

PRIVACY. NORMATIVA E CASI*
Dott. Gianluigi Fioriglio

1.1 Origine del diritto alla privacy

I cambiamenti politici, sociali ed economici avvenuti nell'Ottocento hanno profondamente inciso sulla vita dell'uomo, facendo segnare il passaggio da un'economia rurale ad una industrializzata, con un conseguente accrescimento dei nuclei urbani, che hanno oltretutto facilitato la diffusione di strumenti di comunicazione di massa, in primo luogo i giornali.

Proprio alcuni «pettegolezzi» sulla propria moglie, apparsi sul *Saturday Evening Gazette*, si dice abbiano spinto Louis D. Brandeis a scrivere, insieme con Samuel D. Warren, quel breve saggio intitolato «*The Right to Privacy*», pubblicato nel 1890 sulle pagine dell'*Harvard Law Review*¹, che costituisce la prima compiuta formulazione di tale diritto quale *right to be let alone*.

Già in alcuni procedimenti giudiziari, come *Prince Albert v. Strange*², i giudici avevano affermato la violazione, nel caso di specie, del diritto alla *privacy*, dunque riconoscendolo e rendendo palese la sua importanza non solo dal punto di vista teorico, ma soprattutto pratico, come dimostra la ricostruzione di Warren e Brandeis, nelle cui parole emerge la funzione della riservatezza quale argine contro gli attacchi di un giornalismo finalizzato non ad informare ma piuttosto a scandalizzare.

I due autori riconoscono, dunque, l'esistenza di un generale diritto alla *privacy*, ben distinto dal diritto di proprietà e caratterizzato dalla sua esplicazione mediante entità sia materiali che immateriali. Questo diritto nasce in risposta ai cambiamenti politici, economici e sociali che costituiscono l'evoluzione della società e che recano con sé il bisogno di riconoscimento di nuove posizioni giuridiche soggettive, soddisfatte dall'opera creativa della *common law*, che si dimostra in alcuni casi pronta al recepimento delle istanze mosse in tal senso dalla società.

Quali punti di riferimento normativo, Warren e Brandeis muovono dall'applicazione analogica della disciplina delle leggi dello *slander* e del *libel* nonché della disciplina in tema di proprietà artistica e intellettuale. In concreto, la tutela del diritto alla *privacy* si può ottenere, secondo i due giuristi, tramite un'azione di responsabilità civile, ossia un "*tort for damages*" che si può sempre esercitare, oppure, in casi limitati, tramite una *injunction*. La responsabilità civile sussisterebbe in qualunque caso di "*injury to feelings*"³.

A detta degli autori, non ci si può esimere da responsabilità nel caso in cui si proceda alla pubblicazione di fatti o eventi caratterizzati da verità, poiché in tali ipotesi si verifica una lesione del *right to privacy*, il quale si trova su un differente piano logico, essendo ben distinto dal diritto all'identità personale. Parimenti, l'assenza di dolo e i motivi che hanno spinto a violare il diritto alla riservatezza non costituiscono una scusante se il fatto si è verificato, visto che una volta che questo è stato compiuto non si può più tornare alla situazione *quo ante*. A queste conclusioni spinge un esame dell'intera *law of torts*, ai sensi della quale ciascuno è responsabile degli atti che compie intenzionalmente, anche se questi sono commessi in perfetta buona fede.

Secondo Warren e Brandeis, sarebbe necessario apprestare anche una tutela penale nei confronti del diritto alla riservatezza, soprattutto nei casi di estrema gravità della lesione che si realizzano, ad esempio, quando una eventuale pubblicazione abbia ampia diffusione⁴. Ovviamente, in tali eventualità è necessario un espresso intervento legislativo, poiché non si può procedere alla creazione di nuovi reati in via interpretativa. La necessità di una così forte forma di tutela è dovuta

* Estratto, con modificazioni, da G. FIORIGLIO, *Temi di informatica giuridica*, Aracne, Roma, 2004.

¹ S. D. WARREN, L. D. BRANDEIS, *The right to privacy*, in «*Harvard Law Review*», 1890, 4, p. 193, ora in «*Landmarks of Law*», 1960, p. 261.

² *Prince Albert v. Strange*, 1 McN & G. 25 (1849).

³ S. D. WARREN, L. D. BRANDEIS, *op. cit.*, p. 275.

⁴ *Ibid.*

al fatto che, mediante una tutela individualizzata dei vari cittadini si riuscirebbe ad ottenere la tutela della società nel suo complesso⁵.

Le tesi dei due giuristi statunitensi stupiscono ancor oggi per la loro modernità, soprattutto se si considera l'enorme divario tecnologico che separa gli Stati Uniti del finire dell'Ottocento dall'odierna società dell'informazione⁶. Oggi, all'acceleramento dei progressi in campo tecnico-scientifico e ai conseguenti benefici, si accompagna una pluralità di situazioni potenzialmente lesive della *privacy* di ciascuno di noi: basti pensare agli strumenti di acquisizione visiva e sonora, alla capillare diffusione dei *mass media*, all'avvento dell'informatica, alla diffusione di Internet.

Tutti questi nuovi strumenti riescono a fornire una enorme libertà all'uomo, ma allo stesso tempo possono renderlo un «uomo di vetro», sottoposto ad infiniti sguardi indiscreti altrui. In merito, il problema principale sussiste quando si verifica lo scontro fra diritti configgenti, in primo luogo fra la riservatezza e il diritto di cronaca e di manifestazione del pensiero.

Queste circostanze fanno da più parti ritenere superato il concetto di *privacy* quale diritto dell'uomo ad essere lasciato solo, spostando l'attenzione sul diritto all'autodeterminazione informativa quale prerogativa di ciascun soggetto cui i dati personali fanno riferimento.

Ciò risponde a quelle tendenze evolutive ben individuate da Stefano Rodotà, che possono indicarsi nel «diritto di mantenere il controllo sulle proprie informazioni» e conseguentemente come il citato «diritto all'autodeterminazione informativa»; vi sono, inoltre, due ulteriori passaggi, «dalla *privacy* alla non discriminazione» e «dalla segretezza al controllo»⁷.

Si potrebbe comunque sostenere che la vecchia concezione di Warren e Brandeis, nell'affermare un diritto ad essere lasciato solo, implichi anche la possibilità di decidere dell'uso, o del non uso, di tutte quelle informazioni che riguardano solo ed esclusivamente quella certa persona.

Nella società odierna, tuttavia, in cui l'informazione assume sempre più rilevanza, anche e soprattutto da un punto di vista economico, sancire un diritto all'autodeterminazione informativa permette di centralizzare il ruolo dell'uomo quale unico soggetto legittimato a decidere dell'uso di tutti i suoi dati personali. La vera essenza del diritto alla *privacy* non sta comunque nella sua eventuale patrimonialità potenziale, ma piuttosto 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, come quelle legate a dati sensibili ed inerenti le scelte religiose e sessuali, le concezioni filosofiche, ecc. La lesione della riservatezza, inoltre, si riverbera anche sulla sfera psichica della 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'effettuazione di un'operazione di bilanciamento fra diritti configgenti.

2. Cenni sull'evoluzione del diritto alla *privacy* in Italia

Il diritto alla riservatezza ha inizialmente trovato riconoscimento e tutela nell'ordinamento italiano in via interpretativa, grazie all'apporto di dottrina e giurisprudenza, cui si sono contrapposti per lungo tempo pochi interventi legislativi, sporadici oltretutto inadeguati, ispirati a logiche settoriali e non incentrati sulla protezione di un diritto umano fondamentale.

I primi contributi *in subiecta materia* risalgono agli anni trenta, periodo nel quale dobbiamo ricordare il contributo di Ravà⁸, il quale individua, nel novero dei diritti della personalità, «un

⁵ *Ibid.*

⁶ Sul diritto alla *privacy* v.: J. MICHAEL, *Privacy and human rights. An international and comparative study, with special reference to developments in information technology*, Aldershot-Paris 1994; A. WESTIN, *Privacy and freedom*, New York 1967.

⁷ Sul punto vedi S. RODOTÀ, *Privacy e costruzione della sfera privata*, in «Pol. dir.», 1991, e ora in *Tecnologie e diritti*, 1995, p. 108, e ID., *Persona, riservatezza, identità. Prime note sistematiche sulla protezione dei dati personali*, in «Riv. crit. dir. priv.», 1997, 4, p. 589.

⁸ A. RAVÀ, *Istituzioni di diritto privato*, Padova 1938, p. 197.

generale diritto alla riservatezza»; pochi anni più tardi anche De Cupis⁹ si mostra favorevole al riconoscimento di questo diritto. Inizia dunque un dibattito che coinvolge alcuni fra i più importanti studiosi italiani di diritto, divisi fra chi ritiene che la legge italiana tutela il diritto alla riservatezza¹⁰ e fra chi sostiene il contrario¹¹.

Le discussioni in materia trovano nuovo vigore negli anni cinquanta, quando l'autorità giudiziaria viene investita di due procedimenti promossi per tutelare la riservatezza di due personaggi celebri, Enrico Caruso¹² e Claretta Petacci¹³. Nel «caso Caruso», in primo grado si afferma l'esistenza nel nostro ordinamento di un diritto alla riservatezza, tutelabile mediante l'applicazione analogica della disciplina del diritto all'immagine¹⁴. Tale diritto consiste «nel divieto di qualsiasi ingerenza estranea nella sfera della vita privata della persona, e di qualsiasi indiscrezione da parte di terzi, su quei fatti o comportamenti personali che, non pubblici per loro natura, non sono destinati alla pubblicità delle persone che essi riguardano»¹⁵. Il giudizio prosegue poi innanzi la Corte di Cassazione¹⁶, la quale ribalta l'impostazione seguita dai giudici di merito, e, seguendo la tesi prospettata da Pugliese¹⁷, afferma che «il semplice desiderio di riserbo non è stato ritenuto dal legislatore un interesse tutelabile»¹⁸ e quindi che nell'ordinamento italiano non esiste «un generale diritto alla “riservatezza”, o “privatezza”»¹⁹. Questo orientamento non viene formalmente contraddetto dalla Suprema Corte sette anni più tardi²⁰, quando viene chiamata a pronunciarsi sul «caso Petacci»; come nel «caso Caruso», i giudici di merito²¹ riconoscono l'esistenza del diritto alla riservatezza, ma stavolta viene invocata, come norma regolatrice del caso, l'art. 8²² della Convenzione del Consiglio d'Europa per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali, ratificata in Italia con la legge 4 agosto 1955, n. 848. La Cassazione respinge questa tesi e nega ancora l'esistenza di un diritto alla riservatezza, pur tuttavia «deve ammettersi la tutela nel caso di violazione del diritto assoluto di personalità inteso quale diritto *erga omnes* alla libertà di autodeterminazione nello svolgimento della personalità dell'uomo come singolo. Tale diritto è violato se si divulgano notizie della vita privata le quali, per tale loro natura, debbono ritenersi riservate»²³, e le quali trovano tutela nell'art. 2 Cost.

Nonostante questi contrasti, il legislatore interviene solo nel 1970 emanando la legge 20 maggio 1970 n. 300, il c.d. Statuto dei lavoratori, che contiene alcune previsioni a tutela della *privacy* dei lavoratori e pertanto applicabili solo nell'ambito del rapporto di lavoro. Più specificatamente, la legge vieta l'uso di impianti audiovisivi e di altre apparecchiature per finalità di controllo a distanza dell'attività dei lavoratori (art. 4) ed impedisce al datore di lavoro di effettuare accertamenti sulla

⁹ A. DE CUPIS, *I diritti della personalità*, in *Trattato di diritto civile Cicu – Messineo*, Milano 1942, I, p. 148.

¹⁰ Fra gli altri, A. DE CUPIS (v. per tutte: *I diritti della personalità*, cit.) e G. GIAMPICCOLO, *La tutela giuridica della persona umana e il cd diritto alla riservatezza*, in «Riv. trim. dir. proc. civ.», 1958, p. 458.

¹¹ Fra gli altri, G. PUGLIESE (v. per tutte: *Il diritto alla riservatezza nel quadro dei diritti della personalità*, in «Riv. dir. civ.», 1963, p. 605).

¹² Questa vicenda è stata originata dalla realizzazione del film *Leggenda di una voce*, che ricostruiva, in modo romanzato, la vita del celebre tenore Enrico Caruso; gli eredi di questi ritenevano alcune scene del film lesive della memoria, dell'onore e della riservatezza del defunto cantante e convenivano pertanto in giudizio la società produttrice del film.

¹³ La lite era stata provocata dalla pubblicazione di un libro in cui l'autore ricostruiva la personalità di Claretta Petacci, con asserzioni e toni tali da violare, secondo la famiglia della Petacci, la sua *privacy* e quella dei suoi congiunti.

¹⁴ Trib. Roma 14 settembre 1953, in «Foro it.», 1954, I, c. 115; invece App. Roma 17 maggio 1956, in «Foro it.», 1956, I, c. 796, non si pronuncia sul problema dell'esistenza o meno del diritto alla riservatezza.

¹⁵ Così Trib. Roma, *sent. ult. cit.*

¹⁶ Cass., 22 dicembre 1956, n. 4487, in «Giust. Civ.», 1957, I, p.5.

¹⁷ Si veda G. PUGLIESE, *Il preteso diritto alla riservatezza e le indiscrezioni cinematografiche*, in «Foro it.», 1954, c. 116, nota a Trib. Roma 14 settembre 1953.

¹⁸ Cass., *sent. ult. cit.*, p.10.

¹⁹ Cass., *sent. ult. cit.*, p. 5.

²⁰ Cass. 20 aprile 1963 n. 990, in «Foro it.», 1963, I, c. 879.

²¹ Corte d'appello di Milano, 26 agosto 1960, in «Foro it.», 1961, I.

²² «Toute personne à droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance».

²³ Cass., *sent. ult. cit.*, c. 879.

idoneità e sulla infermità per malattia o infortunio del lavoratore dipendente (art. 5). Inoltre, l'art. 6 dispone che «le visite personali di controllo sul lavoratore sono vietate fuorché nei casi in cui siano indispensabili ai fini della tutela del patrimonio aziendale, in relazione alla qualità degli strumenti di lavoro o delle materie prime o dei prodotti. In tali casi le visite personali potranno essere effettuate soltanto a condizione che siano eseguite all'uscita dei luoghi di lavoro, che siano salvaguardate la dignità e la riservatezza del lavoratore e che avvengano con l'applicazione di sistemi di selezione automatica riferiti alla collettività o a gruppi di lavoratori». Infine, l'art. 8 vieta «al datore di lavoro, ai fini dell'assunzione, come nel corso dello svolgimento del rapporto di lavoro, di effettuare indagini, anche a mezzo di terzi, sulle opinioni politiche, religiose o sindacali del lavoratore, nonché su fatti non rilevanti ai fini della valutazione dell'attitudine professionale del lavoratore».

Le norme dello Statuto dei lavoratori fanno segnare dunque un passo avanti nella tutela della *privacy*, ma manca un intervento legislativo che esplicitamente lo riconosca e lo tuteli effettivamente. Fortunatamente, all'inerzia del legislatore fa seguito un intervento suppletivo della giurisprudenza della Suprema Corte, la quale nel 1975 muta orientamento nella sua pronuncia sul c.d. «caso Soraya»²⁴, che rappresenta il *leading case* in materia e il formale riconoscimento dell'esistenza del diritto alla *privacy* nel nostro ordinamento, diritto «consiste[n]te nella tutela di quelle vicende strettamente personali e familiari le quali, anche se verificatesi fuori dal 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 giustificate da interessi pubblici preminenti»²⁵. Le norme a fondamento del diritto alla riservatezza individuate dalla Cassazione sono numerose: gli artt. 2, 3, 14, 15, 27, 29, 41 Cost.; l'art. 1 legge 8 aprile 1974 n. 98; gli artt. 5, 6–10, 2105, 2622 cod. civ.; gli artt. 21, 24, 93 legge aut.; gli artt. 595 comma 2, 614, 616 cod. pen.; l'art. 48 legge fall.; l'art. 8 st. lav.; gli artt. 8 e 10 n. 2 della Convenzione del Consiglio d'Europa per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali; ed altre norme ancora cui sarebbe inutile accennare.

Risulta pertanto di palese evidenza che il diritto alla riservatezza ha trovato accoglimento in Italia grazie al lavoro di dottrina e giurisprudenza, ed a parte alcuni disegni di legge mai approvati dalle Camere per svariati motivi²⁶, il silenzio legislativo fino al 1996 (anno in cui viene emanata la legge 31 dicembre 1996, n. 675, ossia la c.d. legge sulla *privacy*) è rotto solo dalla legge 1 aprile 1981, n. 121 sull'amministrazione della pubblica sicurezza²⁷.

Negli anni successivi al «caso Soraya», la riflessione dottrinale e giurisprudenziale in tema di riservatezza non si è comunque arrestata, in virtù della sempre crescente problematicità del rapporto tra la tutela della vita privata dell'individuo e il diritto costituzionalmente garantito di libertà di

²⁴ Cass., 27 maggio 1975, n. 2129, in «Foro it.», 1976, I, c. 2895. Il caso è stato provocato dalla pubblicazione sul n. 29 del 1968 del periodico «Gente» di un servizio fotografico, realizzato con teleobiettivo, da cui risultavano ripresi in vari atteggiamenti, anche molto intimi, il regista Franco Indovina e la principessa Soraya Esfandiari, nell'interno della villa di quest'ultima. La Esfandiari lamentava la violazione del suo domicilio, della sua riservatezza e della sua immagine, con pregiudizio del decoro, dell'onore e della reputazione. Il fatto aveva anche un diretto risvolto economico, dal momento che alla principessa era stato attribuito un appannaggio a condizione che mantenesse una vita integra ed illibata.

²⁵ Cass., *sent. ult. cit.*, c. 2905.

²⁶ Nel 1980 veniva affidato, con decreto del Ministro di Grazia e Giustizia, ad una commissione, presieduta dall'allora Primo Presidente della Corte di Cassazione Giuseppe Mirabelli, il compito di predisporre uno schema di disegno di legge relativo alla tutela dei dati personali; il lavoro veniva consegnato il 20 luglio 1982 al Ministro di Grazia e Giustizia, che lo presentava al Parlamento il 5 maggio 1984 (il c.d. disegno di legge Martinazzoli); tuttavia non seguì l'approvazione delle Camere, anche per via delle forti critiche mosse al testo, fra cui quella di eccessiva rigidità, a causa di una sola disciplina delle banche dati. Il 4 febbraio 1988 il Guardasigilli istituiva la seconda commissione Mirabelli, il cui lavoro, consegnato al Ministro di Grazia e Giustizia il 30 settembre 1989, veniva modificato dal successivo Ministro in più punti: è questo il c.d. disegno di legge Martelli, anch'esso non approvato dal Parlamento.

²⁷ Ai sensi della quale ogni ente, impresa od associazione che detiene archivi magnetici per l'inserimento di dati od informazioni di cittadini, di ogni natura, deve notificarne l'esistenza al ministero degli interni, consegnandone copia presso la questura territorialmente competente. In caso di dati erronei, incompleti o illegittimamente raccolti, l'interessato può chiedere al tribunale la cancellazione o l'integrazione (se incompleti); questa legge, emanata nel c.d. periodo dell'«emergenza», è stata poi parzialmente abrogata dall'art. 43 comma 1 legge n. 675/96.

manifestazione del pensiero, con riferimento soprattutto al diritto di cronaca²⁸. Nel 1984 il dibattito in materia è diventato molto acceso, in seguito all'emanazione della nota sentenza della Corte di cassazione che ha stabilito il c.d. «decalogo dei giornalisti»²⁹, ossia l'identificazione di quelle condizioni al verificarsi delle quali il diritto di cronaca può prevalere sul diritto alla riservatezza.

Più precisamente, la Suprema Corte individua tre limiti:

- il *pubblico interesse*, ossia l'utilità sociale della notizia,
- la *verità* dei fatti divulgati;
- la *continenza*, cioè la forma civile dell'esposizione, non eccedente rispetto allo scopo informativo ed improntata a serena obiettività, con esclusione di ogni preconcetto intento denigratorio.

Inoltre, in virtù dell'evoluzione delle concezioni in materia di rispetto della vita privata, parallelamente ai profili sinora citati, si registra la progressiva emersione di diritti che si pongono in condizione di complementarità rispetto alla *privacy*, come nel caso del diritto all'oblio, consistente nella pretesa dell'individuo che le vicende che lo riguardano non vengano più divulgate qualora la conoscenza di esse abbia perso il connotato dell'attualità³⁰.

Le riflessioni anzidette subiscono poi un ulteriore acceleramento, che ne rende ancor più manifesta l'importanza, perché l'avvento dei mezzi telematici ha consentito la trasmissione di informazioni in tempi prima impensabili, e già nel 1983 a queste ipotesi faceva acutamente riferimento Vincenzo Zeno-Zencovich, il quale ipotizzava una evoluzione tecnologica che nella sostanza si è oggi realizzata con la rete Internet³¹, per mezzo della quale la violazione del diritto alla *privacy* può avvenire senza confini ed uscire totalmente fuori dal controllo del soggetto autore dell'illecito, con danni irreparabili per la persona la cui riservatezza è stata violata: Internet ha infatti una «formidabile capacità moltiplicatrice»³². Si conviene dunque con autorevole dottrina nell'affermare la necessità di rivedere ed aggiornare i criteri di valutazione degli strumenti di tutela della vita privata delle persone³³. Con precipuo riferimento all'ordinamento italiano, è indispensabile che il progresso tecnologico, che nella pratica viene per lo più portato avanti da imprese private, venga instradato nel rispetto del disposto di cui all'art. 41 Cost., rispettando dunque quei diritti fondamentali della persona previsti dall'art. 2 Cost.

Proprio la disposizione da ultimo citata ha costituito la base per il riconoscimento della tutela di nuovi diritti che costituiscono l'attuazione concreta e il riconoscimento dei valori fondamentali della persona umana ed una giusta interpretazione del suddetto articolo ha contribuito a tutelare la *privacy* anche prima della legge n. 675/96 grazie all'apporto della giurisprudenza, che si è dimostrata molto più pronta del legislatore nel riconoscimento di un diritto fondamentale della persona umana. Tale diritto assume un carattere di "garanzia-presupposto" dell'esercizio di altri diritti fondamentali perché violando la sfera intima si può dissuadere l'individuo dal compiere quelle scelte esistenziali per mezzo delle quali esercita il suo diritto di autodeterminarsi³⁴.

Il concreto soddisfacimento di queste istanze, a volte anche inconsce, della società, è dunque dovuto all'impegno di dottrina e giurisprudenza, che hanno più volte colmato i vuoti di tutela colpevolmente lasciati dal legislatore. Tuttavia, l'assenza di normative cogenti, ha in alcuni (rari) casi portato a posizioni indifendibili da una parte, seppur infinitesimale, della magistratura: basti pensare a quella sentenza del 1996 del Tribunale di Roma³⁵, nella quale si afferma che [se l'attore]

²⁸ G. GIACOBBE, *Il diritto alla riservatezza: da diritto di elaborazione giurisprudenziale a diritto codificato*, in «Iustitia», 1999, 2, p. 111.

²⁹ Cass. 18 ottobre 1984, n. 5259, in «Dir. inf.», 1985, 1, p. 143, con nota di S. FOIS, G. GIACOBBE, F. MOROZZO DELLA ROCCA.

³⁰ G. GIACOBBE, *op. cit.*, p. 112.

³¹ V. ZENO-ZENCOVICH, *Telematica e tutela del diritto all'identità personale*, in «Pol. dir.», 1983, 2, pp. 345 ss.

³² S. RODOTÀ, *Se non ci sono più confini qualche limite è necessario*, in «Teléma», 1997, 8.

³³ G. GIACOBBE, *op. cit.*, p. 116.

³⁴ M. AIMO, *I «lavoratori di vetro»: regole di trattamento e meccanismi di tutela dei dati personali*, in «Riv. giur. prev. soc.», 2002, 1, p. 48.

³⁵ Trib. Roma 24 gennaio 1996, in «Dir. inf.», 1996, 4-5, p. 572, con nota di V. ZENO-ZENCOVICH; il caso di specie

«avesse davvero voluto tutelare la propria riservatezza, alla quale sembra tenere nel presente procedimento, avrebbe dovuto trovare una diversa forma di tutela dei propri diritti e non rivolgersi all'autorità giudiziaria!» Vi è di più: «nel caso di specie, non si tratta evidentemente di divulgazione di fatti gravi o riprovevoli, ma di una vicenda insolita e sotto certi aspetti stuzzicante perché collegata alla sfera sessuale». Questa è dunque «una visione nullificante dei diritti della personalità e della crescente area di loro tutela»³⁶, e in merito (correttamente) Giuseppe Cassano afferma che «le poche affermazioni dell'organo giudicante sembrano aver mandato al macero intero biblioteche sul diritto alla riservatezza»³⁷.

Tuttavia, ferma restando l'inconcepibilità di una siffatta sentenza, con la quale il giudice romano sembra voler incentivare l'idea di farsi giustizia da sé, bisogna purtroppo ammettere che nel caso di violazione del diritto alla *privacy* il processo, per sua natura pubblico, potrebbe contribuire all'aggravamento della lesione suddetta. Si pensi al caso Soraya, il quale, come detto, costituisce il *leading case* in materia e che per tale motivo è citato in qualsiasi lavoro che si occupi della ricostruzione storica del diritto alla riservatezza, dunque ben al di fuori dei limiti della vicenda processuale. Sarebbe dunque auspicabile la predisposizione di una procedura *ad hoc* in tutti i casi in cui venga denunciata la violazione del diritto alla riservatezza, per evitare ulteriore pubblicità a vicende che dovrebbero invece essere private, anche se l'art. 128 cod. proc. civ. prevede che le udienze di discussione³⁸ possano svolgersi a porte chiuse ove ricorrano ragioni di ordine pubblico o buon costume.

In ogni caso, un sacrificio della *privacy* si verificherà sempre e comunque, successivamente alla emissione di un atto giudiziario, ragion per cui l'attenzione dovrebbe spostarsi verso forme di tutela preventiva che impediscano che si realizzi l'offesa, secondo il brocardo di *common law* "*remedies precede rights*", perché una volta che questa si concretizza nessuna forma di riparazione può consentire un effettivo ripristino della situazione preesistente, potendosi ottenere, al più, un risarcimento monetario.

L'emanazione della legge n. 675/96 ha comunque posto termine alla lunga inerzia del legislatore italiano in materia di tutela del diritto alla riservatezza, in netto ritardo rispetto ai similari interventi normativi che in alcuni paesi (Svezia, Danimarca, Francia, ecc.) si erano avuti già negli anni settanta, ma appena in tempo per rispettare le prescrizioni dettate dall'Accordo di Schengen del 1985 e dalla direttiva della Comunità Europea 24 ottobre 1995, n. 46. Indipendentemente dalla valutazione qualitativa della legge in oggetto, è evidente che essa, anche grazie all'ottimo operato del Garante per la protezione dei dati personali, ha avuto grande risonanza a livello di riflessione scientifica, come dimostrano i numerosi contributi in materia³⁹, e, soprattutto, è stata progressivamente recepita dalla popolazione.

riguardava l'ex-dirigente di un'azienda, che, a seguito del proprio licenziamento, aveva proposto azione avanti il Pretore di Frosinone per impugnare l'atto ed ottenere il risarcimento dei danni conseguenti, compreso il danno biologico in quanto l'attore lamentava disturbi alla sfera sessuale. Le parti giungevano poi ad una transazione, nella quale si riconosceva anche il risarcimento del danno biologico. Proprio quest'ultimo aspetto veniva ritenuto (oltre che stuzzicante dai giudici romani) anche interessante da quotidiani e periodici, i quali titolavano *Impotenza da licenziamento risarcita con 225 milioni – Perde lavoro e virilità* ("La Repubblica") e *Un'insolita causa tra azienda e dipendente dimostra che il licenziamento fa male anche sotto le lenzuola – È vero: chi non lavora non fa l'amore* ("Visto").

³⁶ V. ZENO-ZENCOVICH, *op. ult. cit.*, p. 572.

³⁷ G. CASSANO, *I diritti della personalità e le aporie logico-dogmatiche di dottrina e giurisprudenza*, in «Dir. fam.», 2000, p. 1407.

³⁸ A norma dell'art. 84 disp. att. c.p.c., invece, le udienze del giudice istruttore non sono pubbliche.

³⁹ Oltre alle opere già citate, cfr., fra gli altri: AA. VV., *Società dell'informazione tutela della riservatezza*, Atti del congresso di Stresa, 16-17 maggio 1997, Milano, 1998; R. ACCIAI, *Privacy e banche dati pubbliche. Il trattamento dei dati personali nelle pubbliche amministrazioni*, Padova 2001; C. M. BIANCA, F. D. BUSNELLI. (a cura di), *Tutela della privacy*, in «Nuove leggi civ. comm.», 1999, 2-3; G. BUTTARELLI, *Banche dati e tutela della riservatezza. La privacy nella Società dell'Informazione*, Milano 1997; V. CUFFARO, V. RICCIUTO, V. ZENO-ZENCOVICH (a cura di), *Trattamento dei dati e tutela della persona*, Milano 1998; E. GIANNANTONIO, M. G. LOSANO, V. ZENO-ZENCOVICH, *Commentario alla legge 31 dicembre 1996, n. 675*, Padova 1997; G. P. ZANETTA, C. CASALEGNO, *La tutela della privacy nella sanità*, Milano 1998.

Come ribadito di recente dalla Suprema Corte, la fonte primaria del diritto alla riservatezza rimane comunque l'art. 2 Cost., ancorché esso sia previsto da altre norme più specifiche, e la sua violazione dà luogo ad un fatto illecito i cui effetti pregiudizievoli sono risarcibili. La risarcibilità non è tuttavia automatica, giacché il non è danno *in re ipsa*: «il pregiudizio, morale o patrimoniale che sia, attesa la maggiore ampiezza dell'illecito in questione rispetto a quello che si realizza nel caso di lesione del decoro, dell'onore o della reputazione, deve essere provato secondo le regole ordinarie. La parte che chiede il risarcimento del danno prodotto da tale illecito dunque deve provare il pregiudizio alla sua sfera patrimoniale o personale, quale ne sia l'entità e quale che sia la difficoltà di provare tale entità»⁴⁰.

3. Il c.d. «codice della privacy»: aspetti generali

In pochi anni la legge n. 675/96 ha subito numerose modifiche, effettuate mediante alcuni decreti legislativi che si sono succeduti sin dal 1997⁴¹, che ne hanno modificato aspetti assai importanti, ed il suo contenuto è stato in gran parte trasfuso, seppur in alcuni casi con notevoli variazioni, nel d. lgs. 30 giugno 2003, n. 196, ossia il «Codice in materia di protezione dei dati personali» già detto «Codice della *privacy*» (d'ora in poi cod. priv.), la cui entrata in vigore è stata disposta per il 1° gennaio 2004⁴². Il codice, assai vasto, è diviso in tre parti: nella prima sono contenute le disposizioni generali e nella seconda quelle relative a specifici settori, mentre nella terza trovano posto le norme relative alle forme di tutela, alle sanzioni ed all'ufficio del Garante per la protezione dei dati personali (d'ora in poi Garante). La vastità del d.lgs. in oggetto rende palese la sempre maggiore importanza della tutela del diritto alla *privacy* in una molteplicità di situazioni, e sorprende come in pochi anni la normativa in tema di diritto alla riservatezza abbia fortunatamente colmato una pluridecennale lacuna legislativa, evolvendo da una legge approvata con poca cura per ottemperare ai citati obblighi internazionali dell'Italia ad un codice che «rappresenta il primo tentativo al mondo di conformare le innumerevoli disposizioni relative anche in via indiretta alla *privacy*»⁴³. Esso costituisce, inoltre, il recepimento, oltre che di gran parte della legge n. 675/96 e delle norme che l'hanno modificata, anche delle pronunce emanate del Garante e dei pareri forniti dalla medesima *authority*, la cui attività è stata connotata da ragionevolezza e capacità di comprensione delle istanze avanzate da più parti nell'ambito dell'odierna società dell'informazione.

Il cod. priv. si apre, all'art. 1, con una importante disposizione: «chiunque ha diritto alla protezione dei dati personali che lo riguardano». Tale principio era comunque già desumibile in via implicita, come è emerso nel corso della ricostruzione evolutiva del diritto alla *privacy*, ma è importante che esso sia sancito in maniera chiara ed esplicita.

L'art. 2, ampliando la previsione di cui all'art. 1 comma 1 legge n. 675/96, dispone che il cod. priv. «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». Il riferimento esplicito sia al diritto alla riservatezza che al diritto alla protezione dei dati personali fa emergere il carattere di generalità del diritto alla *privacy*, del quale il diritto alla protezione dei dati personali costituisce,

⁴⁰ Cass. 25 marzo 2003, n. 4366, in «Dir. inf.», 2003, 3, p. 523.

⁴¹ Prima dell'emanazione del codice della *privacy*, la legge n. 675/96 è stata modificata dai seguenti decreti legislativi: n. 467 del 28 dicembre 2001; n. 282 del 30 luglio 1999; n. 281 del 30 luglio 1999; n. 135 dell'11 maggio 1999; n. 51 del 26 febbraio 1999; n. 389 del 6 novembre 1998; n. 171 del 13 maggio 1998; n. 135 dell'8 maggio 1998; n. 255 del 28 luglio 1997; n. 123 del 9 maggio 1997.

⁴² La vastità del cod. priv. ne impone, in questa sede, una trattazione esigua, se paragonata alla molteplicità di questioni che scaturiscono dal suo esame, ma comunque finalizzata a fornire al lettore gli elementi di base necessari per una prima lettura del testo in oggetto, anche grazie ai riferimenti diretti alla nuova normativa.

⁴³ Così si legge nella *Newsletter* n. 176 del Garante per la protezione dei dati personali. Nel cod. priv., del resto, trovano posto disposizioni che toccano tematiche e settori importanti e delicati, come il lavoro e la previdenza sociale, i sistemi bancari, finanziari ed assicurativi, le comunicazioni elettroniche, e così via.

comunque, una specificazione.

Le norme del cod. priv. possono, inoltre, essere integrate dalle disposizioni contenute nei *codici di deontologia e buona condotta*. Difatti, l'art. 12 dispone che «il Garante promuove nell'ambito delle categorie interessate, nell'osservanza del principio di rappresentatività e tenendo conto dei criteri direttivi delle raccomandazioni del Consiglio d'Europa sul trattamento di dati personali, la sottoscrizione di codici di deontologia e di buona condotta per determinati settori, ne verifica la conformità alle leggi e ai regolamenti anche attraverso l'esame di osservazioni di soggetti interessati e contribuisce a garantirne la diffusione e il rispetto». Ai sensi del comma 3 della medesima norma, «il rispetto delle disposizioni contenute nei codici di cui al comma 1 costituisce condizione essenziale per la liceità e correttezza del trattamento dei dati personali effettuato da soggetti privati e pubblici».

La citata verifica di conformità dei codici deontologici alle leggi, operata dal Garante, riconosce loro «il valore di criterio di riferimento per determinare la legittimità del trattamento», per cui il rispetto delle regole ivi contenute costituisce elemento certo per la valutazione, eventualmente anche in sede giudiziaria, del rispetto dei suddetti principi di liceità e correttezza del trattamento. Ne consegue che «il codice deontologico assume valenza di norma, sebbene di grado secondario rispetto alla legge e ha l'inegabile pregio di penetrare meglio e più tecnicamente nei singoli settori di riferimento regolati»⁴⁴. Al Garante è, dunque, affidato un compito assai delicato, perché, nella valutazione di ciascun codice, dovrà contemperare le opposte esigenze delle altre categorie coinvolte dalla creazione di siffatte disposizioni⁴⁵.

Il *trattamento di dati personali* consiste in «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». Pertanto, tale amplissima definizione fa agevolmente comprendere che qualsiasi operazione compiuta sui dati personali rientra nel campo di applicazione della normativa in oggetto.

I *dati personali* sono definiti come «qualunque informazione relativa a persona fisica, identificata o identificabile, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale» (art. 4 comma 1 lett. b). All'interno del novero dei dati personali la legge individua la categoria dei *dati identificativi*, ossia quei «dati personali che permettono l'identificazione diretta dell'interessato» (art. 4 comma 1 lett. c), e dei *dati sensibili*, il cui trattamento deve avvenire con modalità particolari, essendo 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» (art. 4 comma 1 lett. d).

L'art. 3, inoltre, impone un principio di carattere generale nell'ambito del trattamento dei dati personali, che deve avvenire secondo il *principio di necessità* del trattamento, con la conseguenza che bisogna configurare i sistemi informativi e i programmi informatici in modo da minimizzare l'utilizzazione di dati personali ed identificativi, così «da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi⁴⁶ od opportune modalità che permettano di identificare l'interessato solo in caso di necessità». Per quanto tale norma non sancisca un principio di stretta necessità del trattamento, essa

⁴⁴ R. IMPERIALI, R. IMPERIALI, *Danno risarcito anche senza prova della colpa*, in «Guida dir.» – Doss. mens., 2003, 8, p. 111.

⁴⁵ Del resto, «non si poteva [...] lasciare esclusivamente alle sole categorie dei titolari coinvolti, il compito di "scriversi" le disposizioni che le riguardavano, senza tenere in debito conto gli interessi contrapposti delle altre categorie coinvolte (compito che, opportunamente, è stato in tal modo affidato al Garante)» (G. BUSIA, *Deontologia parametro di liceità delle operazioni*, in «Guida dir.» — Doss. mens., 2003, 8, p. 151).

⁴⁶ È detto anonimo quel «dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile» (art. 4 comma 1 lett. n).

rappresenta comunque «una vera e propria rivoluzione nell'approccio alla protezione dei dati trattati con sistemi automatizzati, soprattutto nella sua applicazione al commercio elettronico e al funzionamento dei servizi di comunicazione»⁴⁷.

3.1 I soggetti del codice della privacy

Il cod. priv., come già la legge n. 675/96, opera una tipizzazione dei soggetti che rilevano nell'ambito della attività di trattamento di dati personali. Prima delle modifiche apportate al cod. priv. dal d.l. 201/2011 (convertito con modificazioni dalla l. 214/2011), l'*interessato* era definito come «la persona fisica, la persona giuridica, l'ente o l'associazione cui si riferiscono i dati personali» (art. 4 comma 1 lett. i). La legge forniva una definizione onnicomprensiva, che teneva conto del fatto che la riservatezza non è un diritto proprio solo delle persone fisiche, ma anche di altri soggetti, cui viene dunque riconosciuto nella sua specifica accezione di diritto all'autodeterminazione informativa. Tuttavia, in modo inopinato, con il d.l. 201/2011, il legislatore ha ridotto l'ambito di applicazione unicamente alle persone fisiche, escludendo esplicitamente persone giuridiche, enti e associazioni.

Il *titolare* del trattamento è, ai sensi dell'art. 4 comma 1 lett. f), «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». Questa definizione rende palese il ruolo apicale che il titolare occupa nella piramide gerarchica prospettata dal cod. priv., dato il particolare rilievo che rivestono i compiti attribuiti a questa figura, che, nel quadro dei soggetti che si occupano, in vario modo, del trattamento, risulta l'unica assolutamente necessaria, in quanto è proprio il titolare a dar vita al trattamento. Rispetto alla normativa previgente, si rileva l'introduzione della possibilità espressa che vi siano più titolari.

Dalla norma sopracitata si evince che il legislatore non ha inteso occuparsi esplicitamente della problematica relativa alla fonte od al titolo dal quale può derivare il potere decisionario sulla finalità e sulle modalità del trattamento, potere che automaticamente comporta l'assunzione della qualifica di titolare; si può quindi ritenere che il rinvio sia implicito nei confronti delle vigenti disposizioni di legge o di regolamento (nazionali, comunitarie o derivanti da accordi internazionali).

Sul titolare grava sempre, ex art. 29 comma 5, l'obbligo di assidua vigilanza sui preposti da lui eventualmente nominati: non può disinteressarsi del trattamento ed affidarne *in toto* la gestione ad altri soggetti, ma deve assumere un ruolo attivo in tutte le fasi che connotano il trattamento, da quelle preliminari a quelle che ne comportano la cessazione.

Recependo un principio già sancito in via interpretativa dal Garante⁴⁸, il cod. priv. dispone che «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).

Il *responsabile* del trattamento di dati personali è «la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali» (art. 4 comma 1 lett. g); la nomina di questo soggetto è facoltativa, ai sensi dell'art. 29 comma 1, ed è espressione del potere di autonomia organizzativa del titolare, il

⁴⁷ M. ATELLI, *Software configurati per l'utilizzo dei dati anonimi*, in «Guida dir.» — Doss. mens., 2003, 8, p. 108.

⁴⁸ Il titolare è da individuarsi nell'entità nel suo complesso e non in «talune delle persone che operano nella relativa struttura e che concorrono, in concreto, ad esprimerne la volontà o che sono legittimati a manifestarla all'esterno; [...] in molti casi, tali soggetti potrebbero assumere, semmai, la qualifica di "responsabile"» (Decisione 11 dicembre 1997 del Garante per la protezione dei dati personali). È di tutta evidenza, inoltre, che per l'espressione esterna della volontà di una persona giuridica, di una pubblica amministrazione o di un qualsiasi altro ente, associazione od organismo, è imprescindibile l'intermediazione dell'organo rappresentativo, i cui atti sono ovviamente da imputarsi al soggetto collettivo nella sua interezza; ciò vale anche, e non potrebbe essere altrimenti, per le decisioni inerenti al trattamento, le quali, automaticamente, comportano l'assunzione della qualifica di titolare (così anche S. FADDA, *Art. 1 comma 2*, in E. GIANNANTONIO, M. G. LOSANO, V. ZENO-ZENCOVICH, *op. cit.*, p. 19).

quale, anche effettuando tale nomina, non viene comunque liberato da responsabilità. Il responsabile deve essere nominato tra soggetti che possano garantire, per esperienza, capacità ed affidabilità, il pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo della sicurezza dei dati; non deve necessariamente essere un unico soggetto, poiché l'art. 29 comma 3 permette la designazione di più responsabili, anche mediante suddivisione dei compiti, i quali devono sempre essere analiticamente specificati per iscritto (art. 29 comma 4). Quest'ultima disposizione non consente, quindi, che la designazione di tale figura avvenga in via implicita, ma la legge non pone preclusioni al cumulo di qualifiche all'interno della struttura del titolare, il quale può pertanto nominare responsabile anche un soggetto che ha già ulteriori qualifiche all'interno della predetta struttura, oltre a poterlo scegliere fra altre persone fisiche o servirsi di un organismo esterno incaricato di elaborare i dati.

L'ampiezza dell'autonomia decisionale concessa al responsabile è stabilita dal titolare, al quale è affidato il diritto-dovere di esercitare penetranti poteri di vigilanza e di controllo per tutta la durata del trattamento.

Nel caso in cui fra il responsabile ed il titolare intercorra un rapporto di lavoro subordinato, potrà trovare applicazione l'art. 2049 cod. civ., il quale sancisce la responsabilità dei padroni e committenti per i danni arrecati dal fatto illecito dei loro domestici e commessi nell'esercizio delle incombenze a cui sono adibiti. Nell'opposta eventualità in cui il responsabile non sia legato da un rapporto di lavoro subordinato, si renderà necessaria la conclusione di un contratto per mezzo del quale il titolare conferisca al responsabile l'incarico di gestire il trattamento; in dottrina è stata ipotizzata, in tal caso, l'applicazione delle norme che disciplinano l'appalto di servizi, con la conseguenza di spostare dal titolare al responsabile i rischi connessi allo svolgimento dell'attività⁴⁹.

I compiti del responsabile sono analiticamente specificati per iscritto dal titolare; si possono qui ricordare l'evasione delle domande di accesso, di rettifica, di integrazione, di cancellazione e di blocco dei dati, compiti effettuati sì in autonomia, ma comunque sempre nel rispetto degli ordini impartiti dal titolare.

Il responsabile ha pertanto il compito di dare concreta esecuzione e rilevanza esterna alle disposizioni del titolare e può essere chiamato a rispondere di illeciti civili, penali e amministrativi; assumendo dunque un ruolo fondamentale nell'economia del trattamento.

Bisogna infine fare riferimento agli *incaricati* del trattamento, che nel cod. priv. trovano una definizione esplicita, a differenza di quanto avvenuto con la legge n. 675/96: essi sono «le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile» (art. 4 comma 1 lett. h). L'art. 30, inoltre, dispone che «le operazioni di trattamento possono essere effettuate solo da incaricati che operano sotto la diretta autorità del titolare o del responsabile, attenendosi alle istruzioni impartite» e che «la designazione è effettuata per iscritto e individua puntualmente l'ambito del trattamento consentito. Si considera tale anche la documentata preposizione della persona fisica ad una unità per la quale è individuato, per iscritto, l'ambito del trattamento consentito agli addetti all'unità medesima».

3.2. Il trattamento di dati personali: alcuni cenni

In linea generale, il cod. priv. si applica a tutti i trattamenti di dati personali effettuato da chiunque è stabilito nel territorio dello Stato o in un luogo comunque soggetto alla sovranità dello Stato ed anche se i dati sono detenuti all'estero. Questa normativa, inoltre, si applica anche nell'ipotesi opposta, ossia quando il trattamento di dati personali è effettuato da un soggetto che non è stabilito nell'UE, ma che a tal fine impiega strumenti (anche non elettronici) situati nel territorio italiano, salvo che essi siano utilizzati solo ai fini di transito nel territorio dell'UE. Nei casi di applicazione del cod. priv., il titolare del trattamento deve designare un proprio rappresentante stabilito nel territorio italiano ai fini dell'applicazione della disciplina sul trattamento dei dati personali.

⁴⁹ S. FADDA., *op. cit.*, p. 93.

Ricalcando l'art. 3 legge n. 675/96, l'art. 5 comma 3 dispone, poi, che il cod. priv. non trova applicazione nella fattispecie di trattamento di dati personali effettuato da persone fisiche per fini esclusivamente personali, a meno che i dati non siano destinati ad una comunicazione sistematica od alla diffusione. Una eccezione a tale regola generale è contenuta nella medesima norma, ove si sancisce, anche in tali ipotesi, l'applicabilità delle norme in tema di responsabilità e di sicurezza dei dati.

In materia di trattamento di dati personali, per i soggetti pubblici, ad eccezione degli enti pubblici economici, il cod. priv. delinea regole particolari, ma, in linea generale, si prevede che «qualunque trattamento di dati personali da parte di soggetti pubblici è consentito soltanto per lo svolgimento delle funzioni istituzionali» (art. 18 comma 2).

Le operazioni che costituiscono trattamento ai sensi del cod. priv. possono essere suddivise in base alle seguenti fasi inerenti le banche dati⁵⁰:

- la fase *costruttiva* della banca dati (raccolta, registrazione, organizzazione, conservazione, elaborazione, modificazione);
- la fase *elaboratoria* (selezione, estrazione, raffronto, utilizzo, interconnessione);
- la fase *circolatoria* (blocco, comunicazione, diffusione);
- la fase *eliminatoria* (cancellazione, distruzione).

L'art. 11 detta i *principi qualitativi* circa la raccolta e i requisiti dei dati personali oggetto di trattamento⁵¹, che devono essere:

- trattati in modo lecito e secondo correttezza⁵²;
- raccolti e registrati per scopi determinati, espliciti e legittimi, ed utilizzati in altre operazioni del trattamento in termini compatibili con tali scopi;
- 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.

Al comma 2, inoltre, si dispone l'inutilizzabilità dei dati personali trattati in violazione della normativa in materia di trattamento dei dati personali.

Prima di procedere al trattamento dei dati è necessario, innanzi tutto, fornire l'*informativa* al soggetto i cui dati potranno essere oggetto di trattamento. Queste informazioni possono essere rese oralmente o per iscritto⁵³ e, ai sensi dell'art. 13 e salvo diverse disposizioni, devono indicare:

- le finalità e le modalità del trattamento cui sono destinati i dati;
- la natura obbligatoria o facoltativa del conferimento dei dati;
- le conseguenze di un eventuale rifiuto di rispondere;
- i soggetti o le categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di responsabili o incaricati, e l'ambito di diffusione dei dati medesimi;
- i diritti dell'interessato previsti dall'art. 7;

⁵⁰ Si segue qui la divisione di M. AMBROSOLI, *La tutela dei dati personali e la responsabilità civile*, in «Riv. dir. priv.», 1998, 2, p. 305.

⁵¹ S. SICA, *Danno morale e legge sulla privacy informatica*, in «Danno e resp.», 1997, 3, p. 283.

⁵² Questo riferimento alla liceità e alla correttezza può essere letto come espressione di un atteggiamento di apertura ed interesse nei confronti di una realtà bisognosa di regolamentazione (V. COLONNA, *Il danno da lesione della privacy*, in «Danno e resp.», 1999, 1, p. 22).

⁵³ Questa norma riprende l'art. 10 legge n. 675/96, così come modificato dal d.lgs. 9 maggio 1997, n. 123. Nell'impianto originario della legge, invece, tali informazioni dovevano essere necessariamente rese per iscritto, rendendo assai più semplice l'eventuale dimostrazione che l'informativa fosse stata effettivamente resa. Con la sua modifica, però, risulta alquanto arduo riuscire a provare tale circostanza.

— gli estremi identificativi del titolare e, se designati, del responsabile⁵⁴ e del rappresentante nel territorio dello Stato di cui all'art. 5.

Tali indicazioni possono essere integrate da quelle previste da specifiche disposizioni del cod. priv., ma possono anche non comprendere gli elementi già noti alla persona che fornisce i dati o la cui conoscenza può ostacolare in concreto l'espletamento, da parte di un soggetto pubblico, di funzioni ispettive o di controllo svolte per finalità di difesa o sicurezza dello Stato oppure di prevenzione, accertamento o repressione di reati.

Se i dati personali non sono raccolti presso l'interessato, l'informativa, comprensiva delle categorie di dati trattati, è a lui data al momento della registrazione dei dati o, quando è prevista la loro comunicazione, non oltre la prima comunicazione, fatte salve alcune eccezioni. Esse si verificano quando i dati sono trattati per ottemperare ad un obbligo previsto dalla legge, da un regolamento o dalla normativa comunitaria, o per lo svolgimento di investigazioni difensive o, comunque, per far valere o difendere un diritto in sede giudiziaria⁵⁵, o, ancora, se l'informativa all'interessato è, a giudizio del Garante, impossibile oppure troppo gravosa con riferimento al diritto tutelato.

Il rispetto delle regole relative all'informativa assicurano, o dovrebbero assicurare, che il *consenso* al trattamento dei dati personali sia libero e consapevole. In merito, si registra una diversità di disciplina fra soggetti pubblici e privati. Ai sensi dell'art. 18 comma 4, infatti, i primi non devono richiedere il consenso dell'interessato, mentre, a norma dell'art. 23 comma 1, il trattamento di dati personali da parte di privati o di enti pubblici economici è ammesso solo con il consenso espresso dell'interessato.

L'art. 24, tuttavia, prevede numerose ipotesi nelle quali il trattamento può avvenire a prescindere dal consenso, qualora il trattamento stesso sia necessario per adempiere ad un obbligo previsto dalla legge, da un regolamento o dalla normativa comunitaria o 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. Il consenso non è altresì richiesto se il trattamento 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) oppure dati relativi allo svolgimento di attività economiche (trattati nel rispetto delle leggi di settore), o, ancora, se è necessario per la salvaguardia della vita o dell'incolumità fisica di un terzo⁵⁶.

Con esclusione dell'ipotesi di diffusione dei dati, il consenso non è richiesto se il trattamento è necessario ai fini, cui si è accennato, dello svolgimento delle investigazioni difensive o per far valere o difendere un diritto in sede giudiziaria, oppure se è necessario, nei casi individuati dal Garante sulla base dei principi sanciti dalla legge, per perseguire un legittimo interesse del titolare o di un terzo destinatario dei dati, anche in riferimento all'attività di gruppi bancari e di società controllate o collegate, qualora non prevalgano i diritti e le libertà fondamentali, la dignità o un legittimo interesse dell'interessato, e lo

⁵⁴ Quando il titolare ha designato più responsabili è indicato almeno uno di essi, indicando il sito della rete di comunicazione o le modalità attraverso le quali è conoscibile in modo agevole l'elenco aggiornato dei responsabili. Quando è stato designato un responsabile per il riscontro all'interessato in caso di esercizio dei diritti di cui all'art. 7, è indicato tale responsabile.

⁵⁵ «Sempre che i dati siano trattati esclusivamente per tali finalità e per il periodo strettamente necessario al loro perseguimento» (art. 13 comma 5 lett. b).

⁵⁶ Se la medesima finalità riguarda l'interessato e quest'ultimo non può prestare il proprio consenso per impossibilità fisica, per incapacità di agire o per incapacità di intendere o di volere, il consenso è manifestato da chi esercita legalmente la potestà, ovvero da un prossimo congiunto, da un familiare, da un convivente o, in loro assenza, dal responsabile della struttura presso cui dimora l'interessato. Si applica così l'art. 82 comma 2, ai sensi del quale «l'informativa e il consenso al trattamento dei dati personali possono altresì intervenire senza ritardo, successivamente alla prestazione, in caso di: a) impossibilità fisica, incapacità di agire o incapacità di intendere o di volere dell'interessato, quando non è possibile acquisire il consenso da chi esercita legalmente la potestà, ovvero da un prossimo congiunto, da un familiare, da un convivente o, in loro assenza, dal responsabile della struttura presso cui dimora l'interessato; b) rischio grave, imminente ed irreparabile per la salute dell'interessato».

stesso vale per le associazioni *no profit* con riferimento ai propri soci ed aderenti, fatta eccezione per la comunicazione all'esterno e per la diffusione. Infine, il consenso non deve essere prestato nel caso in cui il trattamento sia necessario (in conformità ai rispettivi codici deontologici), per esclusivi scopi scientifici, statistici o storici (in quest'ultimo caso, presso archivi privati dichiarati di notevole interesse storico).

Per i *dati sensibili* sono invece predisposte regole diverse, in ragione dell'importanza che tali dati rivestono, poiché essi riguardano i più intimi aspetti dell'uomo, e dunque essi possono essere trattati solo con il consenso scritto dell'interessato e previa autorizzazione del Garante. Tale regola non si applica, tuttavia, al trattamento dei dati relativo agli aderenti alle confessioni religiose e ai soggetti che con riferimento a finalità di natura esclusivamente religiosa hanno contatti regolari con le medesime confessioni, effettuato dai relativi organi, ovvero da enti civilmente riconosciuti, sempre che i dati non siano diffusi o comunicati fuori delle medesime confessioni; non si applica, inoltre, al trattamento dei dati riguardanti l'adesione di associazioni od organizzazioni a carattere sindacale o di categoria ad altre associazioni, organizzazioni o confederazioni a carattere sindacale o di categoria. Infine, la tutela dei dati personali idonei a rivelare lo stato di salute è ancor più incisiva, considerando il divieto di diffusione di tali dati posto dall'art. 26 comma 5.

3.3. I diritti dell'interessato

Il titolo II della I parte del cod. priv. è dedicato ai *diritti dell'interessato*. In particolare, l'art. 7 dispone che «l'interessato ha 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».

Inoltre, 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'art. 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 oppure, 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 cui alle lettere a) e b) sono state portate a conoscenza, anche per quanto riguarda il loro contenuto, 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: a) per motivi legittimi al trattamento dei dati personali che lo riguardano, ancorché pertinenti allo scopo della raccolta; b) al trattamento di dati personali che lo riguardano a fini di invio di materiale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato o di comunicazione commerciale.

I diritti di cui si è detto possono essere esercitati mediante richiesta rivolta senza formalità al titolare o al responsabile, anche per il tramite di un incaricato, alla quale è fornito idoneo riscontro senza ritardo. Se la richiesta riguarda i diritti di cui all'art 7, commi 1 e 2, può essere effettuata anche oralmente, mentre in tutti gli altri casi può essere proposta tramite raccomandata, fax, posta elettronica o altro sistema idoneo individuato dal Garante in base all'evoluzione tecnologica, e può essere riproposta, salvo giustificati motivi, non prima di novanta giorni dalla prima richiesta.

Quando i dati trattati non hanno carattere oggettivo, non può tuttavia essere chiesta la rettificazione o l'integrazione di dati personali di tipo valutativo, relativi a giudizi, opinioni o ad altri apprezzamenti di tipo soggettivo, nonché l'indicazione di condotte da tenersi o di decisioni in via di assunzione da parte del titolare del trattamento.

L'interessato può esercitare personalmente (anche con l'assistenza di una persona di fiducia) i diritti di cui all'art. 7, o per mezzo di altri soggetti (persone fisiche, enti, associazioni od organismi) cui viene conferita, per iscritto, delega o procura. Qualora i diritti in oggetto si riferiscano a dati personali concernenti persone decedute, essi possono essere esercitati da chi ha un interesse proprio, o agisce a tutela dell'interessato o per ragioni familiari meritevoli di protezione.

Salvo specifica richiesta, il *riscontro* comprende tutti i dati personali che riguardano l'interessato e che sono trattati dal titolare, il quale deve, da un lato, adottare tutte le misure idonee ad agevolare all'interessato l'accesso ai propri dati, dall'altro, semplificare le modalità ed ottimizzare i tempi per il riscontro di cui sopra (art. 10). Il responsabile o gli incaricati si occupano dell'estrazione dei dati, che possono poi essere comunicati al richiedente in via orale oppure essere offerti in visione mediante strumenti elettronici, purché non ne venga pregiudicata la comprensibilità. Inoltre, è possibile, dietro richiesta, provvedere alla loro trasposizione su supporto cartaceo o informatico, oppure alla loro trasmissione per via telematica. Se l'estrazione dei dati risulta particolarmente difficoltosa, il riscontro può avvenire anche attraverso l'esibizione o la consegna in copia di atti e documenti contenenti i dati personali richiesti.

3.4. Le misure di sicurezza

Alla sicurezza dei dati e dei sistemi è dedicato il titolo V della I parte del cod. priv. Nel capo I trovano posto le norme in tema di misure di sicurezza, mentre nel II sono disciplinate le misure minime di sicurezza. Questa tematica ha un ruolo centrale nella regolamentazione del trattamento dei dati personali, anche in considerazione del fatto che l'omessa adozione delle misure minime di sicurezza costituisce un illecito penale. Si consideri, inoltre, che «la sicurezza dei dati costituisce una garanzia "esterna" diretta, in via preventiva, a ridurre al minimo il rischio di interazioni di situazioni patologiche estranee con le libertà e i diritti sottesi al trattamento» e da ciò risulta «l'*indisponibilità* della disciplina da parte dei soggetti coinvolti nel trattamento dei dati, che verosimilmente si potrebbe tradurre nella rinuncia da parte dell'interessato alle misure di sicurezza, [...ma] la mancata predisposizione delle stesse potrebbe comportare una lesione alla dignità umana, [...che] costituisce l'asse portante ed inviolabile di equilibrio tra gli interessi contrapposti»⁵⁷.

L'art. 31 stabilisce, in linea generale, gli *obblighi di sicurezza*: «i dati personali oggetto di trattamento sono 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». L'art. 32, invece, disciplina il caso in cui il titolare è un fornitore di un servizio di comunicazione elettronica accessibile al pubblico.

Con riferimento alle *misure minime di sicurezza* l'art. 33 dispone, in maniera generica, che nel quadro dei più generali obblighi di sicurezza (di cui all'art. 3 o previsti da speciali disposizioni), il titolare deve comunque adottare le misure minime (individuata nel II capo o ai sensi dell'art. 58 comma 3) volte ad assicurare un livello minimo di protezione dei dati personali. Ovviamente, le misure minime variano a seconda che il trattamento avvenga con strumenti elettronici (art. 34) oppure senza il loro ausilio (art. 35).

In particolare, l'art. 34 prevede che «il trattamento di dati personali effettuato con strumenti elettronici è consentito solo se sono adottate, nei modi previsti dal disciplinare tecnico contenuto nell'allegato B), le seguenti misure minime:

— autenticazione informatica;

⁵⁷ S. PARDINI, *Art. 15*, in C. M. BIANCA, F. D. BUSNELLI (a cura di), *Tutela della privacy*, in «Nuove leggi. civ. comm.», 1999, 2-3, II, p. 439.

- adozione di procedure di gestione delle credenziali di autenticazione;
- utilizzazione di un sistema di autorizzazione;
- aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici;
- protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di dati, ad accessi non consentiti e a determinati programmi informatici;
- adozione di procedure per la custodia di copie di sicurezza, il ripristino della disponibilità dei dati e dei sistemi;
- 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».

Con il d.l. 201/2011 è stato abolito l'obbligo di redigere e aggiornare il Documento Programmatico sulla Sicurezza (c.d. DPS).

Inoltre, ai sensi dell'art. 35, «il trattamento di dati personali effettuato senza l'ausilio di strumenti elettronici è consentito solo se sono adottate, nei modi previsti dal disciplinare tecnico contenuto nell'allegato B), le seguenti misure minime:

- aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unità organizzative;
- previsione di procedure per un'adeguata custodia di atti e documenti affidati agli incaricati per lo svolgimento dei relativi compiti;
- 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».

Pertanto, nell'allegato B del cod. priv. sono contenute le norme che stabiliscono le misure minime di sicurezza che devono essere adottate dal titolare, dal responsabile e dagli incaricati per non essere responsabili penalmente *ex art. 169 cod. priv.* L'allegato in oggetto è suddiviso in ventinove punti, nei quali si regolamentano il sistema di autenticazione informatica, il sistema di autorizzazione, le ulteriori misure di sicurezza, il documento programmatico sulla sicurezza, le misure da adottare in caso di trattamento di dati sensibili e giudiziari, nonché quelle da adottare per trattamenti senza l'ausilio di strumenti elettronici.

3.5. Il Garante per la protezione dei dati personali

Con l'emanazione della legge n. 675/96 è stata creata una nuova *authority*, il *Garante per la protezione dei dati personali*, che ha sinora confermato la bontà della scelta legislativa, «conseguendo il non semplice obiettivo di affermare la "cultura" della riservatezza, senza cedimenti o "sterilizzazioni" della legge, e, al contempo, di porsi in un atteggiamento dialogico con i soggetti concretamente chiamati a dare applicazione alla disciplina»⁵⁸.

Alla regolamentazione dell'*authority* in oggetto è dedicato il titolo II della III parte del cod. priv. Riprendendo l'art. 30 comma 2 della legge n. 675/96, l'art. 153 dispone che «il Garante opera in piena autonomia e con indipendenza di giudizio e di valutazione». Esso è un organo collegiale, costituito da quattro componenti, nel cui ambito viene eletto il Presidente, il cui voto prevale in caso di parità. I componenti durano in carica quattro anni e possono essere rieletti solo una volta.

L'art. 154 comma 1 attribuisce al Garante i seguenti *compiti*:

- controllare se i trattamenti sono effettuati nel rispetto della disciplina applicabile e in conformità alla notificazione, anche in caso di loro cessazione;
- esaminare i reclami e le segnalazioni e provvedere sui ricorsi presentati dagli interessati o dalle associazioni che li rappresentano;
- prescrivere anche d'ufficio ai titolari del trattamento le misure necessarie o opportune al fine di

⁵⁸ S. SICA, *D. Lgs. n. 467/01 e «riforma» della privacy: un vulnus al «sistema» della riservatezza*, in «Dir. inf.», 2002, 2, p. 264.

- rendere il trattamento conforme alle disposizioni vigenti;
- vietare anche d'ufficio, in tutto o in parte, il trattamento illecito o non corretto dei dati o disporre il blocco ai sensi dell'art. 143, e di adottare gli altri provvedimenti previsti dalla disciplina applicabile al trattamento dei dati personali;
- promuovere la sottoscrizione di codici di deontologia e buona condotta;
- segnalare al Parlamento e al Governo l'opportunità di interventi normativi richiesti dalla necessità di tutelare i diritti, le libertà fondamentali e la dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali;
- esprimere pareri nei casi previsti;
- curare la conoscenza tra il pubblico della disciplina rilevante in materia di trattamento dei dati personali e delle relative finalità, nonché delle misure di sicurezza dei dati;
- denunciare i fatti configurabili come reati perseguibili d'ufficio, dei quali viene a conoscenza nell'esercizio o a causa delle funzioni;
- tenere il registro dei trattamenti formato sulla base delle notificazioni;
- predisporre annualmente una relazione sull'attività svolta e sullo stato di attuazione del cod. priv., che è trasmessa al Parlamento e al Governo entro il 30 aprile dell'anno successivo a quello cui si riferisce.

La *tutela dell'interessato* è affidata, in primo luogo, al Garante. Ad esso l'interessato può rivolgersi in tre modi. Innanzi tutto, può proporre un *reclamo* circostanziato, per rappresentare una violazione della disciplina rilevante in materia di trattamento di dati personali; può inoltre effettuare una *segnalazione*, se non è possibile presentare un reclamo circostanziato, al fine di sollecitare un controllo da parte del Garante sulla disciplina medesima; infine, può presentare un *ricorso*, se intende far valere gli specifici diritti di cui al citato art. 7.

In quest'ultimo caso il ricorrente può scegliere se rivolgersi, in via alternativa, al Garante od all'*autorità giudiziaria ordinaria*. Vige, in tal caso, il principio per cui *electa una via non datur recursus ad alteram*. Ne consegue che, proposto ricorso all'*authority*, non si può più adire il Tribunale, salvo che per chiedere il risarcimento del danno, per il quale sussiste la competenza esclusiva del giudice togato. Ai sensi dell'art. 152 comma 1, inoltre, «tutte le controversie che riguardano, comunque, l'applicazione delle disposizioni del presente codice, comprese quelle inerenti ai provvedimenti del Garante in materia di protezione dei dati personali o alla loro mancata adozione, sono attribuite all'autorità giudiziaria ordinaria».

Il Garante può richiedere al titolare, al responsabile, all'interessato o a terzi di fornire informazioni e di esibire documenti (art. 157) e può inoltre disporre accessi a banche di dati, archivi o altre ispezioni e verifiche nei luoghi ove si svolge il trattamento o nei quali occorre effettuare rilevazioni comunque utili al controllo del rispetto della disciplina in materia di trattamento dei dati personali (art. 158). Tali accertamenti sono effettuati da personale dell'Ufficio del Garante (ma è possibile avvalersi, se necessario, della collaborazione di altri organi dello Stato) e se devono essere svolti presso dimore private è necessario ottenere l'assenso informato del titolare o del responsabile oppure l'autorizzazione del Presidente del Tribunale territorialmente competente con riferimento al luogo dell'accertamento.

3.6. La responsabilità civile nel codice della privacy

La delicatezza delle informazioni contenute nelle banche dati ha spinto il legislatore a riprodurre nel cod. priv. il testo dell'art. 18 della legge n. 675/96, per cui, ai sensi dell'art. 15 cod. priv., «chiunque cagiona danno ad altri per effetto del trattamento di dati personali è tenuto al risarcimento ai sensi dell'art. 2050 del codice civile», il quale a sua volta dispone che «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». Per l'interpretazione dell'art. 15 è possibile far riferimento alla produzione dottrinale relativa all'art. 18 della legge n. 675/96, poiché, come detto, le due norme coincidono.

In merito si registra una divergenza di opinioni fra chi ritiene che il legislatore abbia qualificato *ipso iure* il trattamento dei dati come attività pericolosa⁵⁹ e chi sostiene invece che tramite il rinvio all'art. 2050 cod. civ. sia stata sancita l'applicabilità del regime relativo alla prova liberatoria prevista in materia di attività pericolose⁶⁰. A sostegno della prima tesi è stato affermato che è possibile considerare pericolosa l'attività di trattamento dei dati personali per sua natura, «in relazione al rischio che essa presenta di ledere i diritti fondamentali dell'interessato»⁶¹; pertanto, il rischio tipico dell'attività di trattamento di dati personali appare essere quello di ledere posizioni particolari, particolarmente qualificate, dell'interessato, rischio che sussiste anche al di fuori dell'ipotesi di trattamento concernente dati sensibili⁶². Nel caso in cui si propenda per questa tesi, la disciplina di cui all'art. 2050 cod. civ. risulterà applicabile solo in caso di lesione di diritti fondamentali dell'interessato, mentre per eventuali altri pregiudizi (come la perdita economica determinata dalla distruzione della banca dati) la norma invocabile sarà l'art. 2043 cod. civ.⁶³; ciò in base alla regola secondo la quale si risponde in base alla disciplina speciale di responsabilità oggettiva per i danni cagionati a causa, e non in occasione, dell'attività pericolosa. Qualora si accetti la seconda teoria, il regime della prova liberatoria *ex art.* 2050 cod. civ. sarà sempre applicabile, anche quindi se il danno non sia collegato alla lesione di un diritto fondamentale⁶⁴. In ogni caso, non si può assolutamente ritenere che la normativa configuri un'ipotesi di semplice inversione dell'onere della prova, poiché ciò comporterebbe la liberazione da responsabilità se colui sul quale grava il suddetto onere riuscisse a dimostrare la mancanza di colpa, ossia di aver agito con prudenza, diligenza, perizia.

La seconda teoria poggia invece sulla considerazione che, secondo la *communis opinio*, l'attività dovrebbe dirsi pericolosa in quanto ne possano derivare danni all'incolumità delle persone; orbene, qualificare l'attività di trattamento di dati personali in termini di pericolosità comporterebbe un'applicazione forse troppo ampia del suddetto attributo; inoltre, rileva giustamente Comandè, l'attività di trattamento di dati personali sarebbe stata esplicitamente classificata come attività pericolosa «senza l'inutile *fiction* del rinvio»⁶⁵.

La presunzione di responsabilità prevista dall'art. 2050 cod. civ. (e quindi anche dall'art. 15 del cod. priv.) può essere vinta solo con una prova alquanto rigorosa, dal momento che il danneggiante deve dimostrare di aver adottato tutte le misure idonee ad evitare il danno. Non è quindi sufficiente la prova negativa di non aver violato alcuna disposizione di legge o di regolamento o comunque le norme di comune prudenza: per liberarsi dalla responsabilità occorre la prova positiva di aver impiegato ogni cura o misura valida ad impedire l'evento dannoso⁶⁶, ragion per cui sovente solo la dimostrazione della dipendenza causale del danno da un caso fortuito (che consiste in un «elemento imprevisto ed imprevedibile che, inserendosi in un determinato processo causale e soverchiando ogni possibilità di resistenza da parte delle forze dell'uomo, rende inevitabile il compiersi

⁵⁹ M. BIN, *Privacy e trattamento dei dati personali: entriamo in Europa*, in «Contr. e impr./Europa», 1997, 2, p. 475; G. BUTTARELLI, *Banche dati e tutela della riservatezza. La privacy nella Società dell'Informazione*, Milano 1997, p. 350; G. DE NOVA, *Trattamento dei dati personali: responsabilità degli intermediari bancari e finanziari*, in «Danno e resp.», 1997, 4, p. 401; S. SICA, *Art. 18*, in E. GIANNANTONIO, M. G. LOSANO, V. ZENO-ZENCOVICH, *Commentario alla legge 31 dicembre 1996, n. 675*, cit.; P. ZIVIZ, *Trattamento dei dati personali e responsabilità civile: il regime previsto dalla l. 675/96*, in «Resp. civ.», 1997, p. 1300.

⁶⁰ F. D. BUSNELLI, *Il "trattamento dei dati personali" nella vicenda dei diritti alla persona: la tutela risarcitoria*, in V. CUFFARO, V. RICCIUTO, V. ZENO-ZENCOVICH (a cura di), *Trattamento dei dati e tutela della persona*, Milano 1998, p. 185; G. COMANDÈ, *Art. 18*, in C. M. BIANCA, F. D. BUSNELLI (a cura di), *Tutela della privacy*, cit., p. 488; V. FRANCESCHELLI, *La tutela della privacy informatica. Problemi e prospettive*, Milano 1998, p. 54; M. FRANZONI, *Dati personali e responsabilità civile*, in «Resp. civ.», 1988, 4-5, p. 903; M. GRANIERI, *Una proposta di lettura sulla tutela risarcitoria nella vicenda del trattamento di dati personali*, in «Danno e resp.», 1998, 3, p. 222; G. VISINTINI, *Trattato breve della responsabilità civile*, Padova 1999, p. 404.

⁶¹ P. ZIVIZ, *op.cit.*

⁶² *Ibid.*

⁶³ *Ivi*, p. 1301.

⁶⁴ *Ibid.*

⁶⁵ G. COMANDÈ, *op. cit.*, p. 488.

⁶⁶ Cass. 29 aprile 1991, n. 4710, in «Mass. foro it.», 1991, c. 397.

dell'evento⁶⁷) o dal fatto esclusivo del danneggiato viene considerata quale prova liberatoria ai sensi dell'art. 2050 cod. civ. In ogni caso, la giurisprudenza è molto rigorosa in questa operazione interpretativa e richiede che il caso fortuito abbia provocato un effetto interruttivo del nesso causale tra il danno e l'attività pericolosa⁶⁸.

Il risarcimento del danno conseguente alla lesione del diritto alla *privacy* può essere sia patrimoniale che non: l'art. 15 comma 2 dispone infatti che il danno non patrimoniale è risarcibile anche nei casi di violazione dell'art. 11, il quale ultimo detta i già ricordati principi qualitativi circa la raccolta e i requisiti dei dati personali, affermando che questi devono essere: a) trattati in modo lecito e secondo correttezza; b) raccolti e registrati per scopi espliciti, determinati e legittimi; c) esatti e se necessario aggiornati; d) pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti e successivamente trattati; e) 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.

Risulta evidente l'importanza di questa norma, perché i principi da essa sanciti, se non rispettati, comportano l'obbligo di risarcire il danno. Essa, pertanto, assume valenza centrale nell'ambito del risarcimento del danno cagionato per effetto del trattamento di dati personali: soprattutto la clausola generale della liceità e correttezza del trattamento ben si presta a sopperire ad eventuali carenze delle lettere b) – e) del medesimo articolo⁶⁹. Dunque la sfera di responsabilità appare tanto vasta, che risulterebbe possibile, in ipotesi, chiedere il risarcimento del danno anche al di fuori di una specifica violazione di legge, purché il trattamento sia avvenuto infrangendo le regole della *lawfulness and correctness*⁷⁰.

3.7. Le sanzioni previste dal codice della privacy

Nel cod. priv. sono previste sia *sanzioni* di carattere amministrativo che illeciti penali. Le prime, irrogate dal Garante (art. 166), consistono nell'omessa o inidonea informativa all'interessato (art. 161), nell'illecita cessione di dati personali e nella violazione dell'art. 84 comma 1 (art. 162), nella illecita conservazione dei dati di traffico (art. 162-bis), nell'omessa o incompleta notificazione (art. 163), nell'omessa informazione o esibizione al Garante (art. 164). Nei casi di cui agli artt. 161, 162 e 164 può essere applicata la sanzione amministrativa accessoria della pubblicazione dell'ordinanza-ingiunzione, per intero o per estratto, in uno o più giornali indicati nel provvedimento che la applica (art. 165).

Gli illeciti penali consistono nel trattamento illecito di dati (art. 167), nella falsità nelle dichiarazioni e notificazioni al Garante (art. 168), nell'omissione delle misure minime di sicurezza (art. 169), nell'inosservanza di provvedimenti del Garante (art. 170), nella violazione degli artt. 113 comma 1 e 114 (art. 171). Alla condanna per ciascuno dei delitti ora citati segue la pena accessoria della pubblicazione della sentenza (art. 172).

⁶⁷ S. MERZ, *Manuale pratico della liquidazione del danno*, Padova 1999, p. 5.

⁶⁸ Cass. 21 novembre 1984, n. 5960, in «Mass. Foro It.», 1984, c. 1176.

⁶⁹ S. SICA, *Danno morale e legge sulla privacy informatica*, cit., p. 283.

⁷⁰ G. VETTORI, *Privacy e diritti dell'interessato*, in «Resp. civ.», 1998, 4–5, p. 898.