La tutela dei dati personali e il diritto alla privacy nella legislazione nazionale.

di Wanda D'Avanzo

Sommario: 1) Introduzione. – 2) La nozione di dato personale. – 3) Il titolare del trattamento. – 4) I diritti dell'interessato. – 5) L'informativa e il consenso al trattamento dei dati personali. – 6) Obblighi di sicurezza. – 7) Il trattamento dei dati in ambito pubblico. – 8) Il trattamento dei dati in ambito giudiziario. – 9) Il sistema sanzionatorio del codice della privacy. – 10) Conclusioni.

1) *Introduzione*

L'art. 1 del Codice in materia di protezione dei dati personali, D.Lgs. del 30 giugno 2003, n. 196 (G.U. n. 174 del 29 luglio 2003), così dispone: "Chiunque ha diritto alla protezione dei dati personali che lo riguardano". Finalità del codice, prosegue l'art. 2, comma 1, è quella di garantire 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".
Il diritto alla protezione dei dati personali viene riconosciuto qui come un autonomo diritto positivo, rispetto al passato in cui era considerato solo come un'accezione più evoluta del concetto di diritto alla riservatezza. L'art. 2, comma 2, introduce, poi, il principio della semplificazione nell'elevata tutela, con cui il legislatore ha voluto bilanciare, da un lato, la garanzia di un elevato livello di tutela di diritti di rango costituzionale e, dall'altro, l'esigenza di assicurare "procedure snelle ed efficaci per l'esercizio dei diritti degli interessati per l'adempimento da parte dei titolari". (1)
Il diritto alla protezione dei dati personali è, dunque, riconosciuto dal D.Lgs. 196/2003 come un diritto fondamentale della persona accanto al diritto alla riservatezza ed all'identità personale, che si inscrive nell'elenco dei diritti della personalità, che già la giurisprudenza ed ulteriori leggi speciali avevano ampliato ben oltre le ipotesi contenute nell'art. 5 cod. civ. (2)
Secondo la giurisprudenza, il diritto alla riservatezza, in particolare, consiste nella tutela di quelle situazioni e vicende strettamente personali e familiari che, anche se verificatesi fuori del domicilio domestico, non hanno per i terzi un interesse socialmente apprezzabile, contro le ingerenze che, sia pure compiute con mezzi leciti, per scopi non esclusivamente speculativi e senza offesa per l'onore, la reputazione o il decoro, non siano tuttavia giustificate da interessi pubblici preminenti. Esso non può essere, inoltre, negato ad alcune categorie di persone, solo in considerazione della loro notorietà, salvo che un reale interesse sociale all'informazione od altre esigenze pubbliche lo esigano. Tale diritto non solo trova implicito fondamento nel sistema, ma trova una serie di espliciti riferimenti alle norme costituzionali e ordinarie e in molteplici deliberazioni di carattere internazionale. (3)
L'interesse della persona, fisica o giuridica, a preservare la propria identità personale, nel senso di immagine sociale, cioè di insieme di valori rilevanti nella rappresentazione che di essa viene data nella vita di relazione, nonché correlativamente, ad insorgere contro comportamenti altrui che menomino tale immagine, pur senza offendere l'onore o la reputazione, ovvero ledere il nome o l'immagine fisica, deve ritenersi qualificabile come posizione di diritto soggettivo, alla stregua dei principi fissati dall'art. 2 della Costituzione in tema di difesa della personalità nella complessità ed unitarietà di tutte le sue componenti, ed inoltre tutelabile in applicazione analogica della disciplina dettata dall'art. 7 cod. civ. con riguardo al diritto al nome, con la conseguente esperibilità, contro i suddetti comportamenti, di azione inibitoria e di risarcimento del danno, nonché della pubblicazione della sentenza che accolga la domanda. (4)
La vera essenza del diritto alla privacy sta, quindi, nel suo carattere di diritto fondamentale ed inviolabile dell'uomo, che consente l'esercizio di

altri diritti che sono legati alla possibilità di evitare inopportuni giudizi altrui, con riferimento a scelte di per sé insindacabili. La lesione della riservatezza si riverbera anche sulla sfera psichica del soggetto che vede violato un suo diritto di rango costituzionale, che dovrebbe cedere solo dinanzi a casi concreti di particolare gravità ed in seguito all'affermazione di un'operazione di bilanciamento fra interessi in conflitto. (5)
Oggi, la notevole evoluzione del progresso tecnologico consente l'elaborazione e la conservazio¬ne di quantità di dati prima impensabili. Ciò che rileva nell'attuale società dell'informazione è il dato, in tutte le sue molteplici sfaccettature. Per questo motivo le legislazioni moderne stanno cercando di stabilire un equilibrio tra il libero flusso delle informazioni e dei dati e la tutela della riservatezza e della vita privata di ogni individuo.
Si è, dunque, oltre l'originaria definizione di privacy come semplice "diritto ad essere lasciato solo", così come originariamente teorizzata da Warren e Brandeis alla fine dell'Ottocento. (6)
Nata come diritto dell'individuo borghese ad escludere gli altri da ogni forma di invasione della propria sfera privata, riproducendo lo schema tipico del diritto di proprietà, la tutela della privacy, anche a seguito della rivoluzione informatica e telematica, finisce con il simboleggiare l'insieme delle libertà implicate dal trattamento dei dati personali, il diritto al mantenimento del controllo sui propri dati. (7)

2) *La nozione di dato personale*

L'Italia si è dotata di una normativa organica sul trattamento dei dati personali, inizialmente, con la L. del 21 febbraio 1989, n. 98 (G.U. n. 66 del 20 marzo 1989), di ratifica della Convenzione del Consiglio d'Europa n. 108, sulla protezione delle persone rispetto al trattamento automatizzato dei dati di carattere personale, adottata a Strasburgo il 28 gennaio 1981; e successivamente, con la L. del 31 dicembre 1996, n. 675 (G.U. n. 5 del 8 gennaio 1997, suppl. ord. n. 3), che ha dato attuazione alla Direttiva 1995/46/CE del Parlamento europeo e del Consiglio del 24 ottobre 1995 (G.U.CE n. L 281 del 23 novembre 1995). (8)
L'entrata in vigore del codice in materia di protezione di dati personali, nel 2003, rappresenta l'ultimo fondamentale intervento normativo, che ha raccolto tutte le disposizioni vigenti nel nostro ordinamento relative alla tutela dei dati personali, provvedendo contestualmente all'abrogazione dei provvedimenti nei quali erano originariamente contenute. (9)
Il codice è stato aggiornato, più di recente, con il D.Lgs. del 30 maggio 2008, n. 109 (G.U. n. 141 del 18 giugno 2008), che ha dato attuazione della Direttiva 2006/24/CE (G.U.CE n. L 105 del 13 aprile 2006), riguardante la conservazione dei dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione. Ancora, è intervenuta a modificare le disposizioni del codice, la L. del 27 febbraio 2009, n. 14 (G.U. n. 49 del 28 febbraio 2009, suppl. ord. n. 28), di conversione del Decreto Legge del 30 dicembre 2008, n. 207, recante proroga dei termini previsti da disposizioni legislative e disposizioni finanziarie urgenti.
Il codice è suddiviso in tre parti. La prima detta i principi generali in materia di protezione dei dati personali ed è applicabile alla generalità dei soggetti; la seconda contiene le disposizioni che regolano il trattamento dei dati personali(10) in relazione a specifici settori di appartenenza; mentre, la terza parte raccoglie tutte le disposizioni relative alla tutela dell'interessato ed alle sanzioni previste in caso di violazione della normativa in materia.
Nell'ambito dei principi generali che regolano la materia, l'art. 3 introduce il principio di necessità nel trattamento dei dati personali e prescrive che i sistemi informativi e i programmi informatici siano configurati in modo tale da ridurre al minimo l'utilizzazione di dati personali e di dati identificativi, fino ad escluderne il trattamento quando le finalità perseguite nei singoli casi possano essere realizzate mediante dati anonimi o opportune modalità che permettano di identificare l'interessato solo in caso di necessità.
Il dato è anonimo quando, già in origine o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile (art. 4, comma 1, lett. n).
Secondo l'art. 4 del codice della privacy, per dato personale si intende

qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, iden¬tificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, compreso un numero di identificazione personale.
Nell'ambito della categoria dei dati personali il legislatore ha, poi, distinto i dati sensibili che 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 o organizzazioni a carat¬tere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale; e i dati giudiziari definiti come quei dati personali idonei a rivelare provvedimenti in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato.
Diversamente, i cosiddetti dati semisensibili, cui si riferisce l'articolo 17 del codice, sono dati diversi da quelli sensibili e giudiziari il cui trattamento presenta rischi specifici per i diritti e le libertà fondamentali, nonché per la dignità dell'interessato, in relazione alla natura dei dati o alle modalità del trattamento o agli effetti che può determinare.

3) *Il titolare del trattamento*

Oggetto del codice è la disciplina del trattamento dei dati personali, anche detenuti all'estero, effettuato da chiunque sia stabilito nel territorio dello Stato, o in un luogo comunque soggetto alla sovranità dello Stato. Esso trova applicazione anche nel caso di trattamento di dati personali effettuato da chiunque sia stabilito nel territorio di un Paese non appartenente all'Unione europea che impieghi, per il trattamento stesso, strumenti situati nel territorio dello Stato anche diversi da quelli elettronici, salvo che essi siano utilizzati solo ai fini di transito nel territorio dell'Unione europea. Il codice si applica, infine, al trattamento di dati personali effettuato da persone fisiche per fini esclusivamente personali, ma solo se i dati sono destinati ad una comunicazione sistematica o alla diffusione (art. 5, D.Lgs. 196/2003).
Titolare del trattamento è la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza (art. 4, comma 1, lett. f). Quando il trattamento è effettuato da una persona giuridica, da una pubblica amministrazione o da un qualsiasi altro ente, associazione od organismo, titolare del trattamento è l'entità nel suo complesso o l'unità od organismo periferico che esercita un potere decisionale del tutto autonomo sulle finalità e sulle modalità del trattamento, ivi compreso il profilo della sicurezza (art. 28, comma 1).
Il titolare, a sua volta, ha la facoltà di nominare un responsabile, definito dall'art. 4, comma 1, lett. g) del codice come la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali. Se designato, il responsabile è individuato tra soggetti che, per esperienza, capacità ed affidabilità, forniscano idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza. Ove necessario per esigenze organizzative, possono essere designati, in qualità di responsabili, più soggetti. I compiti affidati al responsabile sono analiticamente specificati per iscritto dal titolare. Il responsabile effettua il trattamento attenendosi alle istruzioni impartite dal titolare il quale, anche tramite verifiche periodiche, vigila sulla puntuale osservanza delle disposizioni di legge e delle proprie istruzioni (art. 29).
Gli incaricati, invece, sono quelle persone fisiche autorizzate a compiere operazioni di trattamento (art. 4, comma 1, lett. h), che operano sotto la diretta autorità del titolare o del responsabile. La designazione è effettuata per iscritto e individua, puntualmente, l'ambito del trattamento consentito (art. 30).
Nel caso in cui i dati che si intende trattare riguardino dati genetici, biometrici o dati che indicano la posizione geografica di persone od oggetti mediante una rete di comunicazione elettronica; dati sensibili, trattati a fini di procreazione assistita, prestazione di servizi sanitari per via telematica relativi a banche di dati o alla fornitura di beni, rilevazione di malattie mentali, infettive e diffusive, trapianto di organi e tessuti; dati

trattati con l'ausilio di strumenti elettronici volti a definire il profilo o la personalità dell'interessato, o ad analizzare abitudini o scelte di consumo; dati sensibili registrati in banche di dati a fini di selezione del personale per conto terzi, nonché dati sensibili utilizzati per sondaggi di opinione, ricerche di mercato e altre ricerche campionarie; dati registrati in apposite banche di dati gestite con strumenti elettronici e relative al rischio sulla solvibilità economica, alla situazione patrimoniale, al corretto adempimento di obbligazioni, a comportamenti illeciti o fraudolenti, il titolare deve provvedere a notificare all'Autorità Garante per la protezione dei dati personali il trattamento cui intende procedere (art. 37, comma 1).
La notificazione deve essere trasmessa, attraverso il sito del Garante, prima dell'inizio del trattamento ed è effettuata con unico atto anche quando il trattamento comporta il trasferimento all'estero dei dati.

4) *I diritti dell'interessato*

L'interessato al trattamento, che è la persona fisica, la persona giuridica, l'ente o l'associazione cui si riferiscono i dati personali (art. 4, comma 1, lett. i), ha il diritto di ottenere la conferma dell'esistenza o meno di dati personali che lo riguardano, anche se non ancora registrati, e la loro comunicazione in forma intelligibile (art. 7, comma 1).
L'interessato ha diritto di ottenere l'indicazione dell'origine dei dati personali, delle finalità e modalità del trattamento, della logica applicata in caso di trattamento effettuato con l'ausilio di strumenti elettronici, degli estremi identificativi del titolare, dei responsabili e del rappresentante designato ai sensi dell'articolo 5, comma 2, dei soggetti o delle categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di rappresentante designato nel territorio dello Stato, di responsabili o incaricati (art. 7, comma 2).
L'interessato ha diritto di ottenere l'aggiornamento, la rettificazione ovvero, quando vi ha interesse, l'integrazione dei dati, la cancellazione, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge, compresi quelli di cui non è necessaria la conservazione in relazione agli scopi per i quali i dati sono stati raccolti o successivamente trattati, l'attestazione che le operazioni di aggiornamento, rettificazione, integrazione, cancellazione e trasformazione in forma anonima sono state portate a conoscenza di coloro ai quali i dati sono stati comunicati o diffusi, eccettuato il caso in cui tale adempimento si rivela impossibile o comporta un impiego di mezzi manifestamente sproporzionato rispetto al diritto tutelato (art. 7, comma 3).
L'interessato ha diritto di opporsi, in tutto o in parte, per motivi legittimi, al trattamento dei dati personali che lo riguardano. Inoltre, può opporsi al trattamento di dati utilizzato a fini di invio di materiale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato o di comunicazione commerciale (art. 7, comma 4).
I diritti di cui all'articolo 7 sono esercitati con richiesta rivolta senza formalità(11) al titolare o al responsabile, anche per il tramite di un incaricato, alla quale è fornito idoneo riscontro senza ritardo (art. 8, comma 1).
Per garantire all'interessato l'effettivo esercizio dei suoi diritti, il titolare del trattamento è tenuto ad adottare idonee misure volte, in particolare, ad agevolare l'accesso ai dati personali, anche attraverso l'impiego di appositi programmi per elaboratore finalizzati ad un'accurata selezione dei dati che riguardano singoli interessati identificati o identificabili, nonché a semplificare le modalità e a ridurre i tempi per il riscontro al richiedente, anche nell'ambito di uffici o servizi preposti alle relazioni con il pubblico (art. 10, comma 1).
I dati sono estratti a cura del responsabile o degli incaricati e possono essere comunicati al richiedente anche oralmente, ovvero offerti in visione mediante strumenti elettronici, sempre che, in tali casi, ne sia agevole la comprensione, considerata anche la qualità e la quantità delle informazioni. Se vi è richiesta, si provvede alla trasposizione dei dati su supporto cartaceo o informatico, ovvero alla loro trasmissione per via telematica (art. 10, comma 2).
Salvo che la richiesta sia riferita ad un particolare trattamento o a specifici dati personali o categorie di dati personali, il riscontro all'interessato comprende tutti i dati personali che lo riguardano

comunque trattati dal titolare (art. 10, comma 3).
Quando l'estrazione dei dati risulta particolarmente difficoltosa il riscontro alla richiesta può avvenire anche attraverso l'esibizione o la consegna in copia di atti e documenti contenenti i dati personali richiesti (art. 10, comma 4).

5) *L'informativa e il consenso al trattamento dei dati personali*

I dati personali oggetto di trattamento devono essere trattati in modo lecito e secondo correttezza; raccolti e registrati per scopi determinati, espliciti e legittimi, ed utilizzati in altre operazioni del trattamento in termini compatibili con tali scopi; devono, poi, essere esatti e, se necessario, aggiornati; pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti o successivamente trattati; 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 (art. 11).
I dati personali trattati in violazione della disciplina in materia non possono essere utilizzati.
L'interessato deve essere previamente informato, oralmente o per iscritto, delle finalità e delle modalità del trattamento cui sono destinati i dati; della natura obbligatoria o facoltativa del conferimento dei dati; delle conseguenze di un eventuale rifiuto a rispondere; dei soggetti o delle categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di responsabili o incaricati, e dell'ambito di diffusione dei dati medesimi; dei diritti di cui all'articolo 7 del codice; degli estremi identificativi del titolare e, se designati, del rappresentante nel territorio dello Stato e del responsabile (art. 13, comma 1).
In caso, poi, di cessazione, per qualsiasi causa, di un trattamento, l'art. 16 stabilisce che i dati vengano distrutti, oppure ceduti ad altro titolare se destinati ad un trattamento in termini compatibili agli scopi per i quali i dati sono raccolti; conservati per fini esclusivamente personali e non destinati ad una comunicazione sistematica o alla diffusione; conservati o ceduti ad altro titolare, per scopi storici, statistici o scientifici, in conformità alla legge, ai regolamenti, alla normativa comunitaria e ai codici di deontologia e di buona condotta.
Il trattamento di dati personali da parte di privati o di enti pubblici economici è ammesso solo con il consenso espresso dell'interessato, che può riguardare l'intero trattamento ovvero una o più operazioni dello stesso. Il consenso è validamente prestato solo se è espresso liberamente ed in riferimento ad un trattamento chiaramente individuato, se è documentato per iscritto, e se è stata resa all'interessato l'informativa (art. 23). (12)
I dati sensibili possono essere oggetto di trattamento solo con il consenso scritto (art. 23, comma 4) dell'interessato e previa autorizzazione del Garante, nell'osservanza dei presupposti e dei limiti stabiliti dal codice, nonché dalla legge e dai regolamenti (art. 26, comma 1).
Il trattamento di dati giudiziari da parte di privati o di enti pubblici economici è consentito soltanto se autorizzato da espressa disposizione di legge o provvedimento del Garante che specifichino le rilevanti finalità di interesse pubblico del trattamento, i tipi di dati trattati e di operazioni eseguibili (art. 27).

6) *Obblighi di sicurezza*

Per quanto riguarda la sicurezza del trattamento dei dati il codice individua due tipologie di misure di sicurezza, le misure idonee e le misure minime.
L'art. 31 del codice, trattando delle misure idonee, dispone che i dati personali oggetto di trattamento devono essere custoditi e controllati, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.
Alle misure minime è, invece, dedicato il successivo art. 33.

Nel quadro dei più generali obblighi di sicurezza di cui all'articolo 31, o previsti da speciali disposizioni, i titolari del trattamento sono comunque tenuti ad adottare le misure minime, volte ad assicurare un livello minimo di protezione dei dati personali.
Invero le misure minime rappresentano, ex art. 4, comma 3, lett. a), il complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza che configurano il livello minimo di protezione richiesto in relazione ai rischi previsti nell'articolo 31.
Nel caso di trattamento dei dati personali effettuato con strumenti elettronici, devono essere adottate secondo il comma 1, dell'art. 34, alcune misure minime specificamente individuate, tra cui l'autenticazione informatica; l'adozione di procedure di gestione delle credenziali di autenticazione; l'utilizzazione di un sistema di autorizzazione; l'aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici; la protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di dati, ad accessi non consentiti e a determinati programmi informatici; l'adozione di procedure per la custodia di copie di sicurezza ed il ripristino della disponibilità dei dati e dei sistemi; la tenuta di un aggiornato documento programmatico sulla sicurezza; l'adozione di tecniche di cifratura o di codici identificativi per determinati trattamenti di dati idonei a rivelare lo stato di salute o la vita sessuale effettuati da organismi sanitari. (13)
Il trattamento di dati personali effettuato, invece, senza l'ausilio di strumenti elettronici è consentito solo se sono adottate misure minime di aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unità organizzative; di previsione di procedure per un'idonea custodia di atti e documenti affidati agli incaricati per lo svolgimento dei relativi compiti; di previsione di procedure per la conservazione di determinati atti in archivi ad accesso selezionato e disciplina delle modalità di accesso finalizzata all'identificazione degli incaricati (art. 35).
La mancata adozione, da parte del titolare, delle misure minime di sicurezza al trattamento dei dati personali, previste dall'art. 33, comporta l'applicazione di sanzioni di carattere penale, secondo la previsione dell'art. 169 del codice.

7) *Il trattamento dei dati in ambito pubblico*

Qualunque trattamento di dati personali da parte di soggetti pubblici è consentito soltanto per lo svolgimento delle funzioni istituzionali. Nel trattare i dati il soggetto pubblico è tenuto ad osservare i presupposti e i limiti stabiliti dal codice, anche in relazione alla diversa natura dei dati, nonché dalla legge e dai regolamenti.
I soggetti pubblici non devono richiedere il consenso dell'interessato al trattamento dei dati personali che lo riguardano (art. 18).
Il trattamento dei dati sensibili, invece, da parte di soggetti pubblici è consentito solo se autorizzato da espressa disposizione di legge nella quale sono specificati i tipi di dati che possono essere trattati e di operazioni eseguibili e le finalità di rilevante interesse pubblico perseguite. Il trattamento di dati giudiziari da parte di soggetti pubblici può essere autorizzato, oltre che da espressa disposizione di legge, anche da un provvedimento del Garante che specifichi le finalità di rilevante interesse pubblico del trattamento, i tipi di dati trattati e di operazioni eseguibili (artt. 20 e 21).
Il trattamento dei dati sensibili e giudiziari da parte di soggetti pubblici deve, comunque, essere effettuato secondo modalità volte a prevenire violazioni dei diritti, delle libertà fondamentali e della dignità dell'interessato (art. 22, comma 1). E, in ogni caso, i soggetti pubblici possono trattare solo i dati sensibili e giudiziari indispensabili per svolgere attività istituzionali che non possono essere adempiute, caso per caso, mediante il trattamento di dati anonimi o di dati personali di natura diversa (art. 22, comma 3).
I dati sensibili e giudiziari contenuti in elenchi, registri o banche di dati, tenuti con l'ausilio di strumenti elettronici, sono trattati con tecniche di cifratura o mediante l'utilizzazione di codici identificativi o di altre soluzioni che, considerato il numero e la natura dei dati trattati, li rendono temporaneamente inintelligibili anche a chi è autorizzato ad accedervi e permettono di identificare gli interessati solo in caso di necessità(art. 22, comma 6).

I dati idonei a rivelare lo stato di salute e la vita sessuale sono conservati separatamente da altri dati personali trattati per finalità che non richiedono il loro utilizzo (art. 22, comma 7).
I dati idonei a rivelare lo stato di salute non possono essere diffusi (art. 22, comma 8). (14)
I presupposti, le modalità e i limiti per l'esercizio del diritto di accesso a documenti amministrativi contenenti dati personali, e la relativa tutela giurisdizionale, restano disciplinati dalla legge 7 agosto 1990, n. 241, e successive modificazioni e dalle altre disposizioni di legge in materia, nonché dai relativi regolamenti di attuazione, anche per ciò che concerne i tipi di dati sensibili e giudiziari e le operazioni di trattamento eseguibili in esecuzione di una richiesta di accesso. Le attività finalizzate all'applicazione di tale disciplina si considerano di rilevante interesse pubblico (art. 59).
Quando, però, il trattamento concerne dati idonei a rivelare lo stato di salute o la vita sessuale, il trattamento è consentito se la situazione giuridicamente rilevante che si intende tutelare con la richiesta di accesso ai documenti amministrativi è di rango almeno pari ai diritti dell'interessato, ovvero consiste in un diritto della personalità o in un altro diritto o libertà fondamentale e inviolabile (art. 60).
Gli artt. 59 e 60 del codice della privacy si occupano entrambi del medesimo oggetto, poiché il trattamento di cui all'art. 60 è sempre quello finalizzato a garantire la richiesta di accesso, di cui al 59. L'art. 60, invero, si pone in rapporto di integrazione con l'art. 59, fissando una regola speciale, più restrittiva, per particolari categorie di dati, nell'ambito di una regola generale valevole per tutti i dati. L'obiettivo è quello di fornire una regola generale in materia di rapporto tra trasparenza dell'azione amministrativa e protezione dei dati personali. (15)
Occorre, in proposito, considerare l'ipotesi in cui il richiedente cerchi di accedere a documenti in cui sono contenuti dati relativi ad un altro soggetto, caso che pone questioni relative al bilanciamento tra interessi e obiettivi normativi contrapposti. E il bilanciamento individuato dal codice sembra nel senso di riconoscere la prevalenza del diritto di accesso come regola generale, di fronte alle limitazioni funzionali alla protezione dei dati personali intese come eccezioni, rinviando alla disciplina della L. 241/90. (16)
Nel momento, poi, in cui il trattamento concerne i dati idonei a rivelare lo stato di salute o la vita sessuale, l'art. 60 pone due confronti. Nel primo si contrappongono elementi non omogenei, diritti da un lato, e situazioni giuridicamente rilevanti dall'altra del soggetto che richiede l'accesso. In questo senso, il confronto non può farsi che caso per caso, dovendo la pubblica amministrazione verificare la prevalenza tra le aspettative del richiedente l'accesso a conoscere i dati e le aspettative dell'interessato a non consentire tale conoscenza. Un secondo confronto è tra elementi omogenei, vale a dire tra diritti dell'interessato e diritti della personalità, o altri diritti o libertà fondamentali e inviolabili del soggetto richiedente l'accesso. Anche qui, il diritto dell'interessato alla protezione dei propri dati, non potrà che essere considerato in riferimento alla fattispecie. L'art. 60, nella sua generica formulazione, dunque, si limita semplicemente ad affermare implicitamente che quando il diritto di accesso va a scontrarsi con la protezione dei dati personali particolarmente sensibili, è comunque necessaria una valutazione del contenuto particolare delle rispettive situazioni giuridiche soggettive. (17)

8) *Il trattamento dei dati in ambito giudiziario*

Per quanto riguarda, invece, il trattamento dei dati in ambito giudiziario, l'art. 46 stabilisce che gli uffici giudiziari di ogni ordine e grado, il Consiglio superiore della magistratura, gli altri organi di autogoverno e il Ministero della giustizia sono titolari dei trattamenti di dati personali relativi alle rispettive attribuzioni conferite per legge o regolamento.
Nei casi in cui l'autorità giudiziaria di ogni ordine e grado può acquisire in conformità alle vigenti disposizioni processuali dati, informazioni, atti e documenti da soggetti pubblici, l'acquisizione può essere effettuata anche per via telematica. A tale fine gli uffici giudiziari possono avvalersi delle convenzioni-tipo stipulate dal Ministero della giustizia con soggetti pubblici, volte ad agevolare la consultazione da parte dei medesimi uffici, mediante reti di comunicazione elettronica, di pubblici registri,

elenchi, schedari e banche di dati (art. 48).
In materia di banche dati in ambito giuridiziario, particolare attenzione va prestata alla Rete Unitaria della Giustizia (RUG) che comprende il Centro elettronico di Documentazione (CED) della Corte di Cassazione; il sistema informativo del dipartimento dell'amministrazione penitenziaria; il sistema informativo della direzione nazionale antimafia; il sistema informativo del casellario giudiziale, dell'anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti.
Tra questi, in particolare, il sistema informativo della Direzione nazionale antimafia, il sistema informativo del casellario giudiziale, dell'anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, perseguono finalità di giustizia.
Ad essi si applicano le disposizioni di cui all'art. 47, ai sensi del quale si intendono effettuati per finalità di giustizia i trattamenti di dati personali direttamente correlati alla trattazione giudiziaria di affari e di controversie, o che, in materia di trattamento giuridico ed economico del personale di magistratura, hanno una diretta incidenza sulla funzione giurisdizionale, nonché le attività ispettive su uffici giudiziari.
Diverso è il caso del CED che offre la possibilità di consultare on line testi normativi e giurisprudenziali organizzati in banche dati. In tale caso manca il nesso funzionale che costituisce il fondamento dell'art. 47, per cui il regime derogatorio non potrà essere applicato, mentre si applicherà tutta la disciplina generale dettata dal codice della privacy. (18)
Secondo l'art. 51, fermo restando quanto previsto dalle disposizioni processuali concernenti la visione e il rilascio di estratti e di copie di atti e documenti, i dati identificativi delle questioni pendenti dinanzi all'autorità giudiziaria di ogni ordine e grado sono resi accessibili a chi vi abbia interesse anche mediante reti di comunicazione elettronica, ivi compreso il sito istituzionale della medesima autorità nella rete Internet.
Le sentenze e le altre decisioni dell'autorità giudiziaria di ogni ordine e grado depositate in cancelleria o segreteria sono rese accessibili anche attraverso il sistema informativo e il sito istituzionale della medesima autorità nella rete Internet.
Inoltre, ai sensi dell'art. 52, fermo restando quanto previsto dalle disposizioni concernenti la redazione e il contenuto di sentenze e di altri provvedimenti giurisdizionali dell'autorità giudiziaria di ogni ordine e grado, l'interessato può chiedere per motivi legittimi, con richiesta depositata nella cancelleria o segreteria dell'ufficio che procede prima che sia definito il relativo grado di giudizio, che sia apposta a cura della medesima cancelleria o segreteria, sull'originale della sentenza o del provvedimento, un'annotazione volta a precludere, in caso di riproduzione della sentenza o provvedimento in qualsiasi forma, per finalità di informazione giuridica su riviste giuridiche, supporti elettronici o mediante reti di comunicazione elettronica, l'indicazione delle generalità e di altri dati identificativi del medesimo interessato riportati sulla sentenza o provvedimento.
Sulla richiesta provvede in calce con decreto, senza ulteriori formalità, l'autorità che pronuncia la sentenza o adotta il provvedimento.

9) *Il sistema sanzionatorio del codice della privacy*

L'art. 15 del codice della privacy, che riguarda il caso di danni cagionati per effetto del trattamento, rinvia all'art. 2050 cod. civ., configurando un'ipotesi di responsabilità per l'esercizio di un'attività pericolosa. Di conseguenza, il titolare che cagioni un danno nello svolgimento del trattamento dei dati personali, è tenuto al risarcimento se non prova di aver adottato tutte le misure idonee ad evitare il danno. Si avrà, dunque, in sede processuale, un'inversione dell'onere della prova a suo carico.
Al fine di essere tutelato, l'interessato, può rivolgersi al Garante per la protezione dei dati personali o all'autorità giudiziaria ordinaria.
Il Garante opera in piena autonomia e con indipendenza di giudizio e di valutazione. È un organo collegiale costituito da quattro componenti, eletti due dalla Camera dei deputati e due dal Senato della Repubblica con voto limitato. I componenti eleggono nel loro ambito un presidente, il cui voto prevale in caso di parità. Eleggono anche un vicepresidente, che assume le funzioni del presidente in caso di sua assenza o di suo impedimento.
Il presidente e i componenti durano in carica quattro anni e non possono

essere confermati per più di una volta (art. 153).
L'interessato può adire il Garante mediante reclamo circostanziato, per rappresentare una violazione della disciplina rilevante in materia di trattamento di dati personali; mediante segnalazione, laddove non sia possibile presentare un reclamo circostanziato, al fine di sollecitare un controllo da parte del Garante sulla disciplina medesima; oppure, mediante ricorso, se intende far valere gli specifici diritti di cui all'articolo 7 (art. 141).
I diritti di cui all'articolo 7 possono essere fatti valere, alternativamente, o con ricorso al Garante o dinanzi all'autorità giudiziaria. Il ricorso al Garante non può essere proposto se, per il medesimo oggetto e tra le stesse parti, sia stata già adita l'autorità giudiziaria. Allo stesso modo, la presentazione del ricorso al Garante rende improponibile un'ulteriore domanda dinanzi all'autorità giudiziaria tra le stesse parti e per il medesimo oggetto (art. 145).
D'altro canto, competente a conoscere la richiesta di risarcimento del danno è solo l'autorità giudiziaria ordinaria.
Salvi i casi in cui il decorso del termine esporrebbe taluno a pregiudizio imminente ed irreparabile, il ricorso al Garante può essere proposto solo dopo che sia stata avanzata richiesta sul medesimo oggetto al titolare o al responsabile e il titolare o il responsabile non abbiano dato riscontro alla richiesta entro il termine di quindici giorni dal suo ricevimento, ovvero abbiano opposto alla richiesta un diniego anche parziale (art. 146).
In seguito al ricorso e se la particolarità del caso lo richiede, il Garante può disporre in via provvisoria il blocco, in tutto o in parte, di taluno dei dati, ovvero l'immediata sospensione di una o più operazioni del trattamento. Assunte le necessarie informazioni il Garante, se ritiene fondato il ricorso, ordina al titolare, con decisione motivata, la cessazione del comportamento illegittimo, indicando le misure necessarie a tutela dei diritti dell'interessato e assegnando un termine per la loro adozione. La mancata pronuncia sul ricorso, decorsi sessanta giorni dalla data di presentazione, equivale a rigetto (art. 150).

10) *Conclusioni*

Il Garante per la protezione dei dati personali ha, recentemente, affermato, alla Conferenza annuale di primavera delle Autorità europee per la protezione dei dati, la necessità che il diritto alla protezione dei dati personali trovi ulteriori sviluppi al fine di poter esercitare effettivamente una funzione di garanzia in un contesto sociale in continua evoluzione, sottolineando, con ciò, l'importanza di una necessaria ridefinizione del significato della protezione dei dati e del tipo di regole di cui si ha effettivamente bisogno. (19)
Il passaggio, infatti, da "un mondo in cui le informazioni personali erano sostanzialmente sotto il controllo esclusivo degli interessati a un mondo di informazioni condivise con una pluralità di soggetti" (20), impone una "costruzione sociale" (21) che renda la protezione dei dati personali più sentita come diritto fondamentale di ogni individuo, ma soprattutto più effettiva.
Ciò che occorre è innalzare in concreto il livello di protezione e di tutela dei cittadini, a fronte del dilagare delle tecnologie della sorveglianza e del controllo da un lato e delle comunicazioni elettroniche dall'altro, affinché sia possibile mantenere il controllo sulle proprie informazioni, cui corrisponda un dovere per gli altri di rispettare il diritto alla autodeterminazione informativa e la libertà alle scelte esistenziali.

NOTE:
(1) P. VICENZOTTO, La riservatezza e la sicurezza del sistema informativo negli uffici giudiziari, in G. RIEM, A. SIROTTI GAUDENZI, La giustizia telematica e la procedura informatizzata, Maggioli, Rimini, 2005, p. 121, spec. nota 8
(2) S. SICA, Tutela dei dati personali, in D. VALENTINO (a cura di), Manuale di diritto dell'informatica, ESI, Napoli, 2004, p. 195.
(3) Cass. 27 maggio 1975, n. 2129, in L. CIANFARDINI, F. IZZO, Codice civile annotato con la giurisprudenza, Simone, Napoli, 2006, p. 80.

(4) Cass. 22 giugno 1985, n. 3769, in ivi, p. 80.
(5) G. FIORILLO, Temi di informatica giuridica, Aracne editrice, Roma, 2004, p. 197.
(6) S.D. WARREN, L.D. BRANDEIS, The right to privacy, in Harward Law Riview, 1890, pp. 193.
(7) S. RODOTÀ, Tecnopolitica, Laterza, Roma-Bari, 2004, p. 166 e p. 168.
(8) La Direttiva 1995/46/CE ha introdotto una disciplina quadro del trattamento dei dati personali, incentrata, prevalentemente, sulla garanzia della tutela dei diritti e delle libertà fondamentali con riguardo al trattamento dei dati personali. Ha attribuito speciale risalto al diritto alla vita privata, richiamando con ciò una figura prevista a livello normativo dagli accordi internazionali sui diritti dell'uomo e in particolare, in ambito comunitario, dall'art. 8 della Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali, firmata a Roma il 4 novembre 1950. La direttiva del 1995 è stata soltanto il primo tassello del sistema del trattamento dei dati personali, implementato progressivamente dalle Direttive 1997/66/CE (G.U.CE n. L 024 del 30 gennaio1998), sulla riservatezza nelle telecomunicazioni, e 2002/58/CE (G.U.CE n. L 201 del 31 luglio 2002), sulla riservatezza delle comunicazioni elettroniche. Si veda, sul punto, S. SICA, cit., p. 194.
(9) G. SCORZA, Elementi di diritto dell'informatica, Simone, Napoli, 2004, p. 77.
(10) Rientra nella nozione di "trattamento" qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca di dati (art. 4, comma 1, lett. a).
(11) La richiesta rivolta al titolare o al responsabile può essere trasmessa mediante lettera raccomandata, telefax o posta elettronica. Il Garante può individuare altro idoneo sistema in riferimento a nuove soluzioni tecnologiche. Quando riguarda l'esercizio dei diritti di cui all'articolo 7, commi 1 e 2, la richiesta può essere formulata anche oralmente e, in tal caso, è annotata sinteticamente a cura dell'incaricato o del responsabile (art. 9, comma 1).
La richiesta di cui all'articolo 7, commi 1 e 2, è formulata liberamente e senza costrizioni e può essere rinnovata, salva l'esistenza di giustificati motivi, con intervallo non minore di novanta giorni (art. 9, comma 5).
(12) In alcuni casi, il consenso non è richiesto, ad esempio quando il trattamento è necessario per adempiere ad un obbligo previsto dalla legge, da un regolamento o dalla normativa comunitaria; o è necessario per eseguire obblighi derivanti da un contratto del quale è parte l'interessato o per adempiere, prima della conclusione del contratto, a specifiche richieste dell'interessato; o, ancora, quando riguarda dati provenienti da pubblici registri, elenchi, atti o documenti conoscibili da chiunque, fermi restando i limiti e le modalità che le leggi, i regolamenti o la normativa comunitaria stabiliscono per la conoscibilità e pubblicità dei dati.
(13) Il nuovo comma 1-bis dell'art. 34 sancisce che, per i soggetti che trattano soltanto dati personali non sensibili e che trattano come unici dati sensibili quelli costituiti dallo stato di salute o malattia dei propri dipendenti e collaboratori anche a progetto, senza indicazione della relativa diagnosi, ovvero dall'adesione ad organizzazioni sindacali o a carattere sindacale, la tenuta di un aggiornato documento programmatico sulla sicurezza è sostituita dall'obbligo per il titolare del trattamento di autocertificare che tali dati siano trattati solo in osservanza delle altre misure di sicurezza prescritte.
(14) Per quel che riguarda le problematiche connesse al trattamento dei dati sanitari, in relazione soprattutto all'innovazione tecnologica, il Garante per la protezione dei dati personali ha adottato, da ultimo, con Deliberazione n. 8 del 5 marzo 2009, le Linee guida in tema di fascicolo sanitario elettronico e di dossier sanitario (G.U. n. 71 del 26 marzo 2009).
"Nel quadro del processo di ammodernamento della sanità pubblica e privata – così il punto 1 delle Linee guida – sono in atto numerose iniziative volte a migliorare l'efficienza del servizio sanitario attraverso un ulteriore sviluppo delle reti e una più ampia gestione informatica e telematica di atti, documenti e procedure".
Al di là delle iniziative, già intraprese, volte ad archiviare, mediante

nuove tecniche, la svariata documentazione di cui gli organismi sanitari si avvalgono a diverso titolo nei processi di cura dei pazienti, di cui costituisce un esempio la cartella clinica digitale, la cui disciplina normativa rientra nelle previsioni del codice sulla protezione dei dati personali, le Linee guida esaminano "la condivisione informatica, da parte di distinti organismi o professionisti, di dati e documenti sanitari che vengono formati, integrati e aggiornati nel tempo da più soggetti, al fine di documentare in modo unitario e in termini il più possibile completi un'intera gamma di diversi eventi sanitari riguardanti un medesimo individuo e, in prospettiva, l'intera sua storia clinica" (punto 1).
Questi dati e documenti, da tempo oggetto di specifica attenzione, costituiscono il fascicolo sanitario elettronico e dossier sanitario.
La peculiarità della condivisione da parte di più soggetti delle informazioni sanitarie che documentano un insieme di eventi di rilevanza medica occorsi ad uno stesso individuo giustifica la formulazione di particolari considerazioni rispetto alla gestione cartacea di analoghi documenti e alla più generale tematica dell'informatizzazione sanitaria.
Nelle more di un possibile intervento normativo che regoli alcuni aspetti di fondo, il Garante ha ritenuto opportuno individuare un primo quadro di cautele, al fine di delineare per tempo specifiche garanzie e responsabilità, nonché alcuni diritti (punto 1).
(15) J. MONDUCCI, G. SARTOR (a cura di), Il codice in materia di protezione dei dati personali, Commentario sistematico al D.Lgs. 30 giugno 2003, n. 196, Cedam, Padova, 2004, pp. 238-239.
(16) Ivi, p. 240.
(17) Ivi, pp. 242-243.
(18) P. VICENZOTTO, cit., p. 131.
(19) Si veda, sul punto, il comunicato stampa, Pizzetti: migliorare e rendere più effettiva la protezione dei dati dei cittadini europei, sull'intervento dell'Autorità garante italiana alla Conferenza annuale di primavera delle Autorità per la protezione dei dati personali, tenutasi a Edimburgo il 23 aprile 2009, in www.garanteprivacy.it.
(20) S. RODOTÀ, cit., p. 151.
(21) Ivi, p. 163.