dati sanitari

Gli esercenti le professioni sanitarie e gli organismi sanitari nello svolgimento della loro attività tipica compiono costantemente trattamenti di informazioni relative a persone fisiche, identificate o identificabili, anche indirettamente, e quindi di informazioni cosiddette "personali": certamente con riferimento ai loro pazienti/clienti, poi in relazione ai loro dipendenti/collaboratori, infine rispetto ai loro fornitori. Di queste tre categorie di utilizzo dei dati personali quella che si caratterizza in maniera peculiare nel settore in esame, rispetto ad altre figure professionali o attività economiche, è la prima: il trattamento delle informazioni relative ai propri pazienti per il medico, al paziente/"cliente" per l'organismo sanitario. Infatti, in tale caso, il modello di dato che viene tipicamente richiesto, utilizzato, conservato, eventualmente comunicato, è quello relativo alla salute della persona, e dunque un'informazione di particolare delicatezza, di natura "sensibile": questo chiaramente perché la persona entra in contatto con medico od organismo

Avvocato, professore a contratto titolare della cattedra di Informatica giuridica dell'Università Luiss Guido Carli, Roma.
Pervenuto il 25 maggio 2015.

proprio al fine della cura della propria salute, e quindi comunica informazioni che la riguardano in genere delicate e riservate. Peculiarità che, alla luce delle recenti (e inarrestabili) evoluzioni tecnologiche nella gestione quotidiana del proprio lavoro per tali categorie, eufemisticamente ricomprese nella dizione "sanità digitale" (dematerializzazione, ricette digitali, cartelle cliniche elettroniche, dispositivi medici *mobile*, referti *on line*, dossier e fascicolo sanitario elettronico, ecc.), rendono immediatamente applicabili, e con particolare importanza, discipline specifiche volte a tutelare l'individuo e i suoi dati.

Il riferimento è al D.Lgs. 30 giugno 2003 n. 196, il Codice in materia di protezione dei dati personali, e alle pronunce dell'autorità demandata all'applicazione di questa complessa normativa, il Garante per la protezione dei dati personali. A circa 12 anni dalla sua pubblicazione (che diventano 19 se si estende la considerazione anche alla precedente legge 675/1996) tale disciplina dovrebbe essere elemento "scontato", pacifico, acquisito della cultura della legalità dei soggetti preposti a utilizzare le informazioni sanitarie dei cittadini. Ma in realtà risulta essere ancora non completamente applicata, o comunque non in maniera corretta o con la dovuta attenzione, portando, di conseguenza, a non tutelare i dati personali oggetto di trattamento, e allo stesso tempo rendendo estremamente complessa a livello organizzativo la gestione degli stessi cercando di rispettare la legge.

Le ragioni di tale anomala e preoccupante situazione sono diverse, generali o specifiche del settore: così, da una parte è la normativa ad essere di non facile applicazione alla tecnologia, in particolare alla luce della costante necessità di confronto con la realtà in continuo mutamento, non ultimo a causa della repentina evoluzione dell'informatica e della telematica (che nel nostro Paese trova anche una quasi totale assenza di cultura della nuove tecnologie); dall'altra è la realtà dell'utilizzo delle informazioni relative agli individui a livello professionale, e specialmente nel settore della sanità, a creare ulteriori difficoltà rispetto a quelle normalmente affrontate da chi effettua trattamenti delle stesse per finalità non esclusivamente personali.

Dal primo punto di vista, pacifico il rilievo circa la scarsa confidenza del nostro Paese con le nuove tecnologie dell'informazione e della comunicazione (ICT), e la carente offerta formativa su di esse per qualsiasi ciclo di studi (dalle elementari ai corsi specialistici universitari), il repentino e costante diffondersi dell'ICT, delle sue applicazioni, in ogni settore lavorativo, come in quello personale, in maniera sempre più invasiva e pervasiva, crea discrasie di difficile gestione. Questo in particolare quando il diritto cerca di disciplinarne i più diversi aspetti, in maniera evidente rispetto al tentativo di proteggere le informazioni personali che nell'evolversi dell'indicato fenomeno ne costituiscono il suo costante oggetto.

Con riferimento invece alle difficoltà connesse all'utilizzo delle informazioni relative all'individuo per scopi professionali, le ragioni delle stesse sono le più diverse:

- la peculiarità dell'argomento, familiare un po' a tutti, radicato nella coscienza di ognuno, che quindi ha fatto ritenere spesso quasi superfluo l'approfondimento di quanto invece stabilito dettagliatamente e con specifiche modalità nella legge;
- certamente la non totale chiarezza del testo normativo, tra l'altro fortemente condizionata (con riferimento alla precedente disciplina della legge 675/1996, ma con ricadute anche in quella attuale dettata con il D.Lgs. 196/2003) dai numerosi interventi correttivi successivi alla sua emanazione;
- la cattiva informazione, che pur al sincero scopo di diffondere la consapevolezza dell'argomento, spesso ha solo reso più oscuro il testo già difficile.

Tutti questi fattori, ed altri ancora, hanno avuto come conseguenza il sorgere in molti interpreti, e comunque in chi si trova nella condizione di doversi riferire a tale complessa disciplina per doverla rispettare nella propria attività, di numerosi equivoci che certo non hanno aiutato e non aiutano nella corretta applicazione della legge, e forse addirittura stimolano in assoluto a una sua disapplicazione.

L'uso delle informazioni personali in sanità

Quanto detto vale in particolare per l'uso delle informazioni personali nel settore della sanità, dove alle cause indicate si è anche aggiunta da una parte quella della tradizione culturale dell'esercente le professioni sanitarie rispetto a sensibilità per lui "storiche", come il rispetto del segreto professionale a tutela della riservatezza del proprio paziente; dall'altra, quello della confusione terminologica tra concetti simili utilizzati in contesti simili con significati diversi (si pensi alla nozione di "consenso informato", che per un operatore sanitario è lo strumento necessario per intraprendere l'attività diagnostica e/o terapeutica, e quindi solo con riferimento a questa, mentre nel "mondo privacy" costituisce allo stesso tempo uno degli obblighi del titolare del trattamento ed uno dei diritti dell'interessato a cui i dati si riferiscono, e quindi la sua raccolta costituisce l'adempimento necessario per potere trattare in assoluto le informazioni relative a un individuo).

Ma le cause delle peculiarità della disciplina dettata a tutela dei dati personali in tale settore sono anche altre: non ultimo il fatto che il trattamento quotidiano dei dati relativi alla salute da parte degli esercenti le professioni sanitarie e degli organismi sanitari avviene non già e non solo per motivi economico-commerciali, ma soprattutto nello svolgimento di una funzione essenziale per la collettività.

Altra ragione della specificità della materia in esame deriva dalla natura stessa delle informazioni trattate. Infatti i "dati sanitari", vale a dire quel complesso di informazioni idonee a rivelare lo stato di salute di un individuo, sono come si è detto informazioni dalle caratteristiche assai peculiari, avendo a oggetto gli aspetti più intimi della persona ed essendo dunque in grado potenzialmente di incidere in maniera rilevante sulla sua dignità e sul suo diritto alla riservatezza: tanto da costituire il cosiddetto "nucleo duro" tra i dati personali, sia per la delicatezza che li contraddistingue, sia per il concreto pericolo di una loro utilizzazione a fini discriminatori.

In genere, infatti, le informazioni possono essere distinte in:

a) informazioni obiettivamente neutre, la cui conoscenza non può in alcun modo arrecare pregiudizio alla persona;
b) informazioni che l'interessato potrebbe voler tenere riservate, ma la cui divulgazione è resa opportuna da finalità sociali;
c) informazioni la cui diffusione non è desiderata dall'interessato e non è socialmente necessaria (come quelle sulle opinioni politiche o religiose, sulla salute e sulla vita sessuale, ecc.). Queste ultime costituiscono i dati di maggiore sensibilità o, come si esprimono alcuni autori, il "nucleo duro della riservatezza".

Banche dati e sistemi informatici

Tali peculiarità si estendono anche alle banche dati e ai sistemi informatici che permettono l'elaborazione di queste particolari informazioni: essi devono infatti trattare numerosi dati, di vario genere, per consentire di fornire al meglio prevenzione, cure e servizi medici. Ma allo stesso tempo, a causa dell'estrema delicatezza delle notizie a cui accedono, e dell'estrema facilità con cui le rendono accessibili, ciò deve avvenire rispettando con maggiore attenzione, anche e soprattutto tecnologica, dignità e *privacy* della persona interessata (e questa volta non solo nei confronti dei terzi, che non devono essere informati delle notizie personali che riguardano l'individuo, ma anche dell'interessato stesso, che talvolta, proprio in tale ambito, può risultare danneggiato in prima persona dall'apprendere informazioni sulla sua salute: si pensi ai soggetti cardiopatici). Infatti, se l'applicazione delle nuove tecnologie nella sanità[a] da una parte soddisfa la necessità di velocità, completezza ed esattezza delle informazioni, caratteristiche basilari, talvolta addirittura vitali in questo settore; dall'altra e allo stesso tempo, rende opportuno che l'utilizzazione automatizzata dei dati sanitari avvenga in modo consapevole e controllato nell'uso dei nuovi strumenti. Questo in particolare attraverso non solo l'investimento negli apparati informatici e telematici, completi, adeguati, aggiornati, ma anche quello nella cultura di coloro che li utilizzeranno, in modo da renderli attenti gestori dell'innovazione in campo sanitario, e non sprovveduti gestiti. Si pensi a tale proposito al difficile rapporto tra l'obbligo al rispetto della vita privata del malato, che pone rilevanti limiti alla registrazione e diffusione dei dati medici, con il diritto alla salute di ciascun individuo, che esige che tutti possano approfittare dei progressi della scienza medica realizzati grazie all'utilizzazione intensiva dei dati sanitari: tenendo presente anche il fatto che la qualità e la certezza delle informazioni, e il controllo della loro circolazione, rivestono un'importanza sempre crescente nel campo della salute (in un'epoca di costante aumento della mobilità delle persone, lo scambio rapido di informazioni esatte e pertinenti è una necessità per la sicurezza dell'individuo). Si pensi ancora al fatto che l'accesso alle banche dati sanitarie non è limitato al solo personale medico, tenuto al rispetto della deontologia professionale, ma implica l'ausilio tecnico e organizzativo di numerosi altri soggetti (ad esempio, degli esperti informatici). Tutti aspetti da coordinare con l'accelerazione degli ultimi mesi circa l'avvio, il completamento o il consolidamento di diversi progetti di sanità digitale.

Le normative in materia

Le normative emanate nella presente materia hanno quindi dovuto cercare di adottare discipline appropriate che permettessero di trovare e raggiungere un saldo punto di incontro tra i diversi interessi implicati, tenendo in particolare considerazione quelli del soggetto interessato (cioè il soggetto i cui dati costituiscono oggetto di trattamento): cercando di realizzare, attraverso sottili equilibri, una tutela della salute e non un potere sulla salute. Da qui, come si vedrà, la giustificazione della regolamentazione più severa, attraverso ampie limitazioni e un rigido assoggettamento, per la raccolta delle informazioni sanitarie e per la loro comunicazione, al vincolo del consenso della persona a cui si riferiscono o a un regime autorizzatorio gestito da un organo di controllo. Requisiti che seppure apparentemente rigidi e rigorosi, non rispondono in realtà pienamente alle esigenze di tutela delle raccolte di dati sanitari: l'autorizzazione perché soggetta alla valutazione discrezionale e più o meno accurata dell'organo di controllo; il consenso perché, a fronte delle diverse situazioni in cui può essere manifestato, e delle condizioni psicologiche del soggetto interessato,

[a] La diffusione degli elaboratori elettronici nel settore sanitario e gli sviluppi delle tecnologie informatiche per la gestione automatica dei dati clinici producono evidenti vantaggi dal punto di vista amministrativo, medico-legale, e soprattutto sotto il profilo scientifico: non solo, infatti, l'elaborazione informatica di tali dati consente un coordinamento sul piano organizzativo, offrendo omogenee modalità di raccolta e gestione dei documenti sanitari, ma risulta addirittura determinante per effettuare indagini statistiche, per reperire velocemente informazioni utili, per ricavare nuova conoscenza ai fini di ricerca, di prevenzione e cura.

può essere variamente influenzato e condizionato (si pensi a una raccolta effettuata in occasione di interventi urgenti, cioè quando il consenso possa essere percepito come inevitabile ai fini di una cura efficace).

Da qui, ancora, il riconoscimento di un diritto di accesso alle banche dati da parte del soggetto interessato, analogamente a quanto accade per i dati personali in genere, e inteso nelle sue tre accezioni classiche: facoltà di conoscere che un proprio dato personale sia inserito in una raccolta, e di quale informazione si tratti; facoltà di verificare l'esattezza del dato; facoltà di controllare che il dato sia utilizzato in conformità agli scopi della raccolta. Tuttavia, come già accennato, in campo sanitario occorre rilevare come il diritto di accesso debba essere circondato di particolari cautele, non solo per le possibili difficoltà di comprensione da parte del paziente della terminologia diagnostica adoperata dal medico, che può vanificare ogni facoltà di controllo sull'esattezza del dato; ma soprattutto per evitare le pericolose conseguenze di ordine psicosomatico che una errata e troppo brusca conoscenza delle notizie sullo stato di salute possono generare. Pertanto, anche in relazione a tale aspetto, una disciplina efficace deve essere in grado di bilanciare il diritto del malato di essere informato con un comportamento responsabile da parte del medico, idoneo a evitare possibili riflessi negativi. Di difficile configurabilità appare inoltre anche un altro diritto strettamente connesso alla tutela della riservatezza, il cosiddetto "diritto all'oblio" (di recente divenuto oggetto di ampio dibattito per quanto riguarda la sua effettiva realizzazione nella realtà di Internet: il riferimento è al caso "Google Spain" e alla pronuncia della Corte di Giustizia, causa C-131/12), come diritto a non conservare le informazioni oltre il tempo strettamente necessario. La materia sanitaria, infatti, può ritenere essenziale al progresso della medicina o, più semplicemente, alla tutela della salute del singolo, che vengano mantenuti a lungo i quadri clinici dell'individuo, talvolta anche dopo la sua morte.

Così, spiegate le ragioni della peculiarità della disciplina dettata in materia di trattamento dei dati sanitari in genere, e di quelli utilizzati dagli esercenti le professioni sanitarie in particolare, si procederà ora dapprima ad esporre i principi base della normativa italiana in materia, il D.Lgs. 30 giugno 2003 n. 196, e quindi si analizzeranno le modalità concrete con cui si applicano al settore in esame, allo scopo di risolvere i sottili equilibri riportati. Ferma restando infatti l'importanza della progettazione posta in essere da parte delle Autorità sanitarie del nostro Paese per la realizzazione della sanità digitale, tesa a migliorare la qualità del servizio al cittadino grazie all'implementazione sempre più massiva delle tecnologie dell'informazione e della comunicazione, nei loro più innovativi aspetti e attraverso le loro più utili applicazioni, non può essere trascurata la necessità di adeguare tali attività a quanto disposto dal D.Lgs. 196/2003 con riferimento alla protezione dei dati personali, e dunque l'importanza della conoscenza dello stesso.

Il D.Lgs. 30 giugno 2003 n. 196: principi generali e ambito di applicazione

Il 1° gennaio del 2004 è entrato in vigore nel nostro Paese (GU n. 174 del 29 luglio 2003 – Supplemento Ordinario n. 123) il D.Lgs. 30 giugno 2003 n. 196, il *Codice in materia di protezione* dei dati personali, in sostituzione della legge 31 dicembre 1996 n. 675, di recepimento della Direttiva comunitaria 95/46/CE, che aveva introdotto, per tutti gli Stati membri, l'articolata disciplina a tutela delle informazioni relative agli individui.

Il D.Lgs. 196/2003 ha un oggetto molto ampio, che lo rende di applicazione diffusa: difatti può interessare, sotto diversi punti di vista, una vasta maggioranza della collettività, certamente tutti coloro che svolgono trattamenti di dati personali nell'ambito di un'attività non personale. "Trattamenti" che, proprio alla luce della definizione prodotta dalla stessa legge, coinvolgono una qualsiasi attività collegata all'utilizzo di informazioni relative alla persona che permettono in qualche modo la sua identificazione, anche in maniera indiretta. In tale ambito occorre chiarire che la disciplina che stiamo analizzando, comunemente intesa e richiamata quale "legge sulla privacy", in realtà riguarda in genere il trattamento dei dati personali, e quindi *anche* la privacy[b]: per capire la correlazione tra i due concetti, ma anche le loro differenze, basti pensare che si possono avere trattamenti di dati personali pur senza in alcun modo influire sulla riservatezza del soggetto interessato (come potrebbe essere quello relativo alla realizzazione e gestione di un Albo professionale, ad esempio quello per i medici: pur non contenendo informazioni riservate. tale attività deve essere svolta applicando la disciplina del D.Lgs. 196).

Altro equivoco ricorrente sulla legge in esame è il ritenerla applicabile alle sole banche dati, e comunque unicamente all'utilizzo di strumenti elettronici: non è così, infatti ad essa si deve fare riferimento nei trattamenti di dati personali in genere, anche a prescindere dall'uso di un computer, e dunque anche a quelli con strumenti tradizionali come carta e penna, o addirittura senza supporti, come ad esempio nelle conversazioni.

Sempre con riferimento all'ambito di applicazione, ma questa volta a livello soggettivo, il D.Lgs. 196/2003 deve essere rispettato non solo dalle persone fisiche, ma anche da quelle giuridiche e da ogni altro ente o associazione: e quindi non solo

[b] Art. 2, comma 1, D.Lgs. 196: "1. Il presente testo unico, di seguito denominato "codice", garantisce che il trattamento dei dati personali si svolga nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali".

persone, ma anche società, associazioni, enti collettivi, ministeri (e in genere P.A.) che possono essere tutti soggetti attivi del trattamento dei dati, cioè titolari. Mentre, dopo gli interventi del Governo Monti nel 2012, solo le persone fisiche sono tutelate dalla normativa, e dunque unicamente esse possono assumere il ruolo di "interessati", ai sensi della definizione normativa contenuta nell'art. 4 del D.Lgs. 196/2003.

I PRINCIPI DELLA DISCIPLINA

Chiariti alcuni degli equivoci che maggiormente si riscontrano nell'applicazione della disciplina in materia di trattamento delle informazioni relative all'individuo, si ritiene utile dare un'iniziale impostazione generale all'analisi del D.Lgs. 196: e quindi l'attenzione deve essere innanzitutto portata su alcune affermazioni di principio contenute nel testo della legge.

La prima è riscontrabile nell'art. 1 della normativa, dove si esplicita per la prima volta un nuovo diritto soggettivo assoluto della persona, quello alla protezione dei dati personali ("*chiunque ha diritto alla protezione dei dati personali*") che, insieme al diritto alla riservatezza ed a quello all'identità personale, sempre previsti nella stessa disposizione, sono tutelati dalla legge in esame. Un nuovo diritto che deve essere ritenuto assorbente rispetto agli altri due, e caratterizzante l'intera disciplina, che dovrebbe dunque essere identificata non già, o non solo, come "legge sulla *privacy*", legge sulla riservatezza, ma come insieme di regole da rispettare nel caso vengano utilizzate, ai più disparati fini, informazioni relative alla persona: e, dunque, correttamente esposta come normativa sui "trattamenti dei dati personali". E quindi, di conseguenza, si dovrebbe parlare di "Garante per la protezione dei dati personali", e non di "Garante per la *privacy*": ma, come spesso accade, l'esterofilia terminologica, oltre alla seduzione dello slogan, hanno reso invalso l'uso errato, accettabile solo a patto che sia ben chiara la differenza sostanziale alla base dei due concetti.

In particolare, per quanto riguarda le finalità della legge, il Codice è chiamato a garantire che le attività svolte sui dati che si riferiscono alla persona avvengano rispettando proprio i diritti, le libertà fondamentali e la dignità dell'individuo, assicurando un loro elevato livello di tutela, anche attraverso il rispetto dei principi di semplificazione, armonizzazione ed efficacia delle modalità che vengono previste per l'esercizio dei diritti degli interessati e per l'adempimento degli obblighi da parte di chi svolge il trattamento.

Per quanto riguarda poi gli altri principi riportati nel D.Lgs. 196, risulta particolarmente rilevante quello affermato nell'art. 3 (il cosiddetto principio di necessità del trattamento), e in particolare il chiarimento riportato circa il fatto che non debba essere considerata "normale" la raccolta di informazioni che permetta di identificare, anche indirettamente, la persona a cui si riferiscono, ma "eccezionale": cioè solo limitata ai casi in cui non sia possibile usare dati anonimi od opportune modalità che permettano di identificare l'interessato solo in caso di necessità. Ancora, sempre nell'individuazione di tali modalità di trattamento, la legge richiede che i dati personali che vengono utilizzati dal titolare per un qualsiasi fine debbano essere gestiti in modo lecito e secondo correttezza, raccolti e registrati per scopi determinati, espliciti e legittimi, ed utilizzati in altre operazioni di trattamento in termini compatibili con tali scopi; le informazioni relative alla persona che subiscono una qualsiasi delle operazioni indicate dal Codice nella definizione di "trattamento" riportata al suo art. 4, comma 1, lett. *a*, debbono poi essere esatte e, se necessario, aggiornate, pertinenti, complete e non eccedenti rispetto alle finalità per le quali sono state raccolte o successivamente usate; infine, tali dati personali devono essere conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati (così l'art. 11 del D.Lgs.). Dalle indicazioni appena riportate è possibile ricostruire diversi principi che devono essere rispettati nella prassi (come per quello di pertinenza e non eccedenza, o quello di liceità e correttezza, quello di protezione dei dati, di finalità, ecc.), principi generali da cui derivano poi molti degli adempimenti richiesti dalla disciplina in esame.

Con riferimento all'ambito di applicazione, la normativa (fin dai tempi della legge 675/1996) si è sempre caratterizzata per un'estrema invasività, dovendo essere rispettata in tutti i casi in cui si svolga una qualsiasi attività che entri in contatto con informazioni relative alla persona (si ricordi la definizione di "trattamento" riportata in precedenza), se ed in quanto tale attività venga svolta da un soggetto che sia stabilito nel territorio italiano. Gli unici limiti all'applicazione della disciplina sembrerebbero essere, da una parte, la natura non personale del dato (cioè, in caso di trattamento di informazioni che *non* permettono di identificare la persona, direttamente o meno, la legge non si applicherà)[c], dall'altra l'uso dell'informazione personale per "fini esclusivamente personali" (concetto non definito dalla normativa, ma che potrebbe essere inteso come indicazione della non professionalità del trattamento, cioè del fatto

[c] L'art. 4, comma 1, lett. b, definisce il dato personale come "qualunque informazione relativa a persona fisica identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale": devono quindi essere considerati tali, oltre ai dati tipo l'indirizzo e/o il numero telefonico, la data di nascita, chiaramente il codice fiscale e la partita I.V.A., le caratteristiche fisiche peculiari, ma anche il PIN del Bancomat (anche se segreto, almeno presso il proprio istituto bancario, oltre che presso i gestori del circuito, è conosciuta l'associazione tra questo numero segreto e il titolare dello stesso, fatto che rende quel numero comunque un dato personale) e l'indirizzo e-mail.

che tale trattamento non sia riferibile all'attività commerciale, imprenditoriale o professionale eventualmente svolta dal titolare dello stesso), sempre che ciò non integri l'eventualità che i dati siano destinati a una comunicazione sistematica o alla diffusione: anche se, nell'ipotesi di fine esclusivamente personale, pur non applicandosi l'intero Codice, si devono però rispettare le indicazioni relative alle misure di sicurezza e quelle in tema di risarcimento del danno eventualmente procurato (rispettivamente gli articoli da 31 a 36, oltre all'allegato B, e l'art. 15 del D.Lgs. 196).

Il Codice risulta avere quindi un ambito di applicazione "globale", coinvolgendo come si è detto tutti i casi di utilizzo di informazioni relative alla persona, e non già e non solo quelli che si riferiscono alla sua *privacy*: e in questo occorre prestare attenzione, come si è appena detto nel testo, non all'eventuale interferenza con la *privacy*, la riservatezza dell'individuo (accezione comune circa l'oggetto della legge), quanto al fatto di utilizzare, in qualsiasi modo, suoi dati personali. Unico limite a tale ampia applicabilità risiede unicamente nelle diverse interpretazioni date dal Garante con riferimento a specifiche fattispecie: con ciò aumentando, almeno parzialmente, l'indeterminatezza delle singole disposizioni e le difficoltà di chi deve applicarle. Disposizioni che comunque devono essere applicate e osservate.

Gli obblighi del titolare e i diritti dell'interessato

Chiunque ponga in essere un'attività che comporti un trattamento dei dati personali, ed è la persona a cui spettano le decisioni sulle finalità e modalità dello stesso, ai sensi della normativa in esame viene considerato *titolare* del trattamento dei dati raccolti: in quanto tale dovrà dunque adempiere agli obblighi previsti dal D.Lgs. 196/2003, obblighi volti a tutelare con diverse modalità i soggetti cui le informazioni si riferiscono (cosiddetti *interessati*) nei confronti di tale attività di utilizzo di informazioni personali.

L'analisi relativa agli obblighi da adempiere da parte di colui che ha potere decisionale rispetto all'attività di trattamento si può strutturare nell'ambito di tre diverse realtà, quella del trattamento dei dati dei propri clienti, dei dati dei propri fornitori (qualora siano persone fisiche), ed infine quella del trattamento dei dati dei propri dipendenti.

A livello schematico, ed in via generale, i principali obblighi che vengono disciplinati in diverse norme del D.Lgs. 196/2003 (e che, insieme all'affermazione di numerosi diritti in capo al soggetto i cui dati personali vengono trattati, consentono una corretta regolazione dell'attività di trattamento) sono:

- l'obbligo di notificare al Garante i trattamenti previsti dall'art. 37 commi 1 e 2 (e solo nei casi esplicitati da tale norma), allegando eventualmente, nelle ipotesi di trattamento dei cosiddetti "dati sensibili" [d], anche la richiesta di autorizzazione al trattamento (e all'eventuale trasferimento extra UE degli stessi - art. 37 comma 3 e 41);
- obbligo di fissare le modalità di raccolta ed i requisiti dei dati da trattare (artt. 11);
- obbligo di informazione all'interessato (la cosiddetta "informativa", disciplinata nell'art. 13);
- obbligo di richiedere il consenso dell'interessato (art. 23);
- obbligo di adottare le adeguate misure di sicurezza, idonee e minime (art. 31 e ss.);
- obbligo di vigilanza sull'osservanza della legge nell'ambito della propria struttura (art. 29);
- obbligo di rispettare determinate regole in caso di cessazione del trattamento e/o per l'eventuale cessione dei dati (art. 16);
- obbligo di rispettare i limiti richiesti per l'utilizzazione delle valutazioni della personalità e del comportamento basate sul trattamento dei dati personali (art. 14);
- obbligo di risarcimento degli eventuali danni causati a seguito del trattamento dei dati, compresi quelli non patrimoniali (art. 15).

Nell'ambito di tale elenco di adempimenti che deve porre in essere il titolare, si devono poi individuare, approfondendo di conseguenza la precipua disciplina per la categoria, quelli specifici della tipologia di trattamento presa in considerazione.

Paralleli agli obblighi in capo al titolare del trattamento, nella legge vengono anche introdotti una serie di diritti dell'interessato, spesso corrispondenti ai primi, che concorrono, insieme alla creazione di un organo di controllo "terzo", il Garante per la protezione dei dati personali, a costruire un sistema di protezione dell'individuo efficace e adeguato: la cui struttura (obblighi-diritti-controllo di un organo pubblico) risulta essere comune a quella dei Paesi maggiormente informatizzati, dotati di normative sulla materia da un periodo maggiore di quello italiano. Con riferimento ai diritti dell'interessato, è possibile individuare nell'art. 7 e ss. del D.Lgs. 196/2003 le seguenti figure:

- il diritto, assoggettato a deroghe, di esprimere il consenso al trattamento dei dati;
- il diritto di essere informato sull'identità del titolare e del responsabile, nonché sulle modalità e finalità del trattamento dei dati;
- il diritto di intervenire sui dati, modificandoli, integrandoli, correggendoli;

[d] Sono quei "dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale", considerati di alta potenzialità lesiva del soggetto a cui si riferiscono (rappresentano, secondo la dottrina specializzata, il cosiddetto "nucleo duro della riservatezza"), e quindi sottoposti ad un regime maggiormente rigido.

- il diritto a ottenere il risarcimento di eventuali danni, qualora si sia proceduto a trattamenti illegittimi dei propri dati;
- il diritto di opporsi, in tutto o in parte e per motivi legittimi, al trattamento dei dati, ancorché conforme alle finalità dichiarate;
- il diritto di opporsi al trattamento dei dati personali effettuato per finalità commerciali, pubblicitarie, di vendita diretta, di ricerca di mercato o di comunicazione commerciale interattiva;
- il diritto di opporsi al trattamento dei dati personali volto a delineare il profilo o la personalità dell'interessato.

Diritti che, oltre a rappresentare spesso l'elemento che porta alla creazione dei corrispondenti obblighi in capo al titolare, nel loro insieme costituiscono il punto di riferimento per un adempimento generale che deve essere affrontato da chi sottopone a trattamento le informazioni personali di un individuo: deve cioè essere predisposta la propria struttura in modo tale da rendere possibile l'esercizio di tali facoltà concesse dalla legge all'interessato, attraverso l'individuazione di una procedura semplificata creata a tal fine e di una serie di figure nell'ambito di questa (ci si riferisce ai responsabili e agli incaricati).

Il Garante per la protezione dei dati personali: compiti, funzioni, modalità di attivazione

Esplicitati gli obblighi e indicati i diritti stabiliti dalla legge in capo ai vari soggetti deve ora essere esaminato il terzo caposaldo della struttura di tutela dell'individuo nell'ambito di un'attività di trattamento dei suoi dati personali: l'organo pubblico di controllo che nel nostro Paese è rappresentato dal Garante per la protezione dei dati personali.

La figura del Garante, organo collegiale costituito da quattro componenti (eletti due dalla Camera e due dal Senato, che al loro interno nominano un presidente), è disciplinata nel Titolo II della terza parte del D.Lgs. 196/2003. Rappresenta l'organo di controllo del nostro sistema, al fine di permettere un'effettiva tutela dell'interessato i cui dati sono oggetto di trattamento, opera in piena autonomia e con indipendenza di giudizio e di valutazione (art. 133, comma 1), ed ha specifici poteri di monitoraggio, controllo, vigilanza, sanzionatori, consultivi, di informazione, di promozione (art. 154).

Per quanto riguarda in particolare l'attività ispettiva (che comprende la possibilità di monitoraggio, controllo e vigilanza sull'adempimento della disciplina in materia di trattamento dei dati), la legge prevede che il Garante possa disporre accessi alle banche dati o altre ispezioni e verifiche presso i titolari del trattamento, al fine di controllare la corretta applicazione della legge, e il suo rispetto (art. 158). Il Garante può avvalersi in questa attività della collaborazione di altri organi dello Stato, quando ciò sia necessario per assicurare la tempestività, la speditezza e la completezza degli interventi: a tale proposito, alla fine del 2003 è stata avviata una collaborazione tra l'Autorità e la Guardia di finanza, che è dunque andata a costituire lo strumento di controllo nel territorio da parte della stessa Autorità. I criteri dell'attività ispettiva sono contenuti nell'art. 159 del D.Lgs. 196/2003, che ne definisce il programma in base al principio di pubblicità e trasparenza delle scelte operate, e a una serie di priorità che tengono conto, tra l'altro, delle risorse a disposizione dell'Autorità: in particolare, a proposito di priorità, nella pianificazione della sua attività per l'anno in corso, è stato previsto dal Garante un aumento del 35% di quella ispettiva. Nella programmazione poi del suo lavoro in generale, si è ritenuto opportuno stabilire che metà degli interventi riguardino i reclami presentati dai cittadini o dalle associazioni che li rappresentano per denunciare presunte violazioni della riservatezza, un quarto riguardi le verifiche disposte dal Garante nel caso in cui si sospettino delle irregolarità, da ripartire equamente tra soggetti privati ed organismi pubblici, e l'ultimo quarto sia, infine, destinato all'esecuzione di accertamenti per verificare lo stato di attuazione della legge da parte di amministrazioni ed enti pubblici o di soggetti privati.

Devono essere ora indicati gli strumenti che possono essere utilizzati al fine di attivare l'Autorità di controllo. È molto importante però prima chiarire che il Garante non ha un potere "esclusivo" sulla materia. Infatti l'art. 145 comma 1 del D.Lgs. 196 dispone che " i diritti di cui all'articolo 7 possono essere fatti valere dinanzi all'Autorità giudiziaria o con ricorso al Garante": quindi nel valutare costi e benefici del porre in essere una seria attività di adeguamento a quanto disposto dalla normativa in esame (ed evitare magari superficiali, e pericolosi, "disinteressamenti" per l'argomento in esame), sicuramente si deve tenere presente non solo il rischio di un controllo della propria struttura ad autonoma ed esclusiva iniziativa della stessa Autorità, per così dire "dall'alto" (da molti ritenuto poco rilevante); ma anche quello di dover affrontare il problema del rispetto del D.Lgs. 196 di fronte ad un giudice magari nell'ambito di una più ampia procedura (ad esempio, di un'azione per licenziamento illegittimo di un proprio collaboratore), e quindi "dal basso". La proposizione del ricorso ad un'autorità esclude comunque la possibilità di ricorso all'altra (art. 145, commi 1 e 2).

Nello specifico, gli strumenti a disposizione dell'interessato per attivare il Garante sono la *segnalazione,* il *reclamo* o il vero e proprio *ricorso.* Il *reclamo* può essere presentato al Garante per la presunta violazione di qualsiasi norma in materia, deve essere circostanziato, o deve poter indicare in modo dettagliato fatti e circostanze su cui si fonda (art. 142). Qualora non si possa proporre un reclamo circostanziato perché non è possibile fornire le informazioni richieste, si procede con una sem-

plice *segnalazione*, che ha il fine di sollecitare un controllo del Garante sul trattamento (art. 144). Il *ricorso* si può presentare o al Garante o all'Autorità giudiziaria, ma come si è detto le due azioni non possono concorrere, e quindi una esclude l'altra. Il *ricorso* è proponibile solo per la presunta violazione dei diritti dell'interessato riconosciuti dall'articolo 7 del D.Lgs. 196/2003, ed elencati sinteticamente nelle precedenti pagine: propedeutico al ricorso (senza non può cioè essere proposto) è poi l'*interpello* fatto al titolare o al responsabile, cioè la preventiva richiesta allo stesso sul medesimo oggetto, tranne nel caso in cui il decorso del tempo esporrebbe il soggetto a pregiudizio grave e irreparabile (così l'art. 146).

Il Garante, se nell'ambito di un controllo o di un accertamento (attivato da un ricorso, un reclamo o una segnalazione, oppure nell'ambito dell'esercizio del suo autonomo potere ispettivo), riscontra una particolare situazione di illegittimità o di pericolo di illegittimità, ha inoltre il potere di vietare o disporre il blocco del trattamento dei dati preventivo al realizzarsi di una situazione pregiudizievole per l'interessato: questo in particolare in presenza di un concreto rischio di recare danno all'interessato, qualora il trattamento risulti illecito, non corretto, ovvero non uniformato alle indicazioni di modifica in precedenza segnalate dallo stesso Garante perché ritenute da questo "opportune e necessarie". Oltre al potere di vietare o disporre il blocco del trattamento, l'Autorità può anche comminare l'applicazione delle severe sanzioni amministrative e penali previste dalla normativa, dal Titolo III della parte terza della legge (vedi box).

Trattamento dei dati personali da parte dell'organismo sanitario: gli obblighi stabiliti

Analizzata seppure sinteticamente la disciplina generale in materia di protezione dei dati personali del nostro Paese, risulta ora interessante approfondire i suoi aspetti particolari relativi all'ambito sanitario: e quindi verificare quali siano le modalità concrete di adeguamento agli obblighi in materia da parte di un modello tipo, e rispetto a un modello generico di attività, di organismo sanitario. Questo con un approccio pratico e in maniera "verticale", cioè indicando gli specifici adempimenti necessari per il pieno rispetto della legge, non potendo certamente, in queste poche pagine, approfondire l'indagine.

Nonostante le indicate difficoltà, apparentemente insormontabili, si è cercato comunque di riportare un modello di adeguamento convinti che, una volta indicati e chiariti i principi generali stabiliti nel D.Lgs. 196/2003 (compito esaurito seppure sinteticamente nel precedente paragrafo) e "aperta la strada" con quanto verrà indicato in questo circa gli obblighi da rispettare, sarà poi possibile per il lettore interessato a questo argomento "personalizzare" il discorso nell'ambito della propria realtà di trattamento: e magari, senza immaginare di provvedere in maniera autonoma, affidarsi con maggiore consapevolezza al consulente esperto della materia più adatto per le proprie esigenze.

Chiarito il punto, si specifica che gli adempimenti che verranno presi in considerazione riguardano l'obbligo di notificazione, di richiesta di autorizzazione al Garante per il trattamento di dati sensibili, di rilascio delle informative e di richiesta di consenso preventivo, di procedure per l'esercizio dei diritti da parte dell'interessato, di attivazione delle misure di sicurezza.

Le attività di trattamento di dati personali da parte dell'organismo sanitario

Anche per l'organismo sanitario, a prescindere dal livello di complicatezza della sua struttura e della sua attività, si possono distinguere tre diverse aree di trattamento di dati personali relative all'utilizzo delle informazioni rispettivamente dei propri pazienti/clienti, dei propri dipendenti e dei propri fornitori. In questo caso, però, sulla costruzione tipica appena riportata si creano diverse commistioni e ampliamenti, conseguenza della presenza in alcune realtà di rilevanti aspetti commerciali (si pensi alle cliniche o ai laboratori di analisi privati che, pur svolgendo una utile funzione sociale, certo tengono presenti anche gli aspetti più prettamente lucrativi dell'attività sanitaria), nonché di livelli di articolazione molto variegati (si pensi ancora alle cliniche che locano propri spazi per l'attività di medici specialisti privati, i quali rispetto alla struttura dell'organismo sanitario possono sempre essere considerati clienti, ma intendendo tale figura in senso più ampio di quanto indicato fino ad ora, limitato solo ai pazienti). Mentre con riferimento alla realtà degli organismi sanitari "pubblici" gli aspetti maggiormente commerciali vengono sostituiti dalle peculiarità tipiche delle P.A., non ultimo per le finalità perseguite e le spesso complesse regolamentazioni normative di riferim ento.

Nella specie, per la prima area di trattamento vengono gestite numerose informazioni personali, certamente anche sensibili, dei pazienti, sia quali soggetti a cui si riconduce il trattamento sanitario, sia quali clienti del servizio che viene offerto dalla struttura: informazioni acquisite dall'organismo sanitario direttamente (sempre nell'esempio della clinica, magari al momento del ricovero del soggetto, o in seguito all'espletamento di esami diagnostici), ma anche indirettamente attraverso eventualmente quanto viene riferito dai familiari del paziente; informazioni che possono poi riguardare anche terze persone e che possono essere comunicate e conosciute da un numero imprecisato di soggetti interni all'organismo sanitario, strutturati o meno.

Per la seconda, quella dei propri dipendenti, le problematiche sono le stesse comuni ad altre realtà, in questo caso coinvolgendo differenti figu-

BOX - ILLECITI E SANZIONI STABILITI NEL D.LGS. 196/2003

Il Codice sulla protezione dei dati personali prevede tre tipi di responsabilità, e dunque tre diversi tipi di conseguenze sanzionatorie, in relazione ai differenti illeciti che possono essere compiuti.Chi non osserva le sue disposizioni può cioè essere ritenuto responsabile a livello *civile, amministrativo* o addirittura *penale*.

Illecito civile

È disciplinato nell'art. 15 del Codice, che assimila l'attività di trattamento tra quelle pericolose ai sensi dell'art. 2050 c.c.[a], prassi tipica del Legislatore che più volte ha considerato, probabilmente a causa di una poco chiara percezione delle nuove tecnologie, l'uso dell'informatica come attività ad alta potenzialità lesiva: concezione ereditata dai primi approcci normativi nel settore, ma comunque durante la fase iniziale di sviluppo dell'elaboratore elettronico, quello caratterizzato dai grandi computer, appannaggio di poche rilevanti strutture, e certamente non più adeguata alla realtà attuale della cosiddetta informatica distribuita, quella dei personal computer e degli smartphone ad uso sempre più comune nella collettività. Oltre a rilevare che, nel caso specifico, tale assimilazione risulta non totalmente corretta proprio a causa dell'estensione dell'applicazione della legge ad ipotesi di trattamento di dati personali svolte anche senza l'ausilio di strumenti elettronici: difficile risulterebbe infatti percepire in tali ipotesi l'alta potenzialità lesiva, pur sempre almeno astrattamente possibile. A prescindere da questi rilievi critici, in ogni caso la disciplina della responsabilità oggettiva implica che si prescinda, nella valutazione della responsabilità dell'autore del comportamento lesivo, da qualsiasi giudizio relativo alla presenza di dolo o colpa dell'autore del comportamento dannoso (e quindi dalla valutazione della presenza o meno dell'elemento soggettivo [b]), e allo stesso tempo implica l'inversione legale dell'onere della prova[c]: basterà quindi il solo realizzarsi del danno in nesso causale con la condotta posta in essere dal titolare del trattamento affinché si concretizzi l'obbligo risarcitorio di questo, che dovrà direttamente provare di non essere responsabile. E, a tale proposito, si tenga presente che si rientra in un'ipotesi di responsabilità aggravata, che può essere evitata solo dimostrando di avere adottato "tutte le misure idonee ad evitare il danno"; ma, in tema di misure preventive (quindi, ad esempio, nel caso dell'informativa e del consenso), se queste fossero state idonee il danno non si sarebbe verificato: il risarcimento sembrerebbe quindi evitabile, nell'ipotesi indicata, solo se si riesce a provare il caso fortuito o la forza maggiore.

Illecito amministrativo

Si riconoscono sei fattispecie principali di illecito *amministrativo*, e quindi conseguentemente quattro diverse ipotesi sanzionatorie (fattispecie che nel vigore della precedente normativa, la l. 675 del 1996, erano sanzionate più severamente a livello penale). La prima è l'illecito di *omessa o inidonea informativa all'interessato*, è disciplinata dall'art. 161 del Codice e implica una sanzione base del pagamento di una somma da 6.000 a 36.000 euro; la seconda fattispecie punisce con pagamento della somma da 10.000 a 60.000 euro la *cessione di dati in violazione della normativa del Codice per la privacy* (art. 162); la terza fattispecie sanzionatoria prevede il caso di *omessa o incompleta notificazione*, in conseguenza della quale è prevista la sanzione amministrativa del pagamento di una somma da 20.000 euro a 120.000 (art. 163); la quarta delinea l'illecito di *omesso invio di informazioni o documenti richiesti dal Garante*, e l'art. 164 prevede il pagamento di una somma da 10.000 a 60.000 euro. Abbiamo poi una quinta fattispecie, quella relativa all'inosservanza dei provvedimenti del Garante di prescrizione di misure necessarie o di divieto, sanzionata con il pagamento di una somma da 30.000 a 180.000 euro (art. 162 comma 2-*ter*); viene infine sanzionato anche il trattamento di dati personali in violazione delle misure minime di sicurezza ex art. 33, in particolare con il pagamento di una somma da 10.000 a 120.000 euro (art. 162 comma 2-*bis*). In tutte queste ipotesi l'organo competente a irrogare le sanzioni è lo stesso Garante per la protezione dei dati personali, e la relativa procedura è disciplinata dall'art. 166 del D.Lgs. 196/2003.

Illecito penale

Il Codice disciplina le seguenti figure di *reato*: *il trattamento illecito di dati personali* (art. 167), intendendo per "illecito" quello effettuato in violazione di precise disposizioni del D.Lgs. 196, violazione che implica come conseguenza sanzionatoria, a seconda delle ipotesi, la reclusione da 6 a 18 mesi, oppure da 6 a 24 mesi, o ancora da 1 a 3 anni, sempre che si agisca al fine di trarne per sé o per altri profitto o di recare ad altri un danno; *la falsità nelle dichiarazioni e notificazioni al Garante* (art. 168), sanzionata con la reclusione da 6 mesi a 3 anni (sempre che il fatto non costituisca più grave reato); *l'omissione di adozione delle misure minime di sicurezza*, che porta alla comminazione della contravvenzione dell'arresto sino a due anni, salvo il cosiddetto ravvedimento operoso (art. 169), ipotesi che porterebbe a una situazione di non punibilità; infine, almeno per le fattispecie di maggiore rilevanza, l'inosservanza dei provvedimenti del Garante (art. 170), sanzionata con la reclusione da 3 mesi a 2 anni.

---

[a] Art. 15 D.Lgs. 196/2003: "Chiunque cagiona danno ad altri per effetto del trattamento di dati personali è tenuto al risarcimento ai sensi dell'articolo 2050 del codice civile". Art. 2050 del codice civile: "Chiunque cagiona danno ad altri nello svolgimento di un' attività pericolosa, per sua natura o per la natura dei mezzi adoperati, è tenuto al risarcimento, se non prova di avere adottato tutte le misure idonee a evitare il danno".

[b] Il soggetto che ha causato il danno è quindi responsabile semplicemente perché ha posto in essere il relativo comportamento, a nulla rilevando se lo abbia fatto volutamente, o per mancata attenzione: anzi, se il danno si è realizzato, dovrà risarcirlo anche se ha prestato la massima attenzione perché ciò non avvenisse (caso tipico è quello del trasporto di sostanze pericolose, come quelle esplosive o tossiche).

[c] Normalmente nel nostro sistema processuale civile chi agisce in giudizio per far valere un proprio diritto deve dimostrare il fondamento della sua pretesa: se non ci riesce la sua domanda verrà rigettata e la causa persa. Nel caso di responsabilità civile cosiddetta aggravata (è questa l'ipotesi dell'esercizio di attività pericolose e dell'art. 15 del D.Lgs. 196) il sistema della prova in giudizio è invertito: è infatti il soggetto che ha causato il danno, e che viene chiamato in giudizio, a dover dimostrare la sua non responsabilità, e se non ci riesce perderà la causa (non a caso, nella tradizione giuridica, si parla a tale proposito di "*probatio diabolica*").

re professionali, con diversi livelli di collegamento (dipendenti veri e propri, medici o meno, collaboratori a progetto, tirocinanti, ecc.) alla struttura sanitaria. Anche i trattamenti dei dati personali dei propri fornitori non riportano elementi di specificità particolari per la categoria in esame, che forse si caratterizza più che altro per il tendenziale rilevante numero degli stessi (ma sempre tenendo presente l'esenzione dell'applicazione della legge per le persone giuridiche).

Nell'ambito delle indicate aree di trattamento, e in linea di massima con riferimento alla prima sui dati dei propri clienti/pazienti, deve essere prestata particolare attenzione alla possibilità che la singola struttura avvii alcune attività originali e diverse rispetto a quelle tipiche che implichino comunque un contatto con informazioni relative agli individui: come ad esempio la clinica che inizi operazioni di marketing tipo il rilascio di *fidelity card*, o l'ospedale che per migliorare la propria organizzazione implementi sistemi automatizzati di gestione del personale attraverso carte elettroniche, o il laboratorio di analisi che eventualmente utilizzi la posta elettronica per consegnare al paziente i risultati dei suoi esami e accertamenti, oppure l'adozione di impianti di videosorveglianza per tutelare la sicurezza di persone e cose presenti nei locali, o in alcuni locali, dell'organismo sanitario. In casi come questi si può verificare l'applicazione delle norme più comuni del D.Lgs. 196/2003, ma anche quella di disposizioni specifiche, come ad esempio per gli articoli del Codice in materia di comunicazioni elettroniche o di trattamento di dati personali in ambito lavorativo: nonostante ciò non riteniamo che questo fatto realizzi difficoltà applicative insormontabili, ma dovrà solo prestarsi particolare attenzione nel momento dell'esame e valutazione della singola fattispecie, per poterla inquadrare nel corretto ambito e, quindi, applicare la disciplina adeguata.

Individuati così i trattamenti delle informazioni relative alle persone che avvengono nell'attività dell'organismo sanitario, seppure genericamente e con le puntualizzazioni già svolte circa la completezza dell'operazione, si procede ora ad analizzare, secondo uno schema basato sullo specifico obbligo preso in considerazione, come tale struttura debba adempiere a quanto stabilito nel D.Lgs. 196/2003.

L'obbligo di notificare il trattamento dei dati al Garante (art. 37 D.Lgs. 196/2003)

Con riferimento all'obbligo di notifica, cioè alla comunicazione della propria attività di trattamento da fare all'Autorità garante, l'organismo sanitario dovrà certamente procedere al suo adempimento. Questo sia perché l'attività da esso svolta sicuramente rientra nelle ipotesi previste dall'art. 37, comma 1, sia perché nei vari provvedimenti adottati dal Garante per meglio determinare e chiarire le modalità applicative dell'obbligo di notifica viene espressamente esclusa dalla possibilità di esonero dall'obbligo proprio tale figura[e]. È importante ricordare che anche se è già stata inviata la notificazione al Garante nel vigore della disciplina precedente, quella della legge 31 dicembre 1996 n. 675, si sarebbe dovuto ripetere l'adempimento secondo quanto stabilisce il D.Lgs. 196/2003, in particolare con le nuove modalità ivi previste*: la mancata reiterazione della notifica può infatti essere sanzionata in maniera rilevante (pagamento di una somma da 20.000 a 120.000 euro, secondo l'art. 163 del Codice).

L'obbligo di richiedere l'autorizzazione per il trattamento dei dati sensibili al Garante (art. 26 D.Lgs. 196/2003)

Per quello che riguarda l'obbligo di richiedere l'autorizzazione per il trattamento dei dati sensibili al Garante, nel caso in esame si possono utilizzare due autorizzazioni generali: la prima si riferisce al trattamento di dati sensibili nei rapporti di lavoro e la seconda al trattamento di dati idonei a rivelare lo stato di salute e la vita sessuale.

Così, con riferimento in particolare alla seconda Autorizzazione generale, che maggiormente interessa l'ambito sanitario, l'estensione anche ai soggetti in esame si evince in due diversi punti del provvedimento: nella parte autorizzatoria vera e propria ("… *autorizza* … b*) gli organismi e le case di cura private, nonché ogni altro soggetto privato, a trattare i dati idonei a rivelare lo stato di salute e la vita sessuale, con il consenso scritto dell'interessato;* c*) gli organismi sanitari pubblici, ivi compresi i soggetti pubblici allorché agiscano nella qualità di autorità sanitarie, a trattare i dati idonei a rivelare lo stato di salute anche per il perseguimento delle finalità di rilevante interesse pubblico individuate … qualora ricorrano contemporaneamente le seguenti condizioni:* 1*) il trattamento sia finalizzato alla tutela dell'incolumità fisica e della salute di un terzo o della collettività;* 2*) manchi il consenso scritto (articolo 23, comma 1, ultimo periodo, legge n. 675/1996), in quanto l'interessato non lo ha prestato o non può prestarlo per effettiva irreperibilità, per impossibilità fisica, per incapacità di agire o*

[e] Per quello che riguarda i provvedimenti del Garante in tema di notificazione del 31 marzo e del 23 aprile 2004, il riferimento testuale è sempre all'esercente la professione sanitaria (eventualmente anche associato ad altro professionista), e quindi non all'organismo; invece nella "risposta a quesiti sui trattamenti in ambito sanitario da notificare al Garante" del 26 aprile 2004, con riferimento ai trattamenti di dati genetici e biometrici viene espressamente riportato che "*l'esonero non opera, poi, per i trattamenti di dati genetici o biometrici effettuati da strutture sanitarie, pubbliche o private (quali ospedali, case di cura o di riposo, centri di riabilitazione, ambulatori polispecialistici, laboratori di analisi cliniche e diagnostica per immagini, studi fisioterapici, aziende sanitarie, istituti clinici privati, associazioni sportive), essendo stato disposto solo in favore di persone fisiche esercenti le professioni sanitarie, anziché per i trattamenti dei dati genetici o biometrici in quanto tali*".

* Le nuove modalità, nella specie, sono rinvenibili direttamente nel sito web del Garante (http://www.garanteprivacy.it), che nel dettaglio riporta le istruzioni per procedere alla notificazione.

per incapacità di intendere o di volere; 3*) il trattamento non sia previsto da una disposizione di legge che specifichi i dati che possono essere trattati, le operazioni eseguibili e le rilevanti finalità di interesse pubblico perseguite"*) e nell'art. 1 della stessa, dove viene individuato l'ambito di applicazione e le finalità del trattamento ("*1.1 L'autorizzazione è rilasciata:* a*) ai medici-chirurghi, agli odontoiatri e agli altri esercenti le professioni sanitarie iscritti in albi o in elenchi;* b*) al personale sanitario infermieristico, tecnico e della riabilitazione che esercita l'attività in regime di libera professione;* c*) alle istituzioni e agli organismi sanitari privati, anche quando non operino in rapporto con il Servizio sanitario nazionale*").

L'organismo sanitario non deve quindi richiedere al Garante l'autorizzazione al trattamento dei dati sensibili dei propri pazienti, sulla base dell'Autorizzazione generale n. 2, e dei propri dipendenti, ai sensi dell'Autorizzazione generale n. 1.

L'obbligo di fornire l'informativa all'interessato (art. 13 D.Lgs. 196/2003)

Con riferimento all'obbligo stabilito nell'art. 13 del D.Lgs. 196, che può essere ritenuto di portata generalizzata, anche alla luce delle poche ipotesi di esenzione dello stesso previste dal comma 5 della norma, l'organismo sanitario dovrà certamente attivarsi per porre in essere il relativo adempimento per tutte e tre le aree di trattamento indicate: pazienti/clienti, dipendenti e fornitori.

Per quello che riguarda la prima area, si devono segnalare alcune peculiarità che incidono sulle modalità pratiche di rispetto della legge, sia nel senso di una loro complicazione, sia in quello di una semplificazione. Per il primo aspetto si deve infatti registrare, a fronte della complessa articolazione di attività di trattamento di dati personali dell'organismo sanitario, la necessità di proporre diverse formulazioni di informativa a seconda del contesto: così, ad esempio, anche in questo caso se si è installato un sistema di videosorveglianza, un primo adempimento dell'obbligo deve essere fatto mediante l'affissione di un cartello contenente tale informativa anche in forma sintetica in prossimità dell'apparato di ripresa; ancora, se l'organismo sanitario ha organizzato un accesso controllato alle sue strutture (si pensi in particolare a quelli pubblici, tipo il Ministero della Salute, che hanno maggiori problemi di sicurezza), che porta chi entra nella stessa a venire registrato e catalogato, il foglio che viene compilato dal visitatore con i propri dati dovrà riportare idonea informativa; anche chi usufruisce dei laboratori di analisi di una clinica dovrà essere informato delle modalità di trattamento dei suoi dati personali, magari nel momento in cui ritira la ricevuta dell'avvenuto pagamento del ticket, con l'informativa riportata in calce o nel retro dello stesso. Il compito del titolare, nell'ambito dell'attività di adeguamento della propria struttura al disposto del D.Lgs. 196, con riferimento a tale obbligo sarà quindi quello di individuare con precisione le varie modalità di trattamento di dati personali, e dunque di predisporre il sistema più opportuno per informare l'interessato degli elementi richiesti dalla legge.

Per quello che riguarda le facilitazioni che si possono applicare alla fattispecie in esame, il riferimento è alle norme del Codice che estendono le modalità semplificate di informativa (ma vedremo che quanto si dirà vale anche per la richiesta di consenso) anche agli organismi sanitari, pubblici e privati (artt. 77, 79, 80 e 81). In particolare sarà possibile procedere a una informativa cumulativa per i diversi trattamenti che possono svolgersi a richiesta del paziente, o comunque nel suo interesse, nell'ambito dell'attività di prevenzione, diagnosi, cura e riabilitazione; inoltre, l'adempimento dell'obbligo effettuato da uno dei soggetti che hanno prestato assistenza sanitaria all'interessato estende i suoi effetti anche a tutti gli altri (così, se un reparto dell'ospedale presta l'informativa al paziente, questa svolge il suo effetto anche nei confronti degli ulteriori trattamenti di altri reparti dello stesso ospedale, o comunque della prestazione sanitaria complessiva svolta nei suoi confronti). Nell'art. 80 sono poi riscontrabili le modalità con cui raggiungere tale risultato, norma che in particolare aggiunge la necessità di integrare l'informativa "con appositi e idonei cartelli e avvisi agevolmente visibili al pubblico, affissi e diffusi anche nell'ambito di pubblicazioni istituzionali e mediante reti di comunicazione elettronica, in particolare per quanto riguarda attività amministrative di rilevante interesse pubblico che non richiedono il consenso degli interessati": permettendo in questo modo di aumentare la possibilità concreta che i singoli interessati acquisiscano effettivamente la consapevolezza dei trattamenti posti in essere con i loro dati personali, specialmente nel caso non sia obbligatoria la prestazione del consenso.

L'obbligo di richiedere il consenso dell'interessato per il trattamento (artt. 23-26, 76 e 81-82 D.Lgs. 196/2003)

Il controllo posto in essere dall'interessato per i trattamenti dei dati che lo riguardano effettuati dagli organismi sanitari assume anche in questa ipotesi la forma del consenso. Nel caso specifico esso viene disciplinato da diverse disposizioni del Codice, e in maniera diversa, a seconda che: sia richiesto dal titolare organismo sanitario pubblico o privato; si riferisca a operazioni di trattamento di dati personali comuni, oppure sensibili; sia richiesto per attività di trattamento svolte o meno in ambito sanitario (inteso sia come finalità dello stesso che come ambiente in cui ordinariamente si svolgono le attività di tutela della salute). Queste variabili dovranno poi essere adattate, come al solito, alle ipotesi in cui le informazioni personali riguardino i propri pazienti/clienti, i propri dipendenti, i propri fornitori (ipotesi ultima nella quale non si utilizzeranno certo dati sensibili).

Così, nel caso di organismi sanitari *pubblici* (e quindi per gli enti pubblici che svolgono attività finalizzata alla tutela della salute), per capire se i trattamenti di dati personali comuni o sensibili svolti al di fuori dell'ambito sanitario debbano richiedere il consenso dell'interessato, si deve applicare la regola stabilita nell'art. 18 comma 4 del Codice: tale disposizione infatti espressamente prevede che "i soggetti pubblici non devono richiedere il consenso dell'interessato". Dunque in questa ipotesi di trattamento, sia nel caso dei dipendenti, che in quello dei fornitori, ed eventualmente per quello dei clienti/pazienti ma al di fuori dell'ambito sanitario, l'organismo sanitario pubblico non dovrà richiedere il consenso dell'interessato.

Se invece l'indicato soggetto utilizzi le informazioni personali per trattamenti in ambito sanitario, egli dovrà richiedere il consenso secondo quanto stabilito nell'art. 76, a meno che l'operazione sui dati personali dell'individuo sia posta in essere per *finalità di tutela della salute o dell'incolumità fisica di un terzo o della collettività* (così il suo comma 1 lettera *b*), seppure con le formule semplificate stabilite dall'art. 81 del Codice.

Per quanto riguarda poi gli organismi sanitari *privati*, nel caso di trattamenti di dati personali comuni (ad esempio la partita I.V.A. di un fornitore persona fisica, o l'anagrafica di un dipendente, o ancora l'indirizzo di un ex paziente utilizzato per operazioni di marketing), per svolgere legittimamente tale attività devono richiedere il consenso (informato) dell'interessato secondo quanto previsto dall'art. 23 del Codice, fatte salve le eccezioni stabilite nel suo successivo art. 24. A tale proposito, possono essere richiamate tre ipotesi di non applicazione della norma generale in materia di consenso, e in particolare: quella che si riferisce ai trattamenti necessari per adempiere a un obbligo previsto dalla legge, da un regolamento o dalla normativa comunitaria (art. 24, comma 1 lettera *a*); quella per i trattamenti necessari per eseguire obblighi derivanti da un contratto del quale è parte l'interessato o per adempiere, prima della conclusione dello stesso, a sue specifiche richieste (così il comma 1 lettera *b*); quella infine per i trattamenti necessari per la salvaguardia della vita o dell'incolumità fisica di un terzo (così il comma 1 lettere *e*). Tre ipotesi di esenzione in cui si possono ricondurre gran parte delle realtà di utilizzo delle informazioni personali di dipendenti e fornitori persone fisiche (come per l'uso della partita I.V.A. per la compilazione di una fattura, o dell'anagrafica di un dipendente per la compilazione della busta paga), ma anche di clienti/pazienti, in quest'ultimo caso se al di fuori dell'ambito sanitario.

Se poi il trattamento svolto dall'organismo sanitario privato riguardi dati sensibili, l'obbligo di richiedere il consenso (informato) del soggetto a cui le informazioni si riferiscono è previsto dall'art. 26 del Codice, in forme più rigide rispetto al caso precedente e con pochissime eccezioni. Per la fattispecie in esame fra queste si possono richiamare le ipotesi di esenzione dall'obbligo stabilite per i trattamenti necessari per la salvaguardia della vita o dell'incolumità fisica di un terzo (art. 26 comma 4 lettera *b*) e quelli necessari "per adempiere a specifici obblighi o compiti previsti dalla legge, da un regolamento o dalla normativa comunitaria per la gestione del rapporto di lavoro, anche in materia di igiene e sicurezza del lavoro e della popolazione e di previdenza e assistenza" (art. 26 comma 4 lettera *d*).

Se poi l'organismo privato utilizzi informazioni personali comuni e/o sensibili dei propri pazienti/clienti in ambito sanitario, e quindi in tale specifico contesto, dovrà certamente chiedere il consenso dell'interessato, questa volta sulla base della previsione dell'art. 76, e quindi dell'art. 81, ma con le forme semplificate ivi stabilite. In particolare, esse riguardano determinati aspetti e determinate ipotesi di applicazione dell'obbligo del consenso: con riferimento innanzitutto alla forma di espressione dello stesso che, rispetto alla disciplina generale, può essere orale anche nel caso di trattamenti di dati sensibili; inoltre, per le ipotesi di trattamenti da parte di più soggetti, ipotesi in cui viene prevista la possibilità di documentare l'avvenuto consenso attraverso l'annotazione dello stesso effettuato da parte dell'organismo sanitario che lo ha raccolto; nel caso infine dei trattamenti cumulativi disciplinati dal comma 4 dell'art. 78 (che riteneva sufficiente un'informativa unica valida anche per i medici che, ad esempio, sostituissero il professionista che l'aveva rilasciata al paziente, o per gli specialisti consultati, o per i farmacisti, o per i vari reparti dell'organismo sanitario, …), in cui si prevede la possibilità che il consenso ricevuto, che rende legittima tutta l'ulteriore attività di trattamento posta in essere anche dagli altri organismi, sia reso conoscibile agli stessi con adeguate modalità (nella specie, ad esempio, "anche attraverso menzione, annotazione o apposizione di un bollino o tagliando su una carta elettronica o sulla tessera sanitaria").

L'obbligo di consentire l'esercizio dei diritti da parte dell'interessato; l'organigramma dell'organismo sanitario (artt. 8-10 D.Lgs. 196/2003)

L'adempimento dell'obbligo di consentire all'interessato l'esercizio dei diritti stabiliti dal Codice nel caso dell'organismo sanitario si configura con modalità più complesse rispetto alle precedenti ipotesi del medico e del farmacista: questo chiaramente per la struttura stessa di tale soggetto, in genere organizzato in maniera articolata e di rilevanti dimensioni. Ma è proprio in situazioni di questo genere che con maggiore attenzione si deve adempiere l'obbligo previsto dai suoi artt. 8-10. Se infatti per esercitare i propri diritti nelle ipotesi di trattamento dei suoi dati da parte ad esempio di una farmacia all'interessato probabilmente sarà sufficiente recarsi direttamente nel negozio e chiedere del titolare, la stessa attività svolta nei confronti di un ospedale implicherà ben più rilevanti

livelli di complicazione. Vediamo quali sono i passi da compiere per evitare che queste difficoltà portino all'inadempimento della previsione normativa.

Per adempiere all'obbligo in esame innanzitutto occorre predisporre l'organigramma della struttura ai sensi del D.Lgs. 196/2003. Così per quanto riguarda il titolare del trattamento, come si è detto colui che decide "*in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza*", in genere la scelta sarà quella di considerare tale lo stesso organismo sanitario, in persona del suo legale rappresentante: eventualmente insieme ad altro titolare, nei casi di particolare complessità, ipotesi in cui si verifica la cosiddetta "contitolarità". Nonostante non vi sia più la necessità normativa di nominare il responsabile, cioè il soggetto preposto dal titolare al trattamento dei dati personali, in strutture particolarmente complesse è certamente consigliabile prevedere tale figura: e questo sia per le esigenze di implementazione e gestione delle misure di sicurezza richieste dalla legge nell'organismo sanitario (e quindi per la figura del responsabile della sicurezza), sia per avere chi risponde alle eventuali istanze di esercizio dei diritti riconosciuti dall'art. 7 del Codice all'interessato (e quindi la figura del responsabile per l'esercizio dei diritti, il cui riferimento andrà inserito nel testo dell'informativa dell'organismo sanitario), sia per decentrare l'effettiva gestione dei trattamenti a livello settoriale (si pensi, all'interno di un ospedale, all'utilità di nominare un responsabile del trattamento dei dati personali per il settore amministrativo, uno per la ricerca, ecc.) o a livello territoriale (nel caso l'organismo sanitario abbia più sedi dislocate in luoghi diversi, può essere opportuno nominare un responsabile per ognuna di tali sedi). Con riferimento infine ai soggetti che poi concretamente procedono al trattamento, cioè che entrano effettivamente in contatto con i dati personali di pazienti/clienti, dipendenti e fornitori, i cosiddetti incaricati, essi devono essere designati per iscritto dal titolare, che nella lettera di incarico "individua puntualmente l'ambito del trattamento consentito": questo sarà poi possibile anche attraverso modalità semplificate, ad esempio inserendo tale aspetto nel contratto di lavoro con i dipendenti, oppure differenziandolo per categorie di incaricati e realizzandolo attraverso l'emanazione di apposite circolari.

Una volta predisposto l'organigramma della struttura, il passo successivo per adempiere all'obbligo in esame sarà quello di preparare una procedura (disciplinata appunto dagli artt. 9 e 10 del Codice) affinché sia effettivamente possibile, per l'interessato, esercitare i suoi diritti. Dal punto di vista soggettivo, nel caso l'organismo sanitario sia di dimensione appena superiore alle due realtà esaminate in precedenza, dovrà essere nominato, come già indicato, il "responsabile per l'esercizio dei diritti", cioè la persona più adatta per rispondere, secondo le modalità che verranno scelte, alle eventuali istanze dei soggetti i cui dati personali sono trattati nella struttura. Dal punto di vista oggettivo, inoltre, occorrerà predisporre una modalità di proposizione delle istanze e di risposta alle stesse che possa conciliare le esigenze del titolare con la facilità della procedura per l'interessato, al fine di non frustrarne le richieste: così, utilizzando lettere raccomandate, fax, e-mail, ecc., e facendo in modo di riscontrare la richiesta, magari proprio da parte del responsabile per l'esercizio dei diritti, "senza ritardo".

L'obbligo di adottare idonee misure di sicurezza (art. 31-36 e Allegato B D.Lgs. 196/2003)

L'importanza dell'adempimento dell'obbligo di adottare idonee misure di sicurezza in un organismo sanitario è facilmente intuibile. Numerosi sono infatti i trattamenti di dati personali estremamente delicati che vengono posti in essere, con particolare riferimento alle informazioni che riguardano i pazienti/clienti, come sicuramente comune sarà l'utilizzo delle nuove tecnologie nei più diversi ambiti. Si riassumono ora schematicamente i principali adempimenti, tenendo presente che nel caso dell'organismo sanitario l'adeguamento pratico a questo aspetto della complessa disciplina in materia sarà necessariamente assegnato a soggetti specializzati e professionali (che, come richiesto dalla stessa normativa, dovranno poi rilasciare al titolare una descrizione scritta dell'intervento effettuato che ne attesti la conformità alle disposizioni del Codice).

Nel caso di trattamento di dati personali dei propri pazienti, dei propri dipendenti e dei propri fornitori persone fisiche effettuati senza l'ausilio di elaboratori elettronici di qualsiasi complessità, e quindi unicamente con strumenti cartacei (semmai oggi una simile ipotesi sia configurabile), oppure per gli aspetti più tradizionali di attività di trattamento per così dire "miste", l'organismo sanitario-titolare del trattamento dovrà: dare ai suoi incaricati specifiche istruzioni volte a controllare e custodire atti e documenti contenenti dati personali (tra l'altro in modo che ad essi non accedano persone prive di autorizzazione); organizzare accessi controllati a tali documenti e ai relativi archivi, i cui parametri devono essere aggiornati almeno una volta all'anno; organizzare un modo di identificazione e relativa registrazione delle persone eventualmente ammesse alla struttura durante l'orario di chiusura dello stesso.

Nel caso certamente più comune di trattamenti delle informazioni svolte con l'ausilio delle nuove tecnologie, o comunque per gli aspetti più innovativi di attività di trattamento per così dire "miste", le regole da rispettare sono: configurare il proprio sistema informatico contenente dati personali (il singolo computer e la rete di computer di piccole, nel singolo studio, medie, nel singolo reparto, o grandi dimensioni, in tutta la struttura) in modo tale che venga necessariamente identificato qualsiasi soggetto che vi acceda, al minimo attraverso

un identificativo di utente (*userid*) e una parola chiave (*password*), ma a seconda della dimensione dell'organismo sanitario, o dell'importanza e delicatezza dei dati trattati, più opportunamente attraverso sistemi di identificazione informatica anche più evoluti; *autorizzare* i soggetti identificati (il Codice usa l'espressione "*autenticati*") che svolgono le operazioni di trattamento ad accedere agli specifici dati personali, e/o ad effettuare alcune o tutte le operazioni in cui si articola il trattamento; attivare, sui vari computer e sulla rete, diverse metodologie per evitare attacchi alla sicurezza dei dati, in particolare installando programmi antivirus, aggiornando il sistema operativo e gli altri programmi, proteggendo l'elaboratore collegato a reti telematiche da accessi non autorizzati attraverso l'installazione del cosiddetto *firewall*; prevedere poi anche l'ipotesi che le metodologie indicate non riescano a proteggere il sistema informatico o, più banalmente, che il computer si rompa, e quindi per ovviare a tali eventi il responsabile o i responsabili devono regolarmente fare copie di riserva dei propri dati (e predisporre procedure di ripristino della disponibilità degli stessi e dei relativi sistemi)[f]; adottare specifici programmi che permettano, in linea di massima senza che l'utente se ne accorga, di cifrare i dati personali gestiti con il computer in modo da renderli illeggibili a chi non conosce la tecnica di crittografia utilizzata e le relative chiavi di accesso; infine organizzare diverse iniziative di formazione dei propri dipendenti, non solo limitate agli aspetti relativi alle misure di sicurezza.

Dai registri clinici alla recente disciplina in materia di Fascicolo Sanitario Elettronico

Dopo aver fornito un panorama sintetico dei principali aspetti del D.Lgs. 196/2003, e aver analizzato l'applicazione di tale normativa alle attività di trattamento delle informazioni personali svolta dagli organismi sanitari, nel paragrafo conclusivo del presente approfondimento dedicato agli aspetti legali ed etici dell'utilizzo dei dati forniremo alcune indicazioni relativamente a due specifiche realtà del mondo della sanità, quella dei registri clinici e quella del fascicolo sanitario elettronico.

Il trattamento dei dati nei registri clinici

La disciplina del trattamento dei dati personali coinvolti nella istituzione e gestione di un registro sanitario hanno sempre posto diverse problematiche in ambito giuridico.

I registri di patologia sono sistemi attivi di raccolta sistematica di informazioni anagrafiche e sanitarie allo scopo di registrare e tipizzare tutti i casi di una particolare malattia o di una condizione di salute rilevante in una popolazione definita.

Espresso riferimento a questa figura, in correlazione all'oggetto dell'indagine svolta nel presente capitolo, è rinvenibile in diverse fonti, in particolare nello stesso Codice per la protezione dei dati personali e in un articolo del cosiddetto "Decreto crescita 2.0" del governo Monti, il D.Lgs. 179/2012.

Con riferimento al D.Lgs. 30 giugno 2003 n. 196, è l'art 94 a citare i registri, nel Titolo dedicato ai trattamenti di dati in ambito sanitario:

Art. 94. Banche di dati, registri e schedari in ambito sanitario*1. Il trattamento di dati idonei a rivelare lo stato di salute contenuti in banche di dati, schedari, archivi o registri tenuti in ambito sanitario, è effettuato nel rispetto dell'articolo 3 anche presso banche di dati, schedari, archivi o registri già istituiti alla data di entrata in vigore del presente codice e in riferimento ad accessi di terzi previsti dalla disciplina vigente alla medesima data, in particolare presso:*

a) il registro nazionale dei casi di mesotelioma asbesto-correlati istituito presso l'Istituto superiore per la prevenzione e la sicurezza del lavoro (Ispesl), di cui all'articolo 1 del decreto del Presidente del Consiglio dei ministri 10 dicembre 2002, n. 308;
b) la banca di dati in materia di sorveglianza della malattia di Creutzfeldt-Jakob o delle varianti e sindromi a essa correlate, di cui al decreto del Ministro della salute in data 21 dicembre 2001, pubblicato nella Gazzetta Ufficiale n. 8 del 10 gennaio 2002;
c) il registro nazionale delle malattie rare di cui all'articolo 3 del decreto del Ministro della sanità in data 18 maggio 2001, n. 279;
d) i registri dei donatori di midollo osseo istituiti in applicazione della legge 6 marzo 2001n. 52;
e) gli schedari dei donatori di sangue di cui all'articolo 15 del decreto del Ministro della sanità in data 26 gennaio 2001, pubblicato nella Gazzetta Ufficiale n. 78 del 3 aprile 2001.

Da ultimo, la legge 17 dicembre 2012 n. 221 (che ha convertito, con modificazioni, il D.Lgs.. 179/2012 "Ulteriori misure urgenti per la crescita del Paese", anche detto "Decreto Crescita 2.0") all'art 12, comma 10 riporta che:

"***10****. I sistemi di sorveglianza e i registri di mortalità, di tumori e di altre patologie, di trattamenti costituiti da trapianti di cellule e tessuti e trattamenti a base di medicinali per terapie avanzate o prodotti di ingegneria tessutale e di impianti protesici sono istituiti ai fini di prevenzione, diagnosi, cura e riabilitazione, programmazione sanitaria, verifica della qualità delle cure, valutazione dell'assistenza sanitaria e di ricerca scientifica in ambito medico, biomedico ed epidemiologico allo scopo di garantire un*

[f] Questi adempimenti dovranno essere posti in essere sia a livello centrale, cioè dal sistema nel suo insieme, sia a livello di singoli sottoreti o singole stazioni operative, meglio se in maniera automatizzata.

sistema attivo di raccolta sistematica di dati anagrafici, sanitari ed epidemiologici per registrare e caratterizzare tutti i casi di rischio per la salute, di una particolare malattia o di una condizione di salute rilevante in una popolazione definita.

I Centri che gestiscono i registri, o le Regioni se non hanno demandato la gestione ai Centri, hanno la facoltà di nominare i responsabili del trattamento, individuando i soggetti, anche esterni alla struttura, da designare a tal fine.

Si ricorda che la figura del responsabile del trattamento non è, per legge, obbligatoria: è possibile che il titolare mantenga su di sé tutti i doveri e le responsabilità, in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza, senza delegarli ad altri (si veda l'art.4 del D.Lgs.196/2003). Tuttavia nelle organizzazioni complesse, negli enti pubblici, la nomina dei responsabili è in genere consigliata, così da gestire al meglio le attività e suddividere le responsabilità fra i dirigenti preposti.

La nomina deve essere fatta per iscritto in duplice copia e consegnata a ciascun responsabile indicando l'ambito della responsabilità: quest'ultimo potrà essere esteso al registro nel suo complesso o a singole sezioni dello stesso.

Il soggetto nominato responsabile del trattamento ha a sua volta il dovere di individuare e nominare gli incaricati al trattamento (non più facoltà, perché la nomina a incaricato è un obbligo di legge a tutti gli effetti), cioè i dipendenti o i collaboratori che a vario titolo operano sui dati personali contenuti nei registri: quindi devono essere incaricati coloro che raccolgono e registrano i dati, e ne controllano la correttezza, in sintesi i soggetti che compiono materialmente le operazioni di trattamento sulle informazioni personali dei registri. La nomina anche in questo caso deve essere fatta per iscritto e firmata per accettazione, da conservare agli atti e deve descrivere dettagliatamente i doveri previsti dalla legge per rispettare il diritto alla protezione dei dati personali anche riguardo alla sicurezza dei dati.

Risulta pertanto necessario definire criteri e principi generali cui improntare il trattamento, con particolare riguardo a: sicurezza dei dati personali che vengano acquisiti e conservati, possibilità di copie di dati soltanto per ragioni di sicurezza, divieto di pubblicazione dei dati e comunicazioni a terzi non autorizzati, raccolta dei soli dati pertinenti alle finalità proprie del registro, svolgimento delle sole operazioni necessarie a perseguire queste ultime, rispetto dei principi di liceità e correttezza, del dovere di aggiornamento dei dati.

L'incaricato del trattamento dovrà attenersi alle istruzioni ricevute con la lettera di nomina e alle regole del proprio ente riguardo alla sicurezza, e dovrà rispettare sempre i principi generali del Codice in materia di protezione dei dati personali. A tal fine si ritiene utile predisporre un adeguato piano di formazione per i soggetti responsabili e/o incaricati del trattamento, che oltre a fornire le basi di conoscenza sulla complessa normativa, evidenzi le specificità delle attività di trattamento connesse al registro.

Nei confronti poi dei pazienti i cui dati vengono inseriti nel registro occorrerà, in assenza di specifico provvedimento del Garante che sollevi il Titolare da tale adempimento, rendere l'informativa ex art. 13 del D.Lgs. 196/2003 e, ove necessario, raccogliere il relativo consenso.

Il trattamento dei dati nel fascicolo sanitario elettronico

Anche l'istituzione e gestione del Fascicolo Sanitario Elettronico (FSE) implica un trattamento di informazioni personali che pone rilevanti questioni dal punto di vista normativo.

I dati che compongono il Fascicolo (contenuti in referti, verbali di pronto soccorso, lettere di dimissioni, profilo sintetico, ovvero il documento informatico che riassume la storia del paziente e le sue condizioni attuali, il taccuino, ossia gli appunti inseriti dall'interessato, ecc.), sono sottoposti a rigide regole per essere trattati dai soggetti a ciò abilitati, secondo le linee guida impartite dall'Autorità garante per la protezione dei dati personali ("Linee guida in tema di Fascicolo Sanitario Elettronico e di Dossier sanitario" del 16 luglio 2009, in G.U. n. 178 del 3 agosto 2009).

Innanzitutto la normativa di riferimento si preoccupa di definire chi sia il Titolare del trattamento dei dati trattati, identificando tale figura nel soggetto che produce il dato: ovvero di ciascun dato personale è titolare, ai sensi dell'articolo 4, lett *f*) del D.Lgs. 196/2003, chi ha provveduto al suo inserimento all'interno del FSE, anche se i dati successivamente vengono condivisi dai soggetti autorizzati attraverso un elenco degli eventi occorsi.

Il Titolare così individuato deve valutare, in funzione delle finalità perseguite dal FSE, quali dati inserire perché questi non risultino eccedenti e non pertinenti.

Nel caso sia l'azienda sanitaria oppure ospedaliera, come organismo sanitario nel suo complesso, a risultare titolare (perché presso di essa sono state redatte le informazioni), questa ha il compito di nominare i responsabili del trattamento e gli incaricati, ovvero di individuare i soggetti che materialmente possono operare sui dati personali contenuti nel FSE: impartendo loro specifiche istruzioni, delimitando l'ambito di trattamento consentito a ciascuno, in funzione delle finalità perseguite nello svolgimento delle proprie mansioni, e formandoli in materia di protezione dei dati personali.

Il livello di accesso alle informazioni (e l'eventuale possibilità di integrazione o modifica dei dati personali) deve essere, dunque, attribuito dall'organismo sanitario in funzione delle attività che il singolo deve svolgere, prevedendo abilitazioni differenti in base alle mansioni svolte: andando così a

creare una struttura modulare delle informazioni per consentire di selezionare quelle cui ogni incaricato possa accedere in base alla sua categoria di appartenenza (ad esempio, il farmacista potrà accedere solo alle informazioni necessarie all'erogazione del farmaco, il personale amministrativo solo ai dati necessari alla fatturazione della prestazione o alla relativa prenotazione).

Restano, per legge, sempre esclusi dalla consultazione del FSE alcune categorie professionali, tra cui i periti assicurativi, le assicurazioni, i datori di lavoro, le associazioni scientifiche e i medici nell'esercizio dell'attività medico legale.

Il trattamento dei dati personali contenuti nel FSE può essere operato infatti solo per finalità di cura e riabilitazione dell'interessato, per garantire a quest'ultimo il miglior processo di cure, considerate le informazioni sanitarie che lo riguardano e che devono risultare il più complete possibile, andando a realizzare una cronistoria degli eventi con rilevanza clinica in cui sia incorso il paziente; restano escluse dalla possibilità di utilizzo le finalità di programmazione, gestione, controllo e valutazione dell'assistenza sanitaria, indagini da condurre su dati in forma anonima. Le finalità di natura amministrativa (prenotazione e pagamento delle prestazioni) vanno invece realizzate utilizzando i dati personali strettamente funzionali a tali scopi, conservati separatamente da quelli di natura clinica che non risulteranno accessibili ai soggetti preposti alle funzioni amministrative.

La costituzione del Fascicolo per il paziente è facoltativa e mai obbligatoria e, in osservanza del principio di autodeterminazione, implica il consenso dell'interessato, la cui negazione non deve influire sulla possibilità di accedere alla prestazione sanitaria.

Il consenso, anche se prestato contestualmente a quello medico, deve essere autonomo e specifico: nell'informativa resa ai sensi dell'articolo 13 del D.Lgs. 196/2003, deve essere spiegata in modo chiaro e esauriente l'utilità della costituzione del FSE, ovvero la circostanza che una conoscenza approfondita dei dati clinici che riguardano il paziente, anche relativi a tempi passati, può favorire la scelta di una cura più efficace da parte del medico.

Il modulo della raccolta del consenso prevederà dunque più firme per esprimere il consenso da parte dell'interessato: una generica alla costituzione del Fascicolo, e altre specifiche per l'alimentazione dello stesso e/o per legittimare la sua consultazione da parte di soggetti raggruppati per categorie (farmacisti, medici di medicina generale, pediatri di libera scelta, medici ospedalieri).

Nel caso in cui l'interessato, in un secondo momento, provveda a revocare il consenso prestato, il Fascicolo rimarrà consultabile a chi abbia immesso le informazioni, ma non potrà più essere integrato e implementato.

L'interessato potrebbe non revocare il consenso, ma decidere che uno o più eventi clinici, seppure immessi, non siano consultabili da parte di determinati soggetti, ovvero non a questi accessibili. In tale caso si parla di "oscuramento del dato", e il soggetto non autorizzato a consultare l'informazione non deve avere neanche percezione dell'avvenuto oscuramento (eventualità indicata come "oscuramento dell'oscuramento"): il Titolare può prevedere che la facoltà di rendere non accessibile un dato sia esercitabile dal paziente solo in presenza di un medico che possa illustrargli i rischi dell'oscuramento, ovvero del non permettere la consultazione dell'evento clinico.

In ultimo, la normativa prevede che siano garantiti all'interessato i diritti riconosciuti dall'art. 7 del D.Lgs. 196/2003, riportati nella parte del presente capitolo dedicata alla descrizione degli aspetti più rilevanti della normativa, mentre le Regioni sono indicate quali soggetti che dovranno farsi destinatari delle richieste di esercizio di tali diritti per agevolare il cittadino nel relativo procedimento.

La disciplina appena esposta, sia con riferimento ai registri clinici sia rispetto al FSE, mostra come, anche in presenza di attività di trattamento di dati personali in realtà di particolare delicatezza e nello stesso tempo di grande rilevanza, sia possibile conciliare necessità di accedere alle informazioni con quelle di tutela dei soggetti cui tali informazioni si riferiscono. Possibilità che però è strettamente legata alla consapevolezza delle problematiche coinvolte, consapevolezza che a sua volta nasce dalla conoscenza della complessa normativa, rispetto alla quale spero che il presente scritto possa rappresentare una prima base e un elemento di stimolo per svolgere ulteriori approfondimenti.

Indirizzo per la corrispondenza:
Prof. Gianluigi Ciacci
Cattedra di Informatica Giuridica
Università Luiss Guido Carli
Viale Romania, 32
00197 Roma
E-mail: studiociacciprivacy@jei.it