SEMINARIO GIURIDICO
DELLA UNIVERSITÀ DI BOLOGNA
CCXLIII

GIANLUIGI FIORIGLIO

# IL DIRITTO ALLA PRIVACY. NUOVE FRONTIERE NELL'ERA DI INTERNET

BUP Bononia University Press

Opera stampata con il contributo di



Bononia University Press
Via Farini 37, 40124 Bologna
tel. (+39) 051 232 882
fax (+39) 051 221 019

www.buponline.com
e-mail: info@buponline.com



ISBN 88-7395-371-5
Impaginazione: Irene Sartini

Stampa: Editografica - Rastignano (BO)

Prima edizione: settembre 2008

# INTRODUZIONE

Il diritto alla privacy costituisce un esempio di come l'evoluzione della regolamentazione di un diritto possa talvolta riuscire ad adattarlo per soddisfare le istanze dei diversi soggetti coinvolti, mentre altre volte finisca per stravolgerlo e sortire l'effetto contrario.

La ricostruzione storica della tutela giurisprudenziale e legislativa mostra, infatti, come si assista ad una progressiva involuzione del diritto alla riservatezza, conseguente ad un'ipertrofia normativa *in subiecta materia* sotto numerosi aspetti, cui fa da contraltare una scarsa attenzione verso profili particolarmente delicati come quello della riservatezza genetica.

Ciò è forse dovuto alla difficoltà di regolamentare una privacy sempre più frammentata in molteplici fattispecie, il cui numero aumenta di pari passo al progresso della ricerca scientifica e tecnologica. Essa, tuttavia, ha un incedere molto più rapido di un diritto che si trova dinanzi alle criticità di una società dell'informazione che annulla le distanze e muta il concetto stesso di tempo. Nel ciberspazio, così, non vi è la successione del giorno e della notte, né si pongono, in linea generale, problemi inerenti la territorialità. Però esso è parte della realtà "materiale" contemporanea, inserita nell'ambito di stati tradizionali già in difficoltà in seguito a fenomeni diversi, fra cui la globalizzazione.

Problemi particolari, così, possono assumere valenze generali e l'individuo, sfornito di strumenti giuridici che consentano di tutela-

re i propri diritti, si trova sovente solo nei meandri di una rete che viene vista da molti stati come una minaccia, tanto che si moltiplicano i tentativi di controllare il flusso informativo che la attraversa.

Tali tentativi, però, non hanno solo carattere pubblico, ma sono spesso posti in essere da quei soggetti privati che controllano i microcosmi che si creano all'interno della realtà digitale oppure gli strumenti utilizzati per accedervi e fruirne.

In tale quadro appare necessario garantire il rispetto del diritto alla riservatezza, sempre più proclamato quale diritto fondamentale eppure sempre più soggetto a violazioni.

Nel presente volume si è scelto di partire dal concetto di privacy quale *right to be let alone*, ripercorrendo i principali eventi, giuridici e fattuali, cui è conseguita la sua attuale e principale concezione quale diritto alla protezione ed al controllo dei propri dati personali. Successivamente sono state analizzate le problematiche che oggi appaiono maggiormente idonee ad incidere negativamente sulla riservatezza individuale e collettiva, studiandola principalmente alla luce della comunicazione globale resa possibile dal ciberspazio nonché delle tecnologie e delle metodologie di controllo individuale e collettivo, che assumono una valenza sempre maggiore in virtù della pervasività dei prodotti "concreti", materiali ed immateriali che siano, dell'informatica.

Di essa sono stati poi analizzati alcuni aspetti specifici di quella importante specificazione costituita dall'informatica medica, il cui sviluppo, se improntato al rispetto di determinati principi e valori etici e giuridici, può contribuire grandemente al miglioramento della vita delle persone nei momenti in cui esse sono più indifese. In tal senso, assume un particolare rilievo la successiva analisi degli aspetti bioetici e giuridici della riservatezza genetica, che costituisce quel nucleo più intimo della persona la cui tutela non può, in linea generale, essere pretermessa.

Nonostante le fattispecie considerate siano per molti aspetti eterogenee, grazie al loro studio e all'analisi degli elementi comuni è comunque possibile giungere ad una considerazione unitaria del diritto alla privacy, che pone in luce la sua estrema importanza quale baluardo a difesa di un uomo che sembra essere sempre più traspa-

rente ed oggetto degli indiscreti sguardi della Società dell'informazione.

Questo volume ha origine dalle attività di ricerca in Informatica Giuridica condotte, in particolar modo, nell'ambito del Centro Interdipartimentale di Ricerca in Storia del diritto, Filosofia e Sociologia del Diritto e Informatica Giuridica (CIRSFID) dell'Università di Bologna. Desidero quindi ringraziare il professor Enrico Pattaro, Direttore del CIRSFID e punto di riferimento per l'informatica giuridica; i professori Giovanni Sartor, Carla Faralli, Daniela Memmo e Cesare Maioli, che mi hanno fatto l'onore di leggere il manoscritto e di fornire preziosi commenti nel corso della sua stesura; la dottoressa Claudia Cevenini, per le sue doti umane e professionali; i miei colleghi del CIRSFID, i dottori Giuseppe Contissa, Rossella Rubino, Migle Laukyte e Alessandro Rocchi.

Desidero ringraziare, poi, i gruppi di ricerca delle Università di Roma "Sapienza" e di Teramo, che mi hanno sempre supportato nello svolgimento della mia attività. In particolare, esprimo la mia gratitudine alla professoressa Teresa Serra e alla professoressa Serenella Armellini, nonché al professor Paolo Savarese e ai dottori Mario Sirimarco, Enrico Graziani e Anna Di Giandomenico.

Un ringraziamento speciale va ai miei genitori e a mio fratello, i quali mi hanno sostenuto in ogni momento, così come hanno fatto, ciascuno a suo modo, Daniela, Giuseppe, Fabrizio e Gerardo.

## Capitolo I

# LA NASCITA, L'EVOLUZIONE E L'INVOLUZIONE DEL DIRITTO ALLA PRIVACY

## 1. *Dal "right to be let alone" alle normative sulla privacy informatica*

Il dibattito sul diritto alla privacy ha assunto, oggi, proporzioni tali e tanto vaste da rendere lecito pensare che esso abbia origini ben lontane nel tempo, anche se è stato compiutamente teorizzato e sistematizzato "solo" nel 1890, anno in cui le prestigiose pagine della «Harvard Law Review» hanno ospitato un saggio intitolato *The Right to Privacy*, scritto da Samuel D. Warren e Louis D. Brandeis[1] per esprimere il bisogno di tutela dell'uomo nei confronti della stampa, che in quel periodo andava aumentando vertiginosamente la propria diffusione e conseguentemente il proprio potere. Nella prospettiva dei due giuristi, il diritto alla privacy viene visto "in negativo", quale *right to be let alone*, conferendo al titolare la facoltà di privare estranei della conoscenza di un determinato nucleo di notizie a lui riferite.

Tuttavia, con l'evoluzione tecnologica e sociale la quantità dei dati personali raccolti da istituzioni pubbliche e soggetti privati è aumentata in maniera vertiginosa, per cui anche lo stesso concetto

[1] S.D. Warren, L.D. Brandeis, *The Right to Privacy*, in *Harvard Law Review*, 1890, 5, pp. 193-220.

di privacy si è maggiormente definito, allargandosi contemporaneamente a un ambito non più personale, ma sociale[2].

Ovviamente, un'effettiva tutela dell'individuo e dei gruppi sociali non può aversi se non mediante una costante opera di adeguamento dell'ordinamento giuridico alle esigenze degli uni e degli altre, che mutano progressivamente. Appare, quindi, naturale che "nuovi" diritti sorgano col passare del tempo, in quanto i vari legislatori creano nuove fattispecie al fine di colmare le lacune che derivano dai cambiamenti politici, economici e sociali.

Per quanto il diritto alla privacy fosse stato riconosciuto a livello internazionale già poco dopo il termine della seconda guerra mondiale[3], l'emanazione delle normative europee ed internazionali in materia ha ricevuto un impulso fondamentale con la creazione e la diffusione delle banche dati informatiche, tanto che per lungo tempo si è parlato più di privacy informatica che di privacy *tout court*. La progressiva crescita del numero di dati personali e le sem-

---

[2] «Il mutamento di motivazione fa cambiare significato all'invocazione della privacy: nel primo caso, rifiutandosi le informazioni necessarie ai programmi d'intervento sociale, la privacy si presenta come lo strumento per il consolidamento dei privilegi di un gruppo; nell'altro serve a reagire contro l'autoritarismo e contro una politica di discriminazioni basate sulle opinioni politiche. La privacy, in tal modo, diventa un modo per promuovere la parità di trattamento fra i cittadini, per realizzare l'eguaglianza e non per custodire il privilegio, spezzando il suo nesso di identificazione con la classe borghese» (S. Rodotà, *La privacy tra individuo e collettività*, in *Politica del diritto*, 1974, 3, p. 551). Sulle prime evoluzioni del diritto alla privacy cfr. W.L. Prosser, *Privacy [a legal analysis]*, in *California Law Review*, 1960, 48, pp. 383-423.

[3] Ai sensi dell'art. 12 della *Dichiarazione universale dei diritti dell'uomo*, proclamata il 10 dicembre 1948 dall'Assemblea Generale delle Nazioni Unite, «nessun individuo potrà essere sottoposto ad interferenze arbitrarie nella sua vita privata, nella sua famiglia, nella sua casa, nella sua corrispondenza, né a lesione del suo onore e della sua reputazione. Ogni individuo ha diritto ad essere tutelato dalla legge contro tali interferenze o lesioni». Inoltre, l'art. 8 della "Convenzione per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali", firmata a Roma il 4 novembre 1950, dispone che «ogni persona ha diritto al rispetto della sua vita privata e familiare, del suo domicilio e della sua corrispondenza. Non può esservi ingerenza di una autorità pubblica nell'esercizio di tale diritto a meno che tale ingerenza sia prevista dalla legge e costituisca una misura che, in una società democratica, è necessaria per la sicurezza nazionale, per la pubblica sicurezza, per il benessere economico del paese, per la difesa dell'ordine e per la prevenzione dei reati, per la protezione della salute o della morale, o per la protezione dei diritti e delle libertà altrui».

pre maggiori possibilità di un loro trattamento anche incrociato mediante l'utilizzo degli strumenti informatici hanno infatti dato vita all'esigenza di proteggerli e di stabilire dei limiti non solo alla loro acquisizione, ma anche al loro trattamento una volta acquisiti.

Le normative in materia sono tutte relativamente recenti[4], dal momento che le maggiori questioni pratiche sono state poste dal progresso in ambito informatico e che le relative leggi sono state emanate proprio allo scopo di approntare una tutela dei dati personali.

In ambito europeo, il quadro legislativo è stato abbastanza variegato sino all'emanazione della direttiva n. 95/46/CE, che ha consentito di uniformare, quanto meno a livello generale, la normativa degli stati membri dell'Unione Europea[5]. Le singole legislazioni, infatti, presentano differenze più o meno marcate, pur inserendosi nel quadro generale delineato dal legislatore comunitario[6]. Ciò nonostante, come è stato rilevato dalla Commissione europea, gli stati membri in alcuni casi non hanno recepito importanti disposizioni della direttiva, mentre in altri si sono allontanati da essa o sono an-

---

[4] La Svezia è stata la prima nazione a promulgare una legge statale in materia: è la c.d. *Datalag*, emanata l'11 maggio 1973 e modificata nel 1979 e nel 1982. La suddetta legge ha costituito il modello al quale paesi sia europei che extra-europei si sono ispirati nell'attività di normazione della privacy informatica. La Svezia è stata inoltre la prima nazione a prevedere un generale diritto di accesso ai documenti statali: il *Freedom of the Press Act (Tryckfrihetsfororordning*) risale addirittura al 1766. La legge del 1973 è stata abrogata dalla legge 24 ottobre 1998, n. 204 (*Personal Data Act*), che costituisce anche il recepimento della direttiva 95/46/CE. In Germania, tuttavia, già nell'ottobre del 1970, nei due *Länder* dell'Assia e della Baviera erano state approvate due leggi in materia di protezione dei dati personali. La relativa normativa a livello federale risale invece al 27 gennaio 1977 ed è denominata *Bundesdatenschutzgesetz* (*BDSG*) *(Federal Data Protection Act*).

[5] Sul punto bisogna menzionare la Convenzione di Strasburgo del 28 gennaio 1981, resa esecutiva in Italia dalla legge 21 febbraio 1989, n. 98, e volta ad assicurare la «protezione delle persone rispetto al trattamento automatizzato di dati di carattere personale», nonché l'Accordo di Schengen del 14 giugno 1985, ratificato con la legge 30 settembre 1943, n. 388, che disciplina la libera circolazione delle persone e delle merci per abolire i controlli frontalieri; ciò comporta la predisposizione di un sistema comune di informazione fra polizia, dogane e autorità giudiziarie dei paesi aderenti.

[6] Sul sito della Commissione Europea è possibile reperire un quadro d'insieme della situazione europea in materia (http://ec.europa.eu/justice_home/fsj/privacy/law/implementation_en.htm).

dati al di là del margine di manovra a loro disposizione. Alcuni di essi hanno comunque riconosciuto l'esistenza delle loro lacune legislative e si sono impegnati ad introdurre le necessarie modifiche[7].

In Europa, dunque, il quadro normativo risulta abbastanza armonico in virtù del fatto che gli stati membri hanno ormai adempiuto ai principali obblighi imposti dalla direttiva n. 95/46/CE, seppur con le differenze, appena menzionate, evidenziate dalla Commissione europea. Oltretutto, la tutela del diritto alla protezione dei dati personali è stata affermata anche nella "Carta dei diritti fondamentali dell'Unione Europea", sottoscritta e proclamata a Nizza il 7 dicembre 2000. Più specificatamente, gli artt. 7 e 8 dispongono che «ogni individuo ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e delle sue comunicazioni» e che «ogni individuo ha diritto alla protezione dei dati di carattere personale che lo riguardano. Tali dati devono essere trattati secondo il principio di lealtà, per finalità determinate e in base al consenso della persona interessata o a un altro fondamento legittimo previsto dalla legge. Ogni individuo ha il diritto di accedere ai dati raccolti che lo riguardano e di ottenerne la rettifica. Il rispetto di tali regole è soggetto al controllo di un'autorità indipendente». Le suddette norme sono state poi integrate (anche se è stata operata la sostituzione del termine *individuo* con quello di *persona*) nel "Trattato che istituisce una Costituzione per l'Europa", del quale costituiscono gli articoli II-67 e II-68. Come è noto, però, la Costituzione europea non è attualmente in vigore in quanto non è stata ratificata da tutti gli stati membri[8].

Appare chiaro, pertanto, che l'Europa ha sempre dimostrato una certa attenzione verso la tutela della riservatezza e oggi il quadro normativo europeo appare ben più completo rispetto a quello statunitense, nonostante, come si è visto, il diritto alla privacy sia

---

[7] Comunicazione della Commissione al Parlamento Europeo e al Consiglio sul seguito dato al programma di lavoro per una migliore applicazione della direttiva sulla protezione dei dati, COM (2007) 87, p. 6.

[8] Sulla Costituzione europea cfr., fra gli altri, S. Gambino, *Trattato che adotta una Costituzione per l'Europa. Costituzioni nazionali, diritti fondamentali*, Giuffré, Milano, 2006; G. Marazzita, *La Costituzione europea*, Laterza, Roma-Bari, 2006; G. Morbidelli, F. Donati, *Una costituzione per l'Unione Europea*, Giappichelli, Torino, 2006.

stato teorizzato proprio oltreoceano. Più specificatamente, negli Stati Uniti sono stati emanati vari atti a livello di legislazione federale: il *Freedom of Infomation Act* (*FOIA*) del 1966 e il *Privacy Act* del 31 dicembre 1974, modificato dal *Privacy Protection Act* del 13 ottobre 1980. Il *FOIA* prevede un generale diritto di accesso ai dati detenuti dal Governo federale; nel *Privacy Act* il diritto di accesso viene limitato ai cittadini statunitensi o agli stranieri ivi legalmente residenti. I singoli Stati regolano le banche dati delle amministrazioni statali con proprie norme, generalmente ispirate al *Privacy Act*. Tutte queste normative si occupano del profilo pubblicistico della diritto alla riservatezza, ma sul piano privatistico è nella giurisprudenza che bisogna individuare i profili di tutela del diritto alla privacy[9], che per l'ordinamento rappresenta un vero e proprio baluardo a difesa della libertà, tanto che si fa riferimento ad esso in numerosi casi: «aborto, contraccezione, divorzio, libertà sessuale, autonomia educativa, attività di polizia, libertà terapeutica, invasione della coscienza da parte di tv e *mass-media*, segretezza finanziaria, libertà religiosa, pornografia, consumo di droghe, libertà di associazione e persino critica dello stato assistenziale»[10]. In Italia si è giunti al riconoscimento del diritto alla riservatezza solo dopo un lungo dibattito dottrinale[11] e

[9] La letteratura in materia è vastissima; si segnalano comunque alcuni testi, oltre ai già citati articoli di Warren e Brandeis nonché di Prosser: N. Lugaresi, *Internet, privacy e pubblici poteri negli Stati Uniti*, Giuffré, Milano, 2000; D.J. Solove, M. Rotenberg, P.M. Schwartz, *Information Privacy Law*, Aspen, New York, 2006; A.F. Westin, *Privacy and freedom*, Atheneum, New York, 1967.

[10] S. Scoglio, *Privacy. Diritto, filosofia, storia*, Editori Riuniti, Roma, 1994, p. 17.

[11] Il punto centrale di discussione era costituito, in particolare, dal raffronto fra le teorie monista e pluralista del diritto della personalità. Nel primo caso, si sostiene che esiste un unico e generale diritto della personalità, che comprende anche diritti come il diritto alla privacy; nel secondo, si afferma che esistono più diritti della personalità, i quali devono essere disciplinati dalla legge. Conseguenze della tesi monista sono il riconoscimento dell'atipicità degli interessi della persona giuridicamente protetti e l'interpretazione aperta dell'art. 2 Cost. L'orientamento pluralista, nella versione più radicale, appare restrittivo, essendo rigidamente imperniato sulla tipicità degli interessi della persona meritevoli di tutela e su una concezione "chiusa" dell'art. 2 Cost. (così F. Piraino, *Il codice della privacy e la tecnica del bilanciamento di interessi*, in R. Panetta [a cura di], *Libera circolazione e protezione dei dati personali*, Giuffré, Milano, 2006, I, pp. 697-698). Come ha affermato Giuseppe Santaniello, «la soluzione della discussione sulla personalità unica o plurima si risolve nel senso che la personalità del soggetto è unica, mentre

giurisprudenziale[12], quando la Corte di Cassazione ne ha affermato l'esistenza nell'ordinamento giuridico italiano[13]. Più specificatamente, esso «consiste 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»[14].

L'analisi della definizione data dalla Suprema Corte evidenzia il potenziale carattere di conflittualità del diritto alla privacy con altri diritti i quali siano espressione di interessi pubblici che nel bilanciamento di interessi vadano ritenuti prevalenti. Gli interessi pubblici cui fa riferimento la sentenza del Giudice di legittimità costituiscono, in tale definizione, una sorta di «clausola generale», che si rende necessaria per far fronte ai casi in cui la riservatezza deve cedere dinanzi a pericoli attuali e concreti. Questa operazione, che deve necessariamente essere lasciata all'interprete e che deve essere svolta per ogni caso concreto, richiede una grande accortezza, in quanto il riconoscimento del diritto alla privacy e la sua tutela effettiva costituiscono degli scudi che difendono la dignità della persona.

---

invece sono plurime le sue manifestazioni all'esterno, che il legislatore può far o meno diventare oggetto di specifici diritti soggettivi» (G. Santaniello, *I fattori evolutivi della codificazione concernente i dati personali*, in http://www.interlex.com/675/santaniello11.htm). Sui diritti della personalità cfr. (fra gli altri): G. Alpa, G. Resta, *Le persone fisiche e i diritti della personalità*, UTET, Torino, 2006; G. Giacobbe, G. Giuffrida, *I diritti della personalità*, UTET, Torino, 2000; A. Proto Pisani, *La tutela giurisdizionale dei diritti della personalità: strumenti e tecniche di tutela*, in *Foro italiano*, 1990, V, cc. 1-19; V. Zeno-Zencovich, *I diritti della personalità dopo la legge sulla tutela dei dati personali*, in *Studium Juris*, 1997, 5, pp. 466-469; V. Zeno-Zencovich, voce *Personalità (diritti della)*, in *Digesto delle discipline privatistiche*, sezione civile, Torino, 1997, XIII, pp. 430-444.

[12] In merito hanno assunto una particolare rilevanza i casi Caruso (Trib. Roma 14 settembre 1953, in *Foro italiano*, 1954, I, c. 115) e Petacci (Cass. 20 aprile 1963, n. 990, in *Foro italiano*, 1963, I, c. 879).

[13] Cass. 27 maggio 1975, n. 2129, in *Foro italiano*, 1976, I, c. 2895.

[14] Ivi, c. 2905; le norme che la Cassazione ritiene fondanti il diritto alla riservatezza sono da individuarsi nelle seguenti disposizioni: artt. 2, 3, 14, 15, 27, 29, 41 Cost.; art. 1 L. 98/74; artt. 5, 6-10, 2105, 2622 cod. civ.; artt. 21, 24, 93 l. aut.; artt. 595 c. 2, 614, 616 cod. pen.; art. 48 l. fall.; art. 8 st. lav.

In questo difficile quadro, caratterizzato sia da contrasti dottrinali che giurisprudenziali, il legislatore italiano non ha certo brillato per prontezza: negli anni Settanta, infatti, il suo unico intervento è consistito nell'emanazione della legge 20 maggio 1970, n. 300 (il c.d. Statuto dei lavoratori), che disciplina alcuni profili del diritto alla riservatezza nell'ambito del rapporto di lavoro. Assumono, così, un particolare rilievo gli artt. 4 (che vieta l'uso di impianti audiovisivi e di altre apparecchiature per finalità di controllo a distanza dell'attività dei lavoratori), 5 (che vieta gli accertamenti da parte del datore di lavoro sulla idoneità e sulla infermità per malattia o infortunio del lavoratore dipendente), 6 (che vieta, in linea generale, le visite di controllo sul lavoratore) e 8 (che vieta al datore di lavoro, sia ai fini dell'assunzione sia 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).

Tuttavia, a parte alcuni disegni di legge mai approvati dal Parlamento[15] ed alla legge 1° aprile 1981, n. 121, sull'amministrazione della pubblica sicurezza (oggi parzialmente abrogata)[16], la materia che ci occupa non è stata regolamentata sino all'emanazione della legge 31 dicembre 1996, n. 675 (la c.d. «legge sulla privacy»). Al silenzio legislativo di quegli anni hanno continuato comunque a contrapporsi le intense attività interpretative e propositive di dottrina[17] e giurisprudenza, le quali hanno dovuto occuparsi dello spinoso

---

[15] Su di essi cfr., fra gli altri, M.G. Losano, *I progetti di legge italiani sulla riservatezza dei dati personali*, in *DRT. Il diritto delle radiodiffusioni e delle telecomunicazioni*, 1983, 2, pp. 275-283.

[16] Ai sensi di tale legge ogni ente, impresa od associazione che deteneva archivi magnetici per l'inserimento di dati od informazioni di cittadini, di ogni natura, avrebbe dovuto 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 poteva chiederne al tribunale la cancellazione o l'integrazione.

[17] Cfr., fra gli altri, G. Aiello, *Diritto di cronaca e diritto alla riservatezza*, nota a Pret. Firenze 3 marzo 1986, in *Giustizia civile*, 1986, 9, pp. 2285-2287; V. Frosini, *La protezione della riservatezza nella società informatica*, in *Informatica e diritto*, 1981, 1, pp. 5-14; G. Giacobbe, *Il diritto alla riservatezza nella prospettiva degli strumenti di tutela*, in *DRT. Il diritto delle radiodiffusioni e delle*

problema del rapporto tra la tutela della vita privata dell'individuo e il diritto costituzionalmente garantito di libertà di manifestazione del pensiero. Al contempo, il progredire delle concezioni in materia di rispetto della vita privata ha portato all'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'attualità[18].

Bisogna tuttavia considerare che, sino a pochi anni fa, quando la diffusione delle reti telematiche e degli elaboratori elettronici non aveva assunto le proporzioni odierne, il maggior rischio per la privacy era probabilmente costituito dall'illegittimo esercizio del diritto di cronaca, con il quale, infatti, il diritto alla riservatezza, per sua stessa natura, poteva e può facilmente entrare in conflitto[19].

Prima della legge n. 675/96, la riservatezza è stata tutelata facendo sovente riferimento all'art. 2 Cost., ai sensi del quale «la Repubblica riconosce e garantisce i diritti inviolabili dell'uomo, sia come singolo sia nelle formazioni sociali ove si svolge la sua personalità, e richiede l'adempimento dei doveri inderogabili di solidarietà politica, economica e sociale».

Detta norma ha avuto importanza fondamentale nel riconoscimento di nuovi diritti che consentono di tutelare quei valori fondamentali della persona umana che, in virtù del loro carattere, non possono rimanere sforniti di protezione. Proprio l'art. 2 Cost., interpretato cogliendo quei mutamenti che inesorabilmente sono avvenuti e continuamente avvengono nella società, ha costituito la base per

---

*telecomunicazioni*, 1982, 2, pp. 277-314; R. Zaccaria, *Diritto all'informazione e riservatezza*, in *DRT. Il diritto delle radiodiffusioni e delle telecomunicazioni*, 1982, 3, pp. 527-550; P. Zagnoni, *Sulla tutela penale del diritto alla riservatezza*, in *Rivista italiana di diritto e procedura penale*, 1982, 3, pp. 970-1003.

[18] G. Giacobbe, *Il diritto alla riservatezza: da diritto di elaborazione giurisprudenziale a diritto codificato*, in *Iustitia*, 1999, 2, p. 112.

[19] Ivi, p. 111. La Suprema Corte si è occupata della suddetta problematica nel 1984 con una importante sentenza, nella quale ha stilato il c.d. decalogo dei giornalisti ed ha definito le condizioni al verificarsi delle quali il diritto di cronaca può prevalere sul diritto alla riservatezza (Cass. 18 ottobre 1984, n. 5259, in *Il diritto dell'informazione e dell'informatica*, 1985, 1, p. 143, con nota di S. Fois, G. Giacobbe, F. Morozzo Della Rocca).

il riconoscimento di un diritto fondamentale della persona umana quale la riservatezza.

Questo diritto, oltretutto, ha 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 autodeterminarsi[20].

## 2. *Dalla legge n. 675/96 al Codice della privacy*

Come si è accennato, il diritto alla riservatezza ha trovato una vera e propria tutela legislativa nell'ordinamento giuridico italiano solo con l'approvazione della legge n. 675/96, emanata per ottemperare agli obblighi imposti dall'Accordo di Schengen del 1985 e dalla direttiva n. 95/46/CE. Bisogna considerare che detta legge non tutelava il diritto alla riservatezza in tutte le sue sfumature, bensì lo specifico aspetto della protezione dei dati personali, che, comunque, sembra oggi rappresentare uno dei profili più importanti del diritto alla privacy.

Il testo della legge n. 675/96 era chiaramente espressione di un frettoloso adattamento della normativa europea, tanto da essere poi oggetto di numerosi interventi di ritocco ed aggiornamento[21], ma questo provvedimento ha comunque suscitato un notevole interes-

---

[20] M. Aimo, *I "lavoratori di vetro": regole di trattamento e meccanismi di tutela dei dati personali*, in *Rivista giuridica e della previdenza sociale*, 2002, 1, p. 48.

[21] La legge n. 675/96 è stata infatti 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.

se nella comunità scientifica[22] ed ha colmato una lunga lacuna legislativa[23].

Successivamente alla sua emanazione, la dottrina si è interrogata sulla seguente questione: la legge n. 675/96 si occupa primariamente della disciplina del trattamento dei dati personali o, piuttosto, si pone il primo obiettivo della tutela della personalità sotto gli aspetti dei diritti alla riservatezza e all'identità personale? Nel primo senso, oltre il dato letterale dell'art. 1, vi era la considerazione che le normative sui dati personali sono nate a causa della diffusione degli elaboratori elettronici, grazie ai quali è possibile il trattamento incrociato e istantaneo di un enorme numero di dati, mettendo in pericolo la personalità e i relativi diritti. In senso opposto, si prendono in riferimento sia l'amplissima estensione della nozione di dato personale, che comprende qualsiasi informazione identificativa della persona, sia il ruolo della legge n. 675/96 quale generale "statuto dell'informazione".

Detta legge è stata poi in gran parte trasfusa nel d.lgs. 30 giugno 2003, n. 196, ossia il "Codice in materia di protezione dei dati personali", più brevemente detto "Codice della privacy" (d'ora in poi cod. priv.). In dottrina si è osservato che «l'indubbia duttilità del codice non vale, tuttavia, ad emendarne alcuni eccessi né attenua l'accusa di analiticità che investe larga parte del testo e che si appunta

---

[22] Sulla legge n. 675/96 cfr., fra gli altri, G. Arcudi, V. Poli, *Il diritto alla riservatezza*, Ipsoa, Milano, 2000; C.M. Bianca (a cura di), *Tutela della privacy*, in *Le nuove leggi civili commentate*, 1999, 2-3; G. Buttarelli, *Banche dati e tutela della riservatezza. La privacy nella Società dell'Informazione*, Giuffré, Milano, 1997; V. Cuffaro, V. Ricciuto, *La disciplina del trattamento di dati personali*, Giappichelli, Torino, 1997; V. Cuffaro, V. Ricciuto, V. Zeno-Zencovich (a cura di), *Trattamento dei dati e tutela della persona*, Giuffré, Milano, 1998; E. Giannantonio, M.G. Losano, V. Zeno-Zencovich (a cura di), *Commentario alla legge 31 dicembre 1996, n. 675*, Cedam, Padova, 1997; Ri. Imperiali, Ro. Imperiali, *La tutela dei dati personali*, Il sole 24 ore, Milano, 1997; M.G. Losano (a cura di), *La legge italiana sulla privacy. Un bilancio dei primi cinque anni*, Laterza, Roma-Bari, 2001; M. Maglio, *La tutela dei dati personali*, Simone, Napoli, 1999; T. Minella, *La privacy*, Simone, Napoli, 2001.

[23] V. Zeno-Zencovich, *Una lettura comparatistica della l. n. 675/96 sul trattamento dei dati personali*, in *Rivista trimestrale di diritto e procedura civile*, 1998, 3, p. 737.

sull'attenzione quasi maniacale per il dettaglio e sulla struttura pesante e farraginosa»[24].

Il codice, entrato in vigore il 1° gennaio 2004, è diviso in tre parti: nella prima sono contenute le disposizioni generali, nella seconda quelle relative a specifici settori, mentre nella terza trovano posto le norme relative alle forme di tutela, alle sanzioni e all'ufficio del Garante per la protezione dei dati personali (d'ora in poi Garante). Esso costituisce, inoltre, il recepimento, oltre che di gran parte della legge n. 675/96 e delle direttive n. 96/45/CE e n. 2002/58/CE, anche delle pronunce e dei pareri emanati del Garante per la protezione dei dati personali[25].

Le norme del cod. priv. possono, inoltre, essere integrate dalle disposizioni contenute nei codici di deontologia e buona condotta: «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. […] Il rispetto delle disposizioni contenute nei codici di cui al comma 1 costituisce condizione essenziale per la liceità e corret-

---

[24] F. Piraino, *Il codice della privacy e la tecnica del bilanciamento di interessi*, cit., p. 696. Altra dottrina osserva che il cod. priv. – «che in realtà non è un vero e proprio codice organico, ma un assemblaggio di varie disposizioni normative – ricorda l'immagine di un prisma che, dalle poliedriche sfaccettature, scompone e ricompone la stessa immagine con differenti angolazioni e prospettive» (A. Zucchetti, *Privacy*, Giuffré, Milano, 2005, p. 11).

[25] Sul cod. priv. cfr. Aa.Vv., *Codice della privacy*, Giuffré, Milano, 2004; R. Acciai (a cura di), *Il diritto alla protezione dei dati personali*, Maggioli, Santarcangelo di Romagna, 2004; C.M. Bianca, F.D. Busnelli (a cura di), *La protezione dei dati personali. Commentario al D.lgs. 30 giugno 2003, n. 196 (Codice della privacy)*, Cedam, Padova, 2007; V. Cuffaro, R. D'Orazio, V. Ricciuto (a cura di), *Il Codice del trattamento dei dati personali*, Giappichelli, Torino, 2007; M. De Giorgi, A. Lisi, *Guida al codice della privacy: la protezione dei dati personali alla luce del D.Lgs. 196/2003*, Simone, Napoli, 2004; G. Elli, R. Zallone, *Il nuovo Codice della privacy (commento al D.lgs. 30 giugno 2003, n. 196)*, Giappichelli, Torino, 2004; Ri. Imperiali, Ro. Imperiali, *Codice della privacy. Commento alla normativa sulla protezione dei dati personali*, Milano, 2005; J. Monducci, G. Sartor (a cura di), *Il codice in materia di protezione dei dati personali*, Cedam, Padova, 2004.

tezza del trattamento dei dati personali effettuato da soggetti privati e pubblici» (art. 12 cod. priv.).

Secondo autorevole dottrina, i codici di deontologia e buona condotta «rappresentano una nuova area della strumentazione normativa e una nuova articolazione del sistema delle fonti di produzione del diritto. La flessibilità che li caratterizza conferisce loro il grande vantaggio di poter essere agevolmente modificati, poiché ogni eventuale cambiamento e integrazione delle regole non richiede i tempi lunghi di un complicato procedimento legislativo di riforma; e pertanto sono particolarmente idonei a disciplinare anche materie attraversate da una forte dinamica innovativa come quella delle comunicazioni *on line* e delle incessanti innovazioni tecnologiche»[26].

Altra dottrina, però, evidenzia le storture di un simile sistema, sia perché i destinatari di alcune disposizioni potrebbero trovarsi nella condizione di intervenire *a priori* su una parte non irrilevante delle norme alle quali saranno assoggettati e sia perché sarebbe necessario «interrogarsi anche sulle questioni relative all'applicabilità dei codici stessi a chi non li ha sottoscritti. Se, infatti, il codice deontologico vincolasse soltanto gli aderenti allora si creerebbe una inaccettabile «doppia misura» della responsabilità penale. Che vedrebbe favoriti (o penalizzati) coloro che non accettano di conformarsi allo stato di fatto. Se, al contrario, il codice deontologico avesse validità *erga omnes* allora non si capirebbe la ragione del garantire a un gruppo ristretto di aziende private una vera e propria potestà legislativa in materia penale. Creando, ancora una volta, disparità di trattamento e, con buona probabilità, una serio sconvolgimento di quei principi penalistici che, fino a oggi, sembravano oramai *jus receptum*»[27].

Tanto premesso, bisogna evidenziare che il cod. priv. esprime la tendenza a dare sempre maggiore importanza a quello specifico aspetto del diritto alla riservatezza consistente nella protezione dei

---

[26] G. Santaniello, *Le nuove garanzie nell'era del diritto alla protezione dei dati personali*, in http://www.interlex.it/675/santaniello9.htm.

[27] A. Monti, *Codici deontologici: se chi ruba i dati può scrivere le regole*, in http://www.interlex.it/675/amonti68.htm.

dati personali, che, oltretutto, costituisce «ormai uno degli aspetti più significativi della libertà delle persone»[28].

Il cod. priv. si apre, infatti, con una importante disposizione: «chiunque ha diritto alla protezione dei dati personali che lo riguardano» (art. 1), sancendo finalmente in maniera chiara ed esplicita un principio già desumibile in via implicita[29]. L'ambito di applicazione di questa norma appare vastissimo, poiché il diritto alla protezione dei dati personali, sia per la sua natura di diritto della personalità e sia in virtù dell'utilizzo del termine "chiunque", risulta attribuito a tutte le persone, indipendentemente dalla cittadinanza e dalla residenza[30].

In dottrina si è evidenziato che, nonostante l'indubbio valore giuridico di tale diritto, esso deve tuttavia fare i conti con le tante realtà che caratterizzano l'ambito della protezione dei dati personali, dal momento che si è fatta sempre più intensa la pressione per utilizzare qualsiasi dato personale a fini di sicurezza interna ed internazionale. A tale fattore si accompagnano, inoltre, la resistenza di diversi settori della pubblica amministrazione e la progressiva ed inesorabile innovazione scientifica e tecnologica, che ha reso sempre più complicato garantire un adeguato livello di tutela della riservatezza individuale[31].

Del resto, proprio la consapevolezza dei rischi per la privacy conseguenti alla sempre maggiore diffusione dei sistemi informatici ha probabilmente ispirato la redazione dell'art. 3 cod. priv., che sancisce il principio di necessità nel trattamento dei dati personali. Secondo autorevole dottrina, più che di principio di necessità sarebbe stato più corretto parlare di «principio della riduzione al minimo

---

[28] S. Rodotà, *Trasformazioni del corpo*, in *Politica del diritto*, 2006, 1, p. 11.

[29] «La proclamazione del diritto alla protezione dei dati personali costituisce una novità di assoluto rilievo e conferisce il giusto risalto ad un'espressione breviloquia che designa il complesso dei poteri e delle forme di tutela riconosciuti al soggetto di cui si procede a trattare le informazioni di carattere personale» (F. Piraino, *Il codice della privacy e la tecnica del bilanciamento di interessi*, cit., p. 707).

[30] A. Bardusco, *Articolo 1 (Diritto alla protezione dei dati personali)*, in Aa.Vv., *Codice della privacy*, Giuffré, Milano, 2004, p. 18.

[31] S. Kirschner, *Il codice della privacy, fra tradizione e innovazione*, in R. Panetta (a cura di), *Libera circolazione e protezione dei dati personali*, cit., I, pp. 8-9.

dell'utilizzazione dei dati personali e dei dati identificativi»[32]. Ad ogni modo, per rispettarlo 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 anonimi[33] od opportune modalità che permettano di identificare l'interessato solo in caso di necessità». Il fine della norma è «controllare la circolazione dei dati personali in maniera più efficiente, limitando il pericolo di intrusione esterna al minimo indispensabile e impedendo il reperimento di informazioni sulla vita dell'utente non necessarie con gli scopi dichiarati o in contrasto con le finalità della raccolta»[34].

Oltretutto, si consideri che il medesimo codice «garantisce che il trattamento dei dati personali si svolga nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali» (art. 2 cod. priv.).

## 3. *Aspetti generali del Codice della privacy*

Il cod. priv., come si è detto, è un testo molto complesso e lungo, per cui una sua analisi completa non è possibile in questa sede. Ciò nondimeno, è opportuno tratteggiarne i profili generali maggiormente rilevanti al duplice scopo di rendere più agevole la comprensione delle specifiche tematiche affrontate nel prosieguo del presente volume e di valutare come alcuni profili del diritto alla privacy siano stati positivizzati dal legislatore italiano.

In tal senso, punto di partenza è, intuitivamente, la nozione di "dato personale". Esso consiste in «qualunque informazione relati-

---

[32] V. Italia, *Articolo 3 (Principio di necessità nel trattamento dei dati)*, in Aa.Vv., *Codice della privacy*, cit., p. 40.

[33] 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, cod. priv.).

[34] G. Spoto, *I diritti dei consumatori*, in R. Panetta (a cura di), *Libera circolazione e protezione dei dati personali*, cit., I, p. 393.

va a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale» (art. 4, comma 1, lett. b)[35]. Il legislatore, dunque, non ha operato alcuna distinzione circa la tipologia di dato personale ed ha inoltre scelto di tutelare anche le persone giuridiche, ampliando quindi la sfera di tutela rispetto alla direttiva n. 95/46/CE, nella quale si fa esclusivamente riferimento alle persone fisiche (art. 2, lett. a, dir. n. 95/46/CE).

La suddetta nozione «è caratterizzata da un ampio contenuto che nella normativa in esame assume diverse sfumature a seconda della sua natura o del suo rapporto diretto con l'interessato»[36], 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, cod. priv.). La nozione di interessato, dunque, è vastissima e ciò è coerente con la volontà, già esplicitata agli artt. 1 e 4, comma 1, lett. b, cod. priv., di proteggere i dati personali riferiti a qualsiasi soggetto (sia esso persona fisica o giuridica, ente o associazione).

Gli altri soggetti del cod. priv. sono il titolare, il responsabile e gli incaricati. In particolare, il titolare 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, cod. priv.); il responsabile è invece il soggetto preposto dal titolare al trattamento dei dati personali (art. 4, comma 1, lett. g, cod. priv.). Come il titolare, anche il responsabile non deve necessariamente essere una persona fisica, ma può essere una persona giuridica, una pubblica amministrazione o qualsiasi altro ente, associazione od organismo. Gli incaricati, in-

---

[35] L'interpretazione del concetto di identificabilità viene agevolata dal considerando n. 26 della direttiva 95/46/CE, nel quale si fa riferimento alla «ragionevolezza»: «per determinare se una persona è identificabile, è opportuno prendere in considerazione l'insieme dei mezzi che possono essere ragionevolmente utilizzati dal responsabile del trattamento o da altri per identificare detta persona».

[36] S. Kirschner, *Il codice della privacy, fra tradizione e innovazione*, cit., p. 20.

vece, sono «le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile» (art. 4, comma 1, lett. h, cod. priv.).

Nell'ambito dei dati personali bisogna distinguere i "dati sensibili", ossia 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, cod. priv.). Essi, secondo una definizione oramai di uso comune, costituiscono il "nucleo duro" della riservatezza, per cui, rispetto ai dato "normali", il loro trattamento è sottoposto a regole più severe.

In linea generale, 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» (art. 4, comma 1, lett. a, cod. priv.). Semplificando, una qualsiasi operazione svolta su dati personali costituisce un "trattamento" ai fini della normativa vigente.

Tuttavia, prima di procedere al trattamento dei dati è necessario fornire l'informativa al soggetto i cui dati potranno essere oggetto di trattamento. Queste informazioni possono essere rese oralmente o per iscritto e, ai sensi dell'art. 13 cod. priv. 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 cod. priv.: mediante il loro esercizio il titolare può controllare, in senso lato, i propri dati personali[37]);

– gli estremi identificativi del titolare e, se designati, del responsabile e del rappresentante nel territorio dello Stato.

Una corretta informativa è, chiaramente, fondamentale per assicurare un consenso libero e consapevole da parte dell'interessa-

[37] 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 (art. 7, comma 1, cod. priv.); 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 nel territorio dello Stato, dei soggetti o delle categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in una delle suddette qualità (art. 7, comma 2, cod. priv.); 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; l'attestazione che le suddette operazioni sono state portate a conoscenza di coloro ai quali i dati sono stati comunicati o diffusi, a meno che tale adempimento sia impossibile o comporti un impiego di mezzi manifestamente sproporzionato rispetto al diritto tutelato (art. 7, comma 3, cod. priv.). Infine, l'interessato ha diritto di opporsi, in tutto o in parte: per motivi legittimi al trattamento dei dati personali che lo riguardano, ancorché pertinenti allo scopo della raccolta; 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 (art. 7, comma 4, cod. priv.).

In linea generale, fatte salve le eccezioni di cui all'art. 8, comma 2, cod. priv., i diritti appena menzionati 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. 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. Il riscontro, salvo specifica richiesta, 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 cod. priv.). 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.

to. Il consenso è «uno dei meccanismi predisposti dal legislatore per approdare alla giusta composizione degli interessi contrapposti dell'interessato e del titolare del trattamento: una contrapposizione che, nella varietà ed eterogeneità dei valori e degli interessi coinvolti, può plasticamente raffigurarsi come l'incontro conflittuale tra la libertà di autodeterminare la propria personalità e la libertà informativa»[38].

In merito al consenso bisogna però distinguere fra soggetti pubblici e privati. Ai sensi dell'art. 18, comma 4, cod. priv., infatti, i primi non devono richiedere il consenso dell'interessato, mentre, *ex* art. 23, comma 1, cod. priv., i secondi (ivi compresi gli enti pubblici economici) devono, in linea generale, ottenerlo, fatte salve le eccezioni previste dalla normativa.

Più specificatamente, il consenso non è necessario nei casi previsti dall'art. 24 cod. priv., ossia quando 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. Ancora, il consenso non è richiesto se il trattamento riguarda dati provenienti da pubblici registri, elenchi, atti o documenti conoscibili da chiunque[39] oppure dati relativi allo svolgimento di attività economiche, o, ancora, se è necessario per la salvaguardia della vita o dell'incolumità fisica di un terzo[40]. Il consenso non è, poi, richiesto se il trattamento è necessario ai fini dello svolgimento delle investigazioni difensive o per far valere o difendere un diritto in sede giudiziaria, oppure se è necessario (nei casi individuati dal

---

[38] S. Mazzamuto, *Il principio del consenso e il problema della revoca*, in R. Panetta (a cura di), *Libera circolazione e protezione dei dati personali*, cit., I, p. 993.

[39] Fermi restando i limiti e le modalità che le leggi, i regolamenti o la normativa comunitaria stabiliscono per la conoscibilità e pubblicità dei dati.

[40] 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.

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 stesso vale per le associazioni senza scopo di lucro 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).

È interessante notare come il legislatore abbia delineato un gravoso regime di responsabilità civile. Infatti, «chiunque cagiona danno ad altri per effetto del trattamento di dati personali è tenuto al risarcimento ai sensi dell'art. 2050 del codice civile» (art. 15, comma 1, cod. priv., che ricalca perfettamente l'art. 18 l. n. 675/96): tale norma, dunque, rinvia alla disciplina codicistica in materia di attività pericolose, ai sensi della quale non si è liberati da responsabilità se non si prova di aver adottato tutte le misure idonee ad evitare il danno.

Inoltre, *ex* art. 15, comma 2, cod. priv., «il danno non patrimoniale è risarcibile anche nei casi di violazione dell'articolo 11», il quale, a sua volta, dispone che 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;

– 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.

L'apparato sanzionatorio non si arresta comunque alla responsabilità civile, poiché il cod. priv. prevede alcune fattispecie penali, consistenti nel «trattamento illecito di dati» (art. 167 cod. priv.)[41], nella «falsità nelle dichiarazioni e notificazioni al Garante»[42] (art. 168 cod. priv.)[43], nell'omessa adozione di misure necessarie alla sicurezza dei dati (art. 169 cod. priv.)[44] e nell'inosservanza dei prov-

[41] «Salvo che il fatto costituisca più grave reato, chiunque, al fine di trarne per sé o per altri profitto o di recare ad altri un danno, procede al trattamento di dati personali in violazione di quanto disposto dagli articoli 18, 19, 23, 123, 126 e 130, ovvero in applicazione dell'articolo 129, è punito, se dal fatto deriva nocumento, con la reclusione da sei a diciotto mesi o, se il fatto consiste nella comunicazione o diffusione, con la reclusione da sei a ventiquattro mesi. Salvo che il fatto costituisca più grave reato, chiunque, al fine di trarne per sé o per altri profitto o di recare ad altri un danno, procede al trattamento di dati personali in violazione di quanto disposto dagli articoli 17, 20, 21, 22, commi 8 e 11, 25, 26, 27 e 45, è punito, se dal fatto deriva nocumento, con la reclusione da uno a tre anni».

[42] Appare utile precisare che la notificazione del trattamento di dati personali, di norma, non va effettuata, se non nei casi espressamente previsti dal cod. priv. oppure individuati dal Garante. La notificazione del trattamento va effettuata una sola volta prima che il trattamento abbia inizio, indipendentemente dal numero delle operazioni e dalla durata dello stesso, e può anche riguardare uno o più trattamenti con finalità correlate. Le relative ipotesi riguardano trattamenti di particolari dati sensibili, come i dati riguardanti la solvibilità economica, quelli relativi alla vita sessuale o quelli sanitari.

[43] «Chiunque, nella notificazione di cui all'articolo 37 o in comunicazioni, atti, documenti o dichiarazioni resi o esibiti in un procedimento dinanzi al Garante o nel corso di accertamenti, dichiara o attesta falsamente notizie o circostanze o produce atti o documenti falsi, è punito, salvo che il fatto costituisca più grave reato, con la reclusione da sei mesi a tre anni».

[44] «Chiunque, essendovi tenuto, omette di adottare le misure minime previste dall'articolo 33 è punito con l'arresto sino a due anni o con l'ammenda da diecimila euro a cinquantamila euro. All'autore del reato, all'atto dell'accertamento o, nei casi complessi, anche con successivo atto del Garante, è impartita una prescrizione fissando un termine per la regolarizzazione non eccedente il periodo di tempo tecnicamente necessario, prorogabile in caso di particolare complessità o per l'oggettiva difficoltà dell'adempimento e comunque non superiore a sei mesi. Nei sessanta giorni successivi allo scadere del termine, se risulta l'adempimento alla prescrizione, l'autore del reato è ammesso dal Garante a pagare una somma pari al quarto del massimo dell'ammenda stabilita per la contravvenzione. L'adempimento e il pagamento estinguono il reato. L'organo che impartisce la prescrizione e il pubblico ministero provvedono nei modi di cui agli articoli 21, 22, 23 e 24 del decreto legislativo 19 dicembre 1994, n. 758, e successive modificazioni, in quanto applicabili».

vedimenti del Garante per la protezione dei dati personali (art. 170 cod. priv.)[45].

Il Garante è l'autorità preposta alla tutela dei dati personali cui competono i numerosi compiti stabiliti dall'art. 154 cod. priv.[46], come una generale attività di controllo in ordine alla legittimità dei trattamenti che vengono posti in essere e lo svolgimento di attività ispettive[47]. Ad esso è inoltre affidata la tutela dei diritti dell'interessato (di cui all'art. 7 cod. priv.), in via concorrente con l'autorità giudiziaria ordinaria, ma con la vigenza del principio per cui *electa una via non datur recursus ad alteram*: dunque proposto ricorso all'*authority* non si può più adire il Tribunale, salvo che per chiedere il risarcimento del danno, di esclusiva competenza del giudice togato[48].

---

[45] «Chiunque, essendovi tenuto, non osserva il provvedimento adottato dal Garante ai sensi degli articoli 26, comma 2, 90, 50, commi 1 e 2, e 143, comma 1, lettera c), è punito con la reclusione da tre mesi a due anni».

[46] «Oltre a quanto previsto da specifiche disposizioni, il Garante, anche avvalendosi dell'Ufficio e in conformità al presente codice, ha il compito di: a) controllare se i trattamenti sono effettuati nel rispetto della disciplina applicabile e in conformità alla notificazione, anche in caso di loro cessazione; b) esaminare i reclami e le segnalazioni e provvedere sui ricorsi presentati dagli interessati o dalle associazioni che li rappresentano; c) prescrivere anche d'ufficio ai titolari del trattamento le misure necessarie o opportune al fine di rendere il trattamento conforme alle disposizioni vigenti, ai sensi dell'articolo 143; d) vietare anche d'ufficio, in tutto o in parte, il trattamento illecito o non corretto dei dati o disporne il blocco ai sensi dell'articolo 143, e di adottare gli altri provvedimenti previsti dalla disciplina applicabile al trattamento dei dati personali; e) promuovere la sottoscrizione di codici ai sensi dell'articolo 12 e dell'articolo 139; f) segnalare al Parlamento e al Governo l'opportunità di interventi normativi richiesti dalla necessità di tutelare i diritti di cui all'articolo 2 anche a seguito dell'evoluzione del settore; g) esprimere pareri nei casi previsti; h) 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; i) denunciare i fatti configurabili come reati perseguibili d'ufficio; l) tenere il registro dei trattamenti formato sulla base delle notificazioni di cui all'articolo 37; m) predisporre annualmente una relazione sull'attività svolta e sullo stato di attuazione del presente codice, che è trasmessa al Parlamento e al Governo entro il 30 aprile dell'anno successivo a quello cui si riferisce».

[47] Nel 2006, a titolo esemplificativo, sono state svolte 350 ispezioni e sono state irrogate 158 sanzioni (Garante per la protezione dei dati personali, *Relazione 2006. Diritti dei cittadini, protezione dei dati e attività del Garante*, Roma, 2007, p. 144 e p. 148).

[48] Sulla tutela dei diritti nella normativa sulla protezione dei dati personali cfr. U. Ausiello, *Tutela della privacy e azione inibitoria presso l'Autorità Garante per la protezione dei dati personali*, in *Responsabilità comunicazione impresa*,

Il quadro sanzionatorio è completato dalla previsione di alcune sanzioni amministrative: «omessa o inidonea informativa all'interessato» (art. 161 cod. priv.)[49]; cessione illegittima di dati (art. 162 cod. priv.)[50], «omessa o incompleta notificazione» (art. 163 cod. priv.)[51]; «omessa informazione o esibizione al Garante» (art. 164 cod. priv.)[52].

Ai sensi dell'art. 166 cod. priv., le suddette sanzioni sono irrogate dal Garante e nei casi di cui agli artt. 161, 162 e 164 cod. priv. 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 (nella fattispecie di cui all'art. 163 cod. priv. tale sanzione accessoria è già disposta *ex lege*).

Bisogna infine considerare un ulteriore aspetto di primaria importanza nell'ambito del cod. priv., ossia quello della sicurezza. In merito, l'art. 31 cod. priv. stabilisce che «i dati personali oggetto di

---

2000, 4, pp. 531-561; M. Granieri, *La tutela dei diritti nella normativa sulla protezione dei dati personali: un bilancio provvisorio*, in *Danno e responsabilità*, 2004, 8-9, pp. 827-831.

[49] «La violazione delle disposizioni di cui all'articolo 13 è punita con la sanzione amministrativa del pagamento di una somma da tremila euro a diciottomila euro o, nei casi di dati sensibili o giudiziari o di trattamenti che presentano rischi specifici ai sensi dell'articolo 17 o, comunque, di maggiore rilevanza del pregiudizio per uno o più interessati, da cinquemila euro a trentamila euro. La somma può essere aumentata sino al triplo quando risulta inefficace in ragione delle condizioni economiche del contravventore».

[50] «La cessione dei dati in violazione di quanto previsto dall'articolo 16, comma 1, lettera b), o di altre disposizioni in materia di disciplina del trattamento dei dati personali è punita con la sanzione amministrativa del pagamento di una somma da cinquemila euro a trentamila euro. La violazione della disposizione di cui all'articolo 84, comma 1, è punita con la sanzione amministrativa del pagamento di una somma da cinquecento euro a tremila euro».

[51] «Chiunque, essendovi tenuto, non provvede tempestivamente alla notificazione ai sensi degli articoli 37 e 38, ovvero indica in essa notizie incomplete, è punito con la sanzione amministrativa del pagamento di una somma da diecimila euro a sessantamila euro e con 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».

[52] «Chiunque omette di fornire le informazioni o di esibire i documenti richiesti dal Garante ai sensi degli articoli 150, comma 2, e 157 è punito con la sanzione amministrativa del pagamento di una somma da quattromila euro a ventiquattro mila euro».

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».

Inoltre, ai sensi dell'art. 33 cod. priv. il titolare del trattamento deve sempre adottare le misure minime di sicurezza individuate direttamente nello stesso codice o nel d.p.c.m. emanato *ex* art. 58, comma 3, cod. priv. Più specificatamente, tali misure sono delineate nell'Allegato B al cod. priv., ossia il «Disciplinare tecnico in materia di misure minime di sicurezza». Sul punto il legislatore ha distinto fra trattamenti effettuati con strumenti elettronici (1-26) e senza il loro ausilio (27-29), stabilendo regole più dettagliate nel primo caso. Le suddette misure devono essere adottate, in entrambe le ipotesi, dal titolare, dal responsabile (se designato) e da ciascun incaricato.

## 4. *Aspetti bioetico-giuridici della privacy in ambito internazionale*

L'ambito bioetico-giuridico del diritto alla privacy è intuitivamente uno dei più delicati, poiché è relativo ad uno degli aspetti più intimi e personali della persona umana, che manifesta tutta la sua debolezza nei casi in cui è in gioco la sua salute. Proprio nel momento in cui un individuo è più indifeso sorge la necessità di un incisivo intervento di tutela da parte dello stato affinché la sua posizione di debolezza non venga ad essergli di pregiudizio, per cui in tali ipotesi è necessario assicurare la maggior protezione possibile.

Bisogna considerare, inoltre, che le informazioni di carattere medico – per loro natura – coinvolgono anche altri soggetti (aziende sanitarie, medici, ecc.) e di norma «fuoriescono dalla dimensione individuale»[53]. Si pensi, ad esempio, a quante persone, già fra medici ed infermieri, hanno accesso alla cartella clinica di ciascun paziente

[53] R. Gamberale, *Il settore sanitario*, in R. Panetta (a cura di), *Libera circolazione e protezione dei dati personali*, cit., II, p. 1501.

in ambito prettamente sanitario, senza considerare, poi, che alcuni di tali dati sono sovente comunicati, e non potrebbe essere altrimenti, a datori di lavori ed enti di previdenza ed assistenza. Questo problema è, ovviamente, maggiormente avvertito in sistemi come quello statunitense dove i dati sanitari vengono di norma comunicati anche a strutture private come le società assicurative[54].

È altresì fondamentale che l'attività normativa si adegui ai rapidi ritmi della ricerca scientifica e tecnologica, posto che i più grandi rischi per la privacy derivano proprio dallo sviluppo e dalla diffusione di nuovi e sempre più avanzati strumenti che consentono l'acquisizione ed il trattamento di informazioni sanitarie con modalità prima solo immaginabili, per cui il sempre maggiore utilizzo di dati in formato digitale ne rende e renderà molto più semplice e veloce il trasferimento.

Se, da un lato, bisogna dunque garantire la protezione dei dati sanitari, dall'altro bisogna pure considerare che entrano in gioco anche altri profili. Così, non sempre è possibile ottenere il consenso dell'interessato, ad esempio quando esso si trova in uno stato di incapacità di intendere e di volere temporanea o permanente; ancora, i fini di salute pubblica possono spingere ad una compressione del diritto alla privacy sanitaria individuale, se non addirittura collettiva, qualora ciò si renda necessario per tutelare proprio la salute pubblica.

Oltretutto, bisogna considerare che l'elaborazione delle informazioni risultanti da esperienze diagnostiche, prognostiche e terapeutiche è assai importante per la ricerca scientifica, per cui non può essere impedita o scoraggiata[55].

Intuitivamente, dunque, i dati sanitari hanno un carattere intrinsecamente problematico e ciò ha spinto il legislatore comunitario a prendere in considerazione la possibilità di una loro tutela sin dal 1981: la Convenzione di Strasburgo «sulla protezione delle persone rispetto al trattamento automatizzato di dati di carattere personale», infatti, dispone un generale divieto di elaborazione automatica

---

[54] Cfr. D.J. Solove, M. Rotenberg, P.M. Schwartz, *Information Privacy Law,* cit., p. 345.

[55] F. Di Ciommo, *Il trattamento dei dati sanitari tra interessi individuali e collettivi*, in *Danno e responsabilità*, 2002, 2, p. 123.

di quei dati oggi comunemente denominati «sensibili» (e nella Convenzione considerati quali «categorie speciali»), facendo espresso riferimento a quelli «a carattere personale relativi allo stato di salute ed alla vita sessuale» (§ 6). Tali informazioni possono essere trattate solo se il diritto interno prevede delle appropriate garanzie.

Il 23 gennaio 1981, inoltre, è stata emanata la Raccomandazione n. R (81) 1 sulla regolamentazione delle banche dati sanitarie automatizzate, ossia quelle banche dati «create a scopi di cure mediche, di salute pubblica, di gestione dei servizi sanitari e di salute pubblica, o di ricerche mediche, in cui siano memorizzate informazioni sanitarie e, all'occorrenza, informazioni sociali o amministrative connesse, relative a individui identificati o identificabili» (art. 1, comma 1).

Il 23 gennaio 1986 è stata poi adottata la Raccomandazione n. R (86) 1 sulla protezione dei dati a carattere personale utilizzati a fini di sicurezza sociale. In essa si fa esplicito riferimento, fra l'altro, ai principi di non eccedenza del trattamento di dati personali, di sicurezza nel trattamento di dati personali e di previo consenso dell'interessato relativamente all'acquisizione di dati sensibili.

Un'incisiva tutela dei dati sanitari è altresì tratteggiata nella Raccomandazione n. R (89) 2, del 18 gennaio 1989, sulla protezione dei dati personali utilizzati «ai fini dell'occupazione». Il § 10, comma 2, della suddetta Raccomandazione dispone, fra l'altro, che un lavoratore o un candidato ad un lavoro non può essere interrogato circa il suo stato di salute ed essere oggetto di un esame medico, se non ai fini di determinare la sua attitudine ad un lavoro immediato o futuro, di coprire le necessità della medicina preventiva o di ottenere assistenze sociali[56].

[56] Ai sensi dei commi successivi, «i dati sulla salute non possono essere raccolti presso fonti diverse dallo stesso lavoratore, senza il suo consenso espresso e chiaro, o nel rispetto delle disposizioni del diritto interno» (comma 3); «i dati sulla salute coperti dal segreto medico dovranno essere trattati soltanto da personale vincolato alla regola del segreto medico. Queste informazioni non dovranno essere comunicate ai servizi del personale se non ove ciò si rendesse indispensabile per l'esercizio di funzioni di tale ufficio previste dal diritto interno» (comma 4); «i dati sulla salute coperti dal segreto medico dovranno essere registrati separatamente dalle altre categorie di dati conservate dal datore di lavoro. Dovranno essere prese misure di sicurezza, per evitare che persone estranee al servizio sanitario possano

Successivamente, l'emanazione della già citata direttiva n. 95/46/CE ha fornito un impulso fondamentale per assicurare una maggiore protezione dei dati sensibili, in generale, e dei dati sanitari, in particolare.

Bisogna comunque evidenziare che negli ultimi anni si nota una progressiva sensibilizzazione verso tale tematica: basti pensare alla "Convenzione del Consiglio d'Europa per la protezione dei diritti dell'uomo e della dignità dell'essere umano riguardo all'applicazione della biologia e della medicina" sottoscritta a Oviedo il 4 aprile 1997 ("Convenzione sui diritti dell'uomo e sulla biomedicina", la c.d. "Convenzione di Oviedo"), nonché al Protocollo addizionale del 12 gennaio 1998, n. 168, sul «divieto di clonazione di esseri umani»[57]. L'Italia ha poi ratificato la suddetta Convenzione ed il relativo Protocollo addizionale con la legge 28 marzo 2001, n. 145.

Essa è una «convenzione-quadro la cui ottica è evidentemente quella di orientare le legislazioni degli Stati, di porre delle garanzie certe a difesa dei diritti dell'uomo e del futuro della società»[58] e presenta alcune problematiche dovute alla necessità di contemperare punti di vista e regole assai diverse fra le varie nazioni[59].

Il diritto alla riservatezza trova spazio nella Convenzione di Oviedo, più specificatamente negli artt. 10 e 12. In particolare, l'art. 10 riconosce ad ogni persona il «diritto al rispetto della propria vita privata allorché si tratta di informazioni relative alla propria salute». Inoltre, ai sensi della medesima norma, «ogni persona ha il diritto di

---

avere accesso a tali dati» (comma 5); «il diritto di accesso della persona riguardo ai propri dati sanitari non dovrà mai essere sottoposto a restrizioni, a meno che l'accesso a tali dati non possa portare grave nocumento alla persona interessata; in questo caso, i dati potranno essergli comunicati tramite un medico di sua fiducia» (comma 6).

[57] Sulla Convenzione di Oviedo cfr.: A. Bompiani, *Una valutazione della "Convenzione sui diritti dell'uomo e la biomedicina" del Consiglio d'Europa*, in *Medicina e morale*, 1997, 1, pp. 37-55; E. Pariotti, *Prospettive e condizioni di possibilità per un biodiritto europeo a partire dalla Convenzione di Oviedo sui diritti dell'uomo e la biomedicina*, in *Studium juris*, 2002, 5, pp. 561-570; R. Sapienza, *La convenzione europea sui diritti dell'uomo e la biomedicina*, in *Rivista di diritto internazionale*, 1998, 2, pp. 457-470; E. Sgreccia, *La Convenzione sui diritti dell'uomo e la biomedicina*, in *Medicina e morale*, 1997, 1, pp. 9-13.

[58] E. Sgreccia, *La Convenzione sui diritti dell'uomo e la biomedicina*, cit., p. 9.

[59] Ivi, pp. 10-13.

conoscere ogni informazione raccolta sulla propria salute. Tuttavia, la volontà di una persona di non essere informata deve essere rispettata». A titolo eccezionale possono comunque essere previste delle restrizioni all'esercizio dei diritti di sapere e di non sapere. L'art. 12 (rubricato «test genetici predittivi») dispone, invece, che «non si potrà procedere a test predittivi di malattie genetiche o che permettano sia di identificare il soggetto come portatore di un gene responsabile di una malattia sia di rivelare una predisposizione o una suscettibilità genetica a una malattia se non a fini medici o di ricerca medica, e sotto riserva di una consulenza genetica appropriata».

Nello stesso anno in cui è stato emanata la Convenzione di Oviedo è stata altresì approvata la "Dichiarazione universale sul genoma umano e i diritti umani" dalla Conferenza Generale dell'UNESCO[60]. Essa, pur non avendo efficacia vincolante, è finalizzata ad assicurare il rispetto della dignità umana e la protezione dei diritti umani e delle libertà fondamentali, chiedendo agli Stati di uniformare i propri ordinamenti giuridici ai principi in essa stabiliti.

Alcune norme della suddetta Dichiarazione mirano a tutelare alcuni aspetti specifici del diritto alla privacy. Più specificatamente, l'art. 5, lett. b, dispone che è sempre necessario ottenere il previo consenso libero ed informato da parte di ciascun soggetto interessato dalla ricerca genetica. Qualora la persona non sia in condizione di esprimere il proprio consenso, bisognerà far riferimento alle disposizioni della normativa vigente ma sempre nell'interesse della persona medesima. Ai sensi della successiva lett. e, nel caso di incapacità di intendere e di volere la ricerca sul suo genoma può essere condotta solo se ne riceverà un beneficio diretto; nell'ipotesi in cui la ricerca non abbia un diretto beneficio per la salute della persona oggetto della stessa, si potrà procedere solo in via eccezionale, nel rispetto dei diritti umani, con minimo rischio e, comunque, solo qualora ne possano derivare effetti benefici verso persone che hanno la stessa categoria di età o con le medesime condizioni genetiche. Ai sensi dell'art. 7, poi, i dati genetici associati ad una persona identi-

[60] Su di essa cfr., fra gli altri, A. Bompiani, *Il comitato internazionale di bioetica dell'UNESCO e la redazione della "Dichiarazione universale sul genoma umano e i diritti umani"*, in *Iustitia*, 1998, 1, pp. 62-108.

ficabile e archiviati o trattati a fini di ricerca o a qualsiasi altro fine devono essere conservati come confidenziali nel rispetto della normativa vigente.

## 5. *La privacy sanitaria nella normativa italiana*

I dati idonei a rivelare lo stato di salute e la vita sessuale sono esplicitamente tutelati nel cod. priv.[61]. Essi, come si è detto, rientrano nel novero dei dati sensibili e ai trattamenti effettuati in ambito sanitario è dedicato il titolo V della II parte del cod. priv., ossia quella parte del cod. priv. dedicata agli «specifici settori». In particolare, il capo I delinea i principi generali, il Capo II regolamenta le modalità semplificate per informativa e consenso, il Capo III esplicita le rilevanti finalità di interesse pubblico ed i Capi IV, V e VI disciplinano, rispettivamente, le prescrizioni mediche, il trattamento di dati genetici ed altre ipotesi.

Prima di analizzare la disciplina specifica dei dati idonei a rivelare lo stato di salute e la vita sessuale[62], è d'uopo premettere che

[61] In dottrina si è rivelato che quando si parla di dati sanitari bisognerebbe scomporne la nozione, scorporando tutte quelle informazioni che, a seguito di un'analisi comparata di diversi fattori, non si palesino idonee a porre in serio pericolo la sfera giuridica della persona. Ne consegue che la diversa sensibilità, e quindi il diverso grado di tutela, dovrebbe dipendere dal tipo di interesse che, nel conflitto fra sfera di autonomia della persona e interesse alla conoscenza, sia chiamato a prevalere. Sarebbe dunque proficuo prendere in considerazione: il contesto in cui il dato sanitario è usato; il modo della sua utilizzazione; l'uso che se ne fa; i soggetti che se ne avvalgono. In altri termini, valutando il rapporto fra informazione raccolta e servizio prestato, si possono ottenere utili indicazioni per valutare l'esistenza o meno di un danno (V. Zambrano, *Dati sanitari e tutela della sfera privata*, in *Il diritto dell'informazione e dell'informatica*, 1999, 1, pp. 21-22).

[62] Appare utile rilevare che la protezione della riservatezza delle informazioni sanitarie è esplicitamente prevista anche dal Codice di deontologia medica del 16 dicembre 2006. In particolare, l'art. 10 disciplina il segreto professionale, mentre l'art. 11, rubricato «riservatezza dei dati personali», così recita: «il medico è tenuto al rispetto della riservatezza nel trattamento dei dati personali del paziente e particolarmente dei dati sensibili inerenti la salute e la vita sessuale. Il medico acquisisce la titolarità del trattamento dei dati sensibili nei casi previsti dalla legge, previo consenso del paziente o di chi ne esercita la tutela. Nelle pubblicazioni scientifiche di dati clinici o di osservazioni relative a singole persone, il medico deve assicurare la non identificabilità delle stesse. Il consenso specifico del paziente vale

nell'impianto del cod. priv. il trattamento dei dati sensibili è possibile solo a condizioni differenti da quelle previste per i dati personali generalmente intesi; inoltre, la regolamentazione varia fra soggetti pubblici, da un lato, e privati ed enti pubblici economici, dall'altro.

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, cod. priv.). In tale ipotesi, però, è necessaria la previa autorizzazione di una espressa disposizione di legge che specifichi i tipi di dati che possono essere trattati e di operazioni eseguibili e le finalità di rilevante interesse pubblico perseguite. Se è specificata solo la finalità, ma non i tipi di dati sensibili e di operazioni eseguibili, il trattamento è consentito solo in riferimento ai tipi di dati e di operazioni identificati e resi pubblici a cura dei soggetti che ne effettuano il trattamento, in relazione alle specifiche finalità perseguite nei singoli casi e nel rispetto dei principi di cui all'art. 22 cod. priv., con atto di natura regolamentare adottato in conformità ad apposito parere espresso dal Garante per la protezione dei dati personali, anche su schemi tipo.

In mancanza di espresse disposizioni legislative i soggetti pubblici possono comunque richiedere al Garante l'individuazione delle

---

per ogni ulteriore trattamento dei dati medesimi, ma solo nei limiti, nelle forme e con le deroghe stabilite dalla legge. Il medico non può collaborare alla costituzione di banche di dati sanitari, ove non esistano garanzie di tutela della riservatezza, della sicurezza e della vita privata della persona». Inoltre, l'art. 12, rubricato «trattamento dei dati sensibili», dispone che «al medico, è consentito il trattamento dei dati personali idonei a rivelare lo stato di salute del paziente previa richiesta o autorizzazione da parte di quest'ultimo, subordinatamente ad una preventiva informazione sulle conseguenze e sull'opportunità della rivelazione stessa. Al medico peraltro è consentito il trattamento dei dati personali del paziente in assenza del consenso dell'interessato solo ed esclusivamente quando sussistano le specifiche ipotesi previste dalla legge ovvero quando vi sia la necessità di salvaguardare la vita o la salute del paziente o di terzi nell'ipotesi in cui il paziente medesimo non sia in grado di prestare il proprio consenso per impossibilità fisica, per incapacità di agire e/o di intendere e di volere; in quest'ultima situazione peraltro, sarà necessaria l'autorizzazione dell'eventuale legale rappresentante laddove precedentemente nominato. Tale facoltà sussiste nei modi e con le garanzie dell'art. 11 anche in caso di diniego dell'interessato ove vi sia l'urgenza di salvaguardare la vita o la salute di terzi».

attività, tra quelle loro demandate *ex lege*, che perseguono finalità di rilevante interesse pubblico e per le quali è conseguentemente autorizzato il trattamento dei dati sensibili, con il rispetto delle garanzie di cui all'art. 26, comma 2, cod. priv. (fra le quali rientra, ad esempio, la necessità del consenso scritto dell'interessato). Il trattamento può tuttavia essere effettuato solo dopo che siano stati identificati e resi pubblici i tipi di dati e di operazioni mediante l'emanazione di un atto di natura regolamentare adottato in conformità al parere espresso dal Garante di cui si è detto.

Ai sensi dell'art. 85, comma 1, cod. priv., sono considerate di rilevante interesse pubblico determinate finalità che rientrano nei compiti del Servizio sanitario nazionale e degli altri organismi sanitari pubblici relative alle attività amministrative correlate a quelle di prevenzione, diagnosi, cura e riabilitazione dei soggetti assistiti dal Servizio sanitario nazionale; alla programmazione, gestione, controllo e valutazione dell'assistenza sanitaria; alla vigilanza sulle sperimentazioni, farmacovigilanza, autorizzazione all'immissione in commercio ed all'importazione di medicinali e di altri prodotti di rilevanza sanitaria; alle attività certificatorie; all'applicazione della normativa in materia di igiene e sicurezza nei luoghi di lavoro e di sicurezza e salute della popolazione; alle attività amministrative correlate ai trapianti d'organo e di tessuti, nonché alle trasfusioni di sangue umano; all'instaurazione, gestione, pianificazione e controllo dei rapporti tra l'amministrazione ed i soggetti accreditati o convenzionati del Servizio sanitario nazionale[63].

[63] Ai sensi dell'art. 86 cod. priv., inoltre, «si considerano di rilevante interesse pubblico, ai sensi degli articoli 20 e 21, le finalità, perseguite mediante trattamento di dati sensibili e giudiziari, relative alle attività amministrative correlate all'applicazione della disciplina in materia di: a) tutela sociale della maternità e di interruzione volontaria della gravidanza, con particolare riferimento a quelle svolte per la gestione di consultori familiari e istituzioni analoghe, per l'informazione, la cura e la degenza delle madri, nonché per gli interventi di interruzione della gravidanza; b) stupefacenti e sostanze psicotrope, con particolare riferimento a quelle svolte al fine di assicurare, anche avvalendosi di enti ed associazioni senza fine di lucro, i servizi pubblici necessari per l'assistenza socio-sanitaria ai tossicodipendenti, gli interventi anche di tipo preventivo previsti dalle leggi e l'applicazione delle misure amministrative previste; c) assistenza, integrazione sociale e diritti delle persone handicappate effettuati, in particolare, al fine di: 1) accertare l'handicap ed assicurare la funzionalità dei servizi terapeutici e riabilitativi, di aiuto personale

La disciplina è però diversa per gli esercenti le professioni sanitarie e gli organismi sanitari pubblici, i quali possono trattare i dati personali idonei a rivelare lo stato di salute con il consenso dell'interessato se il trattamento riguarda dati e operazioni indispensabili per perseguire una finalità di tutela della salute o dell'incolumità fisica dell'interessato stesso. Si può prescindere dal consenso, ma è necessaria la previa autorizzazione del Garante, se la finalità sopradetta riguarda un terzo o la collettività.

Il cod. priv., inoltre, impone ai soggetti pubblici un obbligo di aggiornamento e di integrazione periodica dei tipi di dati trattati e delle operazioni eseguibili su di essi. È prescritta anche una verifica periodica dell'esattezza e dell'aggiornamento dei dati sensibili e giudiziari, nonché della loro pertinenza, completezza, non eccedenza e indispensabilità rispetto alle finalità perseguite nei singoli casi, anche se i dati sono stati forniti di propria iniziativa da parte dell'interessato. I dati che, anche a seguito delle verifiche, dovessero risultare eccedenti o non pertinenti o non indispensabili non possono essere utilizzati, salvo che per l'eventuale conservazione, a norma di legge, dell'atto o del documento che li contiene.

L'art. 22, comma 2, cod. priv., impone, poi, ai soggetti pubblici di informare l'interessato in ordine alla normativa che prevede gli obblighi o i compiti in base alla quale è effettuato il trattamento dei dati sensibili e giudiziari. Quelli contenuti in elenchi, registri o banche di dati, tenuti con l'ausilio di strumenti elettronici, devono essere 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.

I dati sensibili e giudiziari non possono essere trattati nell'ambito di test psico-attitudinali volti a definire il profilo o la personalità

---

e familiare, nonché interventi economici integrativi ed altre agevolazioni; 2) curare l'integrazione sociale, l'educazione, l'istruzione e l'informazione alla famiglia del portatore di handicap, nonché il collocamento obbligatorio nei casi previsti dalla legge; 3) realizzare comunità-alloggio e centri socio riabilitativi; 4) curare la tenuta degli albi degli enti e delle associazioni ed organizzazioni di volontariato impegnati nel settore».

dell'interessato (art. 22, comma 10, cod. priv.)[64]. In ogni caso, tali operazioni e trattamenti, se effettuati utilizzando banche di dati di diversi titolari, nonché la diffusione dei dati sensibili e giudiziari, sono ammessi solo se previsti da espressa disposizione di legge.

I dati sensibili possono essere oggetto di trattamento anche senza consenso, previa autorizzazione del Garante, se esso è necessario per la salvaguardia della vita o dell'incolumità fisica di un terzo. Se tale 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 può essere prestato da chi esercita legalmente la potestà, da un prossimo congiunto, da un familiare, da un convivente o, in loro assenza, dal responsabile della struttura presso cui dimora l'interessato. Successivamente alla prestazione, ma al più presto, possono intervenire l'informativa ed il consenso.

Sussiste, poi, l'obbligo di notificare al Garante il trattamento di dati personali se il trattamento riguarda, fra l'altro, dati genetici, biometrici o dati che indicano la posizione geografica di persone od oggetti mediante una rete di comunicazione elettronica, oppure dati idonei a rivelare lo stato di salute e la vita sessuale trattati a fini di procreazione assistita, prestazione di servizi sanitari per via telematica relativi a banche di dati o alla fornitura di beni, indagini epidemiologiche, rilevazione di malattie mentali, infettive e diffusive, sieropositività, trapianto di organi e tessuti e monitoraggio della spesa sanitaria, o, ancora, trattati da associazioni, enti od organismi senza

[64] «Le operazioni di raffronto tra dati sensibili e giudiziari, nonché i trattamenti di dati sensibili e giudiziari ai sensi dell'articolo 14, sono effettuati solo previa annotazione scritta dei motivi». Ai sensi dell'art. 14 cod. priv. «nessun atto o provvedimento giudiziario o amministrativo che implichi una valutazione del comportamento umano può essere fondato unicamente su un trattamento automatizzato di dati personali volto a definire il profilo o la personalità dell'interessato. L'interessato può opporsi ad ogni altro tipo di determinazione adottata sulla base del trattamento di cui al comma 1, ai sensi dell'articolo 7, comma 4, lettera a), salvo che la determinazione sia stata adottata in occasione della conclusione o dell'esecuzione di un contratto, in accoglimento di una proposta dell'interessato o sulla base di adeguate garanzie individuate dal presente codice o da un provvedimento del Garante ai sensi dell'articolo 17».

scopo di lucro, anche non riconosciuti, a carattere politico, filosofico, religioso o sindacale[65].

Ai sensi dell'art. 39 cod. priv., inoltre, il titolare del trattamento deve comunicare previamente al Garante il trattamento di dati idonei a rivelare lo stato di salute previsto dal programma di ricerca biomedica o sanitaria di cui all'art. 110, comma 1, primo periodo, cod. priv.[66]. I trattamenti oggetto di comunicazione possono essere iniziati decorsi quarantacinque giorni dal ricevimento della comunicazione salvo diversa determinazione, anche successiva, del Garante.

Anche per i dati idonei a rivelare lo stato di salute e la vita sessuale sono previste particolari misure qualora il trattamento sia effettuato in ambito pubblico. In particolare, essi devono essere conservati separatamente da altri dati personali trattati per finalità che non richiedono il loro utilizzo. Inoltre, anche quando essi sono tenuti in elenchi, registri o banche di dati senza l'ausilio di strumenti elettronici, devono essere 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[67].

---

[65] Il Garante può, con proprio provvedimento, sottrarre eventuali trattamenti rientranti nella suddetta elencazione all'obbligo di notificazione nonché individuarne di nuovi, qualora possano recare pregiudizio ai diritti e alle libertà dell'interessato, in ragione delle relative modalità o della natura dei dati personali.

[66] «Il consenso dell'interessato per il trattamento dei dati idonei a rivelare lo stato di salute, finalizzato a scopi di ricerca scientifica in campo medico, biomedico o epidemiologico, non è necessario quando la ricerca è prevista da un'espressa disposizione di legge che prevede specificamente il trattamento, ovvero rientra in un programma di ricerca biomedica o sanitaria previsto ai sensi dell'articolo 12 *bis* del decreto legislativo 30 dicembre 1992, n. 502, e successive modificazioni, e per il quale sono decorsi quarantacinque giorni dalla comunicazione al Garante ai sensi dell'articolo 39. Il consenso non è inoltre necessario quando a causa di particolari ragioni non è possibile informare gli interessati e il programma di ricerca è oggetto di motivato parere favorevole del competente comitato etico a livello territoriale ed è autorizzato dal Garante anche ai sensi dell'articolo 40».

[67] Inoltre, «quando 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

L'art. 76 cod. priv. dispone che gli esercenti le professioni sanitarie e gli organismi sanitari pubblici, anche nell'ambito di un'attività di rilevante interesse pubblico (ai sensi dell'art. 85 cod. priv.[68]), trattano i dati personali idonei a rivelare lo stato di salute con il consenso dell'interessato, ma anche senza l'autorizzazione del Garante, se il trattamento riguarda dati e operazioni indispensabili per perseguire la finalità di tutela della salute o dell'incolumità fisica dell'interessato.

Il cod. priv. deroga, in tali fattispecie, alle ordinarie norme in tema di prestazione del consenso, che può essere reso con le modalità semplificate indicate nel capo II («modalità semplificate per infor-

---

un diritto della personalità o in un altro diritto o libertà fondamentale e inviolabile» (art. 60 cod. priv.).

[68] L'art. 76 cod. priv. fa espresso riferimento all'art. 85 cod. priv., che definisce i «Compiti del Servizio sanitario nazionale». Tale norma dispone che: «1. Fuori dei casi di cui al comma 2, si considerano di rilevante interesse pubblico, ai sensi degli articoli 20 e 21, le finalità che rientrano nei compiti del Servizio sanitario nazionale e degli altri organismi sanitari pubblici relative alle seguenti attività: a) attività amministrative correlate a quelle di prevenzione, diagnosi, cura e riabilitazione dei soggetti assistiti dal Servizio sanitario nazionale, ivi compresa l'assistenza degli stranieri in Italia e dei cittadini italiani all'estero, nonché di assistenza sanitaria erogata al personale navigante ed aeroportuale; b) programmazione, gestione, controllo e valutazione dell'assistenza sanitaria; c) vigilanza sulle sperimentazioni, farmacovigilanza, autorizzazione all'immissione in commercio e all'importazione di medicinali e di altri prodotti di rilevanza sanitaria; d) attività certificatorie; e) l'applicazione della normativa in materia di igiene e sicurezza nei luoghi di lavoro e di sicurezza e salute della popolazione; f) le attività amministrative correlate ai trapianti d'organo e di tessuti, nonché alle trasfusioni di sangue umano, anche in applicazione della legge 4 maggio 1990, n. 107; g) instaurazione, gestione, pianificazione e controllo dei rapporti tra l'amministrazione ed i soggetti accreditati o convenzionati del Servizio sanitario nazionale. 2. Il comma 1 non si applica ai trattamenti di dati idonei a rivelare lo stato di salute effettuati da esercenti le professioni sanitarie o da organismi sanitari pubblici per finalità di tutela della salute o dell'incolumità fisica dell'interessato, di un terzo o della collettività, per i quali si osservano le disposizioni relative al consenso dell'interessato o all'autorizzazione del Garante ai sensi dell'articolo 76. 3. All'identificazione dei tipi di dati idonei a rivelare lo stato di salute e di operazioni su essi eseguibili è assicurata ampia pubblicità, anche tramite affissione di una copia o di una guida illustrativa presso ciascuna azienda sanitaria e presso gli studi dei medici di medicina generale e dei pediatri di libera scelta. 4. Il trattamento di dati identificativi dell'interessato è lecito da parte dei soli soggetti che perseguono direttamente le finalità di cui al comma 1. L'utilizzazione delle diverse tipologie di dati è consentita ai soli incaricati, preposti, caso per caso, alle specifiche fasi delle attività di cui al medesimo comma, secondo il principio dell'indispensabilità dei dati di volta in volta trattati».

mativa e consenso»). Esse possono essere utilizzate da determinati soggetti (organismi sanitari pubblici e privati, esercenti le professioni sanitarie, competenti servizi o strutture di soggetti pubblici operanti in ambito sanitario o della prevenzione e sicurezza del lavoro) per informare l'interessato in ordine ai dati personali raccolti presso di lui o presso terzi, per manifestare il consenso al trattamento dei dati personali (se richiesto *ex* art. 76 cod. priv.) e per il trattamento dei dati personali.

Il consenso può essere manifestato, senza particolari formalità, con un'unica dichiarazione, in forma scritta oppure orale; nell'ultimo caso, viene documentato con annotazione dell'esercente la professione sanitaria o dell'organismo sanitario pubblico.

Nei casi di emergenza o di igiene pubblica, l'informativa ed il consenso al trattamento dei dati personali possono intervenire senza ritardo, successivamente alla prestazione, qualora la competente autorità abbia adottato un'ordinanza contingibile ed urgente *ex* art. 117 d.lgs. 31 marzo 1998, n. 112[69] (art. 82 cod. priv.).

L'informativa e il consenso al trattamento dei dati personali possono altresì intervenire senza ritardo, successivamente alla prestazione, se vi è stata l'impossibilità fisica, l'incapacità di agire o di intendere e di volere dell'interessato e non è stato possibile acquisire il consenso da chi può esercitare in sua vece i suoi diritti[70]; lo stesso dicasi se vi è un rischio grave, imminente ed irreparabile per la salute o l'incolumità fisica dell'interessato oppure se la prestazione medica può essere pregiudicata dall'acquisizione preventiva del consenso.

Il cod. priv. disciplina in modo diverso l'informativa del medico di medicina generale e del pediatra, che deve essere resa in forma

---

[69] «1. In caso di emergenze sanitarie o di igiene pubblica a carattere esclusivamente locale le ordinanze contingibili e urgenti sono adottate dal sindaco, quale rappresentante della comunità locale. Negli altri casi l'adozione dei provvedimenti d'urgenza, ivi compresa la costituzione di centri e organismi di referenza o assistenza, spetta allo Stato o alle regioni in ragione della dimensione dell'emergenza e dell'eventuale interessamento di più ambiti territoriali regionali. 2. In caso di emergenza che interessi il territorio di più comuni, ogni sindaco adotta le misure necessarie fino a quando non intervengano i soggetti competenti ai sensi del comma 1».

[70] Ossia chi esercita legalmente la potestà, un prossimo congiunto, un familiare, un convivente o, in loro assenza, il responsabile della struttura presso cui dimora l'interessato.

chiara rendendo palesi 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 di cui all'art. 7 cod. priv., gli estremi identificativi del titolare e, se designati, del rappresentante nel territorio dello Stato e del responsabile (art. 78 cod. priv.).

L'informativa, salvo diversa specificazione del medico o del pediatra, riguarda anche il trattamento di dati correlato a quello effettuato dal medico di medicina generale o dal pediatra di libera scelta, effettuato da un professionista o da altro soggetto, parimenti individuabile in base alla prestazione richiesta, che:

– sostituisce temporaneamente il medico o il pediatra;

– fornisce una prestazione specialistica su richiesta del medico e del pediatra;

– può trattare lecitamente i dati nell'ambito di un'attività professionale prestata in forma associata;

– fornisce farmaci prescritti[71];

– comunica dati personali al medico o al pediatra in conformità alla disciplina applicabile[72].

---

[71] Quanto alle prescrizioni mediche si rileva che la disciplina è differenziata fra medicinali a carico e non del Servizio sanitario nazionale. Le ricette relative ai primi devono essere redatte secondo un modello tipico, conformato in modo da permettere di risalire all'identità dell'interessato solo in caso di necessità connesse al controllo della correttezza della prescrizione, ovvero a fini di verifiche amministrative o per scopi epidemiologici e di ricerca, nel rispetto delle norme deontologiche applicabili. Nelle prescrizioni cartacee di medicinali non a carico, anche parziale, del Servizio sanitario nazionale, le generalità dell'interessato non devono essere indicate, salvo che il medico ritenga indispensabile permettere di risalire alla sua identità, per le particolari condizioni dell'interessato o speciali modalità di preparazione o di utilizzazione.

[72] Nell'informativa devono essere evidenziate analiticamente eventuali trattamenti di dati personali che presentano rischi specifici per i diritti e le libertà fondamentali, nonché per la dignità dell'interessato, in particolare in caso di trattamenti effettuati per scopi scientifici, nell'ambito della teleassistenza o telemedicina, oppure per fornire altri beni o servizi all'interessato attraverso una rete di comunicazione elettronica.

Le modalità semplificate relative all'informativa ed al consenso possono essere utilizzate, a norma dell'art. 79 cod. priv., dagli organismi sanitari pubblici e privati in riferimento ad una pluralità di prestazioni erogate anche da distinti reparti ed unità dello stesso organismo o di più strutture ospedaliere o territoriali specificamente identificati. In tali casi, l'organismo o le strutture hanno l'obbligo di annotare l'avvenuta informativa ed il consenso con modalità uniformi e tali da permettere una verifica al riguardo da parte di altri reparti ed unità che, anche in tempi diversi, trattano dati relativi al medesimo interessato.

Infine, appare utile menzionare l'art. 84 cod. priv., che disciplina la delicata fase della comunicazione di dati all'interessato. Più specificatamente, i dati personali idonei a rivelare lo stato di salute possono essere resi noti all'interessato (oppure a chi può esercitare in sua vece i suoi diritti) da esercenti le professioni sanitarie ed organismi sanitari solo per il tramite di un medico designato dall'interessato o dal titolare.

## 6. *Evoluzione ed involuzione del concetto di privacy*

Il concetto di privacy quale *right to be let alone* viene sempre più spesso ritenuto superato. Ciò si spiega, fra l'altro, qualora si consideri che «le forme assunte dalla protezione dei dati personali rispecchiano ormai una gamma di valori assai più ampia, diventano strumenti essenziali contro le discriminazioni, per la difesa di diritti fondamentali come la salute, per consentire il libero sviluppo della personalità. La stessa parola *privacy* rischia di divenire inadeguata, non più capace di individuare correttamente la realtà che dovrebbe rappresentare, se rimane confinata nel significato dell'origine»[73].

In tal senso bisogna rilevare che la nozione di un diritto non può certo cristallizzarsi, ma deve invece adeguarsi agli incessanti mutamenti che avvengono nella società. In particolare, il diritto alla privacy costituisce un baluardo che dovrebbe difendere i singoli e i

[73] S. Rodotà, *Trasformazioni del corpo*, cit., p. 11.

gruppi sociali dalle condotte invasive di altri soggetti, siano essi individuali o collettivi.

Per delineare i tratti fondamentali dell'evoluzione del diritto alla privacy, com'è ovvio, non si può tuttavia semplicemente fare riferimento al diritto positivo, per quanto esso assuma un'importanza fondamentale non solo per valutare quale sia il quadro normativo entro cui persone fisiche e giuridiche nonché soggetti privati e pubblici possono muoversi. Le regolamentazioni sono, infatti, il risultato del concorso di una molteplicità di fattori e per cercare di capire ciò che la legge dovrebbe proteggere non si può far riferimento unicamente a ciò che attualmente protegge[74].

Il saggio di Warren e Brandeis ha, del resto, fatto partire un "processo evolutivo" del diritto alla privacy, che ha poi attraversato una fase in cui l'accento è stato posto sulla segretezza per giungere ad una in cui il diritto al controllo dei propri dati ha assunto un rilievo centrale. Pertanto, ad una "libertà da" invadenti sguardi esterni sulla vita privata si è affiancata una "libertà di" autodeterminazione nello svolgimento della personalità dell'uomo come singolo.

La persona umana deve sentirsi libera da ingerenze esterne, ma deve anche avere la libertà di controllare le informazioni volutamente comunicate. Stefano Rodotà ha osservato che si è verificato un passaggio fondamentale per la società odierna «dalla privacy alla non discriminazione» e «dalla segretezza al controllo»[75].

Come rilevato in dottrina, nella società dell'informazione il diritto alla privacy non sembra dunque più riassumibile nei termini di un mero *right to be let alone*, posto che esso si caratterizza maggiormente come potere di controllo sulla circolazione delle informazioni personali[76].

---

[74] D.J. Solove, M. Rotenberg, P.M. Schwartz, *Information Privacy Law*, cit., p. 39.

[75] L'illustre autore vi ha fatto riferimento in diverse opere: *Privacy e costruzione della sfera privata*, in *Politica del diritto*, 1991, 4, pp. 521-546; *Tecnologie e diritti*, Il Mulino, Bologna, 1995, p. 108; *Persona, riservatezza, identità. Prime note sistematiche sulla protezione dei dati personali*, in *Rivista critica di diritto privato*, 1997, 4, p. 589.

[76] S. Niger, *Il diritto alla protezione dei dati personali*, in J. Monducci, G. Sartor (a cura di), *Il Codice in materia di protezione dei dati personali*, cit., p. 5.

Inoltre, la richiesta di privacy sembra, negli ultimi anni, acquisire nuove valenze, come l'esigenza di assumere l'identità preferita nell'ambito delle comunicazioni elettroniche: in altri termini, la possibilità di presentarsi con un nome, un sesso, un'età che possono differire da quelli effettivamente corrispondenti ai dati del soggetto. Emerge, dunque, la volontà di veder tutelata un'identità nuova, un'intimità costruita, e ciò viene avvertito come condizione necessaria per svolgere la propria personalità[77], ossia per poter pienamente esercitare il diritto all'autodeterminazione esistenziale ancor più di quello all'autodeterminazione informativa.

L'evoluzione della nozione di privacy ha dunque portato ad una maggiore tutela della persona umana intesa nel suo complesso, dal momento che mediante il rispetto della sua intimità personale nonché attraverso il riconoscimento del fatto che i *suoi* dati personali sono (o dovrebbero essere) *suoi*, diviene possibile scegliere come vivere la propria vita riducendo il timore che altri possano effettuare delle interferenze illecite, e ben sapendo che qualora esse comunque si verifichino può utilizzare degli strumenti effettivi che consentono di rimediare alla lesione eventualmente cagionata.

Il profilo della protezione dei dati personali, chiaramente, assume un'importanza fondamentale soprattutto negli ultimi anni, poiché le tecnologie di comunicazione oggi utilizzate amplificano le problematiche connesse alla tutela della privacy. Tanto più forte è la capacità comunicativa degli strumenti tecnologici disponibili, maggiore è il rischio che informazioni personali vengano diffuse senza che il soggetto interessato possa esercitare una qualsiasi attività di controllo.

Detta problematica assume proporzioni di particolare rilevanza nelle fattispecie inerenti la rete Internet[78], dove è assai facile perdere il controllo dei propri dati personali e dove l'anonimato è sempre più un'utopia. Bisogna però rilevare come lo spostamento dell'attenzione verso il profilo del controllo dei propri dati personali, mag-

---

[77] S. Rodotà, *Tecnopolitica*, Laterza, Roma-Bari, 1997, p. 139.

[78] A tali problematiche ha fatto acutamente riferimento V. Zeno-Zencovich oltre vent'anni fa nel suo *Telematica e tutela del diritto all'identità personale*, in *Politica del diritto*, 1983, 2, pp. 345-355.

giormente tutelato anche dalle normative vigenti in molti stati, costituisca una risposta, seppur non del tutto esaustiva, a tale esigenza.

Difatti, se è vero che non c'è privacy senza sicurezza, come comunemente si afferma, è altresì vero che non ci sono né l'una né l'altra se manca una diffusa presa di coscienza di entrambe le problematiche e ciò sotto il duplice profilo dei diritti e dei doveri sanciti dalle normative e suggeriti dal buon senso.

Può con ogni probabilità sostenersi che l'attenzione dovrebbe spostarsi ancor di più verso forme di tutela preventiva che impediscano che si realizzi un'eventuale 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: non resta altro che ricorrere ad un risarcimento monetario che dovrebbe ripagare il soggetto leso dalle conseguenze negative della violazione del suo diritto.

Di ciò non deve essere cosciente solo il legislatore, ma devono esserlo anche tutte le persone, poiché l'incauta prestazione del consenso al trattamento di dati personali oppure la loro temeraria comunicazione possono portare al verificarsi di spinose problematiche. Si pensi, ad esempio, alla comunicazione dei dati della propria carta di credito, che può cagionare danni economici più o meno ingenti.

Il continuo dibattito sulla privacy, nonché l'emanazione delle normative in materia, contribuiscono tuttavia a farne recepire il concetto da parte di un sempre crescente numero di persone, anche se a tale tendenza evolutiva sembra oggi accompagnarsi, e talvolta addirittura predominare, una di carattere opposto: parlare di involuzione del diritto alla privacy può, oggi, sembrare assai provocatorio, dal momento che, mai sino ad adesso, tanto se ne è discusso e tanto se ne è legiferato. Eppure, da un punto di vista qualitativo, la tutela della riservatezza ha avuto un andamento altalenante.

Si consideri, infatti, che inizialmente, come si è visto, la teorizzazione di tale diritto e la sua considerazione da parte di dottrina e giurisprudenza hanno avuto un ruolo fondamentale per proteggere gli individui, prima, e i gruppi, poi, da interferenze illecite nella loro vita privata, seppure con tempi e modalità diverse da paese a paese. Ciò è avvenuto in risposta alle esigenze connesse alla diffusione di

sempre più evoluti strumenti di comunicazione, che hanno consentito di espandere notevolmente l'ambito potenziale di conoscibilità delle informazioni, prima ristretto a determinati luoghi ed oggi corrispondente a quasi l'intero globo, grazie alla capillare diffusione di Internet.

Sul punto bisogna rilevare un progressivo ampliamento delle tipologie di informazioni diffondibili che appare strettamente connesso alle peculiarità di ciascun strumento di comunicazione. Così, se su una rivista cartacea era possibile inserire prima testi e poi fotografie e disegni, oggi, grazie agli strumenti informatici, caratterizzati da un'estrema duttilità, possono essere trasmesse informazioni di qualsiasi tipologia: testi, immagini, fotografie, audio, video. L'interconnessione reciproca fra i computer e gli altri dispositivi dotati di capacità elaborative (si pensi ai moderni telefoni cellulari che consentono, fra l'altro, di navigare sul web e di controllare la posta elettronica), resa possibile da Internet, permette un accesso continuativo a tali informazioni.

Così, alcuni decenni fa, proprio l'informatica ha dato nuova linfa al dibattito sulla privacy e proprio la diffusione delle banche dati, che consentono di archiviare e di operare sui dati con celerità ed efficienza prima impossibili, ha spinto diversi stati ad emanare leggi al fine di limitare l'invadenza di determinati usi degli strumenti informatici. In tal modo la discussione sulla privacy è maturata ed è emersa con forza l'esigenza di tutelare il nascente diritto all'autodeterminazione informativa[79], ossia al diritto di controllare i propri dati.

La progressiva invasività delle moderne tecnologie ha però radicalizzato le problematiche connesse al diritto alla privacy. Come ha giustamente sottolineato Stefano Rodotà, vi sono mutamenti che

[79] Tale diritto «sembra includere il potere dell'interessato di determinare: se un dato personale possa essere raccolto da un terzo (controllo sulla raccolta dei dati); di determinare se il dato possa essere trasmesso ad altri (controllo sulla diffusione del dato); di determinare le forme dell'impiego del dato (controllo sull'elaborazione del dato); di accedere ai propri dati e di ottenerne la rettifica quando siano inesatti (controllo sulla correttezza del dato); di ottenere la rimozione dei propri dati (diritto alla cancellazione o all'oblio)» (così G. Sartor, *Privacy, reputazione, affidamento: dialettica e implicazioni per il trattamento dei dati personali*, in F. Bergadano *et al.*, *Privacy digitale. Giuristi e informatici a confronto*, Giappichelli, Torino, 2005, p. 82).

giungono addirittura a toccare l'antropologia stessa delle persone. Così, la persona non viene solamente "scrutata" attraverso la videosorveglianza e le tecniche biometriche, ma può addirittura essere "modificata" in seguito all'inserimento di componenti elettronici ed "etichette intelligenti" (si pensi ai chip RFID[80]). L'essere umano diviene, quindi una *networked person*, perennemente in rete e costantemente controllato nei suoi movimenti, abitudini e contatti[81].

Si registra, quindi, una tendenza a non distinguere fra mezzi e fini, ritenendo lecito tutto ciò che sia possibile fare e sacrificando troppo spesso il diritto alla privacy del «buon cittadino».

Alla suddetta tendenza si accompagna, inoltre, un'esasperazione del mezzo «che sembra oscurare il fine stesso, anzi finisce col dettare i fini […]. Tuttavia occorre rendersi conto della necessità, ma anche della difficoltà, di reperire dei principi a cui collegare una eventuale normativa: la scissione tra fini e mezzi è anche la scissione tra principi e norme e sul piano del giuridico il rischio è che la norma stessa, disancorata dai principi, detti fini che possano raggiungersi solo perché esistono mezzi per farlo, accrescendo il senso di deresponsabilizzazione dell'uomo di fronte al proprio mondo […]. Nella inversione mezzi-fini balza in primo piano l'utilizzabilità del mezzo per la definizione dei fini, piuttosto che il problema di trovare mezzi per raggiungere i fini»[82].

Spetta, quindi, al legislatore raggiungere un giusto equilibrio fra le esigenze contrastanti ed, eventualmente, operare la distinzione fra mezzi e fini qualora si renda necessaria. Tuttavia, sembra che la scelta effettuata dal legislatore negli ultimi anni sia caratterizzata dalla volontà di «burocratizzare» il diritto alla privacy, imponendo così tanti limiti e procedure formali che, lungi dal garantire effettivamente il menzionato diritto, lo fanno percepire ai più come un'altra pastoia burocratica.

Si pensi al cod. priv., che se da un lato ha l'indubbio merito di costituire una disciplina organica, dall'altro è caratterizzato da rigidi requisiti, da procedure complesse e da un regime sanzionatorio

---

[80] Su tale tematica si veda *infra*, cap. 3, par. 2.

[81] S. Rodotà, *Trasformazioni del corpo*, cit., pp. 8-9.

[82] T. Serra, *L'uomo programmato*, Giappichelli, Torino, 2003, pp. 97-98.

sin troppo elevato, come si è visto tratteggiandone gli aspetti generali[83].

Del resto, autorevole dottrina ha osservato che «viviamo ormai in una *law-saturated society*, in una società strapiena di diritto, di regole giuridiche dalle provenienze più diverse, imposte da poteri pubblici o da potenze private, con una intensità che fa pensare, più che a una necessità, a una inarrestabile deriva. La consapevolezza sociale non è sempre adeguata alla complessità di questo fenomeno, che rivela anche asimmetrie e scompensi fortissimi, vuoti e pieni, con un diritto invadente in troppi settori e tuttavia assente là dove se ne avvertirebbe il bisogno»[84].

Bisogna sottolineare, però, che la complessità della materia, unitamente all'incessante sviluppo tecnologico, complicano notevolmente l'attività di regolamentazione, per cui ad un impianto normativo più o meno pregevole si affiancano, necessariamente, le attività di controllo e di tutela effettuate dal Garante per la protezione dei dati personali. Nello svolgimento dei suoi compiti l'*authority* in questione ha di norma dimostrato prontezza e sensibilità nel recepire le istanze avanzate da persone fisiche e persone giuridiche, anche se taluni suoi interventi hanno fatto discutere.

Si pensi al caso *Le Iene*, celebre trasmissione televisiva a metà fra il serio e il faceto: in preparazione di un *reportage* giornalistico erano stati raccolti, nei luoghi antistanti il Parlamento, campioni biologici di circa cinquanta parlamentari utilizzati per effettuare un test volto a rilevare l'eventuale uso recente di sostanze stupefacenti. Il Garante è intervenuto, con provvedimento del 14 dicembre 2006, ed ha ritenuto illecito il suddetto trattamento, bloccando così la trasmissione prima che questa andasse in onda. Nel caso di specie, però, i dati erano stati anonimizzati e nessuno avrebbe potuto collegare i tamponi utilizzati per raccogliere i campioni organici

---

[83] Si consideri, a titolo esemplificativo, la minuziosa disciplina delle misure minime di sicurezza di cui all'Allegato B al cod. priv., oppure il delitto di omessa adozione di misure minime di sicurezza di cui all'art. 169, comma 1, cod. priv., ai sensi del quale tale condotta è punita con l'arresto sino a due anni o con l'ammenda da 10.000 a 50.000.

[84] S. Rodotà, *La vita e le regole. Tra diritto e non diritto*, Feltrinelli, Milano, 2006, p. 9.

con l'identità dei singoli interessati[85]. Tale provvedimento, qui citato a titolo esemplificativo, ha suscitato un notevole clamore perché è sembrato finalizzato alla protezione di un interesse non meritevole di tutela. Difatti, dal momento che in Italia vige il divieto di far uso di sostanze stupefacenti e che detto divieto è stato imposto *ex lege* dal Parlamento, sapere se i rappresentanti del popolo rispettano quelle stesse leggi da loro votate costituisce espressione di un interesse pubblico.

Taluni "rappresentati", però, non hanno beneficiato di una simile prontezza nella fase iniziale del c.d. caso Peppermint[86], anche se successivamente l'operato del Garante è risultato fondamentale per garantire la tutela della loro privacy. Il caso appena citato trova origine nei ricorsi della "Peppermint Jam Records GmbH" al Tribunale di Roma, con i quali si richiedeva di identificare, inizialmente, 3.636 intestatari di linee telefoniche che si sarebbero connessi ad Internet ed avrebbero scaricato e/o posto in condivisione file musicali contenti brani di artisti sotto contratto con la suddetta società. Sul presupposto della violazione del diritto d'autore era stata invocata l'applicazione dell'art. 156-*bis* della legge 22 aprile 1941, n. 633, ai sensi del quale il titolare di un diritto d'autore può chiedere e ottenere, anche da soggetti terzi rispetto agli autori della violazione, la comunicazione delle informazioni necessarie all'individuazione degli autori della violazione. Da un punto di vista tecnico, il reperimento degli indirizzi IP è stato reso possibile da un *software*, sviluppato ed utilizzato da una società svizzera (la "Logistep AG"), che ha dunque svolto delle vere e proprie "indagini" al pari dell'autorità giudiziaria. Il Tribunale di Roma ha inizialmente accolto le tesi della ricorrente ed ha ordinato al *provider* resistente di fornire tali nominativi.

Dopo numerose proteste e mobilitazioni *on line*, riportate anche dai mass media, il Garante ha iniziato ad occuparsi della questione e si è poi costituito nei successivi giudizi instaurati dalla società svizzera. Già nel primo di essi la situazione è stata ribaltata e il Tribunale di Roma, con ordinanza del 16 luglio 2007, ha rigettato

---

[85] A. Monti, *Il caso "Le Iene" e le funzioni del Garante*, in http://www.interlex.it/675/amonti87.htm.

[86] Su di esso v. anche *infra*, cap. 2, § 5.

le domande della Peppermint Jam Records GmbH, ritenendo l'inapplicabilità, al caso di specie, degli artt. 156 e 156-*bis* l. n. 633/41: secondo il giudice romano, infatti, la compressione del diritto alla riservatezza può avvenire solo «per la tutela di valori di rango superiore e che attengono alla difesa della collettività ovvero alla protezione dei sistemi informatici».

Tuttavia, nelle more degli ulteriori procedimenti, i 3.636 intestatari delle linee telefoniche di cui si è detto erano già stati individuati e raggiunti da altrettante richieste di risarcimento del presunto danno subito dalla società tedesca. È d'uopo rilevare che la condotta della Logistep AG costituisce una violazione del cod. priv., essendosi concretizzata in numerosi trattamenti illeciti di dati personali, come ha poi ribadito il Garante con provvedimento del 28 febbraio 2008, con cui è stato vietato l'ulteriore trattamento dei dati personali ed è stata disposta la cancellazione dei dati illecitamente acquisiti.

Il caso Peppermint ha mostrato pregi e difetti della normativa sulla protezione dei dati personali, che ha garantito la tutela del diritto alla privacy degli utenti "intercettati" dalla Logistep AG, nonostante alcuni di essi abbiano dovuto sopportarne una violazione che si è poi dimostrata temporanea grazie all'intervento del Garante.

Il caso è tuttavia emblematico di una progressiva involuzione del diritto alla privacy, forse soffocato fra normative sin troppo complesse ed applicazioni concrete, da parte della giurisprudenza, che in alcuni casi sembrano lontane da quelle, lungimiranti, espresse negli anni Sessanta dai giudici di merito e negli anni Settanta dal Giudice di legittimità.

Capitolo II

# ALCUNE PROBLEMATICHE DELLA COMUNICAZIONE GLOBALE

## 1. *Internet: profili problematici*

Internet è stata definita «la base tecnologica della forma organizzativa dell'Età dell'informazione», capace «di distribuire la potenza dell'informazione in tutti i campi dell'attività umana»[1]. La sua celere ed inarrestabile diffusione impone, quindi, una riflessione sulla problematicità di alcune conseguenze che ne derivano soprattutto in tema di privacy. Come si è visto, le varie regolamentazioni *in subiecta materia* sono state emanate, per lo più, al fine di difendere i dati personali (e dunque la persona stessa) dalla creazione di banche dati informatiche e dall'utilizzo di strumenti elettronici idonei a trattare le medesime informazioni.

Conseguenza naturale della progressiva diffusione della rete Internet è dunque una maggiore difficoltà nel garantire un'effettiva protezione del diritto alla riservatezza. Per via telematica è possibile trasmettere una mole anche notevole di informazioni in pochi istanti, per cui gli effetti di un'eventuale violazione di tale diritto non solo possono propagarsi in tutto il mondo, ma addirittura essere inarrestabili: una volta che un flusso di dati è stato trasmesso, esce dalla sfera di controllo del soggetto che ha operato la trasmissione e, qua-

[1] M. Castells, *Galassia Internet*, tr. it., Feltrinelli, Milano, 2001, p. 13.

lora sia stato acquisito da terzi, risulta quasi impossibile impedirne diffusioni ulteriori.

Ciò è dovuto alle caratteristiche strutturali di Internet, che è stata sviluppata come una rete decentralizzatata, nella quale vi sono numerosi elaboratori interconnessi (i c.d. nodi), ai quali, a loro volta, sono connessi altri elaboratori[2]. Risulta così intuitiva la sua definizione di "rete delle reti", posto che, come si è visto, essa è un *network* di computer ai quali, di norma, sono a loro volta connessi altri elaboratori. Pertanto, Internet è una rete che collega più reti[3], uscita dal ristretto ambito militare per essere in seguito utilizzata anche nelle università, nei luoghi di lavoro e nelle comuni abitazioni[4].

Bisogna precisare che l'interconnessione dei diversi sistemi è stata resa possibile dall'adozione di alcuni protocolli di comunicazione che sono stati poi implementati in quasi tutti i sistemi informatici esistenti. Alla base del funzionamento di Internet vi è la modalità di trasmissione dei dati a commutazione di pacchetto; i vari computer dialogano grazie al c.d. protocollo TCP/IP, che in realtà non è un protocollo unico bensì un insieme di protocolli. I protocolli svolgono la stesa funzione del linguaggio per l'uomo: consentono agli elaboratori di identificarsi, di dialogare e di scambiarsi dati. Appare utile evidenziare che ogni elaboratore connesso ad Internet viene identificato mediante il c.d. indirizzo IP, che è composto da quattro triplette di numeri, ciascuna separata da un punto; esso è univoco,

---

[2] Per una storia di ARPAnet e di Internet cfr.: J. Abbate, *Inventing the Internet*, MIT Press, Cambridge, Massachusetts, 1999; G. Fioriglio, *Temi di informatica giuridica*, Aracne, Roma, 2004; C. Gubitosa, *La storia di Internet*, Apogeo, Milano, 1999; sulla storia del *World Wide Web* cfr. T. Berners-Lee, *L'architettura del nuovo Web*, tr. it, Feltrinelli, Milano, 2001.

[3] Più precisamente, Internet è una WAN (*Wide Area Network*) che collega più LAN (*Local Area Network*).

[4] Come è stato rilevato in dottrina, è paradossale che una tecnologia sviluppata per potenziare la più grande potenza militare esistente sia inizialmente diventata il punto d'incontro virtuale della controcultura pacifista universitaria per poi trasformarsi in una zona di extraterritorialità virtuale nella quale va creandosi una comunità globale post-tradizionale, spinta da ideali di solidarietà e di cooperazione e cosciente della fondamentale importanza della propria libertà di opinione (in tal senso A. Viterbo, A. Codignola, *La rete: tecnologia di libertà?*, in *Il diritto dell'informazione e dell'informatica*, 2003, 2, pp. 225-226).

per cui in rete non possono esservi due o più macchine con lo stesso indirizzo.

Ovviamente alla crescita del numero di computer interconnessi conseguirà, prima o dopo, un esaurimento degli indirizzi IP disponibili, poiché, com'è noto, in pochi decenni Internet si è sviluppata e diffusa a macchia d'olio, tanto che oggi viene anche vista come la rete globale: la sua estensione abbraccia praticamente quella dell'intero pianeta. Si consideri, oltretutto, che, anche in assenza di cavi di trasmissione dei dati, è possibile utilizzare connessioni *wireless*, ossia senza fili. La parallela diffusione, forse ancor più rapida, dei telefoni cellulari consente così di avere una connessione ad Internet in moltissimi luoghi e di navigare e comunicare anche in assenza di computer grazie a terminali mobili sempre più evoluti.

Una simile diffusione, però, non sarebbe stata possibile se il *world wide web* non fosse stato inventato. Nonostante ancora alcuni identifichino Internet con il web, essi sono ben distinti. Internet è la rete di comunicazione; il web è un'applicazione che consente di "navigare" consultando pagine scritte in formati ipertestuali ed utilizzando il protocollo HTTP.

Appare chiara la rivoluzione sottesa a tale modello: viene infatti superata la rigida sequenzialità nella comunicazione delle informazioni, avvenga essa mediante libri, riviste, trasmissioni televisive o radiofoniche. Il fruitore dell'informazione può spesso sfruttare i vantaggi degli ipertesti ed utilizzare i collegamenti eventualmente presenti. Ad esempio, se in un testo si cita una norma, è possibile inserire il collegamento ad essa, evitando che il lettore debba cercarla altrove.

Vi è di più. Una rete decentralizzata come Internet dona una grande libertà a chi la utilizza e rende difficili, seppur non impossibili, i tentativi di controllarla, posto che, in ipotesi, addirittura la distruzione di una parte della rete non potrebbe bloccarne il funzionamento.

A tale libertà fa tuttavia da contraltare il cattivo uso che se ne può fare, per cui si pone il problema di assicurare la giusta protezione in caso di violazione di diritti ed interessi meritevoli di tutela, ma bisogna considerare che tutto ciò risulta reso più difficile dall'immaterialità delle informazioni in formato digitale nonché da quella ca-

ratteristica che molti definiscono di a-territorialità di Internet. Più che di a-territorialità potrebbe tuttavia parlarsi di omni-territorialità, poiché la rete abbraccia così tanti territori da renderla onnipresente.

Indubbiamente entrambi questi profili suscitano interesse e sono idonei a mettere in difficoltà i soggetti, dal momento che essi, nel bene e nel male, sono stati sempre legati alla materialità sia dei supporti che contengono le informazioni sia dei luoghi in cui viene condotta la propria esistenza.

Il diritto non può certo restare insensibile a tali mutamenti, ma quando l'immaterialità diventa un suo oggetto si verifica una vera e propria rivoluzione perché la tradizione giuridica è generalmente legata alla corporeità[5].

È ben nota, oltretutto, la forte relazionalità fra l'uomo e il territorio in cui vive; si pensi che ancor oggi le tradizioni sono sovente legate a determinati luoghi, per quanto l'evoluzione della società imponga cambiamenti assai importanti anche sotto tale aspetto in conseguenza di fenomeni come l'emigrazione. Ciò nondimeno, capita sempre più spesso che al mutamento territoriale si accompagni una rivendicazione delle usanze della propria terra di origine, che si vogliono perpetuare anche nel luogo di destinazione.

Tali istanze di norma sono riconosciute anche da molti stati moderni e in particolar modo da quelli democratici, che sovente tutelano tradizioni diverse dalle proprie[6]. Quasi paradossalmente, dunque, alcuni usi e costumi, seppur legati alla territorialità e da essa derivanti, la superano ma al tempo stesso continuano ad esservi indissolubilmente legati.

---

[5] V. Zeno-Zencovich, *Informatica ed evoluzione del diritto*, in *Il diritto dell'informazione e dell'informatica*, 2003, 1, p. 92.

[6] Del resto, oggi la persona umana «si trova a poter disporre di un «patrimonio di diritti» che può spendere, esercitare in luoghi diversi, ricercando proprio quelli dove non esistono divieti o limitazioni che ostacolano le libere scelte delle persone. E proprio la possibilità di agire in una dimensione che si dilata, fino a coincidere con il mondo, rende problematiche molte limitazioni dell'autonomia dei soggetti, poiché ormai ogni restrizione nazionale è destinata a entrare sempre più in concorrenza con le discipline meno rigide offerte da altri paesi» (S. Rodotà, *La vita e le regole. Tra diritto e non diritto*, Feltrinelli, Milano, 2006, p. 55).

Bisogna tuttavia considerare che «l'occupazione del territorio è l'atto primordiale che istituisce il diritto, e senza il suo territorio lo Stato moderno sarebbe un nonsenso»[7]. Lo stato risulta fortemente incentrato su un concetto di spazialità inteso nella sua accezione tradizionale, dal momento che il concetto di territorio può essere ricondotto all'ambito spaziale sul quale esercita il proprio dominio.

L'informatica, così, impone dei cambiamenti che avvengono a livelli diversi e la rete diviene sia il mezzo di trasmissione che il "luogo" dove si trova una derivazione "digitale" della realtà.

La dottrina statunitense ha tuttavia evidenziato che i giudici usano sempre più spesso la metafora del ciberspazio come "luogo" al fine di giustificare l'applicazione ad esso delle leggi tradizionali che regolano la proprietà materiale, con conseguenze spesso discutibili[8]. Tale metafora è stata addirittura ritenuta "ridicola", poiché nessuno è "nel" ciberspazio e la vera novità di Internet consiste in un progetto semplice basato su protocolli di comunicazione condivisi che sono utilizzati da sistemi diversi[9].

Sul punto, potrebbe sostenersi che la maggior parte degli utilizzatori di Internet non la percepisca «come qualcosa di nemmeno minimamente simile allo spazio reale»[10], ma forse ciò è dovuto al fatto che la connessione automatica e praticamente istantanea a pagine provenienti da tutto il mondo provoca nell'utilizzatore la sensazione di viaggiare attraverso il ciberspazio. Appare, dunque, paradossale l'atteggiamento di voler ricondurre a tutti i costi Internet allo spazio fisico, come sembrano fare molte corti statunitensi, con ciò rischian-

---

[7] A.C. Amato Mangiameli, *Diritto e cyberspace. Appunti di informatica giuridica e filosofia del diritto*, Giappichelli, Torino, 2000, p. 8.

[8] Cfr D. Hunter, *Cyberspace as a place, and the Tragedy of the Digital Anticommons*, in *California Law Review*, 2003, 2, pp. 439-519 e M. O'Rourke, *Property Rights and Competition on the Internet: In Search of an Appropriate Analogy*, in *Berkeley Technology Law Journal*, 2001, 1, pp. 561-630.

[9] M. Lamley, *Luogo e cyberspazio*, in V. Colomba (a cura di), *I diritti nell'era digitale. Libertà di espressione e proprietà intellettuale*, Diabasis, Reggio Emilia, 2004, p. 78.

[10] Ivi, pp. 79-80.

do di eliminare l'interconnessione, che costituisce, chiaramente, uno degli aspetti che connaturano l'essenza stessa del ciberspazio[11].

Come è stato giustamente sottolineato, Internet «ridefinisce la distanza ma non cancella la geografia. Dai processi simultanei di concentrazione spaziale, decentramento e connessione, elaborati incessantemente, dalla geometria variabile dei flussi informazionali globali, emergono nuove configurazioni territoriali»[12].

Non si deve però dimenticare che le metafore e i riferimenti alla tradizione giuridica e sociale hanno comunque un'indubbia utilità, poiché consentono di adattarsi alle novità senza farsi travolgere dal loro impatto. Nel caso di specie, non può certo prescindersi dai riferimenti al mondo reale, dal momento che la c.d. realtà "virtuale" non è certo staccata dalla realtà per così dire "tradizionale", ma ne è una componente.

Ciò che accade *on line*, infatti, non avviene in una dimensione parallela, come in un racconto di fantascienza. È tutto "tremendamente" reale e le conseguenze degli atti svolti *on line* hanno sovente effetti immediati e diretti *off line*: basti pensare alle transazioni elettroniche oppure a quanto scritto su un sito web.

Tale considerazione non dovrebbe però portare ad un'applicazione generalizzata e forzata delle normative preesistenti per timore di un *horror vacui* che talvolta è meglio che sussista, poiché è quasi fisiologico che non tutte le fattispecie possano essere aprioristicamente regolamentate dal legislatore, anche nel rispetto dei principi di generalità ed astrattezza delle norme. Ciò potrebbe portare a non tutelare situazioni che, astrattamente, potrebbero essere ritenute meritevoli di protezione giuridica, ma anche la certezza del diritto deve essere garantita poiché mette al riparo da arbitrii effettuati in via interpretativa.

Nei termini sopra esposti, è stato ritenuto che sia giusto riflettere sulle problematiche relative ad Internet facendo riferimento al mondo reale già in virtù del fatto che l'autorità giudiziaria debba applicare in tali casi le leggi del mondo reale a quello virtuale. Conseguenze negative, invece, potrebbero derivare da un'applicazione cie-

---

[11] *Ibidem*.

[12] M. Castells, *Galassia Internet*, cit., p. 195.

ca della metafora per raggiungere un certo risultato, cui potrebbero potenzialmente conseguire fraintendimenti; il ricorso alla metafora sarà quindi utile solo se verranno compresi i suoi limiti, ossia che Internet non è come il mondo fisico[13], anche se, si ribadisce, ciò che accade nel mondo "virtuale" accade nel mondo "fisico"[14].

Non dovrebbe poi essere dimenticato che, come è stato giustamente sottolineato in dottrina, «Internet è senza dubbio una grande occasione per la creazione di una società globale, di una *koinè*, che, di contro ad una globalizzazione che si presenta sempre più come prevalenza dell'economico sulle altre sfere della vita pratica, recuperi la dimensione della relazionalità»[15].

Tali profili, connessi alla carica dirompente di Internet, non hanno però messo in crisi unicamente lo Stato, ma anche i mezzi di comunicazione di massa, i quali, a loro volta, avevano fatto emergere con veemenza la necessità di tutelare il diritto alla privacy.

I mass media tradizionali, com'è noto, sono caratterizzati dalla unidirezionalità della comunicazione, per cui il fruitore ha poca libertà di scelta e può solo ricevere informazioni, ma non fornirle.

Inoltre, i mass media operano come "filtri e guardiani"[16], poiché mediante essi la comunicazione delle idee non può avvenire in modo diretto, ma deve invece essere filtrata da una serie di intermediari. Internet ridimensiona il ruolo di questi "filtri", dal momento che chiunque può, allo stesso tempo, essere fruitore e fornitore di informazioni, oltre ad avere a disposizione un "pubblico" potenzialmente vasto e internazionale.

La comunicazione, così, può essere non solo "da uno a uno", come nel caso della corrispondenza elettronica, ma anche "da uno a molti", come negli esempi di siti web, blog, forum, ecc., dove si può far conoscere il proprio pensiero senza limitazioni ad una platea po-

---

[13] M. Lamley, *Luogo e cyberspazio*, cit., p. 91.

[14] In argomento cfr. anche T. Maldonado, *Reale e virtuale*, Feltrinelli, Milano, 2007.

[15] M. Sirimarco, *Tra apocalittici ed integrati: spunti di riflessione sul rapporto uomo-internet*, in A.C. Amato Mangiameli (a cura di), *Parola chiave: informazione*, Giuffré, Milano, 2004, p. 287.

[16] J. Balkin, *Come cambiano i diritti: la libertà di espressione nell'era digitale*, in V. Colomba (a cura di), *I diritti nell'era digitale. Libertà di espressione e proprietà intellettuale*, cit., p. 3.

tenzialmente indefinita di soggetti. Autorevole dottrina ha dunque evidenziato che, come la diffusione della stampa in Occidente ha creato quella che è stata definita la "Galassia Gutenberg", lo sviluppo e la diffusione di Internet hanno portato alla nascita della "Galassia Internet"[17].

In tal senso, è emblematico il successo dei c.d. blog, termine che corrisponde alla contrazione dell'espressione *web log* e che identifica una tipologia di siti web di contenuto generale: alcuni blog sono infatti paragonabili alle riviste *on line*, ma altri sono più simili a diari *on line* dove ciascun *blogger* può manifestare liberamente il proprio pensiero.

In linea generale tutti i blog possono contenere, oltre che testo, anche immagini, suoni e filmati; la creazione e la gestione di un blog è, a dispetto della complessità che taluni di essi sembrano avere, un'attività rapida, veloce ed economica, posto che sono disponibili diverse piattaforme gratuite, sia per la loro creazione che per la loro pubblicazione, che possono così essere svolte anche da parte di soggetti dotati di conoscenze informatiche tutt'altro che avanzate. Di qui il grande successo dei blog, che sono usciti dal ristretto ambito dei diari *on line*, già diffusi negli anni Novanta ma utilizzati soprattutto in settori riconducibili al mondo dell'informatica, per essere oggi utilizzati non solo da moltissime persone comuni, ma anche da personaggi celebri (comici, politici, cantanti, ecc.) e addirittura da aziende, che in taluni casi mettono *on line* dei blog nei quali promuovono i propri prodotti in maniera diversa rispetto ai metodi pubblicitari tradizionali.

Diviene così assai semplice manifestare liberamente il proprio pensiero, magari cullandosi in un apparente anonimato, e svolgere un ruolo simile a quello svolto dai mass media, seppur con le intuibili differenze: un conto è disporre di una vera e propria redazione giornalistica, tutt'altro è creare e gestire un blog, a meno che un mass media tradizionale non scelga di esprimersi anche con tali modalità.

In ogni caso, il blog è, per lo più, frutto dell'attività di un singolo, ma può capitare che alcuni fatti divengano di pubblico dominio

[17] M. Castells, *Galassia Internet*, cit., p. 14.

grazie all'attività di blogger che segnalano una notizia che viene poi ripresa da altri e quindi inizia a diffondersi, il tutto grazie all'aiuto sia di motori di ricerca generici che di quelli specificatamente dedicati ai blog: questi ultimi, in particolare, consentono ai propri utenti registrati di segnalare le notizie più interessanti in modo che possano essere conosciute anche dalla rispettiva *community*[18].

Le conseguenze che derivano da queste nuove possibilità di manifestare liberamente ed efficacemente il proprio pensiero non sono, però, tutte positive. Posto che Internet dà ai suoi utilizzatori tale possibilità su scala globale (anche se ciò non significa che l'audience reale possa poi essere minimamente paragonabile a quella potenziale) bisogna evidenziare che il giusto prezzo da pagare per godere della libertà è quello di essere responsabili per ciò che si dice e si scrive, per cui se dovesse essere violata la privacy altrui o se, ad esempio, qualcuno dovesse essere diffamato *on line*, l'autore del blog potrebbe essere citato in giudizio per rispondere dell'illecito commesso.

Taluni, però, scrivendo sul web, sembrano cullarsi in un inesistente anonimato e quindi ritengono di godere di una impunità *de facto*, ma tale credenza è chiaramente fallace. Mediante l'indirizzo IP, infatti, è possibile essere identificati, nonostante la maggior parte dei computer connessi abbia un indirizzo dinamico. Anche volendo prescindere dalla conoscibilità della suddetta informazione, può comunque essere possibile risalire all'effettivo creatore di un blog o comunque di determinati contenuti inseriti *on line* mediante l'analisi incrociata dei vari dati personali sparpagliati per il web.

Si pensi, del resto, che in un caso giudiziario il gestore di un blog è stato equiparato al direttore responsabile di una testata giornalistica perché ha un potere di controllo su quanto viene diffuso sul blog medesimo e deve quindi eliminare i contenuti offensivi. Se ciò non avviene, può essere imputato del reato di diffamazione a mezzo della stampa, previsto e punito dall'art. 596-*bis* cod. pen.[19].

---

[18] Come Digg (http://www.digg.com) e Technorati (http://www.technorati.com), sviluppati negli Stati Uniti.

[19] Trib. Aosta, 26 maggio 2006, in *Il diritto dell'informazione e dell'informatica*, 2006, 3, pp. 366-373, nonché in *Diritto dell'internet*, 2006, 5, pp. 486-488, con note di P. Galdieri, *Profili di diritto penale*, pp. 489-493, e di E. Falletti, *Profili di diritto comparato*, pp. 493-498.

Chiaramente, quindi, ad una più ampia libertà di espressione e ad un migliore accesso all'informazione consegue un trasferimento di responsabilità agli individui e ai principali "agenti" sociali, che però non richiede «una maggiore censura, bensì un'educazione del tutto nuova nelle capacità etiche e critiche»[20].

Del resto, Internet dovrebbe rimanere «un luogo dove possano essere esercitate le libertà di comunicazione, informazione, associazione e iniziativa economica»[21]. Il problema principale, dunque, consiste nel trovare il giusto bilanciamento fra la garanzia del rispetto dell'autodeterminazione informativa individuale e collettiva, intesa in senso ampio, e la definizione di criteri che consentano una effettiva protezione delle parti lese qualora si verifichi un illecito.

Appare chiaro che, per quanto l'anonimato *on line* sia quasi una chimera[22], possono sorgere notevoli difficoltà, se non talvolta l'impossibilità materiale, nel giungere all'identificazione dell'autore o degli autori di un illecito. Anche in considerazione di ciò, il legislatore comunitario e quello italiano hanno delineato la disciplina della responsabilità degli Internet *providers*, che sono gli intermediari fra il ciberspazio e coloro che vi navigano, mediante l'emanazione del d.lgs. 9 aprile 2003, n. 70, di attuazione della direttiva n. 2000/31/CE «relativa a taluni aspetti giuridici dei servizi della società dell'informazione, in particolare il commercio elettronico, nel mercato interno».

Il legislatore ha previsto tre tipologie principali di responsabilità del *provider*, denominate rispettivamente responsabilità per sem-

---

[20] P. Levy, *Verso la ciberdemocrazia*, in D. De Kerckhove, A. Tursi (a cura di), *Dopo la democrazia? Il potere e la sfera pubblica nell'epoca delle reti*, Apogeo, Milano, 2006, p. 7.

[21] G. Sartor, *Il diritto della rete globale*, in G. Scorza, *Il diritto dei consumatori e della concorrenza in Internet. Pubblicità, privacy, contratti, concorrenza e proprietà intellettuale nel cyberspazio*, Cedam, Padova, 2006, p. 28.

[22] Oggi, inoltre, si verifica un conflitto fra l'interesse all'anonimato e quello «a conoscere l'identità di chi, presentandosi in forme anonime o con identità diverse da quella ufficiale, tiene comportamenti contrari alla riservatezza altrui. Si gioca una partita più complessa tra una *privacy attiva* ed una *passiva*» (S. Rodotà, *Tecnopolitica*, Laterza, Roma-Bari, 1997, p. 146).

plice trasporto (*mere conduit)*[23], per memorizzazione temporanea (*caching*)[24] e per memorizzazione delle informazioni (*hosting*)[25].

In linea generale, tale disciplina non pone i *providers* nello scomodo ruolo di capri espiatori di eventuali illeciti commessi *on line*, ma ne sancisce la responsabilità qualora la loro condotta sia caratterizzata da negligenza, imprudenza, imperizia[26]. Così, su di essi

---

[23] L'art. 14 d.lgs. n. 70/2003 esonera da responsabilità sia il prestatore di un servizio di trasmissione, su una rete di comunicazione, di informazioni per conto degli utenti (*mere conduit*) che un *access provider*, purché essi non diano origine alla trasmissione, non ne selezionino il destinatario e non selezionino né modifichino le informazioni trasmesse.

[24] L'art. 15 d.lgs. n. 70/2003 esonera da responsabilità il prestatore di un servizio di *caching*, ossia della memorizzazione sui propri elaboratori di determinate informazioni reperite *on line*, al fine di agevolarne l'accesso ai destinatari del servizio, purché il prestatore non modifichi le informazioni, si conformi alle condizioni di accesso alle informazioni ed alle norme di aggiornamento delle informazioni, non interferisca con l'uso lecito di tecnologia ampiamente riconosciuta e utilizzata nel settore per ottenere dati sull'impiego delle informazioni, agisca prontamente per rimuovere le informazioni che ha memorizzato, o per disabilitare l'accesso, non appena venga effettivamente a conoscenza del fatto che le informazioni sono state rimosse dal luogo dove si trovavano inizialmente sulla rete o che l'accesso alle informazioni è stato disabilitato oppure che un organo giurisdizionale o un'autorità amministrativa ne ha disposto la rimozione o la disabilitazione.

[25] L'art. 16 d.lgs. 70/2003 esonera da responsabilità chi effettua la «memorizzazione di informazioni fornite da un destinatario del servizio», ossia l'*host provider*, per le informazioni memorizzate a richiesta di un destinatario del servizio, purché il prestatore del servizio non sia effettivamente a conoscenza del fatto che l'attività o l'informazione è illecita e, per quanto attiene ad azioni risarcitorie, non sia al corrente di fatti o di circostanze che rendono manifesta l'illiceità dell'attività o dell'informazione, non appena a conoscenza di tali fatti, su comunicazione delle autorità competenti, agisca immediatamente per rimuovere le informazioni o per disabilitarne l'accesso (art. 16 d.lgs. n. 70/2003).

[26] Il sistema di responsabilità previsto dal d.lgs. n. 70/2003 sembra «essere basato su una regola di responsabilità per colpa accompagnata da una nozione di conoscenza ricostruita da più indici e collegata al sistema di esenzioni connesse ad attività specificate piuttosto che a categorie diverse di prestatori di servizi. Le esenzioni sono poi di tipo oggettivo […] o di tipo soggettivo in cui oltre a soddisfare determinati requisiti oggettivi è necessario soddisfare ulteriori requisiti soggettivi di diligenza» (G. Comandè, *Al via l'attuazione della direttiva sul commercio elettronico, ma… serve un maggiore coordinamento*, in *Danno e responsabilità*, 2003, 7-8, p. 811). In tale regolamentazione la colpa assume un ruolo centrale nel valutare l'eventuale responsabilità del *provider*: sembra che il legislatore abbia tentato di compiere una delicata operazione di bilanciamento tra due esigenze, ossia quella di individuare sicure figure cui imputare il danno, al fine di non lasciare inascoltate le pretese risarcitorie di chi ha ingiustamente subito un pregiudizio, e quella di non gravare eccessivamente sui soggetti che risultano "colpevoli" solamente di

non grava un generale obbligo né di sorveglianza sulle informazioni che trasmettono o memorizzano né di ricercare attivamente fatti o circostanze che indichino la presenza di attività illecite; devono però attivarsi, informando senza indugio l'autorità giudiziaria o quella amministrativa avente funzioni di vigilanza, qualora siano a conoscenza di presunte attività o informazioni illecite riguardanti un suo destinatario del servizio della società dell'informazione. Devono inoltre fornire senza indugio, a richiesta delle autorità competenti, le informazioni in loro possesso che consentano l'identificazione del destinatario dei suoi servizi con cui ha accordi di memorizzazione dei dati, al fine di individuare e prevenire attività illecite[27].

Bisogna sottolineare, comunque, che l'eventuale previsione di un generale obbligo di controllo da parte del *provider* in ordine al contenuto dei dati immessi in rete dai propri clienti avrebbe certamente contrastato con l'art. 21, comma 1, Cost., ai sensi del quale «tutti hanno diritto di manifestare liberamente il proprio pensiero con la parola, lo scritto e ogni altro mezzo di diffusione»: l'esercizio di tale diritto non può certo essere limitato da soggetti privati, quali, appunto, i *provider*, che non possono divenire dei «censori telematici»[28].

---

essere portatori di una particolare qualifica. La rivalutazione della colpa può dunque assurgere a simbolo della rinuncia sia ad un'aprioristica attribuzione di responsabilità, nei termini di una pura responsabilità oggettiva, che ad una preconcetta negazione di risarcimento nei confronti di chi abbia subito un danno perpetrato per via telematica (così A. Pierucci, *La responsabilità del provider per i contenuti illeciti della Rete*, in *Rivista critica del diritto privato*, 2003, 1, pp. 164-165).

[27] «Il prestatore è civilmente responsabile del contenuto di tali servizi nel caso in cui, richiesto dall'autorità giudiziaria o amministrativa avente funzioni di vigilanza, non ha agito prontamente per impedire l'accesso a detto contenuto, ovvero se, avendo avuto conoscenza del carattere illecito o pregiudizievole per un terzo del contenuto di un servizio al quale assicura l'accesso, non ha provveduto ad informarne l'autorità competente» (art. 17, d.lgs. n. 70/2003).

[28] G. Cassano, I.P. Cimino, *Il nuovo regime di responsabilità dei "providers": verso la creazione di un novello "censore telematico"*, in *I contratti*, 2004, 1, p. 96. Gli autori paventano il rischio che i *provider*, qualora prestino il servizio di *hosting*, preferiranno rendersi inadempienti nei confronti dei clienti che pagano un basso prezzo per tale servizio o che addirittura non pagano nulla, eventualmente rimuovendo informazioni e contenuti che potrebbero essere ritenuti illeciti, ma che potrebbero anche non esserlo.

La necessità di garantire la libertà e la neutralità della Rete, inoltre, può assumere un'importanza fondamentale per lo sviluppo di quelle nuove soggettività che vanno consolidandosi negli ultimi anni, che possono essere inserite nell'ambito di un più generale processo di mutamento delle comunità politiche[29].

Si consideri, infatti, che «le molte forme di aggregazioni "virtuali" che, riunendo transnazionalmente, e a volte anche temporaneamente, molteplici soggetti, modificano i rapporti anche con gli stati e fanno intervenire, per ora, solo virtuali nuovi soggetti che potrebbero però in futuro acquistare forza e visibilità tali da modificare anche gli assetti tradizionali, che diventerebbero non più solo internazionali, perché interstatuali o comunque legati a organizzazioni governative, ma globali, in cui organizzazioni non governative, nuovi soggetti, tra cui anche le organizzazioni virtuali, chiederanno sempre più spazio, forti del loro numero e della consistenza che riusciranno a raggiungere anche grazie a una penetrazione capillare nell'opinione pubblica mondiale in virtù della presenza continua nella rete»[30].

Anche in tal senso, dunque, sembra che l'attuale imposizione di misure di sicurezza, di restrizioni all'accesso al ciberspazio e di censure telematiche debba essere superata per giungere ad una progressiva responsabilizzazione di chi vi si trova, similmente a quanto avviene nei moderni stati democratici, facendo leva sulla possibilità che la persona umana possa comportarsi in modo civile anche *on line*[31].

---

[29] Bisogna sottolineare che ciò non è dovuto unicamente alle potenzialità dei mezzi di comunicazione bidirezionali o interattivi. È stato giustamente affermato, del resto, che il passaggio dalla unidirezionalità all'interattività non garantisce «automaticamente una crescita della democrazia, che non può essere fatta semplicisticamente coincidere con la sostituzione al silenzio di qualche possibilità dei cittadini di manifestare la propria opinione. Può crescere, al contrario, l'uso di un consenso distorto dei cittadini per una attribuire una legittimazione 'democratica' a soluzioni che rimangono sostanzialmente autoritarie o, comunque, legate ad una elaborazione alla quale i cittadini rimangono del tutto estranei. L'interattività, in altri termini, può essere messa al servizio di procedure di ratifica» (S. Rodotà, *Tecnopolitica*, Laterza, Roma-Bari, 1997, p. 40).

[30] T. Serra, *Lo stato e la sua immagine*, Giappichelli, Torino, 2005, p. 131.

[31] D.J. Weitzner *et al.*, *Information Accountability*, MIT Computer Science and Artificial Intelligence Technical Report, MIT-CSAIL-TR-2007-034, 2007, pp. 7-8.

La predisposizione di una sorta di ambiente protetto, nel quale la libertà d'azione viene fortemente limitata, sembra basata sull'idea di un uomo che nel ciberspazio non acquisisce mai la piena capacità di intendere e di volere, ma, piuttosto, risulta incapace da un punto di vista giuridico e fattuale, al pari di un minore o di un interdetto. I diritti, però, non devono e non possono essere tutelati solo all'esterno del ciberspazio.

In virtù di tali considerazioni si comprende la fondamentale importanza di una tutela effettiva del diritto alla privacy, soprattutto inteso nei suoi essenziali profili di diritto all'anonimato e di diritto all'autodeterminazione informativa, sia attiva che passiva. Il *punctum crucis* consiste, tuttavia, nel fatto che l'istanza più avvertita in tali ambiti non sia forse quella di creare strumenti giuridici che consentano l'esercizio dei suddetti diritti, ma, piuttosto, la necessità di evitare l'artificiosa creazione di limiti "legali" al loro esercizio nonché la "legalizzazione" di comportamenti lesivi posti in essere da soggetti pubblici e privati. In altri termini, sembra fondamentale che gli stati contemporanei, democratici e non, lascino il più possibile soli i propri cittadini nella rete, senza soffocare l'esercizio delle loro libertà.

## 2. *Lo sviluppo e l'espansione dei motori di ricerca e dei relativi servizi*

La diffusione di Internet e del web ha portato alla scomparsa di una serie di intermediari tradizionali ed alla nascita di altri, nel cui ambito assumono una particolare rilevanza i motori di ricerca[32].

Bisogna rilevare che la nozione di motore di ricerca (*search engine* in inglese) è, di per sé, più vasta di quella comunemente conosciuta, tendente ad identificarla unicamente con quelli operanti sul web, come i ben noti Google o Yahoo.

Invero, un motore di ricerca è, in linea generale, un programma utilizzato per il reperimento di informazioni archiviate in locale o in

[32] S. Rodotà, *Proprietà, Privacy e Pornografia, le tre "P" di Internet*, in *Problemi dell'informazione*, 2001, 2-3, p. 242.

remoto. Mediante l'interfaccia è possibile inserire una stringa di ricerca, che può essere composta da una o più parole.

Lo svolgimento di una ricerca obbliga, pertanto, l'utente ad individuare le parole chiave in base alle quali effettuarla; di norma la combinazione dei termini viene svolta utilizzando gli operatori logici o booleani[33]. Essi sono fondamentalmente tre, ossia AND (e), che indica la compresenza di due o più elementi; OR (o), che indica l'alternativa fra più elementi; NOT (non), che indica l'inesistenza di uno o più elementi.

Per quanto i motori di ricerca siano strumenti assai utili nell'utilizzo quotidiano di un elaboratore, risultano di fatto indispensabili per navigare sul web, che è composto da una mole notevole di informazioni disorganizzate e decentralizzate; probabilmente senza di essi Internet non avrebbe potuto raggiungere l'attuale diffusione[34].

La considerazione di tali aspetti non deve quindi far stupire in ordine a quanto affermato in uno studio statunitense, secondo cui il marchio attualmente in assoluto più forte è proprio Google[35], che ha superato aziende operanti nei settori "tradizionali" da un numero molto maggiore di anni, visto che esso è stato fondato solo nel 1998.

Di norma i motori di ricerca *on line* operano mediante i c.d. *crawlers*, detti anche *spiders*, i quali sono programmi che esplorano il web seguendo i collegamenti ipertestuali fra le pagine. Una volta reperite le pagine web, essi ne memorizzano il contenuto (operazio-

---

[33] Tali operatori prendono il nome dal matematico inglese George Boole, che li ha teorizzati nell'Ottocento (cfr. G. Boole, *Indagine sulle leggi del pensiero su cui sono fondate le teorie matematiche della logica e della probabilità*, tr. it., Einaudi, Torino, 1976).

[34] È stato giustamente osservato, comunque, che «si sta facendo largo, in numerosi siti, una particolare attenzione alla qualità dell'informazione offerta e alla sua sistemazione organica, tale da garantire un approccio il più "indolore" possibile all'utente che si avvicina alla rete» (G.A. Cavaliere *et al.*, *Manuale breve di informatica per avvocati*, Utet, Milano, 2007, p. 89).

[35] Lo studio, condotto dalla Millward Brown Optimor, è disponibile all'URL http://www.millwardbrown.com/Sites/optimor/Media/Pdfs/en/BrandZ/BrandZ-2007-RankingReport.pdf. È interessante notare che, secondo questo studio, Google è più importante di marchi celebri come Microsoft, Coca Cola e Marlboro. Nel 2006 Google occupava la settima posizione (cfr. http://www.millwardbrown.com/Sites/optimor/Media/Pdfs/en/BrandZ/BrandZ-2006-Top100Brands.pdf).

ne definita di *caching*), in tutto o in parte, che viene analizzato secondo i criteri e le modalità stabilite dai creatori del motore di ricerca.

Reperire ed indicizzare le pagine web è, infatti, una componente fondamentale di un *search engine*, ma la parte intuitivamente più difficile è proprio lo svolgimento dell'analisi automatizzata del contenuto delle pagine al fine di organizzarlo e far sì che chi interroga il motore di ricerca trovi ciò che cerca.

Il problema è che l'acquisizione della conoscenza da parte dei moderni sistemi informatici è molto efficace quando tale attività riguarda unicamente dati per così dire "formali", come il codice HTML di una pagina web, ma la comprensione sostanziale del contenuto di una pagina web è un'operazione che, di norma, può essere efficacemente svolta solo da un essere umano.

Per tale motivo le operazioni di analisi ed organizzazione delle informazioni possono essere agevolate affiancando ad un motore di ricerca automatizzato un'organizzazione gerarchica dei siti web realizzata "a mano" da esseri umani. Ovviamente una tale metodologia impone costi e tempi ben superiori a quelli che derivano dalla devoluzione delle attività di ricerca ed indicizzazione dei siti ad un sistema informatico e possono portare a disomogeneità nei risultati, poiché i criteri da seguire possono essere interpretati in modo più o meno differente da parte dei singoli operatori, mentre una definizione automatizzata dei criteri di ricerca stabilita a priori offre il vantaggio di garantire una maggiore omogeneità dei risultati.

La crescente importanza dei motori di ricerca sia nel reperimento che nell'organizzazione delle informazioni *on line* ha portato la dottrina a rilevare che i motori di ricerca risultano peculiarmente funzionali all'esercizio della libertà di informazione. Più specificatamente, essa viene intesa sia dal lato attivo, come libertà di fornire informazioni sul web, che da quello passivo, quale libertà di ricercare le informazioni su Internet e di non vedersi comunque frapposti ostacoli a tale ricerca. Secondo tale visione, dunque, le regole dettate per l'iniziativa economica privata trovano certamente applicazione nella disciplina dell'attività dei motori di ricerca, che dovrebbero però essere visti anche quali mezzi informativi, poiché incidono sul

fondamentale diritto all'informazione, considerato, a sua volta, essenziale strumento di tutela dei diritti umani[36].

Emergono, quindi, alcuni profili problematici dei *search engines*, soprattutto in riferimento al diritto alla riservatezza. La riflessione su tali aspetti non può essere ignorata, anche perché è probabile che la loro importanza cresca ancor di più in futuro, così come le potenziali violazioni della privacy.

Come si è detto, infatti, già oggi l'incessante sviluppo tecnologico ha portato l'*homo technologicus* ad essere connesso ad Internet in qualsiasi momento ed in qualsiasi luogo, grazie a computer portatili, telefoni cellulari e connessioni senza fili. L'utilizzo di tali strumenti può permettere direttamente *on line* l'identificazione spaziale della persona connessa alla rete grazie al suo indirizzo IP e alle altre informazioni reperibili in virtù della connessione stessa; tali dati potrebbero essere trattati congiuntamente con quelli risultanti dalle ricerche svolte tramite i *search engines*, per cui ciascuna ricerca può essere riferita ad un determinato indirizzo IP e di qui, teoricamente, ad una persona determinata.

Non si può trascurare la circostanza che proprio le stringhe di ricerca, del resto, possono far capire quali siano le preferenze e le opinioni di un soggetto, tanto che essere potrebbero costituire dati sensibili ai sensi della normativa italiana. Una stringa di ricerca, infatti, può certamente «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 «lo stato di salute e la vita sessuale» (art. 4, comma 1, lett. d, cod. priv.), in quanto i termini utilizzati possono chiaramente esplicitare l'interesse di un soggetto verso tematiche relative a tali profili, soprattutto qualora vengano confrontate ricerche svolte in tempi diversi, il cui trattamento incrociato può così portare a delineare parte della personalità di chi ha svolto la ricerca.

Anche nel caso in cui l'indirizzo IP di un elaboratore connesso ad Internet sia dinamico vi sono alcuni dati che possono essere rife-

[36] P. Costanzo, *Motori di ricerca: un altro campo di sfida tra logiche del mercato e tutela dei diritti?*, in *Diritto dell'Internet*, 2006, 6, p. 549.

riti ad una determinata macchina, i quali possono essere salvati nei c.d. *cookies*, ma che possono essere anche ulteriori, come la configurazione *hardware* e *software* della singola macchina mediante la quale viene effettuato il collegamento ad un sito, sia esso di un motore di ricerca o meno.

I *cookies*, in particolare, sono file in formato testuale che vengono creati sul disco rigido del computer di chiunque si colleghi ad un sito web che ne preveda la creazione. Essi possono essere adoperati per raggiungere scopi diversi, come stabilire la frequenza con cui una certa pagina viene visitata da un determinato utente oppure salvare alcune opzioni di personalizzazione della pagine. Inoltre, possono essere riferiti sia al dominio cui ci si collega sia a domini esterni: è questo il caso dei c.d. *cookies* di terze parti, utilizzati soprattutto a fini pubblicitari[37].

Anche i motori di ricerca fanno uso dei *cookies* e la loro conservazione, unitamente a quella di altri dati, può portare alla violazione della privacy dei loro utilizzatori, considerando, oltretutto, la progressiva espansione dell'ambito dei servizi offerti cui può conseguire un trattamento incrociato ed automatizzato delle informazioni archiviate.

In particolare, tutti i maggiori *search engines* offrono il servizio di posta elettronica, ma purtroppo la segretezza delle comunicazioni non viene garantita ovunque e si verificano fattispecie che violano il principio solennemente affermato dalla Costituzione italiana secondo cui «la libertà e la segretezza della corrispondenza e di ogni altra forma di comunicazione sono inviolabili» e dunque «la loro limitazione può avvenire soltanto per atto motivato dell'autorità giudiziaria con le garanzie stabilite dalla legge» (art. 15 Cost.).

Simili norme non sono però oggi vigenti in tutti gli stati, come la Cina, dove l'obiettivo di controllare l'informazione viene perseguito anche mediante collaborazioni con i più noti motori di ricerca, che filtrano i contenuti in modo da non consentirne la conoscenza a chi si trova materialmente nello stato asiatico. In alcuni casi sono sta-

[37] Sugli aspetti giuridici dei *cookies* cfr. V. Caridi, *La tutela dei dati personali in Internet: la questione dei logs e dei cookies alla luce delle dinamiche economiche dei dati personali*, in *Il diritto dell'informazione e dell'informatica*, 2001, 4-5, pp. 763-783.

ti addirittura forniti alle competenti autorità di pubblica sicurezza i dati inerenti gli account di posta elettronica al fine di individuare e punire i dissidenti[38].

I servizi resi dalle aziende che operano nel settore sono tuttavia sempre più ampi ed evoluti: ad esempio, Google offre addirittura una vera e propria suite di programmi da ufficio utilizzabile *on line*. L'integrazione delle funzioni di motori di ricerca e degli altri servizi forniti può però portare ad un controllo di fatto dell'informazione e della vita digitale dell'utente senza che la sua privacy venga effettivamente tutelata.

Si consideri, infatti, che i suddetti servizi sembrano resi gratuitamente, ma invero anch'essi hanno un prezzo da pagare, ossia l'acquisizione automatizzata dei dati personali degli utenti. Basti pensare alla pubblicità personalizzata all'interno delle interfacce web per la consultazione della posta elettronica, come quella che appare, ad esempio, nel servizio email di Google (denominato "Gmail"), che si modifica in maniera dinamica.

Ciò è reso possibile dallo svolgimento di un'analisi automatizzata del contenuto dei messaggi di posta elettronica che mostra poi all'utente solo quelle comunicazioni pubblicitarie pertinenti ai testi delle email, per cui di fatto si verifica una violazione della segretezza delle comunicazioni dell'utente visto che esse vengono scansionate dal sistema, anche se ciò avviene senza alcun intervento umano a quanto riporta la stessa azienda statunitense[39].

Il fatto che l'analisi dei messaggi avvenga automaticamente non implica, tuttavia, che nessuna violazione della riservatezza si verifichi nel caso di specie, posto che tale diritto può essere leso anche tramite sistemi *software* e l'utilizzo di appositi programmi, co-

[38] Si pensi al caso di un giornalista cinese condannato nel 2003 a dieci anni di reclusione per aver diffuso materiale ritenuto sovversivo e che è stato individuato grazie ai dati forniti proprio da un motore di ricerca, nel caso di specie Yahoo. La moglie del giornalista ha però citato in giudizio l'azienda statunitense, chiedendo il risarcimento dei danni e le pubbliche scuse per quanto accaduto (la notizia è stata ripresa da molti siti web; cfr, *ex multis*, http://punto-informatico.it/p.aspx?i=1920381).

[39] Le informazioni sono reperibili all'URL http://mail.google.com/mail/help/intl/it/about_privacy.html (in versione abbreviata) e all'URL http://mail.google.com/mail/help/intl/it/more.html (in versione completa).

me i c.d. agenti *software*. Essi sono sistemi informatici che eseguono compiti specifici previamente determinati e la cui esecuzione avviene senza un controllo diretto da parte dell'uomo. Ovviamente le "azioni" poste in essere direttamente da *software* così evoluti non possono che essere poi giuridicamente riferite ai loro proprietari o utilizzatori e non ci si può certo esimere da responsabilità in virtù della loro autonomia[40].

Inoltre, anche se i dati non vengono comunicati a soggetti terzi, ogni click effettuato dalla pagina in cui si consulta la posta ma che porta poi ad una pagina esterna, visualizzata come collegamento pubblicitario, viene comunque registrato dal sistema al fine di addebitare il click al sito di destinazione, secondo il modello del *pay per click*. In tal modo viene svolto un trattamento di dati personali i quali, in ipotesi, possono addirittura essere sensibili qualora vi siano riferimenti, ad esempio, allo stato di salute o alle preferenze sessuali.

Oltretutto, la riservatezza delle comunicazioni non deve essere vista solo nella prospettiva dell'utilizzatore di servizi di posta elettronica come il citato Gmail, ma anche di coloro che inviano o ricevono messaggi da costoro, che non hanno certo sottoscritto alcuna clausola, vessatoria o meno, che consente a soggetti terzi di operare analisi automatizzate sulla propria corrispondenza resa in forma elettronica.

Sorge, quindi, più di un dubbio sulla liceità di simili trattamenti, anche se l'effettività della tutela in casi simili si scontra con un'ulteriore problematica che non può essere sottovalutata, dovuta al fatto che i servizi sinora menzionati sono resi su scala globale: come tante altre normative, anche quella sulla protezione dei dati personali varia da paese a paese, seppur talvolta, come nel caso delle legislazioni degli stati membri dell'Unione Europea, le regolamentazioni abbiano profili generali comuni grazie all'operato del legislatore comunitario.

---

[40] Sugli agenti *software* cfr. G. Sartor, *Gli agenti software e la disciplina giuridica degli strumenti cognitivi*, in *Il diritto dell'informazione e dell'informatica*, 2003, 1, pp. 55-87. Sulla responsabilità degli agenti *software* cfr. anche C. Cevenini, *I servizi della società dell'informazione. Profili informatico-giuridici*, Gedit, Bologna, 2004, pp. 20-22.

Di qui la difficoltà, anche tecnica, di offrire una rosa di servizi che rispetti i canoni delle diverse normative e che tuteli efficacemente il diritto alla protezione dei dati personali.

L'osservazione della realtà fattuale, però, sembra suggerire che l'ultimo obiettivo citato non sia raggiunto dalle maggiori società che operano su Internet. In particolare, secondo uno studio svolto nel 2007 dall'organizzazione "Privacy International", è proprio Google l'azienda che più di ogni altra rappresenterebbe un pericolo serio ed attuale per la riservatezza individuale e collettiva[41]. I motivi che hanno spinto ad una critica tanto marcata sono diversi, ma fra essi assume una particolare rilevanza il fatto che Google non consenta l'eliminazione dei dati relativi allo storico delle ricerche, non garantendo così il diritto alla protezione dei dati personali. Inoltre, come ha riportato Lawrence Lessig, Google collega le ricerche agli indirizzi IP e, se presenti, addirittura agli *accounts* degli utenti, potendone così effettuare la profilazione[42].

La lettura di questi dati, unitamente a quello sull'importanza oggi assunta dal *brand* Google, potrebbe portare a considerazioni abbastanza problematiche se non addirittura pericolose che derivano da una riflessione: proprio l'azienda accusata più di ogni altra di violare la privacy ha assunto un'importanza fondamentale nella Società dell'informazione.

Tale rilevanza potrebbe essere dovuta non solo ai sofisticati algoritmi e alle geniali intuizioni dei creatori dell'azienda stessa, ma anche alla capacità di acquisire e gestire dati personali e non, poi utilizzati a fini commerciali.

Forse è vero che, come ha osservato Manuel Castells, molte persone rinunciano «al diritto alla privacy pur di utilizzare Internet. Messo da parte il diritto alla privacy, i dati personali diventano proprietà legale delle imprese di Internet e dei loro clienti»[43], e su di essi possono basare la loro fortuna. Dal punto di vista del diritto positi-

---

[41] Privacy International, *A Race to the Bottom: Privacy Ranking of Internet Service Companies*, in http://www.privacyinternational.org/issues/internet/interimrankings.pdf.

[42] L. Lessig, *Code version 2.0*, Basic Books, New York, 2006, p. 204. Sulla profilazione si veda *infra*, § 3.

[43] M. Castells, *Galassia Internet*, cit., p. 166.

vo, però, ciò è vero soprattutto negli Stati Uniti, posto che essi, come si è detto, non sono dotati di una normativa sulla privacy evoluta come quella europea, ma tale tendenza sembra abbastanza diffusa anche in Europa e, soprattutto, in Italia, dove diversi fattori spingono in tal senso.

Così, la lunghezza di molte informative scritte in ottemperanza al cod. priv. porta molte persone ad ignorarne il contenuto e a prestare il consenso al trattamento dei dati personali anche per fini ulteriori alla consultazione del sito stesso o alla possibilità di fruire dei suoi servizi, che sovente si concretizzano nella prestazione del consenso all'utilizzo dei propri dati a fini pubblicitari e di marketing anche da parte di terzi soggetti. Inoltre, l'ancora carente formazione in materia informatica comporta una insufficiente presa di coscienza che quanto avviene *on line* non accade in una dimensione parallela bensì nel modo reale, dove probabilmente non si fornirebbero molti dei propri dati personali a qualcuno cui si chiede, ad esempio, un'indicazione stradale!

Tali profili problematici fanno sorgere alcuni dubbi in ordine alla possibile inutilità di una eventuale tutela *ex post* qualora sia stato posto in essere un trattamento illecito di dati personali. Anche se il diritto al controllo dei propri dati personali può essere più o meno efficacemente esercitato avverso un determinato archivio informatico presente su Internet utilizzando gli strumenti previsti dalla normativa vigente, cui può, ad esempio, conseguire l'immediata rimozione dei dati da un determinato *server*, i dati contestati potrebbero risultare comunque disponibili sul web grazie al *caching* effettuato dai motori di ricerca[44].

Proprio i *search engines*, infatti, possono rendere di fatto impossibile l'esercizio del diritto all'oblio, in quanto essi rendono il ciberspazio «un luogo dove nulla si perde o viene dimenticato»[45], sia in riferimento allo spazio pubblico del ciberspazio che nell'ambito privato relativo alla corrispondenza elettronica.

---

[44] In tal senso P. Sammarco, *Il motore di ricerca, nuovo bene della società dell'informazione: funzionamento, responsabilità e tutela della persona*, in *Il diritto dell'informazione e dell'informatica*, 2006, 4-5, p. 633.

[45] S. Rodotà, *La vita e le regole. Tra diritto e non diritto*, Feltrinelli, Milano, 2006, p. 64.

Si pensi, così, al sito "Internet Archive"[46], che consente di visionare l'evoluzione di numerosi siti web ed accedere a contenuti che, altrimenti, potrebbero risultare persi per sempre. Il numero di pagine web presenti nel suo archivio è impressionante: attualmente sono ben ottantacinque miliardi.

Sul punto sono diversi gli aspetti che devono essere messi in evidenza e bisogna preliminarmente distinguere fra contenuti posti *on line* lecitamente ed illecitamente. Nel primo caso, è notorio che la diffusione di informazioni tramite Internet si riverberi sull'intera rete e che esse possono risultare accessibili da chiunque a meno che non vengano poste in essere delle restrizioni all'accesso che lo consentano solo a determinati soggetti ed, eventualmente, a determinate condizioni. I motori di ricerca possono quindi memorizzare i contenuti ed inserirli nel database di riferimento e, del resto, il porre contenuti *on line* è frutto, in tutta evidenza, della volontà di rendere tali materiali conoscibili al pubblico più vasto possibile od anche ad una ristretta cerchia di amici, ma, di fatto, essi vengono resi disponibili a tutti, ivi compresi i *search engines*.

Bisogna capire se, in tal modo, si abdichi di fatto al controllo sui propri dati oppure sino a che punto e in che modo tale controllo possa successivamente essere effettuato. Il problema consiste nel fatto che la rimozione dei contenuti dallo spazio web proprio o altrui non basta per evitare la loro successiva circolazione qualora sia stato effettuato il *caching* dai motori di ricerca[47] oppure nel caso in cui soggetti terzi abbiano acquisito le informazioni facendole poi circolare nuovamente.

È palese che tali aspetti concretizzino delle vere e proprie criticità qualora i dati siano posti illecitamente *on line* e vengano me-

---

[46] Http://www.archive.org.

[47] Come è stato rilevato in dottrina, è comunque possibile evitare di essere trovati dai motori di ricerca, impedendo così il *caching*, mediante l'inserimento di brevi codici all'interno del codice di ciascun sito (M. Mezzanotte, *La memoria conservata in internet ed il diritto all'oblio telematico: storia di uno scontro annunciate*, in *Diritto dell'internet*, 2007, 4, p. 402). Nel caso di specie, dunque, ci troviamo dinanzi ad una sorta di *opt-out*, poiché diventa necessario un atto volitivo per evitare di inserire indicizzati da un motore di ricerca. Google, comunque, rende disponibile un sistema di rimozione dei contenuti dall'indicizzazione effettuata; esso è accessibile previa creazione di un *account* presso la medesima azienda.

morizzati dai motori dai ricerca. In tali casi, come si è accennato, l'esercizio dei tradizionali rimedi giuridici potrebbe non essere sufficiente, perché, oltre all'autore dell'illecito, bisognerebbe chiedere e ottenere la rimozione dei contenuti a tutti i motori di ricerca (e a tutti i siti) che abbiano memorizzato, in tutto o in parte, tali informazioni.

Il rimedio potenzialmente più efficace potrebbe consistere nel centralizzare la gestione di simili contenuti, ma ciò confliggerebbe con l'essenza stessa del ciberspazio quale rete decentralizzata. Inoltre, in tal caso sarebbe necessario un preliminare accordo fra tutti gli stati che, oltretutto, potrebbe portare alla inaccettabile compressione del diritto alla libera manifestazione del pensiero. Per garantire la libertà e la neutralità della rete, e al tempo stesso il proprio diritto alla privacy, è dunque necessaria la massima accortezza nel divulgare contenuti nel ciberspazio. Del resto, il dovere di diligenza del *pater familias* che il diritto impone a ciascuno nella vita quotidiana non può certo venir meno nella realtà "virtuale".

## 3. *La profilazione*

La profilazione, in linea generale, consiste nella memorizzazione e nella classificazione del comportamento. È, dunque, un trattamento di dati personali, il cui scopo consiste, per lo più, nel definire i gusti, le tendenze e le ideologie di ogni persona, in modo da indirizzare la produzione verso le preferenze delle maggiori tipologie di utenza nonché per personalizzare sempre più l'offerta di mercato. Risulta così possibile ricostruire facilmente la "persona elettronica" grazie alle numerose tracce che lascia nei computer che annotano e raccolgono informazioni sul suo conto[48].

Nascono, dunque, nuove esigenze di tutela, «connesse all'aggressività e alla pervasività delle tecniche di propaganda commer-

[48] M. Iaselli, *Navigazione anonima in Rete*, in A. Maggipinto, M. Iaselli (a cura di), *Sicurezza e anonimato in rete. Profili giuridici e tecnologici della navigazione anonima*, Nyberg, Milano, 2005, p. 17.

ciale rispetto alla sfera privata e intima degli individui»[49], per evitare che determinate caste di consumatori ideali spingano verso nuovi fenomeni discriminatori verso i non aderenti a determinati standard di mercato.

Il problema della profilazione *on line*, in particolare, assume una rilevanza crescente, poiché in un'epoca in cui l'informazione è sempre più digitale o digitalizzabile, le informazioni così acquisite appaiono sempre più importanti, dal momento che sono facili da ottenere, soprattutto all'insaputa degli incauti navigatori del web, e da trattare.

La navigazione su Internet, come si è detto, è infatti ben lungi dall'essere anonima. Qualsiasi "gesto" compiuto *on line* lascia una traccia ed è possibile risalire senza sforzi eccessivi all'identità di chi si trova nel ciberspazio. Ciò è conseguenza del concorso di diversi fattori, fra cui l'utilizzo di metodi ingegnosi per acquisire dati personali e, soprattutto, la diffusa ignoranza circa le dinamiche di funzionamento di Internet: di fatto, la maggior parte delle persone che quotidianamente naviga in rete non è abbastanza esperta in informatica da poter tutelare la propria riservatezza adottando quelle medesime cautele che adotta al di fuori del ciberspazio.

Come ha affermato Stefano Rodotà, «ognuno è implacabilmente seguito dal suo passato. Diventa sempre più arduo non lasciar tracce, o cancellare quelle che indicano quali sentieri abbiano percorso»[50].

L'acquisizione di dati personali, che è la fase prodromica alla profilazione, può avere luogo secondo metodologie diverse, anche al di fuori di Internet. Più specificatamente, ciò può avvenire, fra l'altro, già mediante il fatto stesso di creare un sito web oppure tramite strumenti come le carte di fidelizzazione, i *logs* di *providers* e motori di ricerca, i *cookies*, o, ancora, in seguito ad acquisti effettuati *on line*. Inoltre, le conseguenze del trattamento incrociato dei vari dati così raccolti possono facilmente travalicare l'ambito commerciale in sé e per sé inteso per giungere a delineare un profilo più o meno completo non solo di un individuo, ma altresì di vari gruppi sociali.

---

[49] G. Maccaboni, *La profilazione dell'utente telematico fra tecniche pubblicitarie online e tutela della privacy*, in *Il diritto dell'informazione e dell'informatica*, 2001, 3, p. 427.

[50] S. Rodotà, *Tecnopolitica*, cit., p. 135.

La profilazione individuale o collettiva, infatti, viene di norma già svolta automaticamente da taluni soggetti che scandagliano la rete al fine di rintracciare i siti che possono contenere *software* potenzialmente dannoso o che possono essere veicolo di truffe telematiche. In tal senso assume un particolare rilievo l'operato di Google (vista la sua importanza[51]), che ha creato una "lista nera" (*blacklist*) di siti ritenuti pericolosi. Ovviamente una simile operazione presuppone l'analisi del contenuto di un sito e ciò può portare ad una profilazione del gestore del medesimo, che potrebbe subire conseguenze negative qualora il "giudizio" di Google sia errato, come l'essere ingiustamente etichettato come potenziale truffatore o creatore di virus[52].

Accanto a fattispecie simili, che si verificano unicamente nel ciberspazio, se ne pongono altre a carattere misto, poiché possono verificarsi totalmente nel mondo "materiale" oppure riverberarsi anche su Internet. Si pensi alle carte di fidelizzazione, che sono generalmente utilizzate nel settore della grande distribuzione anche per le transazioni *on line*. Esse sono finalizzate alla creazione o al consolidamento di un rapporto duraturo con la clientela per acquisti e servizi, poiché tramite esse è di norma possibile usufruire di alcuni vantaggi o sconti, il tutto o per il fatto stesso di essere titolari di una simile carta oppure in relazione al genere, al volume di spesa o alle prestazioni richieste.

In tali fattispecie, il trattamento dei dati personali avviene sia nella fase del rilascio delle suddette carte, solitamente in seguito alla compilazione di un modulo di adesione, che in quella, successiva, della loro utilizzazione. In quest'ultima fase, però, si verifica un

---

[51] Si pensi che circa l'ottantacinque per cento delle ricerche svolte in Europa avviene proprio tramite Google. Il dato è riportato da Microsoft, che è uno dei principali concorrenti della stessa Google (http://www.microsoft.com/presspass/press/2008/feb08/02-03Statement.mspx?rss_fdn=Press%20Releases).

[52] Google ha inoltre reso disponibile la "Safe Browsing API" (API sta per interfaccia di programmazione di un'applicazione, dall'espressione inglese *Application Program Interface*), che può essere integrata in un programma per elaboratore al fine di avvisare gli utenti di eventuali connessioni verso siti presenti nella *black list* di Google. In tutta evidenza, dunque, questa sorta di valutatore telematico automatizzato può travalicare l'ambito specifico del motore di ricerca per essere usato in applicazioni di terze parti.

monitoraggio dei comportamenti dei clienti, al fine di operare una profilazione individuale o collettiva, talvolta giungendo addirittura al trattamento di dati sensibili poiché possono essere acquistati beni che, ad esempio, sono idonei a rivelare il proprio stato di salute o la propria vita sessuale.

Il Garante della privacy, vista la delicatezza della questione e l'elevato numero di carte di fidelizzazione ormai presenti, è intervenuto il 24 febbraio 2005 con un provvedimento a carattere generale, chiarendo che possono essere trattati esclusivamente i dati necessari per attribuire i vantaggi connessi all'utilizzo della carta, riducendo al minimo l'uso delle informazioni personali ed evitando, di norma, l'acquisizione di dati relativi al dettaglio dei singoli prodotti acquistati. Inoltre, per l'attività di profilazione occorre il consenso dell'interessato per il trattamento delle informazioni relative agli acquisti effettuati, ma, in ogni caso, non è lecito utilizzare dati sensibili a fini di profilazione, con particolare riguardo a quelli riguardanti lo stato di salute. Infine, i dati raccolti ai suddetti fini e relativi al dettaglio degli acquisti non possono essere conservati per più di un anno, limite che sale a due anni per quelli raccolti a fini di marketing[53].

Parimenti, anche i *logs* dei *providers*, ossia i registri elettronici di tutto ciò che succede nelle loro reti e tramite i loro servizi, possono essere in alcuni casi conservati per un tempo limitato. Più specificatamente, essi devono cancellare o rendere in forma anonima i dati non più necessari per la trasmissione della comunicazione elettronica (art. 123, comma 1, cod. priv.), ma possono conservare i dati relativi al traffico strettamente necessari a fini di fatturazione per l'abbonato; essi possono essere conservati per un periodo massimo di sei mesi, salva l'ulteriore specifica conservazione necessaria per

[53] GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *"Fidelity card" e garanzie per i consumatori. Le regole del Garante per i programmi di fidelizzazione*, 24 febbraio 2005, in http://www.garanteprivacy.it/garante/doc.jsp?ID=1103045. Quanto all'attività di marketing, possono essere raccolti, con il consenso dell'interessato, i dati necessari all'invio di materiale pubblicitario o di comunicazioni commerciali. Successivamente a tale provvedimento, il Garante è intervenuto più volte nei confronti di società che effettuavano un uso troppo ampio e disinvolto delle carte di fidelizzazione (cfr., in particolare, i provvedimenti del 15 novembre 2007 e la *Newsletter* n. 306 del 21 maggio 2008, tutti reperibili sul sito dell'*authority*: http://www.garanteprivacy.it).

effetto di una contestazione anche in sede giudiziale (art. 123, comma 2, cod. priv.).

Si consideri, poi, che «i dati relativi al traffico telematico, esclusi comunque i contenuti delle comunicazioni, sono conservati dal fornitore per sei mesi per finalità di accertamento e repressione dei reati» (art. 132, comma 1, cod. priv.); i medesimi dati sono conservati per ulteriori sei mesi per esclusive finalità di accertamento e repressione di taluni delitti[54], fra cui quelli compiuti in danno di sistemi informatici o telematici (art. 132, comma 2, cod. priv.).

Sino ad oggi, però, tali dati non sono stati cancellati per effetto del d.l. 27 luglio 2005, n. 144, convertito in legge, con modificazioni, dalla l. 31 luglio 2005, n. 155 (il c.d. pacchetto Pisanu), e della sua successiva modificazione da parte dell'art. 34 del d.l. 31 dicembre 2007, n. 248, convertito in legge, con modificazioni, dalla l. 28 febbraio 2008, n. 31. Sino a quando non sarà data attuazione alla direttiva europea n. 2006/24/CE del 15 marzo 2006[55], e comunque entro e non oltre il 31 dicembre 2008, i dati summenzionati devono essere conservati. La direttiva appena citata stabilisce che essi devono essere conservati per un periodo non inferiore a sei mesi e non inferiore a due anni dalla data della comunicazione (art. 6).

La conservazione dei suddetti dati, però, impone anche problematiche relative alla sicurezza dei dati trattati. Con provvedimento generale del 17 gennaio 2008[56], il Garante per la protezione dei dati personali, in ottemperanza a quanto disposto dall'art. 132 cod. priv., ha dettato le regole per la loro conservazione, sia con riferimento al traffico telefonico che a quello telematico[57]. Come ha rilevato l'*au-*

---

[54] I delitti cui fa riferimento la norma sono quelli di cui all'art. 407, comma 2, lett. a, cod. proc. pen.

[55] L'attuazione della direttiva in esame sarebbe dovuta avvenire entro il 15 settembre 2007 (art. 15, comma 1).

[56] Reperibile all'indirizzo http://www.garanteprivacy.it/garante/doc.jsp?ID=1482111.

[57] Secondo il Garante per la protezione dei dati personali, sono tenuti alla conservazione dei dati ai sensi dell'art. 132 cod. priv. i soggetti che realizzano esclusivamente o prevalentemente una trasmissione di segnali su reti di comunicazioni elettroniche, a prescindere dall'assetto proprietario della rete, e che offrono servizi a utenti finali secondo il principio di non discriminazione. Non sono tenuti alla conservazione dei dati i soggetti che offrono direttamente servizi di comunicazione elettronica a gruppi delimitati di persone; i soggetti che, pur

*thority*, il trattamento di tali dati presenta rischi specifici per i diritti e le libertà fondamentali, nonché per la dignità dell'interessato, per cui è necessario adottare particolari cautele.

I *logs* sono stati sempre utilizzati dai *providers* al fine di assicurarsi sia una tutela contrattuale che extracontrattuale; nel primo caso, ad esempio, per dimostrare la correttezza degli addebiti effettuati ai propri clienti e nel secondo per poter verificare l'eventuale commissione di illeciti svolti mediante le linee del *providers*. La legge n. 675/96, prima, e il cod. priv., poi, hanno regolamentato detta questione, che era chiaramente molto delicata, in quanto in tal modo il fornitore di accesso e/o di servizi poteva «creare un dettagliato profilo personale del navigatore virtuale, anche con riferimento a dati sensibili quali, per esempio, orientamento politico o sessuale»[58].

Inoltre, oggi la prassi mostra come alcuni *providers* operino una sorta di profilazione al volo degli utenti che utilizzano il loro servizio di accesso ad Internet: è il caso del c.d. *traffic shaping*, ossia un metodo consistente nell'analisi dei flussi di dati che viaggiano su una determinata rete e nel successivo rallentamento dei pacchetti di dati ritenuti indesiderati. Essi vengono utilizzati normalmente dai fornitori di accesso ad Internet al fine di ridurre l'utilizzo della banda di connessione utilizzata dai programmi di *file sharing*, anche se ciò fa sorgere dei dubbi in ordine ad un loro eventuale inadempimento contrattuale derivante dall'arbitrario rallentamento della velocità di connessione. Alquanto preoccupanti, comunque, sono le conseguenze potenzialmente lesive della privacy dei clienti dei *provider*s, poiché di fatto viene svolta un'analisi della loro condotta telematica che può consentire di capire quale utilizzo facciano della connessione. Si consideri che i fornitori di accesso sono, ovviamente, a conoscenza dell'indirizzo IP dei propri clienti, per cui il trattamento in-

offrendo servizi di comunicazione elettronica accessibili al pubblico, non generano o trattano direttamente i relativi dati di traffico; i titolari e i gestori di esercizi pubblici o di circoli privati di qualsiasi specie che si limitino a porre a disposizione del pubblico, di clienti o soci apparecchi terminali utilizzabili per le comunicazioni, anche telematiche, ovvero punti di accesso a Internet utilizzando tecnologia senza fili, esclusi i telefoni pubblici a pagamento abilitati esclusivamente alla telefonia vocale; i *content providers*; i gestori dei motori di ricerca.

[58] E. Tosi, *Diritto privato dell'informatica e di Internet. I beni – I contratti – Le responsabilità*, Giuffré, Milano, 2006, p. 421.

crociato di tali dati può consentire di ottenere una notevole mole di informazioni personali, come ha altresì sottolineato il Garante per la protezione dei dati personali nel summenzionato provvedimento del 17 gennaio 2008.

Lo stesso può accadere in seguito al trattamento delle informazioni conseguenti alle stringhe di ricerca impostate nei *search engines*, poiché, come si è detto, all'integrazione di più servizi nell'ambito di ciascun portale può conseguire l'acquisizione di molteplici dati di diverse tipologie che possono poi essere aggregati e successivamente utilizzati per tracciare un profilo degli utenti, dal momento che più informazioni vengono sovente riferite ad un utente determinato, come nel caso di Google cui si è fatto riferimento in precedenza.

Anche mediante l'utilizzo dei *cookies*, inoltre, è possibile acquisire dati personali e successivamente effettuare la profilazione dell'utente telematico, come si è visto. È interessante evidenziare, ora, come essa avvenga con strumenti sempre più evoluti soprattutto nel caso di quei siti di commercio elettronico in cui viene svolta un'analisi automatizzata delle preferenze d'acquisto dei vari consumatori in modo da suggerire acquisti che potrebbero potenzialmente essere di loro interesse.

Si pone, dunque, il rischio di automatizzare l'orientamento delle scelte individuali secondo criteri di mercato stabiliti a priori e generalizzati, con la conseguenza di appiattire la molteplicità dei desideri e delle inclinazioni personali.

Pertanto, mediante le metodologie e le tecnologie di profilazione, si riesce a violare il diritto alla riservatezza in maniera più sottile e forse più efficace rispetto a metodi come l'invio di messaggi pubblicitari personalizzati oppure l'effettuazione di comunicazioni telefoniche. Il mercato, infatti, «interviene nel modellare i comportamenti sociali *tout court*, laddove pianifica con l'aiuto della statistica geodemografica l'offerta di merci su segmenti di consumo individuati attraverso la conoscenza delle caratteristiche generali dei consumatori come l'età, la professione, la residenza, la composizione familiare, il genere»[59].

---

[59] A. Di Corinto, T. Tozzi, *Hacktivism. La libertà nelle maglie della rete*, Manifestolibri, Roma, 2002, p. 75.

La creazione automatizzata di profili individuali e collettivi può tuttavia travalicare gli ambiti del mercato per giungere a quelli, ben più delicati, relativi al concreto esplicarsi dei poteri giudiziari ed esecutivi. Gli stati, infatti, hanno sempre acquisito una notevole mole di informazione sui propri cittadini e, in linea più generale, su chiunque varchi le proprie frontiere. Le crescenti potenzialità delle operazioni di trattamento dei dati personali, che divengono sempre più sofisticate grazie agli avanzamenti delle tecnologie informatiche e comunicative, potrebbero tuttavia portare a conseguenze assai spiacevoli, giungendo addirittura all'automatizzazione di provvedimenti giudiziari od amministrativi[60].

Sul punto l'art. 14, comma 1, cod. priv., pone un esplicito divieto: «nessun atto o provvedimento giudiziario o amministrativo che implichi una valutazione del comportamento umano può essere fondato unicamente su un trattamento automatizzato di dati personali volto a definire il profilo o la personalità dell'interessato».

Pertanto, il cod. priv. vieta la riconduzione, svolta esclusivamente in maniera automatizzata, della persona ad una determinata categoria, come quella di «criminale abituale» oppure «debitore inaffidabile»[61], per cui sembra particolarmente rilevante soprattutto in materia di provvedimenti di restrizione della libertà personale[62]. Appare chiaro, dunque, che un trattamento automatizzato dei dati può solo contribuire alla formulazione di un giudizio, offrendo, eventualmente, elementi integrativi.

Bisogna rilevare, poi, che, ai sensi dell'art. 14, comma 2, cod. priv., l'interessato può opporsi ad ogni altro tipo di determinazione adottata sulla base di un simile trattamento, salvo che la determi-

---

[60] Invero ciò già avviene in determinati casi: basti pensare alle tecnologie comunemente utilizzate per sanzionare determinate violazioni al Codice della strada, come l'ingresso non autorizzato in zone a traffico limitato. Tale fattispecie è disciplinata dal d.p.r. 22 giugno 1999, n. 250. In merito si è espresso anche il Garante della privacy con una segnalazione del 7 giugno 1999 e con un parere del 7 marzo 2000. Si veda, altresì, il provvedimento della medesima *authority* del 14 giugno 2007 sul trattamento dati sensibili per l'accesso di medici in zone a traffico limitato.

[61] Così Ri. Imperiali, Ro. Imperiali, *Codice della privacy. Commento alla normativa sulla protezione dei dati personali*, Il sole 24 ore, Milano, 2005, p. 159.

[62] P. Ceccoli, *Articolo 14 (definizione di profili e della personalità dell'interessato)*, in Aa.Vv., *Codice della privacy*, Giuffré, Milano, 2004, p. 195.

nazione sia stata adottata in occasione della conclusione o dell'esecuzione di un contratto, in accoglimento di una proposta dell'interessato o sulla base di adeguate garanzie individuate *ex lege* o di un provvedimento del Garante.

Tuttavia, il divieto di cui all'art. 14 cod. priv. non sembra abbastanza efficace, sia perché non prende in considerazione la veste di consumatore o di utente del cittadino e sia perché tale divieto può essere facilmente aggirato «sostenendo che la decisione non viene presa sulla base del solo profilo automatizzato; e, soprattutto, che non si tratta di decisioni individuali, ma relative a gruppi o categorie (di consumatori, di utenti, di abitanti di un territorio, di appartenenti ad una determinata fascia di reddito), e che la semplice attribuzione di un soggetto ad uno di questi gruppi o categorie non può essere considerata tecnicamente una decisione»[63].

## 4. *Lo "spamming"*

Lo *spamming*, in linea generale, consiste in un'attività di invio di messaggi, solitamente pubblicitari, non richiesti, che vengono detti messaggi di *spam* (o anche *junk mail*, ossia "mail spazzatura"). Può essere effettuato utilizzando mezzi come la posta tradizionale[64] o il telefono, ma la variante più diffusa è quella svolta tramite Inter-

---

[63] S. Rodotà, *Tecnopolitica*, cit., p. 139.

[64] Il Giudice di Pace di Bari, con sentenza del 22 dicembre 2003, ha condannato due aziende a risarcire una persona per aver inserito alcuni volantini pubblicitari nella sua cassetta per le lettere nonostante l'esplicito divieto ivi affisso, con ciò cagionando fastidio e violazione della sfera di riservatezza (la pronuncia è pubblicata in *Danno e responsabilità*, 2004, 8-9, pp. 880-881). Tale decisione è stata criticata in dottrina, che ha ritenuto l'impossibilità di provare il danno da disappunto o da fastidio in simili fattispecie (L. Caputi, *Liti bagatellari, dal paradosso al parossismo: il danno da disappunto per illegittima introduzione di volantini pubblicitari nelle cassette della posta*, in *Danno e responsabilità*, 2004, 8-9, p. 886; nello stesso senso anche G. Catalano, *Di cassette per la corrispondenza piene e danno "esistenziale" derivante*, in *Danno e responsabilità*, 2004, 8-9, pp. 887-889). È d'uopo sottolineare che l'astratta risarcibilità del danno impone comunque la prova di averne subito uno: non sembra che il fastidio di dover gettare alcuni volantini pubblicitari possa addirittura danneggiare l'esistenza stessa di un individuo in modo tanto rilevante.

net mediante l'invio di messaggi di posta elettronica non richiesti, anche se sono abbastanza diffusi anche quelli messi in pratica tramite brevi messaggi di testo (SMS) inviati a telefoni cellulari talvolta dagli stessi operatori di telefonia mobile[65].

Al contrario della posta tradizionale l'invio di una email è gratuito, per cui gli *spammers* si sono concentrati soprattutto su tale metodologia, anche perché un messaggio di *spam* può essere il veicolo, oltre che di comunicazioni che pubblicizzano attività lecite ed illecite, anche di virus e di truffe.

Se in alcune email, infatti, viene ad esempio proposta la vendita di farmaci senza prescrizione medica, in altre vengono allegati virus e altri *malwares* che sfruttano le vulnerabilità dei più comuni programmi utilizzati per consultare ed inviare la posta elettronica.

In altri casi viene effettuato il c.d. *phishing*, che consiste in una frode finalizzata all'acquisizione di dati personali riservati, realizzata mediante l'invio di email nelle quali vengono riportati i loghi ufficiali e la grafica di aziende e istituzioni (generalmente istituti bancari) e viene invitato il destinatario a fornire informazioni assai delicate come nome utente e password oppure il numero della propria carta di credito. Tale richiesta viene spesso giustificata da ragioni di natura tecnica, come presunti malfunzionamenti nei sistemi informatici che richiedono il reinserimento della password.

Ovviamente ad avere un rapporto con la banca o l'azienda il cui nome viene millantato non saranno tutti i destinatari, bensì alcuni

---

[65] Cfr., ad esempio, la sentenza del Giudice di Pace di Napoli del 29 settembre 2005 (con commento, fra gli altri, di A. Mascia, *Lo spamming telefonico e i pregiudizi alla vita privata dell'utente*, in *Responsabilità civile e previdenza*, 2006, 7-8, pp. 1321-1336, V. Viti, *Il danno da "spamming" e la tutela della riservatezza*, nota a Giudice di Pace di Napoli 29 settembre 2005, in *Il corriere del merito*, 2006, 2, pp. 170-175) e la sentenza resa il 19 giugno 2006 dal Tribunale di Latina, sezione distaccata di Terracina, con la quale una compagnia di telefonia mobile è stata condannata a risarcire il danno da «invio di sms non desiderati», quantificato equitativamente in ben mille euro per ogni sms (la sentenza è riportata in *Diritto dell'internet*, 2007, 1, pp. 25-27, con commento di G. Citarella, *Spamming: interferenze nella sfera privata e violazione del diritto alla privacy*, pp. 27-29). Bisogna poi considerare che in alcuni casi l'invio di sms non desiderati ha integrato la condotta di cui all'art. 660 cod. pen., che prevede e punisce il reato di "Molestia o disturbo alle persone" (cfr. Cass. pen. 11 maggio 2006, n. 16.215, in *Diritto dell'internet*, 2006, 4, pp. 373-374, con nota di F. Di Luciano, *Il messaggio sms quale modalità di commissione del reato di molestie telefoniche*, pp. 374-376).

di essi e, probabilmente, una percentuale di gran lunga minore darà credito a quanto riportato nel messaggio di posta elettronica, seguendo le istruzioni ivi riportate[66].

In simili casi la tutela *ex post* delle proprie ragioni può risultare assai difficoltosa dal momento che i siti web di destinazione e/o i truffatori possono trovarsi al di fuori dei confini italiani, per cui un'autotutela *ex ante* della privacy può limitare notevolmente tali fenomeni. Si consideri, infatti, che la maggior parte dei messaggi di *spam* proviene da altre nazioni, come Stati Uniti e Cina[67] e dunque non è certo agevole ed economico rivolgersi alla competente autorità giudiziaria o all'autorità di controllo, se esistente, qualora l'attività di *spamming* venga svolta da soggetti extra-nazionali. Ciò provoca un'impunità di fatto per molti *spammer*, i quali ben sanno che il rischio di dover subire un giudizio non è elevato.

Appare chiara, quindi, l'utilità di una autotutela effettuata sia mediante il ricorso ad appositi strumenti, come i filtri anti-spam presenti ormai in quasi tutti i programmi per la gestione delle email, sia evitando di diffondere eccessivamente il proprio indirizzo di posta elettronica.

Nel caso in cui la legge applicabile ad una fattispecie di *spamming* sia quella italiana, troverà applicazione, in linea generale, l'art. 130 cod. priv. in tema di comunicazioni indesiderate, ai sensi del quale il previo consenso dell'interessato è necessario in tutti i casi in cui vengono utilizzati sistemi automatizzati di chiamata senza l'intervento di un operatore, nonché email, telefax, messaggi MMS o

---

[66] Bisogna considerare che il testo di molte email di *phishing* è spesso tradotto in maniera addirittura ridicola; basti pensare a questa email inviata da "Poste Italiene" (questo il nome che compare nel campo "soggetto" del messaggio, qui riportato includendo gli errori di ortografia): «nell'ambito di un progetto di verifica dei data anagrafici forniti durante la sottoscrizione dei servizi di Posteitaliane e stata riscontrata una incongruenza relativa ai dati anagrafici in oggetto da Lei forniti all momento della sottoscrizione contrattuale». Oltre al millantare di essere chi in realtà non si è, un altro stratagemma utilizzato per non destare sospetti nel destinatario dell'email consiste nel visualizzare un indirizzo Internet che (solo in apparenza) proviene dal sito "istituzionale" e invitare il destinatario a selezionare il collegamento; con ogni probabilità il sito di destinazione sarà costituito da una riproduzione più o meno curata di quello "reale". In realtà basta visualizzare l'indirizzo di destinazione per rendersi conto della truffa.

[67] E.O. Policella, *Il danno da "spamming"*, nota a Giudice di Pace di Napoli 10 giugno 2004, in *Diritto dell'internet*, 2005, 6, p. 661.

SMS o di altro tipo, per l'invio di materiale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato o l'effettuazione di comunicazioni commerciali. Il modello prescelto dal legislatore in tal caso è quello del c.d. *opt-in*, secondo cui è necessario un atto volitivo per ricevere messaggi delle suddette tipologie, al contrario di quanto avviene nel caso del c.d. *opt-out*, ove l'atto volitivo è invece necessario per impedire che vengano inviati ulteriori messaggi.

La violazione dell'art. 130 cod. priv. integra il reato di trattamento illecito di dati personali, previsto e punito dall'art. 167, comma 1, cod. priv.; più specificamente, l'applicazione della norma richiede sia che l'autore dell'illecito lo abbia commesso al fine di trarne per sé o per altri profitto o di recare ad altri un danno e sia che dal fatto sia derivato nocumento. Se entrambi tali condizioni si sono verificate, la pena prevista è della reclusione da sei a diciotto mesi o, se il fatto consiste nella comunicazione o diffusione, con la reclusione da sei a ventiquattro mesi.

Inoltre, un'attività di *spamming* integra anche la fattispecie amministrativa della «omessa o inidonea informativa all'interessato»[68], dal momento che in tali casi si verifica di norma un'omissione dell'informativa, per cui è prevista la sanzione del pagamento di una somma da tremila a diciottomila euro, cifra che può tuttavia essere aumentata sino al triplo quando risulta inefficace in ragione delle condizioni economiche del contravventore (art. 161 cod. priv.).

Il quadro normativo è completato dall'art. 58 del d.lgs 6 settembre 2005, n. 206 («Codice del consumo»), che trova applicazione quando il destinatario dei messaggi di *spam* è un consumatore, ossia una persona fisica che agisce per scopi estranei all'attività imprenditoriale o professionale eventualmente svolta (art. 1, comma 1, lett. a, d.lgs. 206/2005).

La norma summenzionata, al comma 1, vieta l'utilizzo della posta elettronica (nonché del telefono, del fax e di sistemi automatizzati di chiamata) da parte di un professionista nei confronti di un consumatore.

Il successivo comma 2 dispone, poi, che «tecniche di comunicazione a distanza diverse da quelle di cui al comma 1, qualora consentano una comunicazione individuale, possono essere impiegate

[68] Ivi, p. 666.

dal professionista se il consumatore non si dichiara esplicitamente contrario». Sul punto bisogna rilevare che proprio il comma appena citato si applica anche in deroga alle norme di cui al cod. priv., in virtù dell'art. 19-*bis* d.l. 30 dicembre 2005, n. 273 (il c.d. "decreto milleproroghe"), convertito con legge 23 febbraio 2006, n. 51. In dottrina è stato giustamente rilevato che tale norma, che adotta il modello dell'*opt-out*, non può costituire una deroga totale ai principi stabiliti dal cod. priv., anche perché ciò costituirebbe un eccesso di delega, violando così l'art. 76 Cost.[69]. La suddetta norma, comunque, ha un ambito di applicazione limitato, potendo trovare applicazione nei casi in cui la comunicazione avvenga, ad esempio, mediante supporti cartacei.

Un'interpretazione letterale delle disposizioni sopra citate, comunque, unitamente alla considerazione del principio di assicurare la massima tutela al consumatore, dovrebbe far rientrare tutte le comunicazioni svolte per via telefonica (quindi anche MMS e SMS) nella previsione di cui al comma 1, poiché concretizzano comunque un uso del telefono, anche se non per lo svolgimento di comunicazioni vocali. In mancanza di specificazioni da parte del legislatore non può certo operarsi un'esegesi riduttiva della norma, cui oltretutto conseguirebbe un ulteriore squilibrio nei rapporti di fatto fra professionisti e consumatori.

Anche prima dell'emanazione del Codice del consumo il Garante della privacy si era tuttavia occupato in diverse occasioni del fenomeno dello *spamming*, sia accogliendo numerosi ricorsi che emanando, fra l'altro, un provvedimento a carattere generale in data 29 maggio 2003. In esso l'*authority* ha delineato il complessivo quadro giuridico del fenomeno, all'epoca nella vigenza della legge n. 675/96 dal momento che il cod. priv. è entrato in vigore il 1° gennaio 2004.

È importante notare come in tale provvedimento il Garante abbia ribadito «che la circostanza che gli indirizzi di posta elettronica possano essere reperiti con una certa facilità in Internet non comporta il diritto di utilizzarli liberamente per inviare messaggi pubblicitari. In particolare, i dati dei singoli utenti che prendono parte

[69] In tal senso T. Perfetti, *Spamming e comunicazioni indesiderate*, in *Rivista di diritto, economia e gestione delle nuove tecnologie*, 2006, 2, pp. 159-160.

a gruppi di discussione in Internet sono resi conoscibili in rete per le sole finalità di partecipazione ad una determinata discussione e non possono essere utilizzati per fini diversi qualora manchi un consenso specifico […]. Ad analoga conclusione deve pervenirsi per gli indirizzi di posta elettronica compresi nella lista "anagrafica" degli abbonati ad un Internet provider (qualora manchi, anche in questo caso, un consenso libero e specifico), oppure pubblicati su siti web di soggetti pubblici per fini istituzionali. Tali considerazioni valgono anche con riferimento ai messaggi pubblicitari inviati a gestori di siti web – anche di soggetti privati – utilizzando gli indirizzi pubblicati sugli stessi siti, o che sono reperibili consultando gli elenchi dei soggetti che hanno registrato i nomi a dominio. In quest'ultimo caso, infatti, la conoscibilità in rete degli indirizzi è volta a identificare il soggetto che è o appare responsabile, sul piano tecnico o amministrativo, di un nome a dominio o di altre funzioni rispetto a servizi Internet (per la tutela di vari diritti sul piano civile e penale, anche ai sensi della legge n. 675) e non anche a rendere l'interessato disponibile all'invio di messaggi pubblicitari»[70].

Oggi, poi, i messaggi di *spam* stanno diventando sempre più invasivi e in taluni casi alla loro semplice lettura può conseguire un'acquisizione di dati personali. Alcuni di essi, infatti, non sono scritti in semplice formato testuale, bensì parzialmente o totalmente in linguaggio HTML, ossia nello stesso codice utilizzato nella maggior parte delle pagine web. Se il lettore di un simile messaggio è dotato di un programma di posta elettronica in grado di leggere messaggi in tale formato e non viene selezionato il blocco dell'esecuzione del codice, chi ha inviato l'email può potenzialmente ricevere informazioni come l'avvenuta lettura del messaggio, l'indirizzo IP del lettore, l'eventuale inoltro dell'email, ecc.

La maggior parte dei programmi comunemente utilizzati per la gestione della posta elettronica è in grado di leggere simili messaggi, ma il verificarsi delle suddette fattispecie ha portato a svantaggi che esulano dalla violazione del diritto alla riservatezza. Difatti, la lettura delle email è rallentata non solo dalla necessità di "pulire" la propria casella dai messaggi spazzatura, ma anche dal dover rispondere

[70] Garante per la protezione dei dati personali, provvedimento del 23 maggio 2003.

ai sempre più numerosi avvisi mostrati dai programmi stessi (del tipo «i collegamenti HTML nel presente messaggio sono stati disabilitati»), che possono richiedere ulteriori azioni dell'utente per leggere il messaggio desiderato. Se il tempo perso per ciascuna email è in sé trascurabile, bisogna pur considerare che all'aumento del numero di messaggi consegue altresì un più elevato periodo di tempo necessario per "filtrarli" e finalmente leggere quelli desiderati.

Un'altra conseguenza che deriva dalla diffusione dello *spamming* è la giustificazione di eventuali operazioni di scansione automatica delle email poste in essere dai fornitori del servizio o direttamente dal programma all'uopo utilizzato. Se nell'ultimo caso non vi sono problemi di privacy a meno che i risultati delle scansioni non vengano inviati a *server* esterni, altrettanto non può dirsi nel caso in cui tali interventi vengano effettuati a monte dal *provider* stesso al di fuori di un'esplicita richiesta del titolare della casella di posta elettronica di utilizzare sistemi anti-spam.

In linea ipotetica, pertanto, al fine lecito di combattere lo *spam* può accompagnarsi quello, non altrettanto lecito, di acquisire dati personali degli utenti o di effettuarne la profilazione. In tal senso, l'adozione di simili sistemi può essere il cavallo di Troia da utilizzare per mascherare eventuali operazioni tese a procurarsi informazioni in modo non solo apparentemente lecito, ma addirittura desiderabile da parte del titolare della casella di posta.

## 5. *Software di "file sharing" e violazioni della privacy*

L'espressione *file sharing* è ormai divenuta di dominio pubblico in seguito al crescente utilizzo di *software* così denominati, come i ben noti Napster, WinMX, eMule e BitTorrent. Con essa si indica la condivisione di file all'interno di una rete comune, che può avere una struttura del tipo *client-server* oppure *peer-to-peer* (P2P).

Nel primo caso, un computer (*client*) si collega ad un altro elaboratore (*server*) sul quale sono posti i file condivisi; in tal modo è ad esempio possibile utilizzare un *database* centralizzato che viene reso accessibile ad altre macchine.

La seconda fattispecie, però, è quella che ha dato ampia conoscibilità alla suddetta espressione nonché a quella di P2P. Con essa si indica una rete di computer o qualsiasi rete che non possiede *client* o *server* fissi, bensì un numero di nodi equivalenti (*peers*) che fungono sia da *client* che da *server* verso altri nodi della rete.

Napster, creato nel 1999, è (*rectius* era) la prima applicazione di P2P considerevolmente diffusa anche a livello *consumer*. Tramite esso era possibile condividere su Internet file musicali che potevano essere facilmente scaricati da altri utenti. In realtà, Napster non era basato su un modello di P2P "puro", poiché i dati passavano comunque attraverso *server* centrali cui si collegavano periodicamente i vari computer connessi alla rete Napster al fine di inviare i dati identificativi dei file in condivisione; la trasmissione dei file musicali veri e propri avveniva però direttamente da computer a computer secondo un modello in realtà riconducibile a quello *client-server* poiché un computer inviava il file richiesto all'altro.

Napster presentava la grossa limitazione di permettere unicamente la condivisione di file musicali; ciò nonostante ebbe una notevole diffusione successivamente al 2000 poiché tramite esso era possibile trasmettere con notevole celerità file musicali protetti da diritto d'autore e ciò portò a diverse azioni giudiziarie nei confronti di Napster[71], cui conseguirono l'interruzione del servizio e la vendita sia dell'azienda che del marchio ad un'altra società, la quale era intenzionata a renderlo un servizio di vendita *on line* di brani musicali (tuttora esistente) contando proprio sulla notorietà del *brand*.

Il blocco di Napster non ha però interrotto l'attività di sviluppo di altri *software* basati sul modello del P2P che si distinguono per l'utilizzo di altri protocolli nonché per un numero maggiore di funzionalità e caratteristicihe. Sono stati sviluppati programmi che hanno acquisito poi una forte notorietà, come WinMX, Gnutella, eDonkey, BitTorrent.

---

[71] Sul caso Napster cfr., fra gli altri, P. Balsamo, *Distribuzione on line di file musicali e violazione del copyright: il caso Napster*, in *Il diritto d'autore*, 2001, 1, pp. 34-59, e P. Cerina, *Il caso Napster e la musica on line: cronaca della condanna annunciata di una rivoluzione tecnologica*, in *Il diritto industriale*, 2001, 1, pp. 48-59.

Ciascun applicativo opera su una propria rete e consente uno scambio diretto fra i file memorizzati sui computer di ciascun utente. È interessante notare come negli ultimi anni numerose comunità di utenti abbiano creato altri programmi che in alcuni casi fanno uso degli stessi protocolli dei programmi "di origine", utilizzandone la rete e talvolta superandoli in funzionalità e facilità di utilizzo, come nel caso del programma eMule che è basato sulla rete eDonkey oppure di Azureus e uTorrent, entrambi basato sul protocollo BitTorrent.

In ciascuna rete sopra citata ogni file è individuato in maniera univoca per mezzo del c.d. *hash*[72], che corrisponde ad una sorta di "impronta digitale" di ogni file, per cui è possibile individuarne le diverse copie eventualmente presenti nella rete anche qualora esse abbiano denominazione differente.

Il principio che sta alla base dei programmi creati successivamente a Napster è quello di puntare su reti decentralizzate, anche al fine di evitare problemi di carattere legale dovuti all'eventuale condivisione illecita di file protetti dal diritto d'autore. Una rete decentralizzata, infatti, può difficilmente essere "attaccata" da un punto di vista giuridico, poiché non è possibile riferirla ad un singolo soggetto, sia esso una persona fisica o giuridica. Del resto, già nella creazione e nell'utilizzo di Napster si «presumeva che i singoli rendessero i contenuti disponibili ad altri, ma che questi altri non fossero sempre gli stessi in modo da non diventare bersaglio delle sanzioni»[73].

Proprio per questo motivo i detentori dei diritti d'autore o le associazioni di categoria hanno intrapreso, e tuttora intraprendono, sempre più numerose azioni giudiziarie nei confronti di chi fornisce meri collegamenti ai file presenti in queste reti oppure contro i singoli utenti che scaricano o mettono in condivisione opere protette dal diritto d'autore (più che altro a scopo "dissuasivo").

---

[72] Più specificatamente, partendo da un qualsiasi flusso di bit viene restituita una stringa univoca di lettere e numeri.

[73] L. Lessig, *Il futuro delle idee*, tr. it., Feltrinelli, Milano, 2006, p. 134. Lessig sottolinea, poi, che i gruppi di utenti svolgevano l'ulteriore funzione di «favorire lo scambio d'informazioni sulle preferenze tra i propri membri, provocando così un'espansione della domanda da parte dei consumatori di questa musica. E questa domanda poteva a sua volta essere soddisfatta da musica proveniente da Napster o dai canali di distribuzione ordinaria» (ivi, p. 135).

Bisogna precisare che nei moderni programmi di P2P l'attività di scaricamento dei file non può essere scissa da quella di condivisione e di trasferimento verso altri utenti che lo richiedano, poiché i vari segmenti che costituiscono il file stesso vengono automaticamente messi in condivisione da ciascun programma. In tal modo trovano applicazione le normative, come quella italiana, che prevedono e puniscono penalmente le attività di condivisione anche parziale di contenuti protetti dal diritto d'autore: in tal senso sono infatti gli artt. 171, comma 1, lett. a-*bis*[74], e 171-*ter*, comma 2, lett. a-*bis*[75], della legge sul diritto d'autore (legge 22 aprile 1941, n. 633).

I problemi giuridici connessi all'utilizzo di programmi di *file sharing* non si arrestano unicamente alle fattispecie relative alla tutela della proprietà intellettuale[76] ma investono anche il diritto alla privacy.

Le molteplici azioni giudiziarie portate avanti in tutto il mondo nei confronti dei presunti autori di violazioni al diritto d'autore presuppongono, infatti, l'avvenuta identificazione dei singoli utenti, che viene resa possibile dal fatto che il loro indirizzo IP è pubblico e conoscibile dagli altri utilizzatori del programma che stanno scaricando e condividendo uno specifico file.

Prendendo come riferimento la normativa italiana, è d'uopo considerare che in tal modo si verifica la violazione del loro diritto alla protezione dei dati personali, poiché l'indirizzo IP è un dato personale ai sensi dell'art. 4, comma 1, lett. b, cod. priv.: esso, infatti, consiste in un'informazione «relativa a persona fisica, persona

---

[74] «Salvo quanto disposto dall'articolo 171-*bis* e dall'articolo 171-*ter* è punito con la multa da euro 51 a euro 2.065 chiunque, senza averne diritto, a qualsiasi scopo e in qualsiasi forma: […] a-*bis*) mette a disposizione del pubblico, immettendola in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, un'opera dell'ingegno protetta, o parte di essa».

[75] «È punito con la reclusione da uno a quattro anni e con la multa da euro 2.582 a euro 15.493 chiunque: […] a-*bis*) in violazione dell'art. 16, a fini di lucro, comunica al pubblico immettendola in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, un'opera dell'ingegno protetta dal diritto d'autore, o parte di essa».

[76] La letteratura in materia è ormai ben nutrita; in merito cfr., *ex multis*, G.A. Cavaliere, *La tutela della proprietà intellettuale e il file-sharing. Il nuovo business delle major*, in *Diritto ed Economia dei Mezzi di Comunicazione*, 2006, 2, pp. 245-266.

giuridica, ente o associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi informazione». In linea generale, il suo trattamento da parte di soggetti privati richiede il previo consenso da parte di ciascun interessato.

Il cod. priv., però, consente di effettuare un trattamento di dati personali anche senza il consenso dell'interessato qualora esso sia necessario «per far valere o difendere un diritto in sede giudiziaria, sempre che i dati siano trattati esclusivamente per tali finalità e per il periodo strettamente necessario al loro perseguimento, nel rispetto della vigente normativa in materia di segreto aziendale e industriale» (art. 24, comma 1, lett. f, cod. priv.).

È questo il *background* giuridico in cui si è svolto il c.d. caso Peppermint, cui si è già accennato. In merito ad esso bisogna richiamare l'ordinanza del Tribunale di Roma del 19 agosto 2006[77] (cui hanno fatto seguito altre ordinanze analoghe), con la quale è stato imposto all'Internet *provider* che forniva l'accesso ad Internet ai singoli abbonati di fornire alla società ricorrente le generalità complete dei propri clienti o abbonati corrispondenti agli indirizzi IP forniti dalla medesima società.

È doveroso tuttavia precisare che, anche ammesso che un'opera dell'ingegno sia stata illecitamente scaricata e condivisa mediante una linea identificabile grazie al raffronto fra l'indirizzo IP dell'elaboratore mediante il quale è stata posta in essere la condotta illecita e fra la singola linea che corrisponde a quell'indirizzo IP in base a quanto risulta dai registri informatici dell'*Internet provider*, non è detto che l'intestatario della linea stessa abbia materialmente posto in essere la violazione contestata, dal momento che ad una singola linea possono essere connessi in rete più elaboratori, addirittura con-

[77] L'ordinanza è reperibile all'URL http://www.altalex.com/index.php?idnot=2511. Il giudice di merito ha accolto la domanda della Peppermint Jam Records GmbH giustificando la scelta del procedimento cautelare, quanto al *periculum in mora*, poiché il proseguimento dell'attività di condivisione dei file è in sé idoneo a moltiplicare gli effetti negativi connessi all'illecita identificazione dei brani musicali; inoltre, la circostanza che i suddetti dati siano conservati da ciascun Internet *provider* per un tempo non superiore a sei mesi (ai sensi dell'art. 123, comma 2, cod. priv.) consente di ravvisare la sussistenza del *periculum in mora* nel caso concreto, poiché i tempi connessi ad un'eventuale azione giudiziaria in via ordinaria avrebbero leso i diritti della ricorrente.

tro la volontà dell'intestatario della linea stessa. Così, la diffusione di periferiche come i *routers wireless*[78] porta, in alcuni casi, ad accessi non desiderati a reti private, poiché molto spesso la connessione non viene protetta mediante le apposite funzioni supportate dagli stessi apparecchi, con la conseguenza che chiunque si trova nel raggio d'azione della medesima periferica può sfruttare la connessione ad Internet dell'intestatario della linea.

Tanto premesso, nei casi giudiziari sopra citati gli indirizzi IP sono stati memorizzati da un *software* sviluppato dalla società svizzera Logistep AG, che svolge una funzione inquietante secondo quanto affermato dal Tribunale: «si tratta […] di un *software* che registra gli indirizzi IP di tutti gli utenti connessi ad un programma di *file sharing*». Se ciò fosse vero si registrerebbe una palese e generalizzata violazione della privacy di tutti coloro i quali sono connessi ad una determinata rete di P2P, poiché non verrebbe violata la riservatezza dei soli presunti autori di atti illeciti, ma anche di chi utilizza i suddetti programmi per fini assolutamente leciti e ciò va certamente ben oltre l'eccezione di cui all'art. 24, comma 1, lett. f, cod. priv.

Come si è detto, però, le successive e opposte decisioni del Tribunale di Roma hanno chiarito l'illiceità della condotta della Peppermint, ritenendo che la compressione del diritto alla riservatezza possa avvenire solo «per la tutela di valori di rango superiore e che attengono alla difesa della collettività ovvero alla protezione dei sistemi informatici».

Come si è accennato, sul caso Peppermint è poi intervenuto anche il Garante per la protezione dei dati personali, con provvedimento del 28 febbraio 2008, sancendo l'illiceità e la non correttezza del trattamento di dati personali posto in essere da Peppermint

[78] Un *router* è un dispositivo che connette reti diverse ed in grado di instradare i pacchetti fra esse. Oggi in molte abitazioni ed in molti luoghi di lavoro trovano diffusione i *modem/router wireless*, che svolgono sia la funzione di *modem* che quella di *router*. Essi consentono la creazione di una rete locale nonché la condivisione della connessione ad Internet. Qualsiasi computer dotato di connettività *wi-fi* (per lo più in standard 802.11 "b", "g" oppure "n") può accedere alle reti così create, purché sia nel raggio di copertura del *router*. L'accesso può essere ristretto utilizzando protocolli come il WEP e il WPA.

Jam Records GmbH e Logistep AG[79]. L'Autorità ha vietato l'ulteriore trattamento dei dati illecitamente acquisiti e la loro cancellazione entro il 31 marzo 2008.

In prospettiva più ampia, bisogna sottolineare che il diritto comunitario, sulla cui base è stata emanata la normativa italiana, non prevede l'esplicita possibilità di comunicare dati personali nel contesto di un procedimento civile. In tal senso è la sentenza del 29 gennaio 2008 della Corte di Giustizia delle Comunità Europee[80], nella quale è stato rilevato che la legge comunitaria non esclude la possibilità, per gli stati membri, di istituire l'obbligo di divulgare dati personali nell'ambito di un procedimento civile. Un tale obbligo, però, attualmente non sussiste e dunque potrebbe essere sancito dagli stati membri con apposite previsioni legislative, anche se, nel nostro ordinamento, bisognerebbe valutare la legittimità costituzionale di una simile disposizione, vista l'indubbia compressione del diritto alla privacy, che ha rango costituzionale.

In linea più generale, è doveroso mettere in evidenza, comunque, che non si dovrebbe neanche discutere della liceità dei programmi di P2P: essi consentono una rapida e gratuita distribuzione di contenuti digitali di qualsiasi tipologia, poiché consentono a chiunque voglia distribuire un file mediante la rete Internet di farlo senza prendere in locazione un *server* o comunque pagando un *provider* per consentire ad altri di scaricare le proprie opere dell'ingegno, siano esse programmi per elaboratore, brani musicali, filmati, e così via. Un soggetto privato non potrebbe e non dovrebbe, quindi, violare la privacy di tutti gli utilizzatori di una rete solo perché una parte di essi si dedica allo svolgimento attività illecite.

L'identificazione automatizzata degli utenti che viene svolta in simili fattispecie può risultare assai pericolosa qualora i dati personali così acquisiti siano sottoposti ad un trattamento incrociato con altri dati che talvolta vengono messi in condivisione in segui-

---

[79] Nel procedimento era coinvolta anche la "Techland sp.z.o.o.", casa produttrice di videogiochi, che si era rivolta a Logistep AG per gli stessi motivi che avevano spinto la Peppermint Jam Records GmbH.

[80] Reperibile all'URL http://www.dirittodellinformatica.it/sentenze/privacy-e-sicurezza-(sentenze)/la-corte-di-giustizia-ce-e-il-p2p-(corte-di-giustizia-ce-29%1101%112008).html.

to all'incauto comportamento di alcuni utilizzatori di programmi di condivisione di file, i quali talvolta distrattamente condividono anche cartelle di sistema o personali, come quelle che ciascun sistema operativo di norma identifica quali "contenitori" di documenti o immagini.

Pertanto, una condotta imprudente, imperita e negligente può cagionare danni anche assai seri alla privacy degli utenti nelle suddette ipotesi. Così, possono essere colposamente condivisi non solo immagini o testi assolutamente personali, ma anche informazioni assai delicate come le proprie password o il proprio numero di carta di credito se questi sono stati memorizzati nelle cache dei programmi utilizzati per la navigazione su Internet e le cartelle che contengono tali informazioni siano state inavvertitamente condivise. Oltretutto, possono facilmente essere condivisi file, come immagini e testi, nei quali sono presenti informazioni riferibili a soggetti diversi dall'utilizzatore del computer (come, ad esempio, gli appartenenti al proprio nucleo familiare).

Bisogna a questo punto sottolineare che qualora simili dati siano scaricati e messi in condivisione da altri utenti, gli effetti negativi sulla riservatezza possono essere inarrestabili e, come si è detto, possono coinvolgere anche più persone. Difatti, se un contenuto digitale, privo di protezioni che ne impediscono la copia, esce dall'esclusiva disponibilità di un singolo soggetto la sua circolazione non appare più controllabile, poiché i possessori degli eventuali duplicati possono trovarsi in qualsiasi parte del mondo e si verifica una reazione a catena consistente nel fatto che più copie di un determinato file circolano per le reti telematiche più probabilmente esso acquisirà ancora maggiore diffusione.

Tale fenomeno appare assai preoccupante quando viene condiviso materiale relativo alla vita intima delle persone, poiché le cronache giudiziarie riportano casi in cui alcuni soggetti hanno condiviso immagini o filmati raffiguranti i propri partner precedenti in situazioni intime, e ciò a fini diversi, anche se generalmente per vendicarsi della fine del loro rapporto.

## 6. *"Massively Multiplayer Online Games" e potenziali violazioni della privacy*

Con l'espressione *Massively Multiplayer Online Games*, solitamente abbreviata in MMOG, si indicano tutti quei videogiochi che si svolgono in rete su uno o più mondi persistenti e che possono coinvolgere anche milioni di persone.

L'utilizzo del termine videogioco può dare adito ad interpretazioni scorrette e riduttive del fenomeno, riducendo tali esperienze a semplici intrattenimenti dedicati a bambini ed adolescenti. Eppure, il bisogno di svago è un'esigenza ancestrale dell'uomo, che può essere soddisfatta in molteplici modi diversi, nell'ambito dei quali proprio l'esperienza videoludica appare oggi assai interessante non solo dal punto di vista sociologico, ma anche da quelli economico e giuridico.

A titolo esemplificativo, infatti, si pensi che secondo una stima della "Entertainment Software Association" nel 2007 il fatturato relativo alle vendite dei videogiochi negli Stati Uniti ammonta a oltre nove miliardi di dollari[81] e che l'età media dei videogiocatori è di 33 anni[82]; in Italia, il giro di affari è passato dai 741.908.409 euro del 2006[83] a circa un miliardo di euro nel 2007[84]. A titolo comparativo, si pensi che nel 2005 il giro d'affari era superiore a quello generato da altri importanti settori dell'*entertainment* come home video e musica[85].

Questi semplici dati fanno capire l'importanza del fenomeno: del resto, molti MMOG hanno una complessità tale da poter essere proficuamente utilizzati solo da persone adulte e in alcuni casi il

---

[81] Http://www.theesa.com/archives/2008/01/computer_and_vi_1.php.

[82] Http://www.theesa.com/facts/top_10_facts.php.

[83] Associazione Editori Software Videoludico Italiana, *Rapporto annuale sullo stato dell'industria videoludica in Italia*, 2007, in http://www.aesvi.it/cms/attach/editor/Rapporto_Annuale_2006.pdf, p. 8.

[84] Associazione Editori Software Videoludico Italiana, *Quarto rapporto annuale sullo stato dell'industria videoludica in Italia*, 2008, in http://www.aesvi.it/cms/attach/editor/rapporto_2007.pdf, p. 7

[85] Associazione Editori Software Videoludico Italiana, *Secondo rapporto annuale sullo stato dell'industria videoludica in Italia*, 2006, in http://www.aesvi.it/cms/attach/editor/rapp06previewDEF.zip, p. 14.

videogioco si configura come una vero e proprio mondo parallelo a quello reale: è questo il caso del ben noto "Second Life"[86], che è un mondo virtuale raffigurato con tecnologie tridimensionali nel quale chiunque può vivere una sorta di "seconda vita" e che rientra nella categoria dei giochi focalizzati sulla socializzazione fra i giocatori più che sul raggiungimento di obiettivi specifici; tale categoria è comunemente denominata *Massively Multiplayer Online Social Games* (MMOSG).

Gli utilizzatori di "Second Life" ammontano, attualmente, ad oltre dodici milioni e vengono denominati "residenti"; essi operano mediante un *alter ego* digitale (il c.d. *avatar*[87])[88]. In realtà, *Second life* è un vero e proprio simulatore della realtà contemporanea: come nel mondo "reale" vi è una valuta (denominata "Linden Dollars", L$) che può essere utilizzata all'interno del gioco per acquisti o investimenti. In esso, infatti, è possibile comprare lotti di terreno, costruire case e negozi[89], ma è altresì possibile semplicemente dialogare con gli altri utenti. Inoltre, è possibile acquistare L$ pagando con valute utilizzate nel mondo "reale", come il dollaro statunitense oppure l'euro.

Chiaramente, la divisione tra "reale" e "virtuale" risulta in questi casi abbastanza labile, poiché *Second life* rappresenta un qualcosa di più di un "semplice videogioco": è una vera e propria società sviluppatasi in seno alla Società dell'informazione, di cui costituisce, di fatto, un prodotto. È, infatti, il prodotto di una società globalizza-

---

[86] Su *Second Life* cfr. M. Gerosa, *Second Life*, Meltemi, Roma, 2007.

[87] Nel prossimo futuro potrebbe aversi un'evoluzione di «Internet come cyberspazio globale dove ciascun utente possa interagire attraverso il proprio avatar» (S. Cacciaguerra, *Partecipazione a mondi virtuali e utenti mobili*, in *Sistemi intelligenti*, 2007, 1, p. 9).

[88] Tali dati sono riportati sul sito http://secondlife.com/whatis/faq.php.

[89] Si pone, così, il problema del regime giuridico delle proprietà virtuali, generalmente disciplinato, con clausole vessatorie, nell'ambito degli accordi di licenza (sul punto cfr. A. Chein, *A practical look at virtual property*, in *St. John's Law Review*, 2006, 80, 3, pp. 1059-1090, e S.J. Horowitz, *Competing Locklean Claims to Virtual Property*, in *Harvard Journal of Law & Technology*, 2007, 20, 2, pp. 443-458).

ta ove i vincoli spaziali perdono di importanza, poiché i suoi "residenti" sono persone che vivono in tutto il mondo[90].

Tale società, così come altre comunità simili create dalla fantasia umana, non è solo una sorta di imitazione della realtà quotidiana, ma ne costituisce, al contempo, una parte e, per alcuni, una via di fuga da una quotidianità ritenuta forse non appagante. Non a caso l'analisi di questa come di altre esperienze dimostra come la natura umana alfine tenda ad esplicarsi con le stesse modalità con cui va avanti la vita per così dire tradizionale. Nascono così amori, amicizie, rapporti di affari, ma anche attività criminali, compiute talvolta all'interno del gioco. Si creano dei microcosmi che costituiscono delle micro rappresentazioni della realtà oltre che esserne parte.

Inoltre, alcuni tratti comuni fanno capire come i MMOG siano una rappresentazione della società in cui viviamo: ad esempio, l'utilizzo di una valuta per acquistare beni relativi al mondo persistente in cui "vive" ciascun *alter ego* digitale è una caratteristica abbastanza comune, che è utilizzata soprattutto in una diffusa tipologia di MMOG, ossia nei *Massively Multiplayer Online Role Playing Games* (MMORPG)[91]. In essi ciascun giocatore sceglie un proprio *alter ego* digitale, come in *Second life*, ma di norma in tale tipologia di giochi ci si cala in un'ambientazione fantastica abbastanza diversa

---

[90] Sui mondi e le comunità virtuali cfr. J.M. Balkin, B.S. Noveck (eds.), *The State of Play. Law, Games and Virtual Worlds*, New York University Press, New York, 2006; M. Gerosa, A. Pfeffer, *Mondi virtuali*, Castelvecchi, Roma, 2006; L. Giuliano, *Padroni della menzogna. Il gioco delle identità e dei mondi virtuali*, Meltemi, Roma, 1997; P. Harrigan, N. Wardrip-Fruin (eds.), *Second Person. Role-Playing and Story in Games and Playable Media*, The MIT Press, Cambridge, Massachusetts, 2007; S. Johnson, *La nuova scienza dei sistemi emergenti. Dalle colonie di insetti al cervello umano, dalle città ai videogame e all'economia, dai movimenti di protesta ai network*, tr. it., Garzanti, Milano, 2004; F.G. Lastowka, D. Hunter, *The Laws of the Virtual Worlds*, in *California Law Review*, 2004, 92, 1, pp. 1-73; T.L. Taylor, *Play Between Worlds: Exploring Online Game Culture*, The MIT Press, Cambridge, Massachusetts, 2006; S. Tosoni, *Identità virtuali. Comunicazione mediata da computer e processi di costruzione dell'identità personale*, Franco Angeli, Milano, 2004; B. Wooley, *Mondi virtuali*, tr. it., Bollati Boringhieri, Milano, 1999.

[91] Vi sono diverse categorie di videogiochi svolti parzialmente o esclusivamente *on line*: *Massively Multiplayer Online First Person Shooter* (MMOFPS), *Massively Multiplayer Online Real Time Strategy* (MMORTS), *Massively Multiplayer Online Racing* (MMOR), ecc.

da quella odierna, che è invece ben raffigurata proprio nel videogioco da ultimo citato.

Fra i tanti MMORPG attualmente esistenti bisogna menzionare "World of Warcraft", utilizzato da oltre nove milioni di persone in tutto il mondo. Anche in esso si ritrovano alcune caratteristiche di *Second life*, ma non è ad esempio possibile acquistare una casa. Sono presenti, però, un sistema economico abbastanza complesso oltre che strumenti per garantire la comunicazione fra i giocatori. Essi possono anche riunirsi nelle c.d. gilde, che costituiscono una sorta di associazione finalizzata all'aiuto reciproco, poiché in questa tipologia di giochi i personaggi aumentano le proprie doti raggiungendo determinati obiettivi e aumentando il proprio livello. A volte alcune gilde hanno rilevanza nazionale[92] e quindi costituiscono espressione di un implicito o esplicito desiderio di ribadire la propria appartenenza ad una singola realtà statale.

Non è possibile andare oltre nella descrizione di questi seppur interessanti esempi, che sollevano questioni giuridiche tutt'altro che trascurabili, anche in virtù degli imponenti interessi economici in gioco che coinvolgono non solo le case produttrici ma anche gli stessi giocatori. In linea generale, infatti, questa tipologia di videogiochi richiede il pagamento di un canone periodico, giustificato sia dal fatto che il loro sviluppo non si arresta alla fase della commercializzazione ma prosegue anche nei periodi successivi e sia in virtù dei costi necessari per il mantenimento dei *server* di gioco sia per predisporre una continua assistenza tecnica a favore dei giocatori.

La configurazione di MMOG e MMORPG quali società di fatto e quasi autonome ha però spinto molte persone ad utilizzarli più come fonte di lucro che di svago. Sono infatti sorti siti nei quali è possibile acquistare personaggi di livello avanzato oppure oggetti da utilizzare nei giochi o, ancora, effettuare operazioni di cambio valuta[93]. In taluni casi ciò avviene nonostante gli sforzi, anche legali,

---

[92] Ad esempio, in Italia sono presenti, fra le altre, le gilde denominate "Italian Brotherhood" e "Italian Guild".

[93] Nel caso di «World of Warcraft» ciò costituisce una violazione dei termini di utilizzo contrattualmente accettati dai giocatori: «2. C. You agree that you will not […] v. buy or sell for "real" money or exchange gold, weapons, armor, or any other virtual items that may be used in World of Warcraft outside the World of

delle case produttrici dei videogiochi stessi, poiché in tal modo viene falsata l'esperienza di gioco e ciò può portare ad un progressivo calo di interesse verso le stesse piattaforme videoludiche, con ovvie conseguenze dannose per le stesse case produttrici.

Inoltre, la "promozione" di siti che offrono i suddetti servizi viene svolta non solo tramite la presenza di siti dedicati e dunque a mezzo di normali e leciti messaggi promozionali, ma anche mediante comunicazioni non richieste: si verificano, infatti, sempre più numerosi casi di *spamming*, poiché in tutti i giochi *on line* i giocatori possono comunicare grazie a strumenti più o meno evoluti, che spaziano dalla semplice chat a veri e propri servizi postali, con tanto di spese di spedizione, ovviamente nella valuta del gioco medesimo. Lo *spamming* ha così oltrepassato i confini dei mezzi di comunicazioni tradizionali, ivi compresa la posta elettronica, divenuta oramai di uso comune.

In linea teorica, il diritto di non ricevere messaggi pubblicitari indesiderati, comunque, può ritenersi applicabile anche in tali fattispecie, dal momento che nella normativa italiana non sembra siano ravvisabili limiti ostativi ad una simile interpretazione. Il rispetto delle regole "interne" dovrebbe essere assicurato da chi gestisce il gioco (in genere i c.d. amministratori), ma nulla vieta di adire la competente autorità giudiziaria qualora si ritenga che si sia verificata una lesione dei propri diritti. È utile ribadire, infatti, che quanto accade *on line* avviene comunque nella realtà tradizionale. Come si è visto, tali microcosmi, microsocietà o qualsiasi altra definizione si voglia utilizzare, costituiscono delle rappresentazioni della società contemporanea, con i suoi pregi e i suoi difetti. Non è detto che nel prossimo futuro, accanto alle professioni per così dire "manuali" svolte nel gioco al fine di acquisire ricchezza (fabbri, pescatori, ecc.), non si possa o non si debba addirittura arrivare alla possibilità di creare giudici e avvocati.

Alle fattispecie sinora descritte si accompagnano, poi, addirittura atti illeciti, come il c.d. *cheating*[94]. Con tale termine si indicano at-

---

Warcraft platform» (World of Warcraft Terms of Use Agreement, 28 agosto 2007, http://www.wow-europe.com/en/legal/termsofuse.html).

[94] Sul punto cfr. l'interessante ricostruzione del fenomeno operata in M. Consalvo, *Cheating. Gaining Advantages in Videogames*, The MIT Press, Cambridge, Massachusetts, 2007.

tività che consistono nella violazione di regole del gioco che portano taluni giocatori ad avere vantaggi ingiusti sugli altri. Ciò può avvenire in diversi modi, ma assume una particolare rilevanza l'utilizzo di appositi programmi che modificano le caratteristiche e le regole dei giochi a vantaggio dei c.d. *cheaters*.

In linea generale, detti programmi costituiscono una violazione degli obblighi contrattuali assunti dal giocatore, il quale di norma conclude un contratto di licenza d'uso con la casa produttrice o distributrice del MMOG (e delle sue varianti), che può tuttavia costituire un serio pericolo per la tutela della riservatezza degli utenti.

In tal senso, risulta utile esaminare, per gli spunti di riflessione che ne derivano, il caso specifico del già citato "World of Warcraft", i cui termini di utilizzo, che devono essere accettati da ogni giocatore, espressamente vietano la creazione o l'utilizzo di simili programmi[95].

In merito, è di particolare interesse il punto 17.E dei termini di utilizzo, secondo i quali l'utente riconosce alla casa produttrice del videogioco (la Blizzard Entertainment) il diritto di ottenere "certe" informazioni dal suo computer e dai suoi componenti, ivi inclusi la memoria, la scheda video, il processore e le periferiche di memorizzazione, il tutto all'esclusivo fine di assistere la stessa Blizzard Entertainment a vigilare sugli utenti che potrebbero utilizzare *hacks* o *cheats* per trarre un ingiusto vantaggio rispetto agli altri giocatori[96].

Ancora, ai sensi del punto 17.C, la Blizzard Entertainment si arroga il diritto di ottenere "certe" informazioni riguardanti il computer dell'utente ed il sistema operativo ivi installato, inclusi il numero identificativo dei dischi rigidi, del processore, dei sistemi operativi

---

[95] «2. C. You agree that you will not […] ii. create or use cheats, "mods", and/or hacks, or any other third-party software designed to modify the World of Warcraft experience» (World of Warcraft Terms of Use Agreement, 28 agosto 2007, http://www.wow-europe.com/en/legal/termsofuse.html).

[96] «17. E. In order to assist Blizzard Entertainment to police users who may use "hacks" or "cheats" to gain an advantage over other players, you acknowledge that Blizzard Entertainment shall have the right to obtain certain information from your computer and its component parts, including your computer's random access memory, video card, central processing unit, and storage devices. This information will only be used for the purpose of identifying "cheaters", and for no other reason». (World of Warcraft Terms of Use Agreement, 28 agosto 2007, http://www.wow-europe.com/en/legal/termsofuse.html).

nonché l'indirizzo IP, il tutto a fini identificativi e senza ulteriore avviso[97].

Il quadro inerente le presumibili violazioni al diritto alla privacy si completa, poi, con il punto 17.D, ai sensi del quale la casa produttrice ha il diritto di ottenere dati "non personali" dalla connessione a "World of Warcraft" al fine effettuare "certe" valutazioni di carattere demografico riguardo gli utenti del gioco stesso[98]. Anche in questo caso il tutto avviene senza ulteriori avvisi all'utente.

Le suddette attività di acquisizione dei dati costituiscono certamente un trattamento ai sensi dell'art. 4, comma 1, lett. a, cod. priv., dal momento che costituiscono un complesso di operazioni che concerne la raccolta e la registrazione di dati personali.

Tramite queste "clausole generali" la Blizzard Entertainment acquisisce una mole notevole di dati personali dei propri clienti, ma gli scopi della raccolta sembrano violare l'art. 11, comma 1, lett. d, cod. priv., poiché i dati raccolti non si appalesano «pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti o successivamente trattati».

Più specificatamente, la dizione di «certe informazioni» è troppo generica ed arbitraria, dal momento che è la suddetta azienda che sceglie, con propria insindacabile valutazione, quali informazioni raccogliere dal computer dell'utente, e sicuramente lo scopo di vigilare affinché alcuni giocatori non facciano uso di programmi o di tecniche di *cheating*, per quanto meritevole, non può essere perseguito mediante una generale acquisizione di informazioni che costituiscono dati personali ai sensi dell'art. 4, comma 1, lett. b, visto che tramite esse si può identificare il singolo utente mediante il riferimento ad altre informazioni. I dati raccolti sono, quindi, eccedenti

---

[97] «17. C. Blizzard Entertainment has the right to obtain certain identification information about your computer and its operating system, including the identification numbers of your hard drives, central processing unit, IP addresses and operating systems, for identification purposes without any further notice to you» (World of Warcraft Terms of Use Agreement, 28 agosto 2007, http://www.wow-europe.com/en/legal/termsofuse.html).

[98] «17. D. Blizzard Entertainment has the right to obtain "non-personal" data from your connection to World of Warcraft in order to make certain demographic assumptions regarding the users of World of Warcraft without any further notice to you» (World of Warcraft Terms of Use Agreement, 28 agosto 2007, http://www.wow-europe.com/en/legal/termsofuse.html).

rispetto alle finalità del trattamento, anche perché essa è così generica ed eventuale da non poter certo comportare una generalizzata raccolta dei dati personali degli utenti.

Il punto 17.C è tuttavia ancor più delicato, poiché l'identificazione dell'utente già avviene mediante l'inserimento del proprio nome utente e della propria password nell'interfaccia del gioco, per cui la raccolta di tali dati è sicuramente eccedente rispetto alla finalità di identificazione dell'utente, il tutto in chiara violazione dell'art. 11, comma 1, lett. d, cod. priv.

La lettura di tali disposizioni contrattuali unitamente al successivo punto 17.D fa capire quali siano le potenzialità lesive di "World of Warcraft" per la privacy dei suoi utilizzatori, poiché esso comporta la raccolta di dati definiti "non personali" senza però specificare in concreto quali essi siano: all'utente non viene lasciata alcuna possibilità di scelta in ordine al consenso al trattamento di tali dati.

In linea più generale, comunque, bisogna osservare che i problemi di possibile violazione della privacy riguardano l'intera categoria dei mondi virtuali persistenti, considerando, oltretutto, che i loro gestori acquisiscono numerose tipologie di informazioni che permettono di ottenere una visione completa di una persona[99], frammentata in quelle stesse categorie osservabili nel ciberspazio (consumatore, lavoratore, ecc.).

Inoltre, sarebbe necessaria una limitazione *ex lege* dei contratti di licenza conclusi fra i gestori e gli utenti in modo da impedire ai primi l'inserimento di clausole vessatorie come quelle di cui si è detto[100], poiché in tali negozi il rapporto sinallagmatico appare altamente squilibrato in senso negativo per i giocatori, che costituiscono la parte debole del contratto.

Appare chiaro, dunque, che l'essere sempre *on line* pone dei rischi per la propria privacy, sia che ciò avvenga per fini ludici che lavorativi. Se in taluni casi è sufficiente adottare opportune cautele per evitare l'involontaria o l'incauta comunicazione dei propri dati personali, in altri l'alternativa è utilizzare o meno un determinato prodotto poiché il semplice utilizzo richiede la preliminare accetta-

---

[99] T. Zarsky, *Privacy and Data Collection in Virtual Worlds*, in J.M. Balkin, B.S. Noveck (eds.), *The State of Play*, cit., p. 221.

[100] Ivi, p. 222.

zione di clausole contrattuali che si appalesano nulle e dunque da considerare come non apposte. Ciò nonostante violazioni, anche di non rilevante entità, del diritto alla privacy possono verificarsi, con conseguente perdita del controllo sui propri dati personali. Tali vicende non possono essere trascurate, poiché dal trattamento incrociato di più dati possono esserne ricavati di altri e può giungersi ad una illecita raffigurazione digitale di una persona, senza possibilità di tornare alla situazione *quo ante*.

## Capitolo III

# TECNOLOGIE E METODOLOGIE DI CONTROLLO INDIVIDUALE E COLLETTIVO

## 1. *Aspetti generali*

Ai benefici del progresso tecnologico, con particolare riferimento all'interconnessione globale dei sistemi informatici ed alle sempre crescenti potenzialità di acquisizione e di trattamento di dati, si accompagnano le problematiche connesse al cattivo uso che soggetti pubblici e privati possono fare dei nuovi strumenti e dell'evoluzione di quelli già disponibili.

Come ha sottolineato Steven Levy, strumenti come il telefono e il computer hanno fatto sì che chiunque sia sempre raggiungibile ed al loro uso si è accompagnata la fallace credenza di restare nel più assoluto ambito privato quando, nella tranquillità della propria casa o negli spazi del proprio ufficio, si comunica mediante essi per trasmettere pensieri, confidenze, piani di lavoro e addirittura denaro. Il problema che tutto ciò che viene detto o fatto può essere intercettato: «mentre crediamo di bisbigliare, di fatto è come se stessimo diffondendo via radio le nostre informazioni al mondo intero»[1].

Negli stati moderni si registra una crescente tendenza a sorvegliare con strumenti sempre più evoluti tutto ciò che accade sul loro territorio e la vita quotidiana è oggi strettamente monitorata come non mai. Purtroppo alla modernità può conseguire un progressiva-

[1] S. Levy, *Crypto. I ribelli del codice in difesa della privacy*, tr. it., Shake, Milano, 2002, p. 7.

mente maggiore «affidamento sull'informazione e la conoscenza, al fine di generare e mantenere il potere. E poiché quell'informazione è in buona parte costituita da dati di tipo personale, il focalizzarsi dell'attenzione su di essi ha quale conseguenza la sorveglianza»[2].

Certo, gli esseri umani hanno sempre osservato i comportamenti altrui, ma tale fenomeno non aveva le proporzioni odierne e l'osservazione non era generalmente sistematica, ma oggi la «normale sorveglianza di routine, solitamente gestita da agenzie e organizzazioni geograficamente lontane da noi, è radicata in ogni aspetto della vita»[3].

Nella Società dell'informazione il controllo si basa su tecnologie di sorveglianza assai evolute, che consentono di avere un quadro abbastanza preciso di tutti gli aspetti inerenti le persone fisiche e giuridiche. Tuttavia, l'invadenza delle tecnologie «utilizzate a fini di controllo sociale (monitoraggio e sorveglianza, prevenzione e repressione dei comportamenti devianti) ha trasformato la questione della privacy in una questione di libertà»[4].

Tali problematiche sono amplificate dall'utilizzo di Internet, poiché ogni dato che viaggia sulle reti telematiche può essere registrato e su di esso possono essere svolte attività di trattamento automatizzato, eventualmente incrociandolo con altri dati al fine di ottenere informazioni che vanno al di là di quanto sarebbe possibile ottenere dall'esame del dato in sé considerato. Basti pensare a quante informazioni ciascuna persona può reperire su se stessa semplicemente effettuando una ricerca su un *search engine* sul web utilizzando come parole chiave i propri nome e cognome. Ogni collegamento porterà, di norma, a pagine diverse, dalle quali sarà possibile ricostruire un frammento delle attività, delle preferenze o di qualsiasi altra informazione personale riferibile alla persona stessa. Un successivo trattamento incrociato dei dati così rinvenuti può portare ad una composizione dei frammenti secondo un quadro maggiormente completo, risultante dall'unione di più informazioni diverse.

---

[2] D. Lyon, *La società sorvegliata. Tecnologie di controllo della vita quotidiana*, tr. it., Feltrinelli, Milano, 2002, p. 41.

[3] Ivi, p. 1.

[4] A. Di Corinto, T. Tozzi, *Hacktivism. La libertà nelle maglie della rete*, Manifestolibri, Roma, 2002, p. 73.

Ovviamente, le motivazioni e le giustificazioni che spingono a porre in essere dei sistemi di controllo individuale e collettivo sono diverse a seconda che i "controllori" siano pubblici o privati.

Nel primo caso, è d'uopo sottolineare che vi è una stretta correlazione tra potere statuale e controllo nonché tra potere statuale e informazione. Il potere, infatti, consiste anche nel sapere ciò che accade e nel poter intervenire grazie alla propria autorità; esso, però, è anche controllo dell'informazione, che, non a caso, è stata sempre limitata dai regimi autoritari, come è avvenuto in Germania, Italia e Unione Sovietica nelle rispettive epoche naziste, fasciste e comuniste, e come avviene tuttora, ad esempio, in Cina e a Cuba.

L'interconnessione globale dei sistemi informatici *lato sensu* intesi pone, da un lato, difficoltà nel controllare ciò che avviene *on line*[5], ma, dall'altro, presta il fianco alla possibilità di sorvegliare la vita digitale di chiunque si trovi nel ciberspazio.

I regimi democratici, in linea teorica, non potrebbero certo controllare le comunicazioni e, di conseguenza, i propri cittadini, trattandoli come delinquenti presunti. Si consideri, infatti, che in Italia «la libertà e la segretezza della corrispondenza e di ogni altra forma di comunicazione sono inviolabili. La loro limitazione può avvenire soltanto per atto motivato dell'autorità giudiziaria con le garanzie stabilite dalla legge» (art. 15 Cost.).

Ciò nonostante, si moltiplicano i tentativi di controllo su scala nazionale e globale, che fanno leva sulla diffusa insicurezza generata dalla instabilità politica internazionale (si pensi agli atti di terrorismo) e dalle frodi e dai crimini commessi *on line* e *off line*.

Si pensi, così, al periodico bombardamento mediatico sui misfatti che accadono nel ciberspazio o sui delitti che sarebbero stati resi possibili o, quanto meno, ampiamente facilitati dalla sua diffusione.

L'insicurezza informatica dovrebbe, quindi, essere osservata sia nella prospettiva delle problematiche tecniche, connesse alla sicurezza delle infrastrutture tecnologiche e dei sistemi collegati fra di

[5] Si è infatti «realizzato un processo di deterritorializzazione che consente rapporti interpersonali al di là della tradizionale configurazione spaziale sottraendoli in qualche modo all'occhio vigile e garante dello stato» (T. Serra, *Lo stato e la sua immagine*, Giappichelli, Torino, 2005, p. 63).

loro, ma anche in quella, più generale, della Società dell'informazione considerata in tutte le sue molteplici sfumature.

Nel 2000 vi è stata una forte presa di coscienza delle problematiche derivanti dall'insicurezza dei network informatici da parte di molti governi del mondo, che hanno giudicato intollerabile la minaccia del *cybercrime*. Tuttavia, è stato giustamente evidenziato che i danni concreti, sia alla proprietà sia alla persona, derivanti dall'insicurezza delle infrastrutture digitali di comunicazioni, per quanto ingenti, sono enormemente inferiori alla perdita di vite umane, al degrado dell'ambiente e ai danni economici provocati dalle disavventure dell'industria automobilistica o di quella chimica[6].

La nuova forma di comunicazione globale fra gli individui costituisce, però, una potenziale minaccia per i vari governi, poiché è uno strumento formidabile di espressione del dissenso, che, grazie allo sganciamento dai vincoli spaziali e temporali, può assumere una scala globale addirittura quando il dissenso stesso è riferito a fattispecie locali. Si pensi a quanto avviene in Cina, dove i ciberdissidenti riescono a comunicare anche al di fuori del loro territorio superando i filtri comunicativi imposti dal governo locale.

Inoltre, gli atti di *hacking* e di *cracking* possono, potenzialmente, dispiegare i propri effetti in una determinata realtà nazionale ed essere commessi altrove, come nel caso in cui, ad esempio, venga operata la sostituzione di un sito istituzionale italiano con una pagina web di qualsiasi tipo (il c.d. *defacement)* da un *hacktivist*[7] o da

---

[6] M. Castells, *Galassia Internet*, tr. it., Feltrinelli, Milano, 2001, p. 169.

[7] Il termine *hacktivist* deriva dall'unione di *hacker* e di *activist*. Con esso si identifica chi utilizza le tecniche proprie degli *hackers* a fini di attivismo ideologico e politico. Molti *hacktivists*, in particolare, si rendono protagonisti di atti di disobbedienza civile elettronica (su di essa e sulla disobbedienza civile in generale cfr. T. Serra, *La disobbedienza civile. Una risposta alla crisi della democrazia?*, Giappichelli, Torino, 2002). Sugli *hackers* cfr. A. Di Corinto, T. Tozzi, *Hacktivism. La libertà nelle maglie della rete*, cit.; R. Chiesa, S. Ciappi, *Profilo hacker. La scienza del Criminal Profiling applicata al mondo dell'hacking*, Apogeo, Milano, 2007; A. Fici, *Mondo hacker e logica dell'azione collettiva*, Franco Angeli, Milano, 2004; G. Francione, *Hacker. I Robin Hood del ciberspazio*, Lupetti, Milano, 2004; P. Himanen, *L'etica hacker e lo spirito dell'età dell'informazione*, tr. it., Feltrinelli, Milano, 2003; E.S. Raymond (ed.), *The New Hacker's Dictionary*, The MIT Press, Cambridge, Massachusetts, 1999; D. Thomas, *Hacker Culture*, University of Minnesota Press, Minneapolis, Minnesota, 2002.

un *cracker*[8] che si trova in Corea del Nord: in casi simili l'attività delle forze di polizia si scontra con problematiche di carattere territoriale.

Pertanto, per difendere una sovranità che viene gradatemente erosa dal ciberspazio, alcuni stati possono decidere di perderne una parte creando uno spazio comune e globale per le attività di polizia[9]. In tal caso perdono sovranità poiché devono condividere il potere e trovare un accordo su standard comuni di regolamentazione – e così diventano essi stessi un network (di agenzie di regolamentazione e di polizia) – ma riescono tuttavia a conservare collettivamente un certo grado di controllo politico, anche se le eventuali attività di accertamento e di repressione devono necessariamente essere legate alle vecchie forme di potere basate sulla territorialità. In particolare, la repressione sarà differenziata in base alle regole di ciascun paese, mentre la sua base informazionale sarà standardizzata secondo il comune concetto di ragionevole sospetto espresso dai partecipanti al network[10].

In una prospettiva probabilmente utopistica, spostando l'attenzione dagli eventi criminosi e dalle modalità della loro repressione (che può, a sua volta, essere illecita) verso la possibile evoluzione della società contemporanea, Pierre Levy ha affermato che la diffu-

---

[8] I *crackers* sono degli esperti criminali informatici, che hanno le stesse doti degli *hackers* e le utilizzano a fini illeciti. L'*hacker* è, invece, una persona che si diverte ad esplorare i dettagli dei sistemi informatici, migliorando sempre le proprie capacità pensando più all'aspetto pratico che a quello teorico, perché guidata da una sfrenata passione per la programmazione.

[9] Del resto, oggi «la comunicazione supera le regole comunicative ristrette nell'ambito dell'apparato coercitivo degli stati» (così T. Serra, *La democrazia redenta. Il cammino senza fine della democrazia*, Giappichelli, Torino, 2001, p. 49). Nel 1992 in Europa è stato istituito l'Ufficio europeo di polizia (EUROPOL), che comprende i rappresentanti di tutta una serie di servizi incaricati di far osservare le leggi, al fine di migliorare l'efficacia e la cooperazione delle autorità competenti degli stati membri nella prevenzione e lotta a forme gravi di criminalità organizzata internazionale. Sul punto appare altresì utile evidenziare che il 23 novembre del 2001 è stata aperta alla firma la Convenzione di Budapest sulla cybercriminalità: su di essa cfr., fra gli altri, R. Mazza, *Recenti sviluppi nella repressione internazionale dei crimini informatici: la Convenzione di Budapest del 2001*, in *La comunità internazionale*, 2004, 1, pp. 91-117. Detta Convenzione è stata ratificata dall'Italia con la l. 18 marzo 2008, n. 48.

[10] M. Castells, *Galassia Internet*, cit., pp. 169-171.

sione del ciberspazio sta permettendo alla democrazia di raggiungere l'intera razza umana; di qui la necessità, più che la possibilità, di una ciberdemocrazia. La creazione di un governo mondiale, che garantisca il rispetto di un codice legislativo redatto democraticamente dall'intelligenza collettiva umana, potrebbe stabilire una pace universale. In una simile civiltà, l'aggressività umana potrebbe sfogarsi nella competizione economica o nella molteplicità di battaglie d'informazione e conflitti virtuali[11]. Per quanto tale tesi sia suggestiva e la prospettiva di un mondo in cui regna la pace sia certamente più che desiderabile, non sembra che la società possa avere, quanto meno nel prossimo futuro, una simile evoluzione.

Al contrario, la maggiore evoluzione (*rectius* involuzione) della Società dell'informazione sembra consistere nel controllo dell'informazione digitale e delle persone elettroniche, ossia dei profili digitalizzati degli esseri umani, anche grazie al sempre crescente utilizzo di Internet.

Il controllo dei comportamenti *on line* viene attuato mediante una complessa strategia, anche se non si comprende quanto siano consapevoli i vari legislatori nel crearla e darvi esecuzione oppure se, in realtà, sia semplice espressione della loro incompetenza e della loro tecnofobia, che si concretizzano non solo nella stringente regolamentazione e nella criminalizzazione di fattispecie che si realizzano per via telematica o, comunque, mediante l'utilizzo di strumenti informatici, ma anche nell'utilizzo delle nuove tecnologie al fine di sorvegliare ciò che accade nei propri territori e talvolta anche al di fuori di essi.

Ciò comporta un ridimensionamento dell'estensione del diritto alla privacy, il cui esercizio viene limitato o comunque sacrificato in nome della maggiore tutela da assicurare ad altri diritti e, in linea generale, della sicurezza.

L'anonimato, dunque, sembra divenire sempre più un'utopia, dal momento che vengono posti dei precisi limiti all'utilizzo di tecnologie e metodologie che dovrebbero consentire alla persona uma-

---

[11] P. Levy, *Verso la ciberdemocrazia*, in D. De Kerckhove, A. Tursi (a cura di), *Dopo la democrazia? Il potere e la sfera pubblica nell'epoca delle reti*, Apogeo, Milano, 2006, pp. 3-23.

na di "essere lasciata sola", o, in termini diversi, di controllare quali dati personali possano essere conosciuti da terzi.

I tasselli che costituiscono un simile mosaico hanno caratteristiche ed estensioni diverse, ma la loro visione d'insieme fa intuire quanto gli spazi, digitali e non, a disposizione del singolo vadano progressivamente riducendosi.

Così, la volontà di proteggere le proprie comunicazioni elettroniche mediante l'utilizzo di strumenti di crittografia[12] si scontra con le limitazioni imposte dagli stati in materia, dal momento che essi sono considerati *dual-use goods*, al contempo mezzi di protezione della riservatezza e strumenti militari, al pari delle armi vere e proprie. La decrittazione di un messaggio cifrato, infatti, può richiedere anche mesi o anni di calcolo da parte di elaboratori molto potenti qualora se ne voglia tentare la lettura in mancanza della chiave crittografica; tanto più alto sarà il livello di protezione e tanto più tempo sarà necessario per riuscire a decrittare il messaggio. Di qui la forte limitazione che i vari stati, anche mediante la conclusione di accordi internazionali, hanno imposto alle tecniche di crittografia "forte".

La cifratura delle comunicazioni, però, non risponde solo all'esigenza di tutelare la riservatezza delle comunicazioni per così dire "tradizionali" ma rese in formato elettronico, come, ad esempio, quelle svolte mediante strumenti di posta elettronica. Difatti, l'utilizzo di protocolli di comunicazione sicuri che operano la cifratura delle informazioni trasmesse assume una rilevanza fondamentale per la sicurezza delle transazioni telematiche, in quanto assicura la protezione dei dati scambiati durante il loro svolgimento. Intuitivamente questo profilo è fondamentale per il successo del commercio elettronico, in linea generale, e delle attività di vendita di beni e di fornitura di servizi resi mediante Internet.

La considerazione dei suddetti aspetti ha così portato ad un'apertura verso l'utilizzo generalizzato degli strumenti di cifratura dei dati, che in taluni casi devono essere utilizzati *ex lege*, come nel caso

[12] La crittografia è stata intesa per lungo tempo come la scienza che studia i sistemi per rendere le informazioni segrete e leggibili solo a chi possiede la chiave per decifrarle, anche se oggi nel suo ambito vengono studiate tecniche per la verifica dell'integrità dei messaggi, la firma digitale, l'autenticazione dell'identità di chi invia e/o riceve un messaggio, ecc.

dei dati sensibili e giudiziari (ad esempio, quelli sanitari e genetici) contenuti in elenchi, registri o banche di dati, tenuti con l'ausilio di strumenti elettronici.

Purtroppo, però, l'utilizzo di simili strumenti sembra porre in cattiva luce chiunque li utilizzi perché sembra che abbia qualcosa da nascondere, come se l'esigenza di privacy non fosse meritevole di tutela solo perché viviamo in un'epoca caratterizzata da terrorismo e *cybercrime*.

Eppure l'intensa attività di sorveglianza posta in essere dagli stati per risolvere tali problematiche non appare idonea a risolverle: bisogna anche passare all'azione, ma sembra che l'evoluzione degli strumenti di sorveglianza serva più ad automatizzare l'attività sanzionatoria delle violazioni al Codice della strada che a fini di sicurezza!

Se il quadro pubblico è, dunque, alquanto sconfortante, bisogna sottolineare che al controllo e alla sorveglianza posti in essere da soggetti pubblici si affiancano quelli svolti da soggetti privati, a volte nel rispetto di specifiche normative che sacrificano il diritto alla privacy per offrire una maggiore tutela ad altre posizioni giuridiche, altre volte in aperta violazione delle regolamentazioni vigenti.

Emblematiche, nel primo senso, sono le normative sulla proprietà intellettuale emanate dalla maggior parte degli stati, che presentano un aspetto comune consistente in una tutela squilibrata a favore dei detentori dei diritti d'autore o del copyright soprattutto nel caso in cui film, brani musicali o *software* siano posti in condivisione su Internet.

La tendenza in tal senso è, infatti, addirittura nel concedere poteri investigativi più o meno intensi ai titolari dei suddetti diritti, come avviene negli Stati Uniti nei confronti della RIAA, anche grazie al Digital Millennium Copyright Act (DMCA), o come potrebbe avvenire in Europa con l'approvazione della direttiva IPRED2 (*The Second IPR Enforcement Directive*)[13].

[13] L'art. 7 della direttiva IPRED2 dispone che «gli Stati membri assicurano che i titolari dei diritti di proprietà intellettuale interessati, o i loro rappresentanti, e gli esperti possano contribuire alle indagini condotte dalle squadre investigative comuni» sulle violazioni del diritto di proprietà intellettuale definite nella medesima direttiva.

Le ricadute sulla tutela del diritto alla privacy sono, chiaramente, di grandissimo impatto, poiché ad alcuni soggetti privati viene addirittura concessa la facoltà di intercettare le comunicazioni fra gli utilizzatori della Rete qualora ritengano che un loro diritto patrimoniale possa essere messo in discussione. Ne consegue, purtroppo, un generalizzato controllo telematico svolto da questi soggetti privati, che, a sua volta, comporta una diffusa violazione della riservatezza di chi fa uso della rete sorvegliata da essi, che assume scala globale poiché, come si è detto, gli utilizzatori di Internet si trovano in tutto il mondo.

Del resto, l'attività legislativa ha un'importanza fondamentale per le imprese private, poiché, se indirizzata o addirittura squilibrata verso la tutela degli interessi di quest'ultime, consente loro di mantenere i propri diritti, se non di aumentarli, in un'economia incentrata su Internet, ove, del resto, esse hanno bisogno di violare la privacy dei loro clienti, o comunque di chi vi entra in contatto, per vendere le informazioni acquisite e trattate[14]. Dette informazioni hanno un'importanza fondamentale perché sono «alla base di tutti i processi decisionali individuali e collettivi. L'informazione si vende e si acquista, si accumula e si protegge, viene trasformata in prodotti complessi che comprendono conoscenza e attività»[15].

In dottrina è stato così evidenziato che «al mercato interessano profili di consumo basati sui comportamenti, mentre l'attribuzione univoca dell'identità a un determinato comportamento ha più a che fare con le attività di polizia che col mercato»[16].

La "privatizzazione" del controllo dell'attività delle persone e delle loro informazioni, però, non si arresta a simili fattispecie, ma assume un ambito ancor più vasto qualora si consideri che i dati personali assumono un valore vieppiù crescente. Ciò è chiaramente intuibile: il valore dell'informazione è centrale nella società odierna che è definita proprio con tale termine.

---

[14] M. Castells, *Galassia Internet*, cit., p. 172.

[15] V. Zeno-Zencovich, *Il "diritto ad essere informati" quale elemento del rapporto di cittadinanza*, in *Il diritto dell'informazione e dell'informatica*, 2006, 1, p. 2.

[16] A. Di Corinto, T. Tozzi, *Hacktivism. La libertà nelle maglie della rete*, cit., p. 76.

Dall'analisi complessiva delle fattispecie sin qui esposte, dunque, sembra confermarsi ciò che ha affermato Manuel Castells: ossia che più che di un "Grande Fratello" bisogna aver timore di una moltitudine di "piccole sorelle", agenzie di sorveglianza ed elaborazione delle informazioni che memorizzano i dati relativi alle persone ed al loro comportamento e che costituiscono una molteplicità di attori, posti al di fuori delle moderne case di vetro, che giudicano o interpretano le condotte individuali e collettive. Intuitivamente, nei regimi autoritari un'attività di sorveglianza così intensa e frammentata può riverberarsi direttamente sulla vita delle persone[17].

Bisogna però considerare che leggi, tribunali, opinione pubblica, mass media, imprese e agenzie governative sono le aree decisive per il controllo di Internet, poiché, al contrario delle reti globali, le persone che le utilizzano possono essere controllate più o meno facilmente[18].

La presa di coscienza di tale profilo, del resto, era alla base del contestato progetto statunitense denominato "Total Information Awareness" e sviluppato dall'"Information Awareness Office". Lo scopo di tale iniziativa consisteva nello sviluppo di tecnologie informatiche innovative per individuare i gruppi terroristici e le loro attività, ovunque esse si svolgessero[19].

Le numerose polemiche suscitate dall'invasività del suddetto progetto ne hanno decretato l'interruzione in via ufficiale, ma probabilmente la sua struttura composita ha tracciato la strada verso i sistemi di controllo globale che saranno realizzati nel prossimo futuro. Tramite esso, infatti, sarebbe stato possibile un trattamento incrociato ed automatizzato di dati di natura diversa acquisiti in ogni parte del mondo, che avrebbero portato all'identificazione generalizzata e ad una cognizione sempre più completa della vita quotidiana di tutte le persone che vivono nella società odierna.

Probabilmente nel prossimo futuro saranno realizzati sistemi di controllo e di intercettazioni aventi le stesse caratteristiche e la

---

17 M. Castells, *Galassia Internet*, cit., pp. 171-172.

18 Ivi, p. 174.

19 Sull'Information Awareness Office sia consentito rinviare a G. Fioriglio, *La privacy e i sistemi di intercettazione globale: il caso dell'Information Awareness Office*, in *L'ircocervo*, 2003, 1.

stessa invasività del "Total Information Awareness"; il conseguente sacrificio della privacy individuale e collettiva sarà probabilmente "giustificato" dai governanti come il prezzo da pagare per tutelare la sicurezza dei cittadini degli stati che adotteranno simili sistemi.

## 2. *La "Radio Frequency Identification"*

Con l'espressione *Radio Frequency IDentification* si indicano alcune tecnologie, sviluppate a partire dagli anni Settanta ma che trovano origine in studi compiuti sin dal finire degli anni Quaranta, che fanno uso di onde radio al fine di identificare automaticamente persone od oggetti.

La trasmissione in radiofrequenza può essere svolta utilizzando soluzioni che si differenziano per frequenza, potenza del segnale, tecniche di modulazione e protocolli di comunicazione. Nella creazione di sistemi RFID bisogna prendere in considerazione diverse problematiche tecniche; in particolare, le frequenze non devono interferire con altre trasmissioni radio, non devono verificarsi collisioni fra più lettori e fra più *tags*[20], ed inoltre i valori di frequenza e di potenza non possono essere troppo elevati perché altrimenti potrebbero aversi risultati nocivi per la salute dell'uomo[21]. Oltre a questo fondamentale diritto, però, simili tecnologie possono potenzialmente violarne un altro: il diritto alla privacy. Mediante il loro utilizzo, infatti, può essere agevolmente acquisita una notevole quantità di dati, personali e non, di varia tipologia e ciò è conseguenza del loro ampio raggio di utilizzo e della loro duttilità.

---

[20] In particolare, più lettori possono entrare in collisione quando la loro copertura coincide; tale questione può essere risolta adoperando diversi metodi, come la programmazione dei lettori in modo che leggano in tempi diversi nonché la verifica e l'eliminazione di codici duplicati. Nel caso dei *tags*, si pone il problema di evitare che tutti i *tags* trasmettano le proprie informazioni simultaneamente, che può essere risolto mediante la predisposizione di un sequenziamento dei messaggi.

[21] Più specificatamente, le frequenze utilizzate possono essere classificate come: basse frequenze (LF, da 125 e 134 kHz); alte frequenze (HF, circa 15 MHz); altissime frequenze (UHF, da 860 a 960 MHz); micro-onde (oltre 2,45 GHz).

Le tecnologie RFID sono infatti sempre più impiegate, in quanto presentano indubbi vantaggi rispetto a metodi di identificazione tradizionali e concorrenti come, ad esempio, quelli basati sui codici a barre. Le relative tipologie sono, però, assai varie, così come i fini che si possono raggiungere per mezzo della loro adozione; in particolare, esse sono assai efficaci per la sorveglianza (ad esempio, per l'utilizzo nei dispositivi antitaccheggio comunemente apposti su diverse tipologie di beni comunemente in vendita nei negozi) ed il posizionamento (ad esempio, per il tracciamento di animali, oggetti e addirittura persone).

La metodologia di identificazione più utilizzata consiste nel memorizzare un numero di serie che identifica una persona od un oggetto su un chip al quale è connessa un'antenna (l'insieme del chip e dell'antenna è detto "RFID tag" o "RFID transponder"[22]) che consente al primo di trasmettere i dati identificativi ad un lettore (detto anche "RFID transceiver"[23]) deputato a convertire le onde radio ricevute in informazioni digitali che potranno poi essere trattate da sistemi informatici. Intuitivamente, i chip RFID vengono comunemente detti "etichette intelligenti" per via delle loro caratteristiche tecniche, anche se i *tags* RFID possono avere anche altre forme, come quella di *smart card*.

In linea generale, tutti i *tags* dovrebbero essere resistenti ad urti ed agenti esterni, come umidità, polvere, sostanze chimiche. Soprattutto, bisogna tener conto della possibilità di fenomeni di interferenza che potrebbero aversi fra i *tags* ed il lettore, la cui incidenza può non solo limitare il *range* della comunicazione, ma addirittura impedirla.

In particolare, il costo di un *tag* RFID varia in base alle sue potenzialità e si possono distinguere in:

– passivi: non hanno una batteria interna e sono alimentati via radio dal lettore. In particolare, il *chip* presente nel *tag* ottiene la potenza necessaria per effettuare la trasmissione dei dati dal campo elettromagnetico generato dal lettore;

---

[22] Il termine *transponder* deriva dall'unione delle parole *TRANSmitter* e *resPONDER*.

[23] Il termine *transceiver* deriva dall'unione delle parole *TRANSmitter* e *reCEIVER*.

– semi-passivi: sono dotati di una batteria interna, ma non possono trasmettere, per cui fanno uso dell'energia derivante dal fascio di energia inviato dal *transceiver*;

– attivi: hanno una batteria interna e possono iniziare comunicazioni radio. Sono molto più evoluti dei *tag* passivi e semi-passivi ed il loro *range* di trasmissione può arrivare a decine di chilometri.

I *tags* dotati di batteria hanno una durata limitata perché connessa a quella della batteria che li alimenta, al contrario di quelli passivi che hanno una "vita" potenzialmente illimitata ma che ovviamente richiedono la presenza di lettori più potenti.

I *tags*, inoltre, contengono una memoria variabile per quantità e tipologia e in base a ciò vengono distinti in cinque classi[24]:

– classe 0: a sola lettura. I dati ivi inseriti possono essere solamente letti, ma su tale memoria non possono essere effettuate operazioni di scrittura. Solitamente vengono utilizzati quali dispositivi antitaccheggio, finalizzati unicamente a comunicare se un determinato oggetto oltrepassa un certo territorio;

– classe 1: a scrittura unica e lettura multipla. In tali *tags* la scrittura può essere effettuata una sola volta, similmente a quanto avviene nei supporti CD-R e DVD-R;

– classe 2: a lettura e scrittura. La memoria presente in tali *tags* può essere modificata, per cui i *tags* di tale classe vengono utilizzati soprattutto nel caso di prodotti che devono attraversare diverse fasi (ad esempio, produzione, distribuzione e vendita al dettaglio);

– classe 3: a lettura e scrittura con sensore integrato. Essi possono registrare sulla memoria presente nel *tags* i parametri ritenuti utili, come la pressione, l'umidità e la temperatura;

– classe 4: a lettura e scrittura con trasmettitore integrato: essi sono molto evoluti e possono trasmettere dati.

In particolare, i *tags* RFID sono sempre più utilizzati nella logistica al fine di gestire il movimento e l'immagazzinamento delle merci rendendo assai più celeri le operazioni connesse, anche perché non è necessario che ogni singolo oggetto sia visibile all'operatore,

[24] Centro Nazionale per l'Informatica nella Pubblica Amministrazione, *Linee guida per l'impiego di sistemi RFId nella Pubblica Amministrazione*, in *I Quaderni*, 2007, 30, p. 23.

ma piuttosto che ricada nella copertura del lettore. I vantaggi così ottenibili sono numerosi: si pensi, ad esempio, alla maggiore celerità in operazioni come la verifica dell'inventario, che è uno degli aspetti che può interessare non solo soggetti privati, ma anche pubblici (come le biblioteche o, in ambito giuridico, gli uffici giudiziari per la gestione dei fascicoli).

I *tags* RFID vengono utilizzati anche sugli animali, sia per identificarli che per ottenere in maniera assai efficiente schede complete per ciascuno di essi: mediante *tags* di classe 2 è infatti possibile inserire informazioni come le condizioni sanitarie di ciascun animale.

Quando i *tags* vengono adoperati esclusivamente per il tracciamento di prodotti solo all'interno di una catena di distribuzione, le informazioni memorizzate nei *tags* si riferiscono solo ai produttori o ai distributori e dunque non pongono questioni particolari in ordine alla liceità del trattamento di dati ed alla tutela dei soggetti interessati.

Tuttavia, come ha sottolineato la Commissione Europea, «la tecnologia RFID può essere utilizzata per raccogliere informazioni collegate direttamente o indirettamente a una persona, individuabile o identificata, e pertanto da considerarsi dati a carattere personale; le etichette RFID possono contenere dati personali, come sui passaporti o nelle cartelle mediche; la tecnologia RFID potrebbe essere utilizzata per seguire gli spostamenti dei singoli individui o per stabilirne il profilo comportamentale»[25].

Le tipologie di utilizzo delle tecnologie RFID sono assai varie ed in futuro potranno risultare utili nella vita quotidiana. Ad esempio, un frigorifero dotato di lettore RFID potrebbe automaticamente avvertire l'utente qualora determinati alimenti siano scaduti e ciò potrebbe agevolare soprattutto i non vedenti.

Già oggi esse vengono adoperate a fini identificativi quali alternative a metodi tradizionali, come i tesserini di riconoscimento utilizzati nei luoghi di lavoro[26], ed innovativi ma anche più contesta-

---

[25] Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni, *L'identificazione a radiofrequenza (RFID) in Europa: verso un quadro politico*, COM(2007) 96.

[26] In dottrina è stato ritenuto che, qualora i chip RFID siano inseriti su supporti ben identificabili, come i *badges*, e i lettori, ben visibili, siano posizionati

ti, come quelli basati su dati biometrici. Diviene difatti possibile un controllo maggiore di ciò che avviene in una determinata zona sottoposta al raggio d'azione del *transceiver*.

Dall'estrazione di alcuni dati presenti nei *tags* è infatti possibile conoscere il posizionamento degli individui[27], anche se bisogna precisare che ciò può essere altresì la conseguenza dell'utilizzo di dispositivi come i telefoni cellulari (per quanto l'identificazione permessa dai *tags* RFID sia ben più celere, precisa e facile da realizzare). Essi vengono comunemente utilizzati negli *immobilizers* delle automobili nonché come sistemi di pagamento elettronico (si pensi ai sistemi di addebito automatico del pedaggio autostradale, come il ben noto "Telepass").

Un ambito molto delicato è costituito da quello sanitario, nel quale le tecnologie RFID possono essere proficuamente utilizzate in diversi settori. Mediante esse è possibile effettuare, fra l'altro, il tracciamento di protesi sanitarie e di apparati elettromedicali nonché l'identificazione dei pazienti e lo svolgimento di attività di diagnosi, prognosi e terapia.

Più specificatamente, ogni paziente può essere identificato tramite un *tag* RFID (ad esempio, un braccialetto elettronico). La creazione di un sistema basato su tali tecnologie può consentire di automatizzare e perfezionare operazioni come la somministrazione di farmaci: i dati vengono trasmessi dal medico o dal personale infermieristico al competente magazzino nell'ambito della struttura sanitaria, i cui fabbisogni possono così essere gestiti in maniera più efficiente.

---

affinché siano registrati unicamente l'entrata e l'uscita dei lavoratori, rimangano fuori dall'ambito di applicazione dell'art. 4 della legge 20 maggio 1970, n. 300 (il c.d. Statuto dei lavoratori) che impone il divieto di controllo a distanza dei lavoratori mediante impianti audiovisivi ed altre apparecchiature (A. Pradelli, *Nuove tecnologie: privacy e controlli del datore*, in *Diritto & pratica del lavoro*, 2007, 7, p. 476).

[27] La dottrina ha riportato che in Inghilterra alcune grandi imprese hanno imposto a ciascun dipendente di portare al polso un minuscolo computer mediante il quale gli vengono dati ordini e controllati sia i suoi spostamenti che l'intensità della sua attività lavorativa, con una probabile violazione della dignità umana (M. Grauso, *Radio Frequency Identification Technology e tutela della persona*, in *Diritto dell'internet*, 2005, 6, p. 624).

Sinora le tecnologie di RFID non hanno avuto una diffusione ed un'invasività tanto ampie da porre particolari problemi in tema di protezione dei dati personali, ma tale scenario è destinato a mutare assai presto, visto il sempre crescente utilizzo che se ne fa. Più specificatamente, in tutte le diverse fattispecie cui si è fatto sinora riferimento possono verificarsi casi di violazione della privacy della "persona digitale", che può essere tutelata solo qualora vengano poste in essere determinate accortezze.

Le diverse problematiche toccano vari profili dell'essere umano, che potrebbe essere automaticamente scomposto nelle sue distinte qualità di consumatore, cittadino, paziente, automobilista, lavoratore, e così via. Come si è detto, infatti, uno dei grandi vantaggi che le tecnologie RFID recano con loro è la possibilità di identificare un oggetto, un animale o una persona che porti o che contenga un *tag* qualora esso o essa si trovi nel raggio d'azione di un determinato lettore[28].

Le tecnologie RFID potrebbero, però, avere una diffusione simile a quella avuta da Internet qualora ad una diffusa standardizzazione si accompagni un'interconnessione fra sistemi diversi, avvenga essa in tempo reale oppure ad intervalli più o meno regolari. In tal modo potrebbe verificarsi un'acquisizione generalizzata di dati che potrebbero essere in sé anonimi ma il cui trattamento incrociato potrebbe portare a nuovi e più gravosi fenomeni di profilazione e di controllo.

Basti pensare all'acquisto di un bene sul quale è stato apposto un *tag*. Nel caso in cui l'etichetta intelligente non venga disattivata dopo la transazione, potrebbe attivarsi automaticamente qualora entri nella copertura di un lettore posto in un altro luogo. Tale apparecchio potrebbe leggere i *tags* apposti su altri oggetti portati con sé da una persona, che a sua volta potrebbe essere identificata dal lettore medesimo perché, ad esempio, è entrata nel parcheggio

[28] Così sarebbe possibile, ad esempio, utilizzare in movimento lettori RFID per acquisire senza consenso informazioni da più *tag* non solo a fini di polizia (in tal senso, J. Kumagai, S. Cherry, *Sensors & Sensibility*, in *IEEE Spectrum*, 2004, 7, p. 26), ma anche di profilazione commerciale (P.L. Cochran, M.V. Tatikonda, J. Manning Magid, *Radio frequency Identification and the Ethics of Privacy*, in *Organizational Dynamics*, 2007, 2, p. 221).

dell'azienda presso cui lavora. Dal complesso dei dati potenzialmente acquisibili possono così ricavarsi notevoli informazioni su una persona, con particolare riferimento all'ipotesi in cui uno dei *tags* identifichi univocamente una persona.

Difatti, una persona può essere tracciata ma non identificata in un primo momento ed esserlo successivamente, come nel caso in cui un bene oggetto di un acquisto "anonimo" venga poi abbinato a quella stessa persona semplicemente perché questa si trova in seguito nel raggio d'azione di un lettore che, oltre ai dati relativi a quel *tag*, acquisisce anche quelli di un *tag* identificativo univoco. Le informazioni possono dunque passare da una "costellazione" ad un'altra[29] e cagionare in tal modo la perdita del controllo sui propri dati personali.

Si badi: anche un semplice acquisto di libri, dvd video o compact disc musicali può portare a rivelare informazioni tanto personali e delicate su un essere umano da costituire dati sensibili ai sensi del cod. priv. poiché dall'analisi complessiva degli acquisti possono essere rilevate le convinzioni religiose o filosofiche, le opinioni politiche nonché il proprio stato di salute o le proprie preferenze sessuali. I dati relativi ad ogni transazione, inoltre, potrebbero essere aggregati a quelli risultanti dal tracciamento delle preferenze di ciascun cliente risultante dalle carte di fidelizzazione.

Le tutele approntate nei singoli ambiti nazionali, però, non sembrano sufficienti a garantire la privacy in una società caratterizzata dal fenomeno della globalizzazione[30], cui si accompagna la ramificazione di molti soggetti (comprese aziende e organizzazioni non governative) presenti in numerosi stati, per cui la possibilità che vengano creati enormi *database* di individui e di gruppi sociali non appare remota.

---

[29] Così S.L. Garfinkel, A. Juels. R. Pappu, *RFID Privacy: An Overview of Problems and Proposed Solutions*, in *IEEE Security and Privacy*, 2005, 3, p. 38.

[30] In argomento cfr., *ex multis*, M. D'Alberti, *Poteri pubblici, mercati e globalizzazione*, Il Mulino, Bologna, 2008; M.R. Ferrarese, *Diritto sconfinato. Inventiva giuridica e spazi nel mondo globale*, Laterza, Roma-Bari, 2006; M.R. Ferrarese, *Le istituzioni della globalizzazione. Diritto e diritti nella società transnazionale*, Il Mulino, Bologna, 2000; F. Galgano, *La globalizzazione nello specchio del diritto*, Il Mulino, Bologna, 2005; D. Zolo, *Globalizzazione*, in *Digesto delle discipline pubblicistiche*, Aggiornamento, Utet, Torino, 2005, pp. 378-398.

Inoltre, come qualsiasi tecnologia, anche l'RFID pone problemi di sicurezza. È stato ad esempio dimostrato che alcuni *trasponders* presenti in dispositivi *immobilizers* presenti in milioni di autovetture ed in un sistema di pagamento elettronico denominato "Speedpass" possono essere violati in maniera relativamente semplice ed essere clonati[31]. Ciò può portare, com'è ovvio, al compimento di furti d'identità e di frodi finanziarie, e dunque alla violazione della confidenzialità dei dati finanziari.

Oltre a ciò, i dispositivi RFID possono porre problemi di sicurezza informatica, dal momento che molti lettori RFID sono connessi a sistemi informatici e dunque possono costituire una porta di ingresso che potrebbe essere aperta da eventuali criminali informatici in grado di sfruttare le vulnerabilità delle suddette tecnologie.

Simili eventi non dovrebbero accadere: per aumentare la generalizzata accettazione di tali tecnologie sarebbe necessario promuovere ed implementare misure di sicurezza efficaci, rendendo chiari i loro pregi e difetti ai consumatori[32], che possono percepire i *tags* RFID come potenzialmente lesivi della loro privacy[33] o, addirittura, idonei ad agevolare furti o rapine qualora eventuali malintenzionati utilizzino lettori RFID per valutare se le potenziali vittime abbiano con sé, nella propria automobile o nel proprio domicilio oggetti di valore[34].

In linea teorica e generale il livello di sicurezza informatica da garantire dovrebbe essere proporzionale all'interesse tutelato, per cui, ad esempio, le tecnologie RFID utilizzate in ambito sanitario dovrebbero essere sempre allo stato dell'arte per evitare che venga-

---

[31] Cfr. S. Bono *et al.*, *Security Analysis of a Cryptographically-Enabled RFID Device*, in *Proceedings of the 14th Usenix Security Symposium*, 2005, pp. 1-16 (http://www.usenix.org/events/sec05/tech/bono.html).

[32] In tal senso M. Ohkubo, K. Suzuki, S. Kinoshita, *RFID Privacy Issues and Technical Challenges*, in *Communications of the ACM*, 2005, 9, p. 68.

[33] Questa percezione risulta, fra l'altro, da uno studio compiuto in Germania, ove è emerso che i benefici derivanti dall'utilizzo di tali *tag* in ambito commerciali non sembrano sufficienti a giustificare i rischi di potenziale lesione del diritto alla riservatezza (cfr. O. Günther, S. Spiekerman, *RFID and the Perception of Control: The Consumer's View*, in *Communications of ACM*, 2005, 9, pp. 73-76).

[34] In tal senso F. Stajano, *RFID Is X-Ray Vision*, in *Communications of the ACM*, 2005, 9, p. 32.

no illecitamente trattati dati sensibili come quelli relativi allo stato di salute.

La "società sorvegliata", nella quale l'acquisizione dei dati può avvenire automaticamente purché ricorra una prossimità spaziale fra l'interessato ed il lettore, potrebbe dunque essere la prossima evoluzione della Società dell'informazione qualora non venga assicurata una tutela effettiva dell'individuo e delle collettività dall'invasività di tecnologie certamente utili ma anche potenzialmente assai pericolose.

Tali profili sono stati presi in considerazione nella creazione di alcuni standard *in subiecta materia* ed una delle soluzioni generalmente utilizzabili consiste nella disattivazione dei *tags* che può essere effettuata o mediante la loro rimozione oppure mediante un apposito comando (come *kill*). Tuttavia, simili soluzioni possono limitare alcuni benefici delle tecnologie RFID; ad esempio, potrebbero eliminare il beneficio di rendere più efficiente la catena distributiva di un prodotto qualora esso presenti difetti e venga restituito dall'utente finale, o, in linea generale, annullare quei vantaggi connessi alla presenza di un *tag* RFID su un determinato bene[35].

È possibile, inoltre, utilizzare i c.d. *blocker tags*, che impediscono la lettura di altri *tags* senza però disattivarli in via permanente come nell'ipotesi del *killing*. In tal modo è possibile preservare l'utilità futura dei *tags* rispettando la privacy ed evitando comunicazioni indesiderate. Ciò però presuppone che il lettore non cerchi di violare il blocco leggendo comunque il *tag*.

La complessità delle questioni sottese alle tecnologie RFID, con particolare riferimento alle potenzialità lesive della privacy, impone, dunque, un'attenta riflessione ed una presa di coscienza dei vari legislatori affinché venga delineato un quadro uniforme improntato ad un corretto bilanciamento di interessi fra le esigenze del mercato e quelle delle persone. In merito è di particolare interesse la "carta dei diritti" proposta da Simson Garfinkel, secondo il quale i consumatori dovrebbero avere i seguenti diritti:

---

[35] Basti pensare all'esempio dei *tag* RFID presenti negli alimenti, cui si è fatto riferimento in precedenza nel testo, che non potrebbero dunque "segnalare" l'avvenuta scadenza.

– sapere se un prodotto contiene *tags* RFID;
– rimuovere o disattivare il *tag* al momento dell'acquisto;
– utilizzare servizi abilitati all'RFID anche senza *tag*;
– accedere ai dati presenti nel *tag*;
– sapere quando, come e perché i *tags* sono letti[36].

Bisogna rilevare che, anche in assenza di previsioni specifiche, sia la normativa comunitaria che quella italiana in tema di protezione dei dati personali sono potenzialmente idonee a limitare o a bloccare gli eventuali profili di rischio delle tecnologie RFID. In tal senso è anche il Gruppo di lavoro sulla protezione dei dati personali istituito dall'art. 29 della direttiva n. 95/46/CE, il quale nel *Working document on data protection issues related to RFID technology* ha affermato che sono ipotizzabili scenari di utilizzo di tecnologie RFID cui consegua l'acquisizione di dati personali e che, in tali casi, troverà applicazione la normativa vigente[37].

Del resto, un aspetto fondamentale sia della direttiva n. 95/46/CE che del cod. priv. consiste nella duttilità della definizione di dato personale e degli strumenti a sua difesa.

Nell'applicazione delle normative in materia, però, assumono un importante ruolo di guida le *authorities* istituite in numerosi paesi. In Italia il Garante per la protezione dei dati personali è intervenuto con un provvedimento a carattere generale, adottato il 9 marzo 2005, con il quale ha indicato le misure necessarie od opportune per rendere conforme alla normativa vigente il trattamento di dati personali effettuato avvalendosi di tecnologie RFID. Tali prescrizioni si applicano ai casi in cui, per effetto dell'impiego di sistemi RFID, si trattino dati personali relativi a terzi identificati o identificabili (art. 4, comma 1, lett. B, cod. priv.); non operano invece nei casi – che non pongono particolari problemi sul piano della protezione dei dati – in cui l'utilizzo dei suddetti sistemi non comporti un simile trattamento e sia utilizzata, ad esempio, in una catena di distribuzione aziendale al solo fine di garantire una maggiore efficienza del processo di produzione.

---

[36] S.L. Garfinkel, *An RFID Bill of Rights*, in *Technology Review*, 2002, http://www.technologyreview.com/Infotech/12953.

[37] Documento n. 10107/05/En, WP 105.

Il Garante ha sottolineato che vi sono diversi casi in cui l'utilizzo di sistemi basati sulle suddette tecnologie può comportare il trattamento di dati personali relativi a terzi, persone fisiche o giuridiche, enti o associazioni, considerando, oltretutto, che i *tags* potrebbero contenere dati personali od essere utilizzati in modo tale da rendere comunque identificabili gli interessati attraverso il confronto con altre informazioni.

Il Garante ha ribadito la necessità di rispettare, in modo rigoroso, tutti i principi dettati dal cod. priv., facendo espresso riferimento a quelle norme che costituiscono la struttura della normativa sulla protezione dei dati personali. Ha sottolineato, in particolare, che, in ottemperanza al principio di necessità, bisogna evitare di utilizzare dati personali o di identificare gli interessati, salvo che non sia strettamente necessario in relazione alla finalità perseguita, e che, nel rispetto del principio di proporzionalità, «non risulta di regola giustificato il trattamento che comporti il funzionamento delle etichette apposte su prodotti acquistati dall'interessato anche fuori dell'esercizio commerciale, a meno che ciò sia necessario per fornire un servizio specificamente e liberamente richiesto dall'interessato stesso».

Inoltre, sul titolare del trattamento grava l'obbligo di rendere un'articolata informativa all'interessato, che deve contenere degli elementi specifici alle tecnologie RFID. In particolare, bisogna segnalare la presenza di *tags* RFID e la possibilità che tramite essi siano acquisiti dati personali, anche mediante lettori che possano attivare le medesime etichette intelligenti. È necessario, altresì, indicare quali siano le modalità per asportare o disattivare i *tags* o per interromperne il funzionamento. L'informativa può essere resa anche mediante avvisi chiaramente visibili, ma qualora i *tags* rimangano attivi dopo che è stato reso possibile associarli con dati relativi a terzi identificati o identificabili essa deve essere apposta sugli oggetti o sui prodotti che li recano.

All'informativa deve poi seguire il consenso secondo le regole ordinarie. Ad esempio, esso non è necessario qualora le tecniche di RFID siano adoperate, in esercizi commerciali, nell'ambito delle modalità di pagamento, ed i prodotti non siano riconducibili ad acquirenti identificati o identificabili. Il consenso è invece neces-

sario qualora i *tags* rimangano attivi «anche oltre la barriera-cassa dell'esercizio commerciale in cui sono utilizzate». In ogni caso, però, l'interessato ha il diritto di ottenere, gratuitamente e in maniera agevole, la rimozione o la disattivazione dei *tags* RFID al momento dell'acquisto del prodotto su cui è apposto o al termine dell'utilizzo del dispositivo.

Il Garante ha poi affermato l'illiceità, in linea generale, degli impianti sottocutanei di microchip perché contrastanti con il principio di dignità di cui all'art. 2 cod. priv., per cui essi possono essere utilizzati solo in casi eccezionali «per comprovate e giustificate esigenze a tutela della salute delle persone», rispettando il principio di proporzionalità di cui all'art. 11 cod. priv. nonché la dignità dell'interessato, il quale dovrebbe poter essere in grado di ottenere la rimozione del microchip e l'interruzione del relativo trattamento dei dati che lo riguardano senza oneri ed in qualsiasi momento. Oltretutto, sui titolari del trattamento grava l'obbligo di predisporre modalità di impianto e di impiego dei chip sottocutanei in modo da garantire la riservatezza circa la loro presenza nel corpo dell'interessato[38].

Com'è noto, poi, i trattamenti di dati sensibili devono essere preventivamente autorizzati dal Garante in alcuni casi. Non bisogna, del resto, dimenticare che anche nel caso di impiego di sistemi che implementano tecnologie di RFID trovano applicazione le norme che limitano particolari tipologie di trattamento di dati personali.

Ad esempio, nel caso in cui i *tags* siano collegati a sistemi informativi che possono permettere di individuare la posizione geografica di chi detiene il *tag* o il bene su cui esso è apposto, trova applicazione quella parte del cod. priv. che prevede l'obbligo, per il titolare, di notificare al Garante i trattamenti relativi a dati che indicano la posizione geografica di persone od oggetti mediante una rete di comunicazione elettronica (art. 37, comma 1, lett. a, cod. priv.) effettuati con l'ausilio di strumenti elettronici volti a definire il profilo o

[38] Del resto, la presenza sottocutanea dei chip toglie all'individuo la possibilità di avere un controllo diretto sul dispositivo e sul flusso informativo che viene trasmesso (in tal senso A. Masters, K. Michael, *Lend me your arms: the use and implications of humancentric RFID*, in *Electronic Commerce Research and Applications*, 2007, 6, p. 36).

la personalità dell'interessato, o ad analizzarne abitudini e scelte in ordine ai prodotti acquistati (art. 37, comma 1, lett. d, cod. priv.).

## 3. *La biometria*

L'aggravarsi di fenomeni di criminalità e terrorismo hanno portato ad un mutamento della linea di frontiera tra la protezione della privacy e l'agilità investigativa, che va progressivamente trasformandosi in una linea di frontiera fra la tutela di un diritto che viene percepito o fatto percepire come di "lusso", ossia quello alla riservatezza, e la tutela di un diritto essenziale, ossia alla protezione della società. Si arriva, così, a teorizzare il potenziale conflitto fra la tutela dell'individuo e la tutela della collettività[39], anche se bisogna aggiungere che la privacy assume talvolta una valenza collettiva, come nel caso dei dati genetici che possono essere riferiti non solo ad un individuo singolo, ma anche alla sua "famiglia genetica".

La crescente insicurezza della società moderna ed il diffuso timore di attacchi terroristici hanno così portato ad un utilizzo sempre maggiore di tecnologie biometriche, anche sacrificando la riservatezza individuale e collettiva, al fine di controllare la popolazione ed eventualmente identificare i terroristi o coloro che sono sospettati di essere tali.

In linea generale, tali tecnologie consentono l'identificazione automatica della persone mediante l'analisi di caratteristiche fisiche o comportamentali. Più specificatamente, quelle fisiche sono correlate a specifiche parti del corpo: impronte digitali, iride, mani, denti, ecc.; quelle comportamentali si riferiscono a caratteristiche strettamente individuali come la firma, la voce, l'andatura, ecc.

I sistemi sopra citati, dunque, si distinguono dai tradizionali mezzi di identificazione. Oggi una persona può essere identificata, oltre che per conoscenza diretta, anche attraverso i c.d. *tokens*, che si distinguono in *knowledge tokens* (come password, PIN, dati personali) e in *physical tokens* (come carte d'identità, patenti di guida,

[39] M.G. Losano, *La "giuscibernetica" dopo quattro decenni*, in *Il diritto dell'informazione e dell'informatica*, 4-5, 2005, p. 741.

passaporti). Nel caso in cui uno di essi sia compromesso, è possibile revocarlo, modificarlo oppure ricrearlo, ma se i dati biometrici sono compromessi la situazione è irreversibile. È d'uopo sottolineare, comunque, che alcuni dati biometrici non possono essere persi e che altri lo sono con frequenza trascurabile (come nel caso della perdita delle dita di una mano o di un occhio); inoltre essi non possono essere dimenticati, come invece può avvenire nel caso dei *knowledge tokens*. Pertanto, un sistema misto, ossia basato sia su *tokens* che su dati biometrici, può garantire elevati di sicurezza.

Più specificatamente, i sistemi biometrici vengono utilizzati a fini identificativi, per stabilire se l'identità di un soggetto sia effettivamente quella che esso afferma (valenza positiva) oppure per verificare se esso effettivamente non sia chi dice di non essere (valenza negativa). Nel primo caso il sistema verifica se i dati del soggetto corrispondono a quelli memorizzati sotto quel nome e dunque in tal modo non possono verificarsi furti d'identità poiché ad ogni persona corrisponde un'identità univoca. Nel secondo i dati del soggetto sono confrontati con quelli presenti nel *database*.

La diffusione di tali sistemi, però, fa sì che il corpo umano divenga sempre più una *password.* Al posto delle parole chiave si utilizzano dati relativi alla componente fisica delle persone, cui si ricorre sempre più frequentemente non solo per identificare un individuo al fine di garantire l'accesso sicuro a diversi servizi, «ma anche come elementi per classificazioni permanenti, per controlli ulteriori rispetto al momento dell'identificazione o dell'autenticazione/verifica, cioè della conferma di una identità»[40]: le misure di polizia così possono risultare accresciute, «con una progressione in cui anche la mente può essere catturata dalla invasione strisciante delle tecnologie del controllo nella vita quotidiana»[41].

La concreta operatività di un sistema biometrico richiede lo svolgimento di determinate fasi, la prima delle quali è costituita dalla registrazione (o *enrollment*). Essa consiste nell'acquisizione, svolta mediante un apposito dispositivo, di una caratteristica fisica o

---

[40] S. Rodotà, *Trasformazioni del corpo*, in *Politica del diritto*, 2006, 1, pp. 6-7.

[41] Ivi, p. 5.

comportamentale dell'utente; il sistema elabora i dati così acquisiti ed estrae le informazioni ritenute distintive, creando così il c.d. campione (o *sample* o *template*), che viene poi archiviato su un supporto di memorizzazione o all'interno di un *database*.

Tale fase assume un ruolo centrale nella costruzione di un sistema biometrico efficiente ed affidabile. Bisogna però considerare che nell'acquisizione dei dati entrano in gioco anche fattori ambientali, oltre, ovviamente, alla precisione stessa del sistema nella registrazione dei dati, che possono influenzare i risultati. Possono dunque aversi uno o più *false match* (anche detto *false accept*) oppure uno o più *false non-match* (*false reject*)[42] e il punto in cui si verifica l'intersezione fra essi è detto *equal error rate* oppure *crossover point*.

Successivamente, il sistema, quando viene interrogato, effettua una comparazione fra un campione estratto successivamente e quello presente nel *database*.

A questo punto, appare utile richiamare brevemente le diverse caratteristiche fisiche e comportamentali comunemente utilizzate nei sistemi biometrici al fine di poterne valutare in modo più approfondito le caratteristiche:

– *impronte digitali*: com'è noto, esse sono ampiamente utilizzate da molto tempo, soprattutto in ambito investigativo mediante l'analisi dei dati risultanti dalle scene dei crimini. In tali casi, come in un sistema biometrico, viene effettuata la comparazione fra il campione estratto sul luogo del delitto con quello presente in un *database* o estratto da un sospettato. Ovviamente l'acquisizione dei dati richiede il preventivo consenso del soggetto, anche se è possibile realizzare sensori che memorizzino in modo surrettizio le impronte digitali, per cui in tali casi si può porre il problema dell'illecita acquisizione di dati personali. Esse consentono di riconoscere un soggetto con un margine di errore molto basso, ma possono essere facilmente danneggiate (ad esempio, in seguito a lesioni oppure agenti chimici);

– *geometria della mano*: mediante tale tecnica la mano viene posta su una superficie ove essa viene ripresa da una fotocamera digitale che ne elabora i punti salienti. Per quanto ciascuna mano sia

[42] S. Prabhakar, S. Pankanti, A.K. Jain, *Biometric Recognition: Security and Privacy Concerns*, in *IEEE Security & Privacy*, 2003, 2, pp. 34-35.

abbastanza complessa perché costituita da ossa e muscoli, tendini e giunture, essa non è generalmente considerata abbastanza unica da consentire una identificazione certa del soggetto di riferimento. Inoltre, la forma della mano normalmente varia non solo in seguito ad eventi traumatici, ma anche in seguito all'età o al dimagrimento. Pertanto, tale metodo può essere affiancato ad altri per garantire migliori risultati e non pone particolari problemi in ordine al momento acquisitivo dei dati, poiché attualmente è di fatto impossibile che una persona non si renda conto di essere sottoposta ad un'operazione di riconoscimento di geometria della mano, visto che essa richiede la sua collaborazione;

– *scansione della retina e dell'iride*: entrambe le tecniche sono basate sull'acquisizione di dati relativi all'occhio umano ed offrono ottimi risultati. Più specificatamente, la prima è più invasiva e richiede che il soggetto focalizzi la propria vista su un determinato punto di un reticolo che gli viene fatto osservare; la seconda viene realizzata mediante uno scanner a raggi infrarossi che scansiona l'iride da una distanza solitamente variabile da 7 a 25 cm. Nel primo caso, dunque, è realmente difficile riuscire a carpire i dati biometrici relativi alla retina di un soggetto senza il suo consenso, mentre nel secondo ciò potrebbe essere fatto anche a sua insaputa;

– *geometria del volto*: tale tecnica può consentire un controllo globale generalizzato, poiché mediante l'utilizzo di telecamere di alta qualità e in presenza di condizioni di illuminazione favorevoli è possibile effettuare un riconoscimento automatizzato dei tratti facciali di un soggetto anche a distanze più o meno lunghe e senza il suo consenso. L'ampia diffusione dei sistemi di videosorveglianza nei moderni centri urbani, la cui pervasiva presenza potrebbe essere ritenuta addirittura desiderabile da alcuni, può portare nel prossimo futuro alla creazione di sistemi di controllo globale che possono tracciare il movimento delle persone;

– *riconoscimento della voce*: tale tecnica è la più applicata in sottoinsiemi specializzati. Le variabili di cui deve tener conto un sistema di riconoscimento vocale sono numerose e sono relative sia alla voce in sé e per sé (perché variabile in base alle condizioni di salute e all'età) che a fattori esterni, come il rumore di fondo, la cui eliminazione richiede sofisticate operazioni che permettono di isolare

unicamente la voce dagli altri rumori. Qualora siano creati sistemi in grado di riconoscere ed attribuire la voce ad un determinato individuo senza margini considerevoli di errore, potrebbero porsi problemi di privacy e di furto di identità, poiché già oggi è assai semplice acquisire e riprodurre suoni;

– *firma*: la firma autografa è tradizionalmente usata come strumento per riferire un documento cartaceo al sottoscrittore, in quanto la calligrafia è un elemento distintivo della persona. Mediante perizie calligrafiche è possibile essere ragionevolmente sicuri che una determinata firma sia stata apposta da una certa persona. La firma può però essere utilizzata anche in un sistema biometrico, ma ciò può comportare problemi assai delicati qualora essa sia acquisita illecitamente (anche mediante stratagemmi) oppure se di essa siano fatti utilizzi illeciti successivamente alla sua memorizzazione;

– *battitura*: mediante l'analisi del ritmo con cui viene svolta la battitura del testo su una tastiera è possibile identificare il soggetto che la sta utilizzando, ma il margine di errore presente nelle tecnologie attuali non consente di fornire risultati univoci, per cui può più che altro essere utilizzata per confermare l'identità di una persona.

I sistemi biometrici, dunque, possono essere distinti in base alla tipologia di informazioni sulla quale operano. Come ha sottolineato Stefano Rodotà, non v'è dubbio che il loro utilizzo possa offrire a tutti nuove forme di sicurezza nonché semplificazioni delle attività quotidiane. Mediante essi può aumentare il numero di identificazioni certe e, quindi, è estremamente più difficile effettuare sostituzioni o duplicazioni della persona. Non basta, tuttavia, fermarsi a queste considerazioni, poiché vanno considerate analiticamente «le diverse specie di dati biometrici, le finalità per le quali possono essere utilizzati, le modalità delle loro utilizzazioni»[43].

In linea teorica, del resto, potrebbe sostenersi che i sistemi biometrici non solo non violano la privacy, ma addirittura la tutelano, poiché evitano, o dovrebbero evitare, il verificarsi di casi di furto di identità. Inoltre, le problematiche principali potrebbero essere viste unicamente in connessione allo specifico profilo della protezione del

[43] S. Rodotà, *Trasformazioni del corpo*, cit., pp. 12-13.

database, che in tal senso non sarebbe più pericoloso di altri *database* che contengono dati sensibili.

La questione, però, non è così semplice, poiché i sistemi biometrici pongono problematiche assai delicate, che ineriscono sia alle modalità di acquisizione dei dati che alle successive fasi di trattamento degli stessi e che possono essere fonte di violazioni, anche irreparabili, del diritto alla riservatezza, nonché di potenziali discriminazioni verso determinate categorie di persone che presentano disabilità e dunque impossibilità di utilizzare tali sistemi[44].

Già nella fase di acquisizione della conoscenza, infatti, non sempre le informazioni biometriche vengono fornite volontariamente e con coscienza dal soggetto cui esse si riferiscono. Come si è visto, talvolta esse possono essere facilmente carpite: basti pensare alle impronte digitali o ai tratti del volto. In tal senso, il prevedibile progresso tecnologico consentirà di acquisire dati in modo non solo più veloce, ma anche meno percepibile dagli interessati. Anche una eventuale condotta prudente da parte di ciascuna persona potrebbe non essere sufficiente ad evitare di lasciare involontariamente informazioni che potrebbero poi essere acquisite ed utilizzate illecitamente da soggetti terzi grazie a tecnologie sempre più invasive e pervasive, la cui diffusione, anche se evidente, potrebbe essere metabolizzata e dunque non far scattare alcun campanello d'allarme: basti pensare, come si è accennato, all'enorme numero di sistemi di videosorveglianza oggi attivi in tutte le città anche di modeste dimensioni.

Una volta avvenuta l'acquisizione dei dati biometrici, comunque, bisogna garantire livelli di sicurezza allo stato dell'arte, poiché tali dati, essendo inerenti alle caratteristiche fisiche di una persona, nascono e muoiono con essa e sono, in linea di massima, non modificabili. Pertanto, bisogna proteggere e tenere sempre aggiornati i *database*, sia dal punto di vista della sicurezza dei sistemi che delle informazioni contenute. Non sembra, del resto, sostenibile la tesi

[44] «There are some identifiable groups of people, members of which are more likely to be disadvantaged than others, and the risk is that they will be excluded from participation in society, in some cases, more than they currently are» (J. Wickins, *The ethics of biometrics: the risk of social exclusion from the widespread use of electronic identification*, in *Science and Engineering Ethics*, 2007, 1, p. 50).

secondo cui non ci sarebbero rischi ulteriori rispetto ai metodi tradizionali di identificazione basati sui *physical tokens*[45], proprio perché i dati biometrici sono relativi a caratteristiche connaturate intimamente ad una persona.

La problematica della sicurezza dei sistemi biometrici va osservata anche nella prospettiva estrinseca al sistema sia qualora esso sia collegato ad altri sia nell'ipotesi opposta.

Nel primo caso i dati possono essere raccolti in un luogo ma archiviati o trattati in un altro, per cui bisogna adottare tutte le cautele necessarie per garantire la riservatezza delle comunicazioni. Le conseguenze di un'eventuale intercettazione, infatti, potrebbero essere assai gravi, poiché, come si è visto, i dati biometrici si riferiscono a fattispecie che di norma non mutano. Una volta che le informazioni sono state acquisite da un terzo soggetto esse possono essere copiate e, in quanto rese in formato digitale, risultano indistinguibili dalle originali. Soprattutto, il controllo dei dati personali di un individuo può risultare perso per sempre, similmente a quanto avviene alle informazioni diffuse su Internet, ed essi possono essere utilizzati a fini illeciti, come accade nei casi di furto d'identità. Pertanto, anche un sistema sicuro in sé e per sé può in realtà non esserlo se viene considerato nell'ambito dell'interconnessione fra più sistemi.

Anche nella seconda ipotesi, ossia qualora il *database* sia interno al sistema e non sia connesso a reti telematiche, interne o esterne, bisogna adottare misure che consentano di tutelare la segretezza delle informazioni ivi memorizzate. Invero, sembra più probabile che, soprattutto nel prossimo futuro, saranno sempre più diffusi i *database* centralizzati accessibili da diversi sistemi.

Bisogna tuttavia considerare che la standardizzazione dei sistemi e dei formati dei dati potrebbe creare seri problemi, poiché potrebbe agevolare la loro condivisione in più *database* e dunque consentire attività di profilazione sempre più evolute e potenzialmente pericolose per la riservatezza individuale e collettiva. Difatti, le informazioni biometriche, più di altre, potrebbero essere utilizzate a detto fine, facendo corrispondere il comportamento di alcune persone con quello di categorie ben definite. Inoltre, qualora i dati biome-

[45] M. Faundez-Zanuy, *Privacy Issues on Biometric Systems*, in *IEEE Aerospace & Electronic Systems Magazine*, 2005, 2, p. 15.

trici vengano usati come indizi o come prove nei procedimenti penali e civili, potrebbero non essere compresi in maniera sufficiente dall'autorità giudiziaria investita del caso visto l'alto tecnicismo della materia, per cui i consulenti tecnici avrebbero un ruolo ancor più importante nell'ambito di ciascun procedimento.

Queste considerazioni rendono palese l'importanza di garantire la massima certezza sia nell'acquisizione dei dati che nelle successive operazioni di trattamento: può infatti capitare che i dati di un soggetto siano erroneamente attribuiti ad un altro oppure che i dati non siano attribuiti ad alcuno.

Pertanto, i rischi e le problematiche esposti dovrebbero essere bilanciati da ovvi benefici derivanti dall'utilizzo delle tecnologie biometriche, dal momento che alla loro implementazione pratica consegue un sicuro aumento della sorveglianza e del controllo sulle persone, senza tuttavia che sia certo o dimostrato un aumento della protezione da eventi criminosi come gli attacchi terroristici. Inoltre, è possibile prevedere che con l'evoluzione di tali tecnologie nessuno potrà sfuggire ad un monitoraggio costante e globale di quanto avviene in un determinato territorio[46], similmente a quanto ipotizzato da George Orwell nel suo celebre *1984*[47].

Conseguenza di ciò è che l'unione di tecnologie di controllo sia nel mondo "materiale" che in quello "virtuale" non lascerà alla persona non solo alcun controllo sui propri dati personali, ma addirittura nessun ambito nel quale rimanere sola.

Giustamente è stato notato che «il ricorso massiccio alle soluzioni basate sulla biometria può essere presentato e percepito come una panacea tecnologica, sì che l'opinione pubblica tende a sopravvalutare la sua accuratezza, associando impropriamente tali tecnologie con una protezione assoluta contro il terrorismo»[48].

Di certo non dovrebbero essere demonizzati i sistemi tecnologici che utilizzano dati biometrici, perché tramite essi potrebbero essere ottenuti vantaggi consistenti in ambiti e problematiche sempre più centrali nella Società dell'informazione, come, ad esempio, in ordine alla garanzia di certezza e di sicurezza nell'identificazione

---

46 L. Lessig, *Code version 2.0*, Basic Books, New York, 2006, p. 208.
47 G. Orwell, *1984*, Mondadori, Milano, 1989.
48 S. Rodotà, *Trasformazioni del corpo*, cit., p. 14.

di una persona. Non ci si può, tuttavia, affidare ciecamente a tali sistemi, dei quali bisogna sempre accertare sia l'accuratezza che l'uso che ne viene fatto, predisponendo le necessarie cautele nel caso in cui si verifichino eventi che portano alla cessazione dei relativi trattamenti di dati personali al fine di evitare consistenti violazioni del diritto alla riservatezza che potrebbero rendere per sempre inutilizzabili determinate informazioni riferibili ad un determinato individuo. Bisogna dunque garantire la sicurezza dei sistemi biometrici e la certezza delle informazioni da essi trattate, il tutto nel rispetto dei principi fondamentali di tutela della dignità della persona.

## 4. *Il "Digital Rights Management"*

Il legislatore ha iniziato a regolamentare e tutelare il diritto d'autore quando Internet era ancora ben lontana dal divenire realtà e quando non si pensava assolutamente alla possibilità di digitalizzare le informazioni, rendendone superflua la distribuzione mediante supporti materiali. Sorge dunque un conflitto fra la posizione monopolista dell'autore e le esigenze di libera circolazione dell'informazione. «Una società basata sulla diffusione globale della cultura e del sapere rende infatti sempre più importante il diritto dell'autore delle informazioni, e sempre più profittevole economicamente lo sfruttamento delle opere dell'ingegno; d'altro canto, rende la posizione di tipo monopolista dell'autore sempre più precaria e sempre più contestata, in quanto blocca la diffusione delle informazioni e ne impedisce l'accesso globale»[49].

Proprio il *boom* di Internet e la facilità di circolazione di qualsiasi tipo di dato hanno messo in crisi il diritto d'autore, in particolar modo con riferimento ai sempre più diffusi fenomeni di pirateria soprattutto in ambito discografico e cinematografico, per cui negli ultimi anni sia gli ordinamenti nazionali che le organizzazioni internazionali hanno emanato numerose disposizioni al fine di tutelare

[49] S. Nespor, *Internet e la legge. Come orientarsi negli aspetti giuridici della rete*, Hoepli, Milano, 1999, p. 127.

gli enormi interessi coinvolti, con un frenetico susseguirsi di disposizioni che hanno reso assai confusionario il quadro normativo.

In tale ambito assumono un particolare rilievo i sistemi di *Digital Rights Management* (DRM), che consentono ai titolari di diritti d'autore di distribuire contenuti digitali di qualsiasi tipo in maniera sicura attraverso tecnologie informatiche al fine di impedirne eventuali utilizzi illeciti. Essi vengono normalmente utilizzati nel settore dell'intrattenimento e del *software*, per cui su molti cd audio, film su dvd o programmi per elaboratore sono presenti simili sistemi.

In Italia, come si è accennato, il quadro giuridico in materia trova il riferimento principale nella legge sul diritto d'autore (la legge 22 aprile 1941, n. 633). Essa è stata fortemente modificata negli anni, sia per iniziativa autonoma del legislatore italiano che per recepire norme sovranazionali[50]. Il risultato è una normativa confusa, che pone numerosi problemi interpretativi, come nel caso dei DRM, nel cui ambito oltretutto si registra un notevole squilibrio a favore dei titolari dei diritti d'autore[51].

La legge italiana permette ai titolari di diritti d'autore e di diritti connessi di apporre sulle opere dell'ingegno (brani musicali, film, *software*, ecc.) misure tecnologiche di protezione efficaci. Esse consistono in componenti che, nel normale corso del loro funzionamento, sono destinati a impedire o limitare atti non autorizzati dal titolare dei diritti. Grazie alle suddette misure è così possibile, ad esem-

---

[50] Già con riferimento alla legge 29 dicembre 1991, n. 518, sulla tutela dei programmi informatici, Vittorio Frosini scriveva che essa «consiste in un tentativo di adattamento alle nuove condizioni tecnologiche ed alle nuove esigenze sociali della legge sul diritto di autore del 22 aprile 1941, n. 633. Invece di emanare una nuova legge organica, si è infilato nel vecchio sacco, che contiene la normativa creata per proteggere i romanzi di D'Annunzio e di Pirandello, ed assicurare ai discendenti i diritti di autore per un congruo numero di anni, una merce completamente diversa, di rapida obsolescenza e di difficile controllo, come è quella dei programmi informatici» (V. Frosini, *I giuristi e la società dell'informazione*, in *Il diritto dell'informazione e dell'informatica*, 1996, 1, p. 18).

[51] «Nella preoccupazione di molte e autorevoli voci il DRM diviene l'emblema di quella tendenza normativa che – anche in spregio a principi giuridici fondamentali, quali la libertà di manifestazione del pensiero – comprime in misura inaccettabile i diritti degli utenti di contenuti digitali, al fine di ridurre Internet ad un gigantesco jukebox multimediale» (R. Caso, *Digital rights management. Il commercio delle informazioni digitali tra contratto e diritto d'autore*, Cedam, Padova, 2004, p. 11).

pio, che un brano musicale possa essere riprodotto solo su determinati sistemi, che non possa essere masterizzato su un compact disc, che possa essere ascoltato solo per un certo numero di volte o per un tempo determinato, e così via.

Tali sistemi sono sempre più diffusi e sono talvolta utilizzati con cognizione di causa, ma capita anche che l'apposizione delle misure tecnologiche di protezione avvenga senza adeguati avvisi ai legittimi acquirenti o, addirittura, mediante l'inserimento dei c.d. *rootkits*[52]. Più specificatamente, vi sono alcuni siti specializzati nella vendita di brani musicali o filmati in formato digitale, come il ben noto "iTunes Store" creato e gestito dalla Apple Inc. L'utente, previa registrazione al sito, può acquistare singoli brani o interi album, i quali, in linea generale, sono resi disponibili solo protetti da tecnologie di DRM, anche se negli ultimi mesi sembra che tale tendenza stia parzialmente mutando.

Appare utile fare riferimento ad *iTunes Store*, che attualmente è la piattaforma più diffusa e che, per le sue caratteristiche, può costituire un ottimo *case study* anche per le problematiche che pone in ordine alla tutela del diritto alla riservatezza. Nel caso di specie l'utente deve installare sul proprio computer e poi attivare un *software* denominato, per l'appunto, iTunes. Successivamente deve creare un *account* e registrarsi fornendo i propri dati personali. In tale fase, però, non viene fornita una corretta informativa sul trattamento dei dati personali conseguente alla conclusione del contratto, dal momento che vengono utilizzati termini vaghi e generici in ordine alle operazioni che saranno successivamente effettuate sui dati stessi[53].

Per diversi anni, mediante iTunes sono stati resi disponibili unicamente file protetti da una tecnologia di DRM detta *Fairplay*, che consente di stabilire determinate limitazioni: i brani, infatti, possono

---

[52] Un *rootkit* è un programma che consente l'esecuzione di particolari comandi all'insaputa dell'utente, o per favorire l'ingresso di soggetti non autorizzati mediante l'utilizzo delle c.d. *backdoors* (letteralmente "porte di servizio". Nel gergo informatico indicano quelle porte di comunicazione che consentono di superare, in tutto o in parte, le procedure di sicurezza di un sistema informatico).

[53] La «politica sulla tutela della privacy di Apple» è consultabile all'URL http://www.apple.com/it/legal/privacy/index.html.

essere ascoltati su un massimo di cinque computer autorizzati, su un numero illimitato di lettori musicali portatili del tipo Apple "iPod" e masterizzati su compact disc audio per un numero illimitato di volte. Non è dunque possibile ascoltare i brani su altri lettori musicali portatili né farli riprodurre da altri programmi.

Successivamente, però, è divenuto possibile acquistare brani che non hanno le suddette limitazioni e che sono privi di DRM: ciò nonostante, essi pongono particolari problemi di tutela della privacy perché contengono delle informazioni univoche che consentono di riferire il file all'acquirente. In tal modo, a titolo esemplificativo, può essere rintracciato un utente che ha posto in condivisione quel determinato file mediante un programma di *file sharing*. Di ciò, tuttavia, l'utente non viene esplicitamente avvertito, ma di fatto il rischio di violazione della sua privacy è palese perché vengono surrettiziamente inseriti dati identificativi all'interno di un file, che ha oltretutto un costo maggiore perché non dovrebbe essere dotato di alcun tipo di "lucchetto digitale"; in tal caso, invece, è inserita una "filigrana digitale" al fine di tracciare l'utente a sua insaputa. È interessante notare come tale notizia si sia diffusa in tutto il web grazie alla curiosità di varie persone che hanno esaminato i file acquistati e hanno notato la stringa di codice incriminata[54].

Appare utile sottolineare che le tecnologie di DRM non sono utilizzate solo dall'azienda appena citata, ma anche dalla maggior parte dei siti che offrono il servizio di vendita di brani musicali in formato digitale[55].

È d'uopo precisare che le «misure tecnologiche di protezione» devono essere rimosse da chi le ha apposte solo in particolari casi stabiliti dalla legge (ad esempio, «per fini di sicurezza pubblica o per assicurare il corretto svolgimento di un procedimento amministrativo, parlamentare o giudiziario»). Qualora i sistemi di DRM vengano elusi la legge prevede addirittura sanzioni penali, come nel caso degli artt. 171-*bis* (che si applica solo nei casi in cui l'opera

[54] Cfr. http://www.tuaw.com/2007/05/30/tuaw-tip-dont-torrent-that-song.
[55] Si pensi a quelli gestiti da Microsoft e RealNetworks.

dell'ingegno è un «programma per elaboratore»)[56] e 171-*ter* legge n. 633/41[57].

La presenza di sistemi di DRM non può tuttavia impedire al legittimo possessore di un'opera dell'ingegno di effettuarne una copia privata (anche solo analogica) per uso personale. Pertanto, i titolari dei diritti d'autore devono far sì che ciò sia possibile (art. 71-*sexies*, comma 4, legge n. 633/41). Nel caso del *software*, la legge stabilisce che il legittimo utilizzatore di un programma può effettuarne una copia di riserva, qualora essa sia necessaria per l'uso (art. 64-*ter*, comma 2, legge n. 633/41).

Ad una tale incisiva tutela giuridica di cui possono godere i detentori dei diritti di proprietà intellettuale si contrappone l'ampio ventaglio di norme del cod. priv. a tutela dei dati personali. Purtroppo dell'esistenza di tali disposizioni non sembra rendersi conto la maggior parte di chi appone tecnologie di DRM sui contenuti distribuiti. In questi casi, infatti, viene acquisita, a fini contrattuali, una mole notevole di dati personali e si pongono in essere operazioni di profilazione al fine di cogliere l'andamento del mercato ed eventualmente suggerire i futuri acquisti ai propri clienti. Inoltre, l'inclusione di informazioni identificative può portare addirittura a tracciare la

---

[56] Ai sensi della norma citata, è punito con la reclusione e una multa chiunque, per trarne profitto, abusivamente importa, distribuisce, vende, detiene a scopo commerciale o imprenditoriale o concede in locazione programmi o qualsiasi mezzo inteso unicamente a consentire o facilitare la rimozione arbitraria o l'elusione funzionale di dispositivi applicati a protezione di un *software*.

[57] L'art. 171-*ter* l. n. 633/41, poi, punisce penalmente con la reclusione e una multa chiunque – per uso non personale e a fini di lucro – fabbrica, importa, distribuisce, vende, noleggia, cede a qualsiasi titolo, pubblicizza per la vendita o il noleggio, o detiene per scopi commerciali, attrezzature, prodotti o componenti oppure presta servizi che abbiano la prevalente finalità o l'uso commerciale di eludere le misure tecnologiche di protezione; lo stesso accade se le attrezzature, i prodotti o i componenti sono stati principalmente progettati, prodotti, adattati o realizzati per rendere possibile o facilitare l'elusione delle stesse misure. Fra l'altro, lo stesso articolo punisce penalmente anche chi abusivamente rimuove o altera le informazioni elettroniche poste sulle opere dell'ingegno. Tali informazioni identificano l'opera protetta e l'autore (o qualsiasi altro titolare dei diritti). Si consideri, poi, che l'art. 174-*ter* l. n. 633/41 punisce con la sanzione amministrativa di 154 € (oltre la confisca e la pubblicazione del provvedimento) chiunque acquista o noleggia attrezzature, prodotti o componenti atti ad eludere misure di protezione tecnologiche.

condotta delle persone, dunque anche al di fuori della fattispecie sopra citata relativa all'apposizione di una sorta di "filigrana digitale".

Le tecnologie di DRM possono, comunque, andare oltre a quanto sin qui esposto e, in taluni casi, far addirittura uso di sistemi biometrici. Più specificatamente, vi sono sistemi, correntemente utilizzati, che evitano la condivisione di nome utente e password mediante l'analisi delle dinamiche di inserimento del testo. Il sistema è in grado di capire se l'utente sia unico oppure se questi abbia comunicato le credenziali di accesso ad altri[58].

In altri casi sono state utilizzate tecnologie di DRM assolutamente illegali, come nel celebre caso del *rootkit* della Sony BMG Entertainment, avvenuto nel 2005[59]. Nel caso di specie, un programma di tale tipologia si installava, automaticamente e senza alcun avviso, quando veniva inserito nel lettore CD o DVD di un computer uno dei numerosi compact disc musicali prodotti e distribuiti dalla suddetta società dotati di tale *rootkit*. Molti computer hanno presentato blocchi di sistema successivamente a detta installazione.

La notizia della presenza del *rootkit* è stata data su un blog[60] e ha poi trovato una straordinaria diffusione in rete. Successivamente sono state intraprese diverse azioni legali nei confronti della casa discografica, che ha quindi ritirato dalla vendita i compact disc contenenti il *rootkit*. La violazione della privacy degli acquirenti dei suddetti compact disc appare palese. Nel caso di specie, è stato posto in essere un trattamento illecito di dati personali, poiché è stato dimostrato che mediante la tecnologia DRM ivi utilizzata venivano inviati dati identificativi univoci alla Sony BMG Entertainment, dunque in assenza di qualsiasi informativa e tanto meno di consenso in

---

[58] Soluzioni in tal senso sono sviluppate, ad esempio, dalla Biopassword (cfr. http://www.biopassword.com/password-authentication-drm.php).

[59] Su tale caso cfr., fra gli altri, T. Margoni, *Il conflitto tra Digital Rights Management e privacy nel caso Sony-rootkit*, in *Diritto dell'internet*, 2006, 5, pp. 519-524.

[60] M. Russinovich, *Sony, Rootkits and Digital Rights Management Gone Too Far*, in http://blogs.technet.com/markrussinovich/archive/2005/10/31/sony-rootkits-and-digital-rights-management-gone-too-far.aspx.

ordine al trattamento di dati personali conseguente all'installazione del *software*[61].

Appare chiaro, dunque, che i sistemi di DRM hanno una straordinaria potenzialità lesiva della privacy dei legittimi fruitori di un'opera dell'ingegno protetta con simili sistemi. Un problema, evidenziato dalla dottrina statunitense, consiste nel fatto che un'adeguata tutela della privacy in alcuni sistemi di DRM richiede un differente approccio nella loro costruzione[62], ma allo stato attuale non sembra che ciò avvenga, tanto da giungere a sostenere che la privacy degli utenti finali non è solitamente garantita in tali sistemi[63].

I dubbi sulla potenziale violazione della riservatezza originata dalla diffusione di tali piattaforme sono stati, del resto, avanzati anche dal Gruppo di lavoro sulla protezione dei dati personali istituito dall'art. 29 della direttiva n. 95/46/CE nel *Working document on data protection issues related to intellectual property rights*, emanato il 18 gennaio 2005[64]. In tale documento è stato affermato che lo sviluppo degli strumenti tecnici dovrebbe avvenire nel pieno rispetto della privacy degli utenti, limitando al massimo l'utilizzo di identificativi univoci che, ove presenti, dovrebbero comunque essere utilizzati con la massima trasparenza possibile[65].

## 5. *Il "Trusted Computing"*

La ricostruzione dell'evoluzione del diritto alla privacy ha mostrato come esso venga spesso visto (talvolta unicamente) nella sua specifica valenza di diritto alla protezione dei dati personali, che si concretizza soprattutto nella possibilità di un loro effettivo control-

---

[61] Cfr. M. Russinovich, *More on Sony: Dangerous Decloaking Patch, EULAs and Phoning Home*, in http://blogs.technet.com/markrussinovich/archive/2005/11/04/more-on-sony-dangerous-decloaking-patch-eulas-and-phoning-home.aspx.

[62] J.E. Cohen, *DRM and Privacy*, in *Berkeley Technology Law Journal*, 2003, 189, p. 609.

[63] J.S. Erickson, *Fair Use, DRM and Trusted Computing*, in *Communications of the ACM*, 2003, 4, p. 38.

[64] Documento n. 10092/05/EN, WP 104.

[65] Ivi, p. 8.

lo da parte dell'interessato che può così esercitare il proprio diritto all'autodeterminazione informativa.

Ciò è reso possibile anche dall'utilizzo degli strumenti informatici utilizzati da chiunque si voglia accostare non solo al ciberspazio, ma altresì un sempre crescente numero di attività, lavorative e ludiche, che richiedono l'utilizzo degli elaboratori elettronici per gli utilizzi più diversi. Del resto, questa è una naturale conseguenza del fatto che le informazioni sono sempre più spesso rese in formato digitale, per cui non può dubitarsi che quanto avviene nei computer, considerati anche quali porte di ingresso per il ciberspazio, non debba essere conosciuto e discusso solo in ambito prettamente informatico, ma debba altresì essere ben compreso, a grandi linee, da chiunque li utilizzi.

Ignorare tali problematiche è un lusso che oggi difficilmente ci si può concedere qualora si tengano presenti le potenziali conseguenze negative di un uso non consapevole dei sistemi informatici: si pensi ai casi di *phishing*, di diffusione di virus e *software* malevoli, di incauta diffusione dei propri dati personali, e così via. Alla complessità dei computer odierni, ma anche dei c.d. *smartphones*[66], e alla loro diffusione al di fuori dell'ambito prettamente informatico, sono conseguite una semplificazione delle interfacce utente e delle modalità con cui la macchina comunica con il suo utilizzatore, il tutto al fine di consentire una facile interazione anche a chi non è esperto della materia. Per far ciò si tende a nascondere tutte quelle informazioni che potrebbero confondere l'utente e ad automatizzare ciò che accade in ciascun sistema informatico.

Il passo successivo potrebbe consistere nello spogliare il legittimo utilizzatore di un sistema dal controllo dello stesso, in seguito alla diffusione di un complesso di tecnologie che vanno sotto il nome di "Trusted Computing" (TC). Esso consiste in una piattaforma che dovrebbe essere in futuro integrata non solo nei computer, come tuttora avviene, ma altresì nei microprocessori di telefoni cellulari e lettori musicali.

---

[66] Gli *smartphones* sono dispositivi che hanno sia le funzioni proprie di un comune telefono cellulare che di un *Personal Digital Assistant* (PDA).

Secondo i fautori di tale tecnologia, mediante la sua implementazione sarebbero risolte diverse problematiche connesse alla sicurezza informatica, come l'esecuzione di *software* malevoli, il furto di identità, l'accesso abusivo ai sistemi, e così via. In tal modo si avrebbe un più elevato e generalizzato livello di sicurezza informatica cui dovrebbe conseguire la crescita della fiducia (*trust*) da parte degli utilizzatori dei diversi sistemi informatici, con ovvi benefici sia economici (per le mancate perdite dovute ai problemi di sicurezza) sia di usabilità dei sistemi informatici e delle reti telematiche.

Tale fine può tuttavia essere raggiunto in altri modi senza limitare la libertà dell'utente, come invece avverrà in seguito ad una diffusa implementazione del TC, le cui prime realizzazioni concrete risalgono al 1999, quando è stato creato il consorzio "Trusted Computing Platform Alliance" (TCPA)[67]; nel 2003 ha poi assunto la denominazione di "Trusted Computing Group" (TCG). Di esso fanno parte le maggiori aziende del settore, che controllano sia il settore dell'informatica che quelli dell'elettronica di consumo e della telefonia mobile[68].

Il "cartello" creato da tali aziende, di fatto, potrebbe portare ad offrire, nel prossimo futuro, unicamente prodotti o servizi che implementano le tecnologie sviluppate dal TCG, privando così i potenziali acquirenti dei loro beni o servizi di una reale possibilità di scelta sull'utilizzarli o meno, e soprattutto imponendo loro di abdicare al controllo dei beni legittimamente utilizzati e, addirittura, delle informazioni personali che transitano nei sistemi informatici rispondenti alle suddette specifiche.

Difatti, tutti i dati memorizzati temporaneamente o permanentemente in un sistema informatico saranno "vagliati" dal "Trusted Platform Module" (TPM), un chip che costituisce il cuore di un sistema rispondente alle specifiche del TCG. Esso è identificato univocamente da un coppia di chiavi asimmetriche (dette "Endorsement

---

[67] Il TCPA è stato fondato nell'ottobre del 1999 da Compaq, Hewlett-Packard, IBM, Intel e Microsoft con lo scopo dichiarato di migliorare la sicurezza dei sistemi informatici.

[68] Membri promotori sono AMD, Hewlett-Packard, IBM, Infineon, Intel, Microsoft, Sun. Fra gli altri membri si possono ricordare Dell, Lexmark, Motorola, Nokia, Philips, Samsung, Siemens, Sony, Vodafone.

Keys") ed è in grado di cifrare le informazioni che transitano nel sistema; esso può inoltre generare automaticamente le "Attestation Identity Keys" (AIK).

Il primo problema per la privacy, dunque, consiste nel fatto che ogni macchina può essere identificata univocamente e, dunque, può esserlo anche il suo utilizzatore. Il TC, però, va oltre, e a tale controllo sull'identità dell'utente si affianca quello ancor più invasivo su ciò che può essere eseguito, letto o scritto nell'ambito del sistema informatico di riferimento.

Costituisce, quindi, una nuova frontiera del controllo globale, perché non solo identifica l'utente, ma decide anche cosa esso possa fare. Un sistema che implementa le tecnologie di TC può infatti impedire l'installazione di *software* non certificato nonché bloccare l'accesso a file di qualsiasi tipologia che non siano ritenuti *trusted*. La condotta dell'agente può, di conseguenza, svolgersi solo entro confini predeterminati aprioristicamente dal TCG, che potrebbe quindi divenire un "censore informatico", i cui poteri sarebbero così ampi da giungere ad imporre, in via astratta e discrezionale, le tipologie di azioni che, in linea ipotetica, possono essere compiute su un determinato elaboratore. In tal modo potrebbero essere eseguiti solo alcuni programmi, consultati solo determinati documenti e siti web, ascoltati solo certi brani musicali, e così via.

Si verifica, dunque, un netto spostamento dell'asse del controllo di ciascun sistema dall'utilizzatore al produttore, che dunque assume un ruolo di controllo e di gestione dei dati, personali e non, ivi memorizzati stabilmente od anche temporaneamente. A nulla vale quanto sostenuto dal TCG secondo cui il meccanismo utilizzato già per attivare il TC sia quello dell'*opt-in*, per cui risulterebbe sempre necessario un previo consenso dell'utente per rendere attivo il TPM[69].

Il mercato, difatti, può facilmente spingere chiunque ad adoperare, volente o nolente, tale sistema, perché le nuove applicazioni potrebbero richiedere la sua attivazione per funzionare e in alcu-

[69] «The system owner has ultimate control and permissions over private information and must "opt-in" to utilize the TCG subsystem» (cfr. https://www.trustedcomputinggroup.org/faq/).

ni casi il loro utilizzo potrebbe essere necessario a fini lavorativi e non[70]. Se il TC dovesse diventare uno standard, tutti i programmi potrebbero probabilmente essere adeguati o riscritti, per cui se il singolo utente decidesse di disattivare il sistema, il nuovo *software* potrebbe non funzionare o documenti creati da sistemi *trusted* potrebbero non essere leggibili da sistemi che non siano tali. Non si può infatti argomentare che comunque ciascuno goda della facoltà di scelta sull'acquisto di *hardware* e *software*, dal momento che i sistemi informatici, come si è detto, sono indispensabili in un numero crescente di ambiti e che l'integrazione del TC in ogni componente elettronico non lascerà comunque possibilità di scelta, poiché sempre più oggetti che rendono possibile il soddisfacimento di bisogni primari della persona sono dotati di componenti elettroniche.

Sul punto, però, il TCG non si assume alcuna responsabilità, perché lascia questa potenziale libertà di scelta sia ai produttori di *hardware* e *software* che agli utenti finali. Il quadro sin qui delineato, del resto, fa intuire quali e quante limitazioni potrebbe subire la libertà informatica proprio in un'epoca in cui essa si caratterizza sempre più come un diritto fondamentale dell'uomo.

Ciò nonostante, le chiavi di decrittazione non sono fornite ai legittimi utilizzatori dei sistemi. Ne consegue che potrebbero essere eseguite solo applicazioni "certificate" dal TCG e l'utente non avrebbe il controllo dei dati presenti sul proprio sistema, in chiara violazione del diritto all'autodeterminazione informativa.

---

[70] Le conseguenze negative dell'implementazione del TC non potrebbero evitarsi concedendo la possibilità di disattivare il sistema, perché si forzerebbero comunque gli utenti ad utilizzarlo disabilitando al contempo funzioni essenziali: in altri termini, si svuota di qualsiasi significato e contenuto la "concessione" di tale libertà. Inoltre, affinché il TC sia operativo è necessario che il *software* sia scritto appositamente per sfruttarlo, ma se esso venisse integrato in tutti i nuovi computer la creazione di nuovi programmi risulterebbe fortemente ostacolata perché qualsiasi *software* dovrebbe essere certificato dal consorzio, con i relativi costi. In tal modo lo sviluppo individuale dei programmi per elaboratore potrebbe risultare enormemente rallentato, poiché ogni singolo programmatore, oltre alle proprie energie lavorative, dovrebbe investire anche del denaro per fornire un programma alla collettività oppure per il semplice piacere di programmare. Potrebbe dunque venirsi a creare una nuova entità che tutela solo chi ha già raggiunto una posizione di potere e che potrebbe impedire ad altri di affermarsi nel proprio settore, riducendo così l'ambito della concorrenza alle caste già esistenti e violando il diritto alla libertà di espressione che può realizzarsi anche mediante la scrittura di un *software*.

Tuttavia, non sarebbe eticamente e giuridicamente ammissibile risolvere questa problematica mediante la fornitura delle suddette chiavi ad organismi, enti od istituzioni statali. A parte i chiari problemi relativi alla competenza territoriale fra i vari stati, alcuni dei quali potrebbero giungere a creare un efficace sistema di controllo globale del ciberspazio grazie a tali tecnologie, verrebbero comunque violati i principi che garantiscono la riservatezza e la segretezza delle comunicazioni e, comunque, dei propri dati personali. Alcune autorità, infatti, avrebbero una sorta di "mandato generale" al controllo delle informazioni personali di ciascun individuo, in palese violazione della normativa sulla privacy. Le deroghe a questo principio sono tassative e solo l'autorità giudiziaria è legittimata a farlo in casi concreti, non essendo possibile che l'eccezione diventi regola.

Appare chiaro, dunque, che l'avvento del TC rechi con sé la nascita di nuove e delicate problematiche di informatica giuridica, con particolare riferimento al diritto alla protezione dei dati personali. Del resto, l'informatizzazione della società ha sinora portato all'aumento del numero dei casi di lesione della privacy, come aveva previsto anche Negroponte nel 1995[71]; tale tendenza non potrà che consolidarsi di pari passo con la diffusione ed il perfezionamento delle tecnologie di tutela della proprietà intellettuale, perché sempre più invasive ed onnipresenti.

È stato giustamente notato che con l'avvento del TC e lo sviluppo di nuovi sistemi di DRM basati su di esso si avrà una privatizzazione, di fatto, della legge sulla proprietà intellettuale, perché i detentori dei diritti d'autore potranno limitare ancor di più i diritti degli utenti e controlleranno l'atteggiarsi concreto della suddetta normativa[72]; anzi, la diffusione dei sistemi *trusted* comporterà un monitoraggio continuo di quanto avviene *on line*[73].

---

[71] N. Negroponte, *Essere digitali*, Sperling & Kupfer, Milano, 1996, p. 237.

[72] B. Roemer, *Trusted Computing, Digital Rights Management, and the Fight for Copyright Control on Your Computer*, in *UCLA Journal of Law and Technology*, 2003, 8 (http://www.lawtechjournal.com/articles/2003/08_040223_roemer.php).

[73] L. Lessig, *Code Version 2.0*, cit., p. 191.

Il TC, del resto, può effettivamente eliminare la privacy degli utenti[74], ponendosi come il più invasivo e formidabile strumento di tutela dei diritti digitali. Esso impedisce, di fatto, l'anonimato, poiché, come si è visto, ogni sistema avrebbe un numero univoco di identificazione che potrebbe essere aggregato a quelli già presenti (come il *MAC address* delle schede di rete) e a quelli relativi alla connessione ad Internet, come l'indirizzo IP[75]. Sarebbe dunque assai facile risalire all'identità dell'utilizzatore di un elaboratore elettronico mediante il trattamento incrociato di più dati ed effettuare operazioni sempre più sofisticate e precise di profilazione degli utenti, eventualmente utilizzando tecniche biometriche come quella basata sull'analisi delle dinamiche di battitura del testo.

Si può dunque ritenere che il fine, astrattamente lecito, della tutela della sicurezza potrebbe semplicemente essere utilizzato come chiave di volta ottenere il consolidamento del controllo sul mercato economico e per acquisirne uno ancora maggiore sui dati personali dei singoli utenti, i quali perderebbero il controllo su di essi, ivi compresi quelli sensibili.

Come ha sostenuto Lawrence Lessig, mediante il codice informatico è possibile ottenere una tutela dei propri diritti di proprietà intellettuale in maniera molto più efficiente rispetto a quanto astrattamente ottenibile utilizzando gli strumenti forniti dal diritto[76]. Il problema ulteriore è che l'emanazione di normative ampiamente squilibrate a favore di soggetti già economicamente forti, come accaduto con il *Digital Millennium Copyright Act*, dà loro la possibilità di farsi giustizia da sé, seppur con modalità digitali.

I legittimi utilizzatori di un sistema informatico non potranno mai conoscere a sufficienza ciò che accade in esso; soprattutto, essi potranno essere facilmente monitorati perché solo i produttori dell'*hardware* e del *software* sapranno quali informazioni saranno

---

[74] C. Woodford, *Trusted Computing or Big Brother? Putting the Rights Back in Digital Rights Management*, in *University of Colorado Law Review*, 2004, 75, p. 300.

[75] Si può ipotizzare, ad esempio, che le richieste di certificazione inviate ad un *server* remoto possono consentire di tenere traccia delle preferenze degli utenti, i quali perderebbero il controllo delle proprie informazioni a vantaggio di altri soggetti che le otterrebbero gratuitamente.

[76] L. Lessig, *Code Version 2.0*, cit., p. 179.

memorizzate parzialmente o temporaneamente nei medesimi sistemi, visto che, si ribadisce, le chiavi di decrittazione non saranno rese pubbliche. Nel caso di specie, dunque, ciascun utilizzatore di un sistema che implementa le tecnologie di TC perderà il controllo dei propri dati, anche se è d'uopo sottolineare che il cod. priv. fornisce all'interessato i rimedi giuridici per intervenire in caso di eventuali violazioni del suo diritto alla privacy, con l'esplicita possibilità di ottenere il risarcimento anche dei danni non patrimoniali subiti.

Capitolo IV

# IL DIRITTO ALLA PRIVACY NELL'AMBITO DELL'INFORMATICA MEDICA

## 1. *Informatica medica ed "e-health"*

Lo sviluppo dell'informatica è assai celere, ma sia in ambito medico che giuridico non vi sono stati quegli sconvolgimenti ipotizzati negli anni Sessanta. Si pensi, ad esempio, alle diverse ipotesi avanzate nell'ambito della giurimetria[1], come quella dell'applicazione automatica del diritto, di cui si discuteva più in termini di astratta non desiderabilità che di impossibilità pratica[2].

Sino ad alcuni anni fa, e soprattutto negli anni Sessanta quando l'intelligenza artificiale[3] muoveva i suoi primi passi, era notevole l'interesse verso la realizzazione di soluzioni concrete finalizzate a

---

[1] La giurimetria ha posto le basi per il successivo sviluppo dell'informatica giuridica. Il primo contributo in materia è di L. Loevinger, *Jurimetrics. The Next Step Forward*, in *Minnesota Law Review*, 1949, 33, pp. 455-493. Sulla giurimetria e sull'evoluzione dell'informatica giuridica e del diritto dell'informatica sia consentito rinviare a G. Fioriglio, *Temi di informatica giuridica*, Aracne, Roma, 2004.

[2] Ad esempio, Spiros Simitis non dubitava della possibilità di giungere ad un'applicazione automatica del diritto o, comunque, di un'analisi delle future decisioni dei giudici sulla base della giurisprudenza preesistente, ma piuttosto della sua intrinseca necessità. Essa, infatti, concreterebbe un'attività di controllo dell'attività giudiziaria finalizzata a verificare se i giudici si sono attenuti alle norme vigenti ed alle interpretazioni già svolte, dando così rigidità all'attività svolta in sede giurisdizionale (S. Simitis, *Crisi dell'informazione giuridica ed elaborazione elettronica dei dati*, tr. it., Giuffré, Milano, 1977, p. 110).

[3] «L'intelligenza artificiale (*artificial intelligence*) è usualmente definita come la scienza intesa a sviluppare modelli computazionali del comportamento intelligente, e quindi a far sì che gli elaboratori possano eseguire compiti che richiederebbero intelligenza da parte dell'uomo» (G. Sartor, *Intelligenza artificiale e diritto. Un'introduzione*, Giuffré, Milano, 1996, p. 9). Sull'intelligenza artificiale cfr., *ex multis*, S.J. Russell, P. Norvig, *Intelligenza artificiale. Un approccio moderno*,

sostituire l'uomo anche nelle professioni intellettuali, anziché "semplicemente" a coadiuvarlo. Si poteva dunque prevedere la creazione di un medico o di un giudice computerizzato che potesse svolgere le stesse mansioni di uno umano o comunque rimpiazzarne gran parte delle funzioni[4], ma senza commettere quegli errori tipicamente derivanti dalla condotta di una persona umana che possono cagionare conseguenze talvolta gravi ed irreparabili. Si pensi, a titolo esemplificativo, che da uno studio condotto negli Stati Uniti alcuni anni fa è emerso che ogni anno circa 98.000 decessi avvenuti nelle strutture sanitarie statunitensi sono imputabili ad errori umani[5].

Tuttavia, dottori e giudici non sono stati sostituiti da sistemi informatici o da robot come si potrebbe prospettare in un romanzo di fantascienza[6]: anche oggi tali ipotesi sono da ritenersi troppo avveniristiche qualora si guardi allo stato della tecnologia. Più che mediante un enorme passo in avanti, l'informatizzazione può e deve avvenire seguendo più fasi[7]. È paradossale il fatto che pochi decenni fa il problema principale fosse costituito dalla paura circa la presumibile (e futura) eccessiva intelligenza dei sistemi informatici mentre oggi

---

tr. it., Pearson Education, Milano, 2005, e P.H. Winston, *Artificial Intelligence*, Addison Wesley, Reading, Massachusetts, 1993.

[4] In tal senso W.B. Schwartz, *Medicine and the computer: the promise and problema of change*, in *The New England Journal of Medicine*, 1970, 283, pp. 1257-1264.

[5] L.T. Kohn, J.M. Corrigan, M.S. Donaldson (eds.), *To Err is Human: Building a Safer Health System*, National Academy Press, Washington, DC, 2000. «Information Technology can reduce the rate of errors in three ways: by preventing errors and adverse events, by facilitating a more rapid response after an adverse event has occurred, and by tracking and providing feedback about adverse events» (D.W. Bates, A.A. Gawande, *Improving Safety with Information Technology*, in *The New England Journal of Medicine*, 2003, 348, 25, p. 2526). A titolo esemplificativo, si pensi ai risultati di uno studio che ha dimostrato una diminuzione consistente (55%) del numero di errori nelle operazioni inerenti alle diverse fasi di somministrazione dei farmaci (D.W. Bates *et al., Effects of computerized physician order entry and a team intervention on prevention of serious medical errors*, in *Journal of American Medical Association*, 1998, 280, pp. 1311-1316).

[6] Ciò ha portato la dottrina ha chiedersi, un ventennio fa, come mai la rivoluzione non fosse avvenuta, ripercorrendo le esperienze svolte al fine di apprendere dagli errori del passato nello sviluppo dei nuovi sistemi (W.B. Schwartz, R.S. Patil, P. Szolovits, *Artificial Intelligence in Medicine. Where Do We Stand?*, in *The New England Journal of Medicine*, 1987, 316, p. 685).

[7] T. Bodheneimer, K. Grumbach, *Electronic Technology. A Spark to Revitalize Primary Care?*, in *Journal of the American Medical Association*, 2003, 2, p. 263.

ci si concentra più sul fatto che essi possano essere pericolosi perché troppo "stupidi" nonché potenzialmente utilizzabili per fini illeciti.

Tali considerazioni non sono, comunque, finalizzate a far passare in secondo piano tutti quei mutamenti, positivi e negativi, che la creazione e la diffusione degli elaboratori elettronici hanno comportato nella società contemporanea. Con specifico riguardo all'ambito medico è d'uopo sottolineare che in esso si sono registrati progressi notevoli e che le strutture sanitarie sono oggi caratterizzate da un elevato tasso di informatizzazione[8]. Di ciò si avvantaggiano sia lo staff medico e amministrativo, che può contare su un supporto elettronico sempre più evoluto, sia i pazienti, in virtù dell'innalzamento dei livelli qualitativi delle operazioni di diagnosi, prognosi e terapia nonché di maggiore celerità ed efficienza nello svolgimento delle operazioni amministrative e burocratiche. Inoltre, la presenza di banche dati sanitarie, anche *on line*, può consentire un più rapido ed efficiente aggiornamento professionale a medici ed operatori sanitari.

In particolare, i sistemi informativi evoluti, qualora siano correttamente utilizzati, possono velocizzare la trasmissione dei dati relativi allo stato di salute con ovvi benefici soprattutto nei casi in cui sia necessario conoscere con urgenza determinate informazioni (ad esempio, in seguito ad eventi traumatici che impongono interventi di pronto soccorso nel cui ambito può essere vitale conoscere eventuali allergie a determinati farmaci). Inoltre, possono essere creati sistemi di supporto alla decisione finalizzati ad aiutare i medici nello svolgimento del loro lavoro; ancora, *software* di buona qualità inserito in dispositivi medici può migliorare la qualità e l'aspettativa di vita di quei pazienti che devono o che possono farne uso.

Di base, dunque, qualsiasi persona che si trovi a qualsiasi titolo in ambito sanitario può servirsi, anche inconsapevolmente, di *software* assai evoluti e beneficiare dei progressi compiuti nell'am-

[8] In dottrina si è giunti ad affermare che le nuove tecnologie hanno rivoluzionato la medicina e che gli avanzamenti in materia saranno ancora più spettacolari nel corso del secolo attuale (K.I. Shine, *Technology and health*, in *Technology in Society*, 2004, 26, p. 137).

bito dell'informatica medica (ossia dell'informatica applicata alla medicina)[9].

Secondo il Comitato Nazionale per la Bioetica, tale scienza «interessa tutti i cittadini, in generale, ma più direttamente (a seconda dei programmi attivati) gli amministratori sanitari, il personale sanitario di ogni livello, i ricercatori biomedici, i docenti ed i discenti dei corsi di formazione, gli ammalati ecc.» e «ha come obiettivi principali la partecipazione a programmi di: tutela della salute e di cura della malattia, gestione dei sistemi sanitari, facilitazione della ricerca biomedica»[10].

I computer, comunque, non solo «non sono la soluzione ad ogni problema»[11], ma addirittura talvolta creano questioni che possono avere un impatto negativo sui vari sistemi sanitari e sui soggetti che in vario modo vi sono coinvolti.

Il problema principale, da un punto di vista tecnico, consiste nel fatto che tanto più un programma informatico è complesso tanto più alte sono le possibilità che esso contenga degli errori che possano provocarne malfunzionamenti o addirittura blocchi. Si pensi al caso del "Therac 25", un macchinario di radioterapia che fra il giugno del 1985 ed il gennaio del 1987 ha causato a numerosi pazienti forti lesioni, alcune tanto gravi da provocarne poi il decesso, per la presenza di alcuni difetti nel *software* di gestione della macchina stessa[12].

---

[9] Sull'informatica medica cfr., fra gli altri, R. Bellazzi, A. Abu-Hanna, J. Hunter (eds.), *Artificial Intelligence in Medicine. Proceedings of the 11th Conference on Artificial Intelligence in Medicine*, Springer, Berlin, 2007; H. Chen *et al.* (ed.), *Medical Informatics. Knowledge Management and Data Mining in Biomedicine*, Springer science, New York, 2005; C.P. Friedman, J.C. Wyatt, *Evaluation Methods in Biomedical Informatics*, Springer science, New York, 2006; D. Goldstein *et al.*, *Medical Informatics 20/20. Quality and Electronic Health Records through Collaboration, Open Solutions and Innovation*, Jones & Bartlett, London, 2007; E.H. Shortliffe, J.C. Cimino (eds.), *Biomedical Informatics. Computer Applications in Health Care and Biomedicine*, Spinger science, New York, 2006.

[10] Comitato Nazionale per la Bioetica, *Etica, salute e nuove tecnologie dell'informazione*, Roma, 2006, p. 10.

[11] R.A. Miller, K.F. Schaffner, A. Meisel, *Ethical and Legal Issues Related to the Use of Computer Programs in Clinical Medicine*, in *Annals of Internal Medicine*, 1985, 102, p. 529.

[12] N. Leveson, C.S. Turner, *An Investigation of the Therac-25 Accidents*, *IEEE Computer*, 1993, 7, pp. 18-41.

Se, tuttavia, non è di fatto possibile creare un *software* complesso senza alcun margine di errore, è comunque possibile crearne uno che sia ragionevolmente sicuro ed affidabile, rendendo necessarie procedure di test e di monitoraggio la cui accuratezza dovrebbe essere proporzionale ai potenziali rischi connessi al *software* di riferimento.

La storia recente, infatti, mostra come nonostante l'informatizzazione delle strutture sanitarie sia sempre più diffusa e penetrante, non si siano verificati eventi particolarmente catastrofici, mentre i benefici dell'informatizzazione in ambito biomedico sono ben noti; altrettanto non può dirsi dei principi di base del funzionamento dei sistemi informatici e delle loro caratteristiche principali, anche se bisogna pur considerare la loro crescente complessità. Purtroppo, però, ciò che non è conosciuto è spesso fonte di timore, per cui la considerazione dell'estrema complessità dei sistemi informatici utilizzati nel settore sanitario e, più in generale, dei dispositivi medici che includono componenti *software*, può cagionare paure sovente infondate.

Sul punto è interessante notare come anche prodotti ed apparecchiature realizzati allo stato dell'arte possano diventare pericolosi qualora vengano utilizzati oltre il loro ciclo di vita presunto oppure non siano utilizzati ai fini per i quali erano stati realizzati[13].

Le problematiche etiche e giuridiche connesse a tale settore sono state sollevate da diversi anni e, insieme alle questioni connesse alla responsabilità per software difettoso, si è posto in evidenza come la diffusione di sistemi informatici in ambito medico possa ca-

[13] Si pensi al caso dell'incidente avvenuto durante la prima "Guerra del Golfo" che ha cagionato la morte di ventotto uomini dell'esercito statunitense in seguito ad un difetto nel *software* del sistema missilistico "Patriot". In realtà tale componente era stata sviluppata negli anni Sessanta per altri fini (intercettare e colpire aerei, non missili) e l'adattamento di una tecnologia vetusta e differente ha portato a tali tragiche conseguenze (T. Forester, P. Morrison, *Computer Ethics. Cautionary Tales and Ethical Dilemmas in Computing*, MIT Press, Cambridge, Massachusetts, 1994, p. 109). Questo esempio dimostra come bisognerebbe essere sempre cauti nell'attribuzione delle responsabilità e nell'analisi delle problematiche: «the poor old computer gets the blame on these and other occasions, although frequently something else is at fault» (ivi, p. 2).

gionare gravi violazioni della privacy individuale e collettiva[14]. Così, in linea più generale, può affermarsi che, vista la delicatezza dei dati trattati in tali sistemi, l'uso eticamente corretto dell'informazione assume un'importanza fondamentale in ambito bioetico[15].

In particolare, alcuni difetti presenti in tali sistemi possono consistere nel fornire informazioni inesatte potenzialmente idonei a ledere il diritto all'autodeterminazione informativa, con conseguenze assai gravi come nel caso di un errore software presente in un sistema utilizzato presso il dipartimento di immunologia dell'ospedale di Sheffield, in Inghilterra. Nel caso di specie, a numerose donne era stato erroneamente diagnosticato di avere un basso rischio di dare alla luce bambini affetti da sindrome di Down[16].

Al contrario, il corretto funzionamento di sistemi informativi sanitari può consentire l'esercizio del suddetto diritto ed un più celere ed economico accesso alle informazioni relative al proprio stato di salute. In una società globale, dove è sempre più facile ed economico viaggiare da una parte all'altra del pianeta, può essere utile, e talvolta addirittura vitale, che ciascuno abbia a disposizione i propri dati sanitari. Ottenerne la copia può tuttavia comportare un processo lungo e costoso anche in una nazione all'avanguardia come gli Stati Uniti, dove all'elevata informatizzazione delle strutture sanitarie ed all'esplicita previsione del diritto soggettivo ad ottenere una copia dei propri dati sanitari[17] fa da contraltare la realtà di procedure che possono richiedere anche novanta giorni per essere espletate. Nella maggior parte dei casi, inoltre, le informazioni sono fornite unicamente in formato cartaceo e non vi è possibilità di riceverle su supporto informatico[18].

---

[14] Cfr, ad esempio, R.A. Miller, K.F. Schaffner, A. Meisel, *Ethical and Legal Issues Related to the Use of Computer Programs in Clinical Medicine*, cit.

[15] In tal senso Comitato Nazionale per la Bioetica, *Etica, salute e nuove tecnologie dell'informazione*, cit., p. 11.

[16] J.K. Gable, *An Overview of the Legal Liabilities Facing Manufacturers of Medical Information Systems*, in *Quinnipiac Health Law Journal*, 2001, 5, p. 129.

[17] Ciò è previsto dall'*Health Insurance Portability and Accountability Act* (HIPAA) (in particolare cfr. 45 C.F.R. § 164.524 (a)(1)).

[18] Sia consentito rinviare al seguente studio: G. Fioriglio, P. Szolovits, *Copy Fees and Patients' Rights to Obtain a Copy of Their Medical Records: From Law*

In dottrina si è osservato, però, che i timori principali della maggior parte delle persone consistono nella possibilità di una celere e diffusa disseminazione di dati sanitari elettronici nel ciberspazio nonché che possano verificarsi utilizzi non autorizzati[19]. Tali paure traggono origine anche dall'illecito e discutibile interscambio di dati relativi allo stato di salute posto in essere in numerose occasioni fra società operanti nel settore sanitario o comunque interessate all'acquisizione di simili informazioni, come datori di lavoro e società assicuratrici[20].

Del resto, come la creazione e la diffusione delle prime banche dati ha fatto sorgere l'esigenza di apprestare una particolare protezione dei dati personali, così le nuove potenzialità dell'informatica, ed in particolare la possibilità di trasmettere rapidamente una enorme mole di informazioni, rafforzano la medesima esigenza in ambito biomedico. Il suo soddisfacimento è oggi prioritario affinché venga garantita un'ancora maggiore informatizzazione della medicina improntata al rispetto della dignità della persona umana, sia come singolo che come componente di gruppi sociali più o meno estesi.

La tutela dei dati personali, però, non dovrebbe essere realizzata impedendo o limitando l'utilizzo delle *information and communications technologies* nel settore sanitario, ma piuttosto nello sviluppo di tecnologie che consentano la protezione delle informazioni in un ambiente informatico[21], anche perché il rispetto della confidenzialità delle informazioni costituisce una componente fondamentale nella costruzione di un rapporto di fiducia fra il paziente e gli operatori sanitari[22].

---

*to Reality*, in *Proceedings of American Medical Informatics Association Annual Symposium*, 2005, pp. 251-255.

[19] D. Crolla, *Cyberlaw: A Potent New Medicine for Health Law on The Internet*, in S. Callens (ed.), *E-Health and the Law*, Kluwer Law International, The Hague, The Netherlands, 2003, p. 19.

[20] A. Etzioni, *The Limits of Privacy*, Basic Books, New York, 1999, p. 144.

[21] National Research Council, *For the Record. Protecting Electronic Health Information*, National Academy Press, Washington, DC, 1997, p. 161.

[22] In tal senso A. Greenhoug, H. Graham, *Protecting and using patient information: the role of the Caldicott Guardian*, in *Clinical Medicine*, 2004, 4, 3, p. 246 e A. Nicoll, *Protecting health and patient confidentiality, ethics and surveillance*, in *Current Pediatrics*, 2005, 15, p. 588.

La necessità di tutelare i diversi profili del diritto alla privacy sono stati ribaditi anche dalla «International Medical Informatics Association»[23], che nel 2002 ha emanato un Codice etico per chi opera professionalmente nel settore dell'*health information*, redatto dal un gruppo di lavoro su "Data Protection in Health Information". In tale codice viene esplicitamente sancito il fondamentale diritto alla privacy, cui consegue il controllo sull'acquisizione, l'archiviazione, l'accesso, l'utilizzo, la comunicazione, la manipolazione e la distruzione dei dati personali (parte I, B, § 1).

Anche lo "European Group on Ethics in Science and New Technologies", istituito nell'ambito della Commissione Europea, si è da tempo espresso sulle problematiche etiche connesse alla sanità nella Società dell'informazione, richiamando l'attenzione, fra l'altro, sulla necessità di garantire la riservatezza delle informazioni sanitarie mediante l'obbligatorietà, in linea di principio, del consenso alla loro acquisizione e comunicazione, nonché di rispettare la dignità umana, l'autonomia dell'individuo, la giustizia nella distribuzione delle risorse, la solidarietà e i principi di beneficenza e non maleficenza[24].

Già dalle considerazioni sinora svolte, dunque, si può comprendere come in tale settore sia difficile fornire risposte adeguate alle esigenze che sorgono, anche perché esso costituisce il crocevia di diverse discipline: medicina, informatica, diritto, etica[25].

L'incessante progresso dell'informatica medica, da un lato, e la valutazione dei benefici che possono conseguire per l'intero sistema

---

[23] La "International Medical Informatics Association" (http://www.imia.org) è un'organizzazione indipendente istituita nel 1989, anche se creata nel 1967 come comitato tecnico n. 4 dell'"International Federation for Information Processing". Di essa fanno parte associazioni nazionali, istituzioni di ricerca e universitarie nonché aziende private. Ad individui che si sono particolarmente distinti per aver contribuito agli scopi dell'IMIA può essere conferito il titolo onorifico di "Honorary Fellow".

[24] European Group on Ethics in Science and New Technologies, *Opinion on Ethical issues of healthcare in the Information Society*, 30 luglio 1999, n. 13, p. 9.

[25] È stato osservato che «research, ethics and privacy can therefore all be satisfied by a clear legal framework, supported by an effective system of ethics committees to adjudicate alla research protocols» (J.S. Horner, *Research, ethics and privacy: the limits of knowledge*, in *Public Health*, 1998, 112, p. 219).

sanitario, dall'altro, portano comunque ad una progressiva crescita dell'interesse verso l'"e-Health". Con tale termine, in linea generale, viene designato il complessivo fenomeno consistente nella creazione e nell'applicazione delle moderne tecnologie informatiche al sistema sanitario complessivamente inteso[26], nel cui ambito si possono qui ricordare:

– lo sviluppo di reti di sistemi informativi sanitari per velocizzare la trasmissione delle informazioni mediche;

– la predisposizione di servizi sanitari mediante reti telematiche, ivi compresi i servizi di telemedicina;

– la creazione di cartelle sanitarie elettroniche (*Electronic Health Records* o *Electronic Medical Records*) e di tessere sanitarie elettroniche;

– l'utilizzo di strumenti elettronici di comunicazione.

Chiaramente, la diffusione dell'*e-health* può comportare rischi non solo per la privacy ma anche il sorgere di ulteriori problematiche relative a responsabilità professionale, abusivo esercizio della professione medica, giurisdizione, copertura delle spese mediche, diffusione di farmacie *on line*, proprietà intellettuale[27].

In ogni caso, l'evoluzione dell'*e-health* dovrebbe essere condotta ponendo sempre il paziente come componente centrale[28]: con particolare riferimento al diritto alla privacy, ciò dovrebbe concretizzarsi nel garantirgli sempre un effettivo e celere diritto di accesso ai propri dati, nonché di controllarli effettivamente. Si consideri, del resto, che l'*e-health*, per definizione e in linea generale, è proprio basato sulla trasmissione elettronica delle informazioni nonché sulla loro condivisione.

Tali profili appaiono di fondamentale importanza soprattutto nella prospettiva comunitaria, anche perché negli ultimi anni si è intensificata l'azione dell'Unione Europea finalizzata a stimolare la ricerca e le implementazioni di soluzioni tecnologiche di *e-health*, il

---

[26] Cfr. D. Silber, *The Case for eHealth*, European Institute for Public Administration, Maastricht, The Netherlands, 2003.

[27] Su di essi si rinvia, fra gli altri, a F. McMenamin, *Risks for E-Health*, in S.Callens, *E-health and the law*, cit. pp. 45-56.

[28] E.H.W. Kluge, *Secure e-Health: Managing risks to patient health data*, in *International Journal of Medical Informatics*, 2007, 76, p. 405.

tutto nell'ambito del piano "*eEurope 2005"* prima e "*i2010*" («Una società europea dell'informazione per la crescita e l'occupazione») poi[29].

Su un piano più generale, è opportuno fare altresì riferimento alla risoluzione sull'*e-health* dell'Organizzazione Mondiale della Sanità, emanata il 25 maggio 2005, con la quale si è sottolineato che l'*e-health* consiste nell'efficiente e sicuro utilizzo delle tecnologie dell'informazione e della comunicazione al fine di supportare la medicina ed i settori affini; ha inoltre invitato gli stati membri a predisporre un piano strategico a lungo termine per lo sviluppo e l'implementazione di servizi di *e-health* nei vari settori della sanità nonché a sviluppare l'infrastruttura tecnologica di tali servizi affinché l'accesso ai medesimi sia equo, ragionevole e universale[30].

La diffusione di servizi nell'ambito dell'*e-health* non è però unicamente ostacolata da problematiche di carattere informatico, giuridico ed economico, ma anche da barriere culturali, come la riluttanza di alcuni medici all'utilizzo dei computer, anche in considerazio-

---

[29] Con risoluzione del 23 maggio 2007 («sull'impatto e sulle conseguenze dell'esclusione dei servizi sanitari dalla direttiva sui servizi nel mercato interno») il Parlamento europeo ha osservato «che, per ridurre la burocrazia collegata all'uso dei servizi sanitari transfrontalieri, è necessario migliorare i sistemi elettronici di identificazione del paziente e il trattamento delle sue richieste di rimborso» (n. 8) ed ha invitato «la Commissione a esortare gli Stati membri a sostenere attivamente l'introduzione del sistema sanitario in linea e della telemedicina» (n. 9). Inoltre, «anche se i sistemi sanitari non rientrano nelle competenze della Comunità, le questioni connesse a tali sistemi, quali l'accesso ai medicinali e alle cure, l'informazione dei pazienti e la circolazione di società assicurative e di professionisti della sanità, hanno un carattere transfrontaliero», per cui «tali questioni devono essere affrontate dall'Unione europea» (n. 12). Ha altresì chiesto «che vengano esaminati modi per promuovere e sostenere attivamente l'opera volta a rendere corrente l'impiego della Carta europea di assicurazione contro le malattie con una serie standardizzata di dati elettronici sui pazienti, in modo da semplificare le procedure per i cittadini europei che si sottopongono a cure mediche in altri Stati membri» (n. 37). Ha poi rilevato che, «in materia di telesanità e *e-health*, gli sviluppi sono talmente vasti da rendere necessario concordare nuove norme in materia di copertura sociale, finanziamento ed accesso a tali cure» (n. 51).

[30] World Health Organization, *Resolution on eHealth*, WHA58.28, 25 maggio 2005, reperibile all'URL http://www.who.int/gb/ebwha/pdf_files/WHA58/WHA58_28-en.pdf.

ne di eventuali problematiche giuridiche relative alla trasmissione di dati sanitari per via telematica[31].

Oggi, pertanto, il problema principale sembra essere quello di dare attuazione concreta alle intenzioni espresse sia in ambito internazionale che nazionale[32]. Ovviamente non è un compito facile, poiché l'eterogeneità dei soggetti coinvolti non consente una facile concertazione fra interessi di per sé confliggenti, come quelli delle amministrazioni locali di contenere i costi, dei medici di poter disporre di strumenti sempre più evoluti, dei pazienti di ottenere le migliori cure possibili, dei creatori dei sistemi informatici di ottenere profitti sempre più elevati. Probabilmente, però, la riduzione dei costi connessa all'implementazione di tecnologie di *e-health* potrà dare una notevole spinta ad utilizzarle con sempre maggiore continuità. La speranza è che ciò avvenga nel pieno rispetto della dignità della persona, tutelandone la salute e la privacy. In tal senso i cittadini europei possono contare su un impianto normativo ben più avanzato di quello statunitense, soprattutto in tema di protezione dei dati personali. Le disposizioni in materia, infatti, anche in mancanza di previsioni specifiche, sono abbastanza duttili da garantire una tutela efficace a chiunque si trovi nel territorio dell'Unione Europea, sia grazie all'azione dei Garanti europei che mediante l'utilizzo dei rimedi giuridici previsti dalle varie normative che hanno recepito le direttive 95/46/CE e 2002/58/CE.

## 2. *I sistemi esperti e i sistemi informativi sanitari*

L'informatica può contribuire al progresso della medicina fornendo strumenti in grado di coadiuvare gli operatori sanitari nel-

---

[31] D.W. Bates, A.A. Gawande, *Improving Safety with Information Technology*, cit., p. 2533.

[32] Alcuni progetti concretamente realizzati dimostrano come l'informatica possa dare benefici concreti ai pazienti: si pensi, a titolo esemplificativo, al progetto "I-Care", finalizzato alla creazione di un sistema informatico per l'erogazione di servizi socio-sanitari al domicilio di soggetti anziani e alla comunicazione e condivisione dei dati relativi tra gli enti chiamati alla predisposizione di tali servizi. A tale progetto hanno partecipato, fra gli altri, il CIRSFID - Università di Bologna e il Comune di Forlì.

lo svolgimento delle loro delicate mansioni. Nonostante, come si è detto, non vi siano stati avanzamenti rivoluzionari nella creazione di sistemi automatici in grado di sostituirsi ai medici nelle varie fasi di diagnosi, prognosi e terapia, l'esperienza degli ultimi decenni mostra come oggi vi siano tutte le potenzialità per la creazione di sistemi esperti[33] in grado di assistere proficuamente i medici nel prendere decisioni.

Si pensi, del resto, che già negli anni Settanta il sistema esperto denominato MYCIN, creato nell'ambito dell'Università di Stanford, aveva dato ottimi risultati, seppur non perfetti[34]. Successivamente, sistemi simili non hanno trovato utilizzi efficaci nella pratica medica per diversi fattori, fra cui alcuni di carattere etico e giuridico inerenti già al fatto stesso di affidare, in tutto o in parte, decisioni sulla diagnosi, la prognosi o la terapia di una persona umana ad una macchina. Ovviamente tale problema risulta amplificato qualora la macchina effettui la c.d. chiusura del *loop*, ossia sia in grado di prendersi cura del paziente sotto tutti i punti di vista.

In tutti i casi, comunque, si pongono delicate questioni in ordine all'imputazione della responsabilità per eventuali difetti presenti in tali sistemi cui conseguano eventi dannosi anche qualora essi siano utilizzati sotto la supervisione di personale esperto. Probabilmente tali considerazioni hanno comportato un rallentamento dello sviluppo di sistemi effettivamente utilizzabili in grado di chiudere il *loop*, anche se sembra possibile ritenere che nel prossimo futuro i medici elettronici potrebbero entrare a far parte delle strutture sanitarie.

---

[33] I sistemi esperti sono dei sistemi informatici basati su un modello del comportamento intelligente, in grado di effettuare attività che richiedono particolari competenze o cognizioni (G. Sartor, *Intelligenza artificiale e diritto. Un'introduzione*, cit., p. 22). In linea di principio, un sistema esperto è composto da due elementi essenziali: una «base di conoscenza», che contiene una rappresentazione esplicita della conoscenza come un insieme di asserzioni o dichiarazioni che descrivono il dominio del problema, e un «motore inferenziale», ossia un programma in grado di effettuare deduzioni usando la base di conoscenza. Di norma vi è anche un'interfaccia utente agevola l'interazione con il sistema.

[34] V.L. Yu *et al.*, *An Evaluation of MYCIN's ADVICE*, in B.G. Buchanan, E.H. Shortliffe (eds.), *Rule-Based Expert Systems: The MYCIN Experiments of the Stanford Heuristic Programming Project*, Addison Wesley, Reading, Massachusetts, 1984, pp. 589-596.

La speranza è che, in tal caso, non venga pretermessa la riflessione sui profili etici sollevati da simili sistemi e che non si verifichi una "disumanizzazione" della medicina. Bisogna infatti considerare che la medicina interviene spesso nel momento in cui una persona è più fragile e indifesa, ossia quando si trova a soffrire per patologie più o meno gravi, con evidenti ripercussioni anche sulla sua sfera affettiva (familiare e non). Il rapporto umano che si stabilisce fra medico e paziente può assumere, in tali casi, un'importanza fondamentale per quest'ultimo, con modalità che difficilmente potranno aversi qualora egli si relazioni con delle "fredde" macchine.

Tali problematiche sono forse premature, ma la riflessione in materia non può che essere utile per far sì che sia l'uomo a controllare l'evoluzione della ricerca e gli strumenti da esso stesso creati, e non il contrario. Assolutamente attuali sono, invece, le considerazioni sui sistemi informativi sanitari, già oggi diffusi e sempre più perfezionati.

In linea generale, un sistema informativo sanitario può essere utilizzato per lo svolgimento di diverse funzioni sia di carattere medico che amministrativo. In particolare, rende possibile la creazione e l'aggiornamento di un database dei pazienti, ivi comprese le loro cartelle cliniche, nonché l'ordinaria gestione amministrativa della struttura sanitaria che ne fa uso[35].

Grazie ad un sistema ben realizzato risulta possibile migliorare l'assistenza sanitaria, poiché i dati relativi alle condizioni di salute dei pazienti possono venire trasferiti in tempi assai rapidi, evitandone oltretutto la duplicazione qualora si faccia uso di un *database* unico. In tal modo, quindi, non è necessario immettere più volte le medesime informazioni inerenti una stessa persona, con un evidente risparmio di tempo da parte del personale, che si concretizza, chiaramente, in un risparmio economico. Affinché ciò sia possibile devono tuttavia essere condivisi standard che assicurino l'interope-

[35] Sui sistemi informativi sanitari cfr. B. Blobel, *Analysis, design and implementation of secure and interoperable information systems*, IOS Press, Amsterdam, The Netherlands, 2002; P. Cristiani, F. Pinciroli, M. Stefanelli, *I sistemi informativi sanitari*, Pàtron, Bologna, 1996; E.A. McGlynn, *Health Information Systems: design issues and analytic applications*, RAND Health, Santa Monica, California, 1998.

rabilità di sistemi diversi. Del resto, l'interconnessione delle diverse strutture sanitarie, anche a livello sovranazionale, assume sempre maggiore importanza nell'ambito dell'odierna Società dell'informazione, ove alla mobilità delle persone consegue la necessità di poterne reperire i dati sanitari in caso di necessità in qualsiasi posto esse vengano a trovarsi.

Eppure anche nell'ambito di sistemi sanitari moderni i tempi di comunicazione possono ancora essere assai lunghi: in dottrina è stato affermato che, negli Stati Uniti, l'intera Enciclopedia Britannica può essere trasmessa via Internet in meno di un secondo, ma sono necessarie alcune settimane, se non diversi mesi, per comunicare una malattia contagiosa agli ufficiali sanitari[36], nonostante la mole di dati da trasmettere sia notevolmente inferiore.

Pertanto, il mancato utilizzo delle potenzialità dell'informatica medica può cagionare danni assai gravi, essendo idoneo ad incidere direttamente sul diritto alla salute dei cittadini, che potrebbe essere garantito più efficacemente, ad esempio, mediante l'effettivo utilizzo di sistemi informativi sanitari che consentano un rapido accesso ad informazioni sanitarie già acquisite nelle ipotesi di emergenza (ad esempio, per prestare le cure necessarie in seguito ad eventi traumatici) poiché diviene possibile offrire in tempi celeri cure adeguate al soggetto che ne necessita.

Pertanto, nella creazione di un moderno sistema informativo sanitario bisogna tenere in considerazione diversi profili: l'interoperabilità, al fine di consentirne l'implementazione su sistemi di varia tipologia; la sicurezza dei dati contenuti nel sistema, nel rispetto delle normative sulla protezione dei dati personali; la riduzione dei costi, che dovrebbe conseguire all'utilizzo di un sistema ben realizzato; il trattamento automatizzato dei dati, in modo da renderli facilmente accessibili ed utilizzabili.

---

[36] T.R. Eng, *Population Health Technologies. Emerging Innovations for the Health of the Public*, in *American Journal of Preventive Medicine*, 2004, 3, p. 237.

Uno dei problemi più gravi consiste nella mancanza di uno standard unitario sulla maggior parte di dati clinici, ivi incluse le informazioni relative a procedure, terapie ed analisi di laboratorio[37].

La sicurezza, inoltre, ha un'importanza fondamentale[38], poiché tali sistemi presentano due tipologie generali di vulnerabilità, l'una interna, relativa alle ipotesi in cui i soggetti legittimati all'accesso abusano dei loro privilegi e compiono azioni non autorizzate, e l'altra esterna, da parte di chi effettua un accesso abusivo al sistema a qualsiasi fine (sia esso di danneggiamento, di acquisizione illecita di dati od una semplice bravata). Chiaramente, tanto più i *database* saranno interconnessi nel ciberspazio, tanto più elevata sarà la possibilità che si verifichino atti di *hacking* o di *cracking*[39].

Nella valutazione delle problematiche inerenti la confidenzialità dei dati sanitari entrano tuttavia fattori che non sono direttamente riferiti all'utilizzo o alla presenza degli elaboratori elettronici.

Appare chiaro, dunque, che la riservatezza dei dati sanitari può essere garantita da una condotta improntata a diligenza, prudenza e perizia. Si pone però un problema, giustamente posto in luce dalla

---

[37] D.W. Bates, A.A. Gawande, *Improving Safety with Information Technology*, cit., p. 2532.

[38] Secondo il Gruppo di lavoro costituito ai sensi dell'art. 29 della direttiva n. 95/46/CE, il «quadro giuridico relativo alle misure di sicurezza dovrebbe in particolare prevedere: lo sviluppo di un sistema affidabile ed efficace di identificazione e riconoscimento elettronici, così come registri costantemente aggiornati per verificare la necessaria autorizzazione delle persone che chiedono o hanno accesso ai sistemi di CCE; ampia registrazione e documentazione di tutte le fasi del trattamento che hanno avuto luogo nel sistema, specialmente delle richieste d'accesso per leggere o compilare le cartelle cliniche elettroniche, insieme a verifiche interne regolari e controlli dell'autenticità delle autorizzazioni; meccanismi efficaci di *back-up* e recupero dei dati per rendere sicuro il contenuto del sistema; barriere all'accesso o alla modifica non autorizzati dei dati CCE al momento del trasferimento o dello stoccaggio dei *back-up*, ad esempio usando algoritmi criptografici; istruzioni chiare e documentate per tutto il personale autorizzato su come usare correttamente i sistemi CCE e su come evitare rischi e violazioni della sicurezza; una distinzione chiara delle funzioni e delle competenze delle categorie di persone incaricate del sistema o che come minimo vi partecipano, per poter determinare le responsabilità in caso di problemi; controlli interni ed esterni regolari in materia di protezione dei dati» (Gruppo di lavoro Articolo 29, *Documento di lavoro sul trattamento dei dati personali relativi alla salute contenuti nelle cartelle cliniche elettroniche [CCE]*, 00323/07EN, WP 131, 15 febbraio 2007, p. 20).

[39] National Research Council, *For the Record. Protecting Electronic Health Information*, cit., p. 165.

dottrina italiana, circa il concetto medio di sicurezza, che si identifica, di norma, con la difesa fisica della sicurezza e del patrimonio, mentre la difesa dei dati costituisce un fattore residuale. Pertanto, nel porre eccessivamente l'accento su misure di sicurezza "immateriali" si corre il rischio di pretermettere quelle materiali, magari evitando di proteggere i *server* con severe misure di sicurezza che ne impediscano l'accesso "materiale"[40].

Così, basti pensare ai rischi di violazione della privacy che possono conseguire a gesti semplici come il disfarsi di documenti contenenti dati riservati semplicemente riponendoli fra i rifiuti comuni senza averne prima reso illeggibile il contenuto oppure all'orientamento dei monitor in modo che soggetti diversi dai legittimi utilizzatori possano visualizzarne il contenuto.

Ancora, la protezione dei sistemi informatici da intrusioni telematiche appare superflua qualora vengano trafugati proprio i computer che contengono le informazioni, come è accaduto il 14 dicembre 2002 negli Stati Uniti a danno della "TriWest Healthcare Alliance". Nei computer sottratti erano contenuti dati altamente sensibili, ossia le schede cliniche di oltre cinquecentomila persone che facevano parte del programma del Dipartimento della Difesa TRICARE. Una *class action* avanzata nei confronti della Triwest è stata tuttavia rigettata perché, nonostante non si dubitasse del fatto che i dati sanitari degli interessati fossero usciti al di fuori della sfera di controllo dell'organizzazione che li deteneva, gli attori non avevano fornito la prova di aver subito danni.

Bisogna poi considerare che alla progressiva diffusione di computer portatili e minuscole periferiche di memorizzazione nonché allo svolgimento di attività di ricerca al di fuori del luogo di lavoro, possono conseguire aumentate possibilità di smarrimento di dati sanitari (ad esempio, in seguito al furto del computer portatile sul quale erano state memorizzate le informazioni) e di eventuale acquisizione degli stessi da parte di terzi non autorizzati[41].

---

[40] G. Riem, *Privacy e sicurezza*, Simone, Napoli, 2000, pp. 16-17.

[41] Da una ricerca effettuata nel Regno Unito pochi anni fa è emerso che molti dati venivano effettivamente memorizzati su computer portatili (la ricerca è menzionata in A. Greenhoug, H. Graham, *Protecting and using patient information: the role of the Caldicott Guardian*, cit., p. 248).

Si consideri, però, che sovente il problema principale da affrontare non è la garanzia della sicurezza intrinseca di un sistema informativo, ma piuttosto la condotta dei suoi utilizzatori, i quali dovrebbero ricevere un'adeguata formazione per evitare che si verifichino casi di ingegneria sociale[42] e per maneggiare con la dovuta cura gli apparecchi elettronici.

La vera sfida che si pone per i creatori di sistemi informativi sanitari è, pertanto, fare in modo che le informazioni contenute nei relativi *database* siano accessibili solo da soggetti legittimati[43], solo quando l'accesso sia necessario e senza ritardo nei casi in cui l'accesso è consentito. Il sistema, inoltre, dovrebbe essere abbastanza flessibile da consentire la gradualità nell'accesso in base al grado di delicatezza dei dati sanitari ivi contenuti.

Si consideri, comunque, che oggi le tecnologie informatiche possono garantire elevatissimi standard di sicurezza, che devono però essere affiancati da una continua attività di formazione ed aggiornamento del personale, medico ed amministrativo, nonché di aggiornamenti ai sistemi informativi sanitari medesimi. Ovviamente, nella creazione di un sistema informativo sanitario non si può e non si deve prescindere dal rispetto delle sempre più stringenti normative in tema di protezione dei dati personali, dal momento che i dati sanitari, com'è noto, costituiscono il nucleo più duro dei dati sensibili, e che le sanzioni previste da diverse normative, fra cui quella italiana, sono assai gravose.

---

[42] Con tale espressione si indica «l'uso del proprio ascendente e delle capacità di persuasione per ingannare gli altri, convincendoli che l'ingegnere sociale sia quello che non è oppure manovrandoli. Di conseguenza l'ingegnere sociale può usare la gente per strapparle informazioni con o senza l'ausilio di strumenti tecnologici» (K.D. Mitnick, *L'arte dell'inganno. I consigli dell'hacker più famoso del mondo*, tr. it., Feltrinelli, Milano, 2003, p. 10).

[43] Cfr. A. Lioy, *Riservatezza e sicurezza nei sistemi informativi sanitari*, in P. Cristiani, F. Pinciroli, M. Stefanelli, *I sistemi informativi sanitari*, cit., pp. 143-155. Si pensi a quanto accaduto, in Pakistan, nell'ottobre 2003, quando una donna che lavorava per il Medical Center della University of California in San Francisco aveva minacciato di diffondere su Internet i dati personali dei pazienti se non le fosse stata aumentata la retribuzione: per provare che il pericolo fosse reale, aveva inviato una e-mail allo stesso Medical Center, allegando un file contenente i dati in suo possesso. Tale evento rende evidente la necessità di predisporre sistemi di protezione tali da impedire simili illeciti.

Delle problematiche connesse ai sistemi informativi sanitari in relazione agli *Electronic Health Records*[44] si è occupato anche il Gruppo di lavoro costituito ai sensi dell'art. 29 della direttiva n. 95/46/CE con il "Documento di lavoro sul trattamento dei dati personali relativi alla salute contenuti nelle cartelle cliniche elettroniche (CCE)", adottato il 15 febbraio 2007[45]. In particolare è stato sottolineato che i responsabili dei sistemi nei quali vengono utilizzati cartelle cliniche elettroniche devono rispettare tutti i principi stabiliti dalla normativa sulla protezione dei dati personali[46], considerando specificatamente che in tali casi viene operato un trattamento di dati sensibili.

## 3. *Gli "Electronic Health Records"*

Con l'espressione *Electronic Health Record* (EHR), *Electronic Medical record* (EMR) o "cartella clinica elettronica" (CCE) si indica «una documentazione medica completa o documentazione analoga sullo stato di salute fisico e mentale, passato e presente, di un individuo, in forma elettronica, e che consenta la pronta disponibilità di tali dati per cure mediche ed altri fini strettamente collegati»[47].

In linea generale, la cartella clinica rappresenta un insieme di documenti nei quali viene registrato un complesso eterogeneo di informazioni prevalentemente sanitarie, ma anche anagrafiche, sociali, ambientali e giuridiche relative a un paziente determinato. Essa

---

[44] Su di essi si veda *infra*, § 3.

[45] Gruppo di lavoro Articolo 29, *Documento di lavoro sul trattamento dei dati personali relativi alla salute contenuti nelle cartelle cliniche elettroniche (CCE)*, cit.

[46] Ivi, p. 6.

[47] La definizione è riportata in Gruppo di lavoro Articolo 29, *Documento di lavoro sul trattamento dei dati personali relativi alla salute contenuti nelle cartelle cliniche elettroniche (CCE)*, cit., p. 4. Sugli EHR cfr., fra gli altri, R. Gartee, *Electronic Health Records. Understanding and Using Computerized Medical Records*, Prentice Hall, Old Tappan, New Jersey, 2007; H.P. Lehman *et al.* (ed.), *Aspects of Electronic Health Record Systems*, Springer Science, New York, 2006; J.M. Walker, E.J. Bieber, F. Richards (eds.), *Implementing an Electronic Health Record System*, Springer Science, New York, 2005.

è redatta al fine di dedurre diagnosi e terapia, di predisporre gli opportuni interventi medici nonché di usufruire del suo contenuto per indagini di natura scientifica, statistica o medico-legale[48].

L'art. 92 cod. priv. dispone che nei casi in cui organismi sanitari pubblici e privati redigono e conservano una cartella clinica in conformità alla disciplina applicabile, sono adottati opportuni accorgimenti per assicurare la comprensibilità dei dati e per distinguere i dati relativi al paziente da quelli eventualmente riguardanti altri interessati, ivi comprese le informazioni relative a nascituri. In tal senso, appare chiaro che l'utilizzo di sistemi basati sulle CCE potrebbe assicurare sempre la piena comprensibilità dei dati[49].

L'accesso alla cartella clinica ed all'acclusa scheda di dimissione ospedaliera da parte di soggetti diversi dall'interessato, per presa visione o per ottenere il rilascio di una copia, è possibile solo in fattispecie determinate dalla legge[50].

Le CCE costituiscono una delle più importanti innovazioni che l'informatica può portare alla medicina, poiché grazie ad esse è pos-

---

[48] V. Milana, *La cartella clinica*, in F. Buzzi. P. Danesino (a cura di), *Gli esercenti le professioni sanitarie nel recente riassetto formativo. Interazioni e responsabilità nell'attuale cornice normativa delle aziende sanitarie*, Pavia, 26-27 settembre 2002, Giuffré, Milano, 2003, p. 215.

[49] Il Garante per la protezione dei dati personali, con decisione del 30 settembre 2002, ha, del resto, affermato la sussistenza del diritto alla decifrabilità di una cartella clinica: «poiché la leggibilità dei dati richiesti è la prima condizione, necessaria ancorché non sufficiente, per la loro comprensione, qualora la grafia con cui è stata redatta una cartella clinica non risulti comprensibile per l'interessato, questi ha il diritto di ottenere dall'azienda ospedaliera una trascrizione dattiloscritta o, comunque, comprensibile delle informazioni ivi contenute, che debbono essergli comunicate tramite un medico all'uopo designato» (Bollettino «Cittadini e Società dell'Informazione», 2002, 31, pp. 16-17).

[50] È imprescindibile giustificare simili richieste con la documentata necessità di far valere o difendere un diritto in sede giudiziaria ai sensi dell'art, 26, comma 4, lett. c, cod. priv., di rango pari a quello dell'interessato, ovvero consistente in un diritto della personalità o in un altro diritto o libertà fondamentale e inviolabile; oppure di tutelare, in conformità alla disciplina sull'accesso ai documenti amministrativi, una situazione giuridicamente rilevante di rango pari a quella dell'interessato, ovvero consistente in un diritto della personalità o in un altro diritto o libertà fondamentale e inviolabile. Il cod. priv. non chiarisce se sussistano particolari formalità per l'effettuazione della richiesta o circa il soggetto che autorizza la visione od il rilascio della copia, che dovrebbe dunque individuarsi nel titolare dell'organismo sanitario (in tal senso G. Elli, R. Zallone, *Il nuovo Codice della privacy [commento al D.lgs. 30 giugno 2003, n. 196]*, Giappichelli, Torino, 2004, p. 117).

sibile avere un quadro completo delle informazioni sanitarie relative ad una persona. In linea di principio un EHR dovrebbe infatti racchiudere tutti i dati inerenti un individuo, acquisiti in qualsiasi momento della sua vita. Appare chiaro che, in tal modo, non solo non potranno aversi lacune derivanti dalla perdita di talune informazioni o, al contrario, loro duplicazioni, ma inoltre esse potrebbero essere utilizzate rapidamente anche in caso di emergenza.

Nell'implementazione degli EHR il Gruppo di lavoro costituito ai sensi dell'art. 29 della direttiva n. 95/46/CE, con il citato documento del 15 febbraio 2007, ha evidenziato che è fondamentale garantire l'autodeterminazione del paziente, eventualmente mediante procedure diverse in base alla delicatezza dei dati. Si è così proposto di utilizzare il meccanismo dell'*opt-in* nel caso in cui i dati siano particolarmente sensibili ed il loro trattamento sia potenzialmente assai pregiudizievole, mentre potrebbe essere prescelto l'*opt-out* qualora essi siano meno riservati, il tutto al fine di contemperare riservatezza e flessibilità[51].

Appare inoltre basilare garantire l'affidabilità dell'identificazione dei pazienti: si pensi, infatti, alle conseguenze negative che potrebbero derivare da una errata identificazione, per cui ad un individuo potrebbe essere, in ipotesi, essere attribuito l'EHR di un altro[52]. Inoltre, è indispensabile che le tecnologie di riconoscimento di una persona siano assolutamente certe affinché sia impossibile la verificazione di furti di identità[53].

Purtroppo, però, sorgono anche numerosi problemi sia di carattere bioetico-giuridico che informatico. Bisogna infatti considerare che un EHR può potenzialmente contenere una mole anche assai ingente di dati sensibili, per cui le questioni connesse alla sicurez-

---

[51] Gruppo di lavoro Articolo 29, *Documento di lavoro sul trattamento dei dati personali relativi alla salute contenuti nelle cartelle cliniche elettroniche (CCE)*, cit., p. 14.

[52] In simili ipotesi potrebbero verificarsi addirittura lesioni mortali, come nel caso in cui un paziente sia allergico a determinati farmaci che gli potrebbero essere somministrati qualora ciò non sia riportato nell'EHR scambiato.

[53] Gruppo di lavoro Articolo 29, *Documento di lavoro sul trattamento dei dati personali relativi alla salute contenuti nelle cartelle cliniche elettroniche (CCE)*, cit., p. 14.

za delle trasmissioni elettroniche appaiono assai delicate, come si è visto.

Inoltre, bisogna sottolineare il problema della mancanza di standard comuni che consentano a tutte le periferiche e a tutti i dispositivi di dialogare proficuamente, anche se esso potrebbe essere risolto mediante l'adozione del sempre più diffuso standard HL7 ("Health Level 7"), sviluppato da un'organizzazione senza scopo di lucro[54]. La generalizzata accettazione di uno standard appare fondamentale per garantire una reale interoperabilità fra sistemi diversi e, dunque, garantire CCE realmente adatte alle esigenze di una società sempre più globalizzata.

Si consideri, poi, che EHR correttamente implementati possono migliorare la riservatezza e la sicurezza dei dati relativi allo stato di salute, poiché è possibile adottare tecnologie e procedure per impedire accessi non autorizzati oppure scoraggiare potenziali abusi. In tal modo è possibile utilizzare tecnologie di autenticazione e controllo degli accessi, anche mediante sistemi misti (ad esempio, basati su *physical tokens* e dati biometrici), al fine di garantire l'accesso solo a soggetti legittimati a farlo. Inoltre, grazie a file di *log* è possibile tenere traccia degli eventuali accessi alle informazioni in modo da individuare eventuali abusi e, inoltre, la trasmissione degli EHR può avvenire crittando le informazioni allo scopo di garantire la segretezza e la sicurezza delle comunicazioni[55].

In linea generale, risolte le problematiche di carattere tecnico circa la confidenzialità dei dati contenuti negli EHR, dovrebbe essere consentito l'accesso elettronico diretti dei pazienti alla loro cartella clinica elettronica, anche se è stato rilevato che tale concessione «è una questione di fattibilità medica» e che «il diritto d'accesso associato alla tutela dei dati […] non significa sempre necessariamente un accesso diretto. Un accesso diretto potrebbe, tuttavia, contribuire considerevolmente ad instaurare fiducia verso il sistema CCE»[56].

---

[54] Http://www.hl7.org.

[55] National Research Council, *For the Record. Protecting Electronic Health Information*, cit., pp. 161-162.

[56] Gruppo di lavoro Articolo 29, *Documento di lavoro sul trattamento dei dati personali relativi alla salute contenuti nelle cartelle cliniche elettroniche (CCE)*, cit., p. 16. Tale considerazione sembra confermare quanto affermato in dottrina

Sul punto si può tuttavia rilevare che non garantire un accesso pieno, diretto e gratuito dei pazienti ai propri dati sanitari sembra essere in contrasto con la tendenza ad incentrare l'*e-health* proprio sui bisogni dei destinatari delle cure mediche. Il diritto dovrebbe così adeguarsi ai cambiamenti e alle innovazioni della tecnica facendo sì che la persona umana sia sempre al centro di qualsiasi iniziativa, soprattutto in casi in cui, come quello dell'*e-health*, i benefici sono tanto evidenti ed appare finalmente possibile garantire un efficace diritto al controllo dei propri dati personali.

Ragionare in senso contrario porterebbe a rallentare la rivoluzione tecnologica nell'ambito dell'informatica medica, a detrimento dei diritti dei pazienti e di quei valori di dignità, libertà, uguaglianza, solidarietà, cittadinanza e giustizia sui quali sono improntate sia la Carta dei diritti fondamentali dell'Unione Europea che numerose costituzioni, fra cui quella italiana.

Le scelte legislative e le riflessioni etiche non potranno tuttavia essere slegate dall'osservazione empirica della realtà, ma dovranno tener conto della concreta implementazione di sistemi in cui vengono utilizzati gli EMR. In tal senso appare molto delicato il problema di adottare modalità di conservazione degli EHR che consentano di garantire l'efficienza del sistema e la protezione dei dati personali.

Più specificatamente, gli EHR possono essere archiviati seguendo le alternative principali qui elencate[57]:

– memorizzazione decentralizzata: i dati vengono conservati dagli operatori sanitari e l'accesso viene fornito mediante la CCE. In tal caso l'efficacia del sistema dipende dalle concrete modalità di ricerca;

– memorizzazione centralizzata: il personale sanitario deve trasferire la documentazione in un *database* centralizzato. In tal caso

---

sulle conseguenze dell'emanazione delle normative sulla privacy in ambito medico: «Law's regulation of privacy within medicine goes beyond the allocation of rights and responsibilities within private therapeutic relationship and enhances the power of the state as the broker for information flows within health care settings» (R.S. Magnusson, *The Changing Legal and Conceptual Shape of Health Care Privacy*, in *Journal of Law, Medicine & Ethics*, 2004, 4, p. 681).

[57] Gruppo di lavoro Articolo 29, *Documento di lavoro sul trattamento dei dati personali relativi alla salute contenuti nelle cartelle cliniche elettroniche (CCE)*, cit., pp. 17-18.

ciascuna struttura od operatore sanitario dovrà curare unicamente la fase della trasmissione dei dati, mentre le problematiche di riservatezza e sicurezza delle informazioni memorizzate nel *database* saranno di spettanza del relativo responsabile;

– memorizzazione *on line*: il paziente può gestire le proprie cartelle mediche e memorizzare i propri dati su Internet. In tal caso viene realizzata la piena autodeterminazione dell'interessato, anche se in tal modo si impone al paziente un obbligo di continuo aggiornamento della propria cartella clinica.

Nella concreta implementazione degli EHR non può tuttavia essere pretermessa la visione dei desideri dei pazienti. A titolo esemplificativo, appare utile fare riferimento ad uno studio che risulta interessante sotto il profilo del controllo dei dati personali, seppur limitato ad un campione ridotto e relativo al sistema sanitario del Regno Unito. Nel caso di specie, alcuni pazienti hanno manifestato il proprio disaccordo circa la condivisione di alcune tipologie di dati personali all'interno del "National Care Record"; tali informazioni erano per lo più relative a condizioni di sanità mentale e a problemi inerenti la vita sessuale e gli apparati riproduttivi[58].

Prendendo spunto dai risultati del suddetto studio, può presumibilmente sostenersi che i cittadini non avranno alcuna remora alla costruzione di database centralizzati accessibili nell'ambito del sistema sanitario in pochi secondi solo se il diritto alla privacy sarà realmente ed efficacemente tutelato. Come si è detto, infatti, la violazione del diritto alla riservatezza può cagionare danni irreparabili e rendere impossibile il ripristino della situazione *quo ante* poiché una volta che le informazioni personali sono uscite dalla sfera di controllo dell'interessato o di chi è titolare del trattamento non è possibile ottenere la certezza che esse rimangano private. Nel caso di meri fatti ed accadimenti ciò può risultare legato alla cognizione di uno o più individui, a meno che essi non vengano pubblicamente divulgati e dunque acquisiti da un numero più o meno vasto di persone. Qualora i dati siano resi in formato elettronico, come avviene negli EHR, possono tuttavia esserne effettuate infinite copie e le in-

[58] J. Powell, R. Fitton, C. Fitton, *Sharing electronic health records: the patient view*, in *Informatics in primary care*, 2006, 14, p. 56.

formazioni possono viaggiare, al di fuori di ogni controllo, nei meandri del ciberspazio.

Appare chiaro, dunque, che la garanzia della confidenzialità dei dati appare un presupposto primario per la creazione di sistemi nei quali possano venire realmente utilizzate le CCE in tutto il loro potenziale: nell'ipotesi di sussistenza di diffusi dubbi circa la riservatezza delle informazioni idonee a rivelare lo stato di salute o la vita sessuale non potrebbe certo raggiungersi un consenso sufficiente a rendere effettiva questa nuova evoluzione delle strutture sanitarie di qualsiasi tipologia.

## 4. *La Società dell'informazione e la conoscenza medica nel ciberspazio*

L'informazione di carattere medico, intesa in senso lato, pone, intuitivamente, problematiche assai serie e suscita delicate riflessioni in ambito bioetico-giuridico soprattutto attualizzandola nell'odierna Società dell'informazione. Alle maggiori possibilità di acquisire informazioni, infatti, conseguono dubbi circa l'adeguatezza delle informazioni non solo da un punto di vista quantitativo ma anche qualitativo, considerando che esse possono oggi essere fornite con facilità anche da soggetti non in possesso di cognizioni specifiche, ad esempio mediante un blog.

Analizzando la tematica dal punto di vista del paziente, l'acquisizione delle informazioni può avvenire mediante un intermediario qualificato che comunica direttamente con esso (come il proprio medico) oppure in via indiretta tramite altre fonti (ad esempio, mass media "tradizionali" e non). Nel primo caso, come si è visto, l'informazione assume un'importanza fondamentale nell'ambito del rapporto medico-paziente, poiché solo in seguito ad una corretta e completa informativa resa dal personale sanitario al destinatario delle cure appare possibile prestare un consenso consapevole all'effettuazione di trattamenti medici.

In questa sede, però, si vuole focalizzare l'attenzione sulla sempre più ampia possibilità di acquisire informazioni a carattere sani-

tario da parte di soggetti non operanti nel settore medico o comunque al di fuori delle strutture sanitarie. In tal senso, oggi il maggior impatto sulla generalità delle persone consegue ad informazioni rese dai canali mediatici tradizionali come i giornali e la televisione, ma in tali fattispecie non vi è la certezza che le informazioni mediche, o comunque di interesse per la bioetica, vengano trasmesse con il dovuto dettaglio e scevre da sensazionalismo.

Purtroppo, però, molte informazioni su tematiche assai delicate in ambito bioetico vengono spesso fornite come semplici fatti di cronaca, senza destare ulteriori approfondimenti ma facendo scalpore in virtù della delicatezza delle tematiche trattate, delle quali forse non dovrebbe neanche parlarsi qualora non possano essere analizzate adeguatamente. I tempi del giornalismo, ancor più rapidi di quelli della scienza, non consentono di frenare l'impatto emotivo che può colpire i recettori di notizie che vengono per lo più fornite in maniera breve, immediata e sensazionalistica, per cui dettagli rilevanti vengono sovente tralasciati e pensieri e concezioni di terzi possono facilmente essere travisati.

Il rapporto fra informazione e bioetica appare, così, assai delicato; nel vorticoso susseguirsi di notizie spettacolari può facilmente essere leso il diritto alla riservatezza di persone che si trovano oggetto di attenzione dei mass media, perché casi eclatanti possono venire portati all'attenzione del grande pubblico sia volontariamente che involontariamente[59].

---

[59] Basti pensare alla vicenda, accaduta alcuni anni fa, di un bambino di otto anni affetto da una rarissima forma allergica, tale da impedirgli di portare vestiti, che era stata narrata, con toni scandalistici e corredata da fotografie, sia da un quotidiano locale che da una rivista a diffusione nazionale. Dopo la pubblicazione di tali articoli, l'abitazione della famiglia è stata assediata per circa due settimane da giornalisti e fotografi interessati al caso, impedendo una vita normale sia al bambino che ai suoi familiari. Nel caso di specie, la Corte di Appello di Trieste, con sentenza del 13 gennaio 1993, ha ritenuto che si fosse verificata una grave lesione del diritto alla riservatezza, «inteso nel più ampio senso di diritto al riserbo di certe situazioni personali anche fuori del domicilio domestico», sancendo il diritto del bambino e dei suoi genitori al risarcimento dei danni ingiusti subiti (la sentenza è riportata in *Giurisprudenza italiana*, 1994, I [II], c. 358, con nota di P. Zivіz). Vi sono poi casi, come quello, purtroppo assai celebre, di Theresa Marie (detta "Terri") Schiavo, una donna statunitense che ha vissuto per circa quindici anni in stato vegetativo persistente sino a quando non è stata sospesa la somministrazione dell'alimentazione artificiale. Di tale fatto si è discusso e scritto a lungo, anche se,

Oggi tali problematiche possono accadere non solo in seguito a notizie diffuse da riviste e telegiornali, ma anche per mezzo del ciberspazio, che, come si è visto e com'è noto, costituisce un mezzo formidabile di comunicazione delle informazioni. Attualmente molte risorse mediche sono disponibili *on line*, spaziando dalla vendita di farmaci alla prestazione di servizi, da siti specializzati su determinate patologie a forum di discussione.

In particolare, la mole di informazioni mediche poste su Internet è assai elevata e a ciò corrisponde un notevole interesse da parte di molte persone a conoscere informazioni su patologie, farmaci, diete, medici, strutture sanitarie, e così via[60]: si pensi che già nel 1999 il numero di siti in materia era stato stimato in circa centomila[61], per cui sorgono due delicate problematiche di carattere bioetico: «la necessità di garantire la qualità delle informazioni a cui gli utenti possono accedere e la necessità di formarli affinché possano riconoscere le fonti più autorevoli»[62].

Chiaramente, tanto più il ciberspazio sarà utilizzato per acquisire cognizioni di qualsiasi tipo in ambito medico quanto più critiche saranno le suddette questioni, soprattutto considerando che, in linea generale, è stato osservato che l'accesso alle informazioni mediche *on line* avviene partendo da un motore di ricerca per poi proseguire su più siti e che risulta abbastanza diffusa la tendenza a fare affidamento sulle informazioni reperite nel ciberspazio senza verificare, nella maggior parte dei casi, l'affidabilità della fonte delle informa-

---

insieme ad altre problematiche bioetiche di carattere preminente poiché inerenti allo stesso diritto alla vita che è da considerarsi presupposto degli altri, sorge la problematica di una privacy irrimediabilmente violata.

[60] Ad esempio, da uno studio condotto nell'agosto del 2006 negli Stati Uniti su circa tremila individui è emerso che la percentuale, fra coloro i quali navigano abitualmente su Internet, di chi ha cercato almeno una volta informazioni a carattere sanitario *on line* è di circa l'80% (pari a oltre centodieci milioni di americani); nell'ambito di tale percentuale circa il 7% (pari a circa otto milioni di americani) ha consultato quotidianamente siti relativi a tali argomenti (PEW/Internet, *Online Health Search 2006*, Washington, DC, 2006, in http://www.pewinternet.org).

[61] G. Eysenbach, E.R. Sa, T.L. Diepgen, *Shopping around the Internet today and tomorrow: towards the millennium of cybermedicine*, in *British Medical Journal*, 1999, 319, p. 1294.

[62] Comitato Nazionale per la Bioetica, *Etica, salute e nuove tecnologie dell'informazione*, cit., p. 30.

zioni[63]. Si pensi che talvolta non viene neppure visitata l'*home page* dei siti o le sezioni che spiegano chi li gestisce (generalmente denominate "chi siamo" o, in inglese, *about us*) qualora si arrivi a determinate pagine direttamente dai motori di ricerca[64].

Bisogna tuttavia rilevare che, in diversi casi, tale verifica è in *re ipsa*, ad esempio quando le informazioni siano reperite dai siti ufficiali di strutture sanitarie o da siti che fanno uso di codici di condotta volontari[65] come il ben noto "HONcode"[66], creato dalla "Health On the Net Foundation" per aiutare a standardizzare l'attendibilità delle informazioni sanitarie reperibili sul web ed oggi adottato da oltre cinquemila siti. I siti che recano il logo dell'HONcode dovrebbero rispettare i principi ivi stabiliti, fra cui quello della riservatezza e segretezza dei dati personali inviati al sito dal visitatore. Inoltre, il proprietario di ciascun sito si impone l'obbligo di rispettare o eccedere il livello di tutela offerto dalle leggi che trovano applicazione nel luogo in cui il sito web e i suoi eventuali *mirrors* sono situati.

L'HONcode è stato, tra l'altro, esplicitamente citato dalla Commissione delle Comunità Europee nel 2002, anno in cui è stato emanata la comunicazione sui «criteri di qualità per i siti web contenenti informazioni di carattere medico»[67]. Fra essi rientra la privacy: difatti «la politica in materia di privacy e di protezione dei dati e il sistema di trattamento dei dati personali, incluso il trattamento non visibile agli utenti, devono essere definiti chiaramente secondo la le-

---

[63] PEW/Internet, *Online Health Search* 2006, cit., p. iii.

[64] G. Eysenbach, C. Köhler, *How do consumers search for and appraise health information on the world wide web? Qualitative study using focus groups, usability tests, and in-depth interviews*, in *British Medical Journal*, 2002, 324, p. 576.

[65] «The aim [of the adoption of quality codes] has been generally to educate those who provide information on basic standards of information selection and presentation as well a sto guide users about what to expect and more importantly what to suspect» (P. Wilson, *Sealing in the Quality: A Classification of Quality Assurance Initiatives for Health-Related Information on the Internet*, in S. Callens [ed.], *E-Health and the Law*, cit., p. 58).

[66] Http://www.hon.ch/HONcode/.

[67] Commissione delle Comunità Europee, *Criteri di qualità per i siti web contenenti informazioni di carattere medico*, COM(2002) 667, 29 novembre 2002.

gislazione comunitaria sulla protezione dei dati (direttive 95/46/CE e 2002/58/CE)»[68].

La riservatezza può tuttavia essere lesa anche qualora il ciberspazio sia utilizzato a fini di ricerca medica, come nei casi in cui vengano utilizzate affermazioni fatte da partecipanti in forum di discussione o *newsgroups*. Può infatti capitare che alle esperienze narrate facciano seguito comunicazioni indesiderate circa la possibilità di partecipare a ricerche o che esse vengano utilizzate in ricerche scientifiche. Tuttavia, anche mediante frasi anonimizzate può risalirsi all'autore, qualora esse siano state indicizzate da un motore di ricerca, per cui in seguito a semplici operazioni di trattamento incrociato dei dati risulta possibile, ad esempio, identificare un soggetto eventualmente affetto da una determinata patologia. Ne consegue l'opportunità di acquisire il previo consenso dell'interessato anche prima di utilizzare frasi poste *on line*[69], nonostante in tali casi gli utenti non abbiano certo effettuato delle comunicazioni private o addirittura sottoposte al segreto professionale, come quelle fra medico e paziente.

Bisogna porre dunque la massima attenzione anche nel raccontare nel ciberspazio le proprie esperienze più delicate affinché esse non vengano utilizzate senza consenso oppure costituiscano la falla dalla quale potrebbero trovare ingresso comunicazioni indesiderate. In tal senso assume una valenza fondamentale la possibilità di poter godere di un reale anonimato *on line*, nonostante appaia sempre più una chimera, come si è visto. Eppure proprio la possibilità di restare anonimi può talvolta consentire il pieno esercizio del diritto all'autodeterminazione informativa.

---

[68] Ivi, p. 6. Sotto tale profilo viene poi ulteriormente specificato che «se l'utente di un sito raccoglie ed elabora ulteriormente informazioni personali, compreso il trattamento dei dati non visibile agli utenti, bisogna verificare attentamente i requisiti della direttiva 95/46/CE relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, in particolare l'articolo 8 sui dati sensibili e quelli relativi alla salute, e garantire una conformità totale a tale direttiva» (ivi, p. 8).

[69] G. Eysenback, J.E. Till, *Ethical issues in qualitative research on internet communities*, in *British Medical Journal*, 2001, 323, p. 1105.

Non si può, inoltre, dimenticare che, come si è detto, anche mediante strumenti come i *cookies* risulta possibile acquisire dati relativi ai visitatori di un sito, che possono perdere il proprio anonimato qualora effettuino operazioni come, ad esempio, la comunicazione dei propri dati in seguito alla registrazione al sito medesimo (che può essere richiesta per accedere a sezioni riservate o per leggere o inviare messaggi in un forum di discussione). Si consideri che in tali casi l'utente può essere facilmente profilato e dati sensibili, come quelli idonei a rivelare lo stato di salute e la vita sessuale, possono essere acquisiti in modo più o meno lecito.

Ancor più grave appare, tuttavia, la sempre più frequente prestazione di servizi *on line* consistenti nella effettuazione di test genetici, svolti mediante l'invio di campioni anche assai comuni, come un capello, un fazzoletto usato, una cicca di sigaretta, e così via. Dal momento che tali test possono essere svolti anche all'insaputa del soggetto cui i campioni si riferiscono, può aversi un illecito trattamento di dati sensibili. Ciò appare tanto più grave qualora si consideri questo fenomeno in correlazione al sempre più diffuso utilizzo di strumenti di identificazione basati su caratteristiche biometriche, che in tal modo potrebbero essere facilmente clonate rendendo così possibile realizzare dei furti di identità. In simili ipotesi, il problema è che la perdita del controllo sui dati genetici ha conseguenze irreversibili, perché essi sono inscindibilmente legati ad una persona che sempre più sta diventato elettronica e da essi, oltretutto, se ne possono ricavare altri, relativi alla propria "famiglia genetica".

In tal senso, alla globalizzazione della società potrebbe corrispondere una bioetica che, pur nelle differenze, risulti quanto meno unitaria su alcuni diritti fondamentali. Del resto, sia la ricerca scientifica che quella medica hanno ormai rilevanza e diffusione internazionale, per cui la bioetica dovrebbe avere il difficile compito di orientare il progresso scientifico affinché sia rispettoso dei valori fondamentali della persona ovunque essa sia, ivi compreso il ciberspazio.

Ciò può essere possibile solo qualora si verifichi una presa di coscienza globale di alcune problematiche nonché della necessità di riconoscere e tutelare efficacemente alcuni diritti fondamentali. In

proposito si può osservare che il riconoscimento del diritto alla privacy non sembra ormai messo in discussione, come risulta dall'attenzione che trova in trattati, convenzioni e normative nazionali e internazionali.

## Capitolo V

# LA PRIVACY GENETICA FRA BIOETICA E DIRITTO

## 1. *Aspetti generali*

Il percorso di ricostruzione delle varie sfaccettature del diritto alla privacy nell'ambito della società contemporanea ha consentito di verificare sino a che punto ed in quale misura diritto, tecnica ed etica influiscano sul concreto atteggiarsi delle sue nuove valenze e delle sue molteplici specificazioni.

Dinanzi ai numerosi tentativi di controllo e di illecita acquisizione di dati personali l'effettivo riconoscimento del diritto alla riservatezza consente di tutelare la persona dalla sempre maggiore invasività di soggetti pubblici e privati che vogliono rendere sempre più l'individuo un "uomo di vetro", perennemente esposto agli indiscreti sguardi altrui.

Tale efficace espressione sembra attagliarsi perfettamente al profilo forse più intimo: quello della privacy genetica. L'uomo può modificare le proprie convinzioni, il proprio aspetto, il proprio stile di vita; altrettanto non può fare con il suo patrimonio genetico, che è indissolubilmente legato non solo alla corporeità propria, ma addirittura a quella del proprio nucleo familiare (la propria "famiglia genetica") ed al ceppo di appartenenza, per cui accanto al concetto di "salute personale" si affianca quello di "salute familiare"[1].

Il patrimonio genetico, infatti, è sempre uguale a se stesso per l'intero arco della propria vita biologica dell'individuo; addirittura esso è "immortale", perché sopravvive alla vita della persona e ai

[1] A. Conti *et al.*, *I test genetici. Etica, deontologia, responsabilità*, Giuffré, Milano, 2007, p. 5.

suoi caratteri biologici (che appartengono alla linea somatica della persona), potendo essere individuato da parti del suo corpo che non devono necessariamente essere in vita[2].

I dati genetici, così, sono tutti quelle informazioni, «di qualunque tipo, che riguardano i caratteri ereditari di un individuo o che sono in rapporto con quei caratteri che formano il patrimonio di un gruppo di individui affini»[3].

Inoltre, i dati genetici non solo possono essere ottenuti facilmente da materie biologiche anche di dimensioni ridottissime (residui di cellule epiteliali, capelli, ecc.), ma potranno rivelare in futuro molte più informazioni di quante ne forniscono oggi, grazie all'evoluzione continua del progresso scientifico.

Non a caso, dunque, le informazioni genetiche, nell'ambito di quel "nucleo duro" dei dati personali costituito da quelli sensibili, vengono correntemente definite come il "nucleo più duro" della riservatezza, poiché alla loro conoscenza o diffusione possono conseguire discriminazioni in diversi ambiti, che spaziano da quello lavorativo a quello sociale, qualora si dia importanza alla difformità di individui o collettività da certi standard medici o genetici.

Del resto, è nella storia recente che troviamo sanguinari esempi di discriminazione verso determinati gruppi sociali, come l'Olocausto oppure la pulizia etnica nell'ex Jugoslavia avvenuta negli anni Novanta. L'illecita acquisizione di dati genetici da parte di criminali o terroristi, inoltre, potrebbe essere idonea ad aumentare il pericolo di "vulnerabilità sociale", inteso come rischio che interi gruppi di persone potrebbero essere presi di mira da malintenzionati per le caratteristiche genetiche comuni.

Quanto detto non implica una valutazione negativa della ricerca genetica, per quanto essa ponga numerosi e delicati interrogativi per la bioetica e per il diritto[4]. Ciò nondimeno, grazie ai progressi effet-

---

[2] Cfr. S. Rodotà, *Tecnologie e diritti*, Il Mulino, Bologna, 1995, p. 208.

[3] Raccomandazione n. R (97) 5 del Consiglio d'Europa.

[4] Del resto, «il progresso scientifico si evidenzia in maniera particolare nell'ambito della genetica, ingenerando reazioni personali, bilanciate tra fiducia, attesa di sempre nuove possibilità e timore per le eventuali applicazioni non più solo futuribili» (A. Di Giandomenico, *La genetica e l'evoluzione del diritto*, in A. Tarantino [a cura di], *Filosofia e politica dei diritti umani nel terzo millennio. Atti*

tuati *in subiecta materia* appare possibile scoprire l'origine genetica di specifiche caratteristiche (positive o negative) di un organismo e, dunque, prevedere l'eventuale insorgenza di patologie in un futuro più o meno prossimo, grazie all'acquisizione ed all'analisi di dati relativi alla componente più intima di ciascun individuo[5].

Oggi, però, non è possibile unicamente effettuare delle previsioni, ma altresì intervenire sul patrimonio genetico grazie agli studi compiuti nell'ambito dell'ingegneria genetica. Con tale espressione si indicano le modificazioni artificialmente indotte nell'informazione genetica di una cellula tramite l'introduzione in essa di altre informazioni genetiche[6]. Le finalità dell'ingegneria genetica possono essere diagnostiche, terapeutiche, produttive (di animali, di piante, di proteine) e alterative (di esseri umani e animali; potrebbero essere addirittura creati ibridi uomo-animale)[7].

---

*del V congresso dei filosofi politici italiani*, Lecce, 13-14-15 aprile 2000, Milano, 2003, p. 509).

[5] La ricerca genetica si è sviluppata nel corso di pochi decenni, successivamente alla scoperta della struttura a doppia elica del DNA da parte di James Watson e Francis Crick (J.D. Watson, F.H. Crick, *A structure for desoxyribose nucleic acids*, in *Nature*, 1953, 171, pp. 737-738).

[6] Le tecniche di ingegneria genetica possono così suddividersi, in base alla loro finalità: mappatura (localizzazione dei geni, dei quali sono conosciuti i prodotti o gli effetti, sui cromosomi), isolamento (separazione in punti precisi della catena del Dna, rendendo riconoscibili quelli interessanti), clonaggio (riproduzione di un determinato gene, tramite l'inserimento di esso nel patrimonio genetico di microrganismi, la cui successiva moltiplicazione porta anche alla riproduzione del gene inserito), sequenziamento (consente di conoscere l'esatta successione delle basi di cui sono composti i singoli geni) e trasferimento (studia il comportamento di geni inseriti in cellule e tessuti diversi da quelli in cui normalmente agiscono).

[7] Sempre più insistentemente si parla di un c.d. diritto ad ereditare un patrimonio genetico non modificato, dopo che gli sviluppi della ingegneria genetica hanno reso possibili tecniche manipolative del Dna. Questo diritto è stato sancito dall'Unione Europea già il 26 gennaio 1982, con la raccomandazione n. 934, nella quale si afferma che i diritti alla vita e alla dignità umana implicano il diritto di ereditare caratteristiche genetiche che non abbiano subito alcuna manipolazione. La giustificazione del suo riconoscimento viene da taluni individuata nel rispetto della dignità della persona, che esigerebbe il rispetto del diritto della persona alla "differenza genetica", ossia a non essere sconvolta nella sua identità e unicità biologica. Ciò vieterebbe qualunque politica di programmazione biologica tendente a progettare i futuri individui in via artificiale addirittura al livello più intimo possibile.

L'utilizzo delle tecniche di ingegnera genetica consente di conoscere la struttura e la natura dei geni, di identificare i geni patogeni sia prima che dopo l'insorgenza di certe malattie, di produrre anche in scala industriale molecole utili per l'uomo (come insulina, ormone della crescita, vaccini, ecc.) e di produrre vegetali e animali geneticamente modificati per ottenerne caratteristiche che consentano di migliorarne lo sfruttamento industriale (ad esempio, piante che consentano raccolti più abbondanti o specie animali maggiormente resistenti alle malattie).

Le potenzialità di simili studi appaiono infinite e altamente promettenti, ma non si può certo ritenere che le motivazioni delle condotte umane siano scritte nei geni stessi. Il concreto esplicarsi della personalità dell'uomo è infatti dovuto al concorso di una molteplicità di fattori, sia genetici che ambientali, non prevedibili a priori, per cui le notizie che sovente vengono fornite dai mass media circa la scoperta dei geni che causano, ad esempio, la schizofrenia o l'alcolismo, costituiscono chiari esempi di disinformazione, poiché sembrano far ritenere che determinate condotte non siano libere, ma piuttosto compiute in esecuzione di qualcosa che è già scritto nel proprio patrimonio genetico[8].

Fortunatamente, però, l'incidenza dei fattori genetici sull'esistenza umana non è così elevata: in caso contrario dovrebbe ritenersi che la divisione della società in classi sia la soluzione eticamente più corretta, nonché quella più "giusta".

Si comprende, dunque, la necessità di garantire un'informazione che sia libera da sensazionalismi ed eccessive semplificazioni affinché chi non è esperto del settore possa comunque comprendere rischi e benefici di tecnologie e metodologie che potranno avere un impatto, anche profondo, sia sull'esistenza individuale che sul futuro sviluppo della società.

---

[8] C. Queiroz, *The human genome project some social and eugenic implications*, in *Global bioethics*, 1997, 10, 1-4, p. 98. In tal senso anche Q. Renzong, *Human genome and philosophy: What ethical challenge will human genome studies bring to the medical practices in the 21st century?*, in *Life Sciences*, 2001, 324, pp. 1097-1102. Autorevole dottrina ha criticato l'erroneità di un approccio riduzionistico che «risolve l'individuo nella biologia e trascura la biografia» (S. Rodotà, *Sul buon uso del diritto e i dilemmi della clonazione*, in *Rivista critica del diritto privato*, 1999, 4, p. 566).

Un simile obbligo di carattere etico sussiste nei confronti dei mezzi di comunicazione di massa, ma anche e soprattutto verso ricercatori e studiosi. Difatti, chi pratica la scienza dovrebbe sentire la responsabilità di informare chi non la pratica e di fargli capire i problemi (etici e non) sempre più complessi che lo circondano, infondendo fiducia nella scienza, che ha un ruolo fondamentale nel processo evolutivo della società[9]. Anzi, essi stessi dovrebbero stimolare una riflessione interdisciplinare, che coinvolga la bioetica ed il diritto, sull'evoluzione della ricerca scientifica.

Tali considerazioni assumono un'importanza ancora maggiore nelle fattispecie in cui sono coinvolte tecniche di ingegneria genetica, grazie alle quali gli scienziati non solo possono effettuare nuove scoperte, ma addirittura creare delle vere e proprie invenzioni, consistenti nella creazione di nuove cellule con corredo genetico modificato.

In tale ambito il diritto dovrebbe operare una razionalizzazione del presente senza però trascurare la programmazione del futuro, poiché al celere avanzamento della scienza biomedica consegue una trasformazione del "futuribile" in "futuro" e del "futuro" in "presente"[10].

Si consideri, oltretutto, che la ricerca è finanziata sia da fondi privati che pubblici, per cui appare chiaro che l'attività di ricerca scientifica, per quanto libera, non dovrebbe certo essere segreta, anche perché essa interviene in una realtà complessa, nel cui ambito è solo uno dei fattori, seppur importante, che la caratterizzano e che appare idonea a scuotere le coscienze.

Basti pensare a quanto accaduto nel 1997 con la prima clonazione mai effettuata su un mammifero, ossia la ben nota pecora denominata Dolly. Anche se questi procedimenti non sembra siano stati realmente effettuati sull'uomo, l'evento ha provocato sconcerto e

---

[9] S. Piazza, *Il progetto genoma umano e la responsabilità del genetista*, in C.M. Mazzoni (a cura di), *Etica della ricerca biologica*, Olschki, Firenze, 2000, p. 34. Sul punto cfr. anche E. Agazzi, *La filosofia di fronte al problema delle manipolazioni genetiche*, in *Iustitia*, 1985, 1, pp. 159-189.

[10] In tal senso F. Mantovani, voce *Manipolazioni genetiche*, in *Digesto delle discipline penalistiche*, Utet, Torino, 1995, VII, p. 541.

discussioni nel mondo intero, soprattutto riguardo alla liceità di simili operazioni.

Lo specifico profilo della privacy genetica risulta però maggiormente colpito da un altro progetto che ha avuto ampia risonanza, ossia il c.d. "Progetto Genoma Umano", in seguito al quale è stato completato il sequenziamento dell'intero Dna umano[11]. Finalità del "Progetto Genoma Umano" è l'identificazione, la localizzazione e il sequenziamento dei singoli geni e la determinazione della loro funzione, in modo da arrivare ad una dettagliata conoscenza del genoma che consenta di intervenire direttamente sul Dna per fini diagnostici e terapeutici.

Esso ha avuto inizio nel 1990, grazie alla creazione di un consorzio multinazionale coordinato dal "Department of Energy" e dal "National Institute of Health" (entrambi statunitensi). Successivamente, anche un'azienda privata, la "Celera Genomics", ha iniziato un progetto avente il medesimo scopo, seppur utilizzando una metodologia più rapida anche se meno precisa[12], e ciò ha comportato un acceleramento del progetto pubblico[13], tanto che una prima boz-

---

[11] Esso è stato definito è l'emblema della «rivoluzione biotecnologia», «destinata ad apportare importanti mutamenti di ordine concettuale, culturale e sociale» (E. Brovedani, *La decifrazione del genoma umano. Aspetti scientifici e implicazioni etiche*, in *Aggiornamenti sociali*, 2000, 9/10, p. 670). Su di esso cfr., altresì American Society of Human Genetics, American College of Medicine Genetics, *The Human Genome Project: implications for human genetics*, in *The American Journal of Human Genetics*, 1991, 49, pp. 687-691, e Comitato Nazionale per la Bioetica, *Progetto genoma umano*, Roma, 1994.

[12] Il metodo seguito dalla Celera per sequenziare il genoma umano è il c.d. *whole genome shotgun*, consistente nel frammentare l'intero genoma in sequenze casuali che sono successivamente clonate. Ogni clone viene sequenziato e il termine di ognuno di essi dovrebbe coincidere con l'inizio di un solo altro clone a causa della loro sovrapposizione. Infine, un *software* proprietario si occupa del sequenziamento di migliaia di cloni in un unico e completo genoma. Con questo *modus operandi*, tuttavia, si rischia di lasciare molti *gap* fra le sequenze ed inoltre, dato che nel genoma umano vi sono molte sequenze ripetute, potrebbero mancare gli indicatori necessari per porre i numerosissimi frammenti nell'ordine corretto.

[13] La procedura utilizzata prevede la creazione di una mappa dettagliata che costituisce la struttura per il successivo sequenziamento del Dna. Successivamente sono stati generati numerosi marcatori del Dna, ossia segmenti con una locazione identificabile sul cromosoma. Queste prime sequenze sono state a loro volta suddivise in frammenti più piccoli, che sarebbero dovuti essere stati sequenziati sistematicamente per giungere ad una sequenza assai accurata e con pochi *gap*. Nel 1998, probabilmente a causa della nascita della Celera, si scelse invece di

za del genoma umano è stata pubblicata sulle riviste «Nature»[14] e «Science»[15] già nel 2001.

Tuttavia, da un punto di vista tecnico, è d'uopo sottolineare che l'avvenuto sequenziamento del genoma non è sufficiente a fornire le cognizioni necessarie per giungere alla definizione di diagnosi e di terapie generalmente efficaci, ma grazie ad esso sono stati individuati circa 1.800 geni responsabili di altrettante patologie ed oltre 350 prodotti biotecnologici, attualmente in fase di *clinical trial*, sono basati proprio sui risultati del suddetto progetto[16].

Il successivo obiettivo, ancora più difficile, è quello di decifrare il codice appena svelato e svolgere una difficile attività di ricerca su ogni gene, sul suo funzionamento, sull'incidenza reciproca fra geni diversi e sull'impatto delle variabili ambientali. L'attività di ricerca scientifica in materia, dunque, continua, e nei prossimi anni i risultati saranno probabilmente sotto gli occhi di tutti, tanto che il "National Institute of Health" prevede che sarà possibile effettuare il sequenziamento completo del genoma di un individuo a costi assai bassi, addirittura inferiori al migliaio di dollari statunitensi[17].

Il Progetto Genoma Umano ha tuttavia portato con sé diverse problematiche etiche e giuridiche, che spaziano dalla privacy genetica alle problematiche di diritto d'autore, dalla clonazione all'eugenetica. Proprio per studiarne le conseguenze a livello etico, legale e sociologico è stato così intrapreso nel 1990 il progetto ELSI (*Ethical, Legal and Social Implications*) in seno al Progetto Genoma Umano[18].

---

raccogliere solo dati parziali da ogni frammento di Dna, con la conseguenza di giungere ad una "bozza" che copre il 95% del genoma e che ha un'accuratezza del 99%, ma che è divisa in molti segmenti non ordinati e in alcuni casi separati. Con un successivo sequenziamento si può giungere ad una sequenza completa del Dna con un'accuratezza del 99,9%.

14 Numero speciale, 16 febbraio 2001.

15 Numero speciale, 15 febbraio 2001.

16 National Institute of Health, *Human Genome Project. Fact Sheet*, in http://www.nih.gov/about/researchresultsforthepublic/HumanGenomeProject.pdf, p. 1.

17 Ivi, p. 2.

18 Cfr. F.S. Collins *et al.*, *A vision for the future of genomics research. A blueprint for genomic era*, in *Nature*, 422, 2003, pp. 1-13.

Del resto, bisogna considerare che, in linea di principio, l'ingegneria genetica porta con sé problemi che toccano l'etica e diversi settori del diritto, sia nell'ambito del diritto privato (tutela dei diritti dei ricercatori e degli inventori di nuovi prodotti e/o metodi scientifici) che del diritto pubblico e del diritto penale (controllo della diffusione di specie modificate per valutarne l'impatto ambientale e repressione delle eventuali violazioni)[19], fermo restando che le maggiori criticità ineriscono il settore dell'ingegneria genetica applicata all'uomo.

La necessità di una riflessione etica su tali delicati profili, comunque, non implica comunque una valutazione negativa dell'ingegneria genetica in sé e per sé considerata, visti gli enormi benefici che in futuro potranno aversi: basti pensare alla possibilità di eliminare eventuali malformazioni. La ricerca scientifica in tale settore non può quindi essere ostacolata, ma non costituisce l'unico interesse da tutelare ed è inserita in una società sempre più complessa, per cui l'uso delle tecnologie dovrebbe essere sempre preceduto da un'adeguata riflessione sui loro benefici e sui loro potenziali risvolti negativi[20].

Appare necessario, quindi, non dimenticare che non tutto ciò che la tecnica consente di fare sia lecito, confondendo fra fini e mezzi, poiché fini astrattamente leciti possono essere raggiunti con mezzi illeciti, e viceversa. La tendenza più moderna in ambito scientifico, però, sembra oggi essere quella dell'esasperazione del mezzo, dal momento che i fini sembrano essere dettati dai mezzi e la ricerca sembra quasi voler costituire un mondo a sé, non regolamentato dal diritto, unicamente pronta ad accettare quei principi etici emersi unicamente nel proprio ambito.

«Il problema, infatti, non è quello della imperfezione della tecnica, quanto piuttosto quello della liceità o opportunità dell'utilizzo della tecnica stessa dando per scontato che essa sia pervenuta o possa pervenire ad un livello altamente perfezionato, insuscettibile di

---

[19] F. Mastropaolo, voce *Ingegneria genetica*, in *Digesto delle discipline privatistiche*, sezione civile, Utet, Torino, 1999, IX, p. 430.

[20] M. Salvi, *Biotecnologie e bioetica, un ritorno alla metafisica? Terapia genica in utero, clonazione umana e lo statuto morale dell'embrione*, in *Rivista critica del diritto privato*, 1999, 4, p. 594.

dar luogo a effetti indesiderati. Si tratta evidentemente di problemi che toccano il rapporto tra la scienza, e l'uso delle sue "invenzioni", e l'etica con ricadute sul giuridico e sul politico»[21].

## 2. *La medicina predittiva, i diritti di sapere e di non sapere, la consulenza genetica*

La medicina predittiva consente di sapere se persone sane presentano mutazioni che predispongono allo sviluppo di determinate patologie, mediante l'esecuzione di test genetici che permettono di identificare il gene cui imputare la suscettibilità ereditaria a determinate malattie.

La sempre maggiore diffusione della medicina predittiva è dovuta alla diffusione ed all'evoluzione della ricerca scientifica nel campo della genetica, cui consegue una espansione dell'ambito di operatività della medicina tradizionale, inizialmente focalizzata sull'aspetto curativo, ossia su interventi posti in essere successivamente all'insorgenza delle patologie, e poi affiancata dalla medicina preventiva, il cui scopo è prevenire le malattie stesse. La medicina predittiva va oltre, poiché valuta il rischio che grava su un determinato individuo di contrarre la malattia associata alla mutazione di cui è portatore.

In linea generale, i test genetici predittivi «consentono di individuare genotipi che di per sé non determinano la comparsa di una malattia, ma che in seguito all'esposizione a fattori ambientali, oppure in seguito ad altri fattori genetici scatenanti comportano un aumento del rischio (*suscettibilità*) di comparsa di una determinata patologia»[22].

Nasce, dunque, un vero e proprio "potere di predire", cui in ipotesi può conseguire la possibilità di controllare i consociati a seconda dei profili genetici individuati in maniera predittiva. Le categorie sociali, così, possono essere distinte in base alla caratteristiche gene-

---

[21] T. Serra, *L'uomo programmato*, Giappichelli, Torino, 2003, p. 115.

[22] A. Conti *et al.*, *I test genetici. Etica, deontologia, responsabilità*, cit., p. 12.

tiche, la cui conoscenza può essere sfruttata per finalità sociali, amministrative e lucrative.

Tuttavia la medicina predittiva consente di conoscere la probabilità, non la certezza, di contrarre una determinata patologia, poiché, come si è detto, la molteplicità di fattori che possono concorrere nei casi di specie non consente di raggiungere, in linea generale, risultati sicuri. Si pensi, del resto, all'impossibilità *de facto* di valutare l'incidenza di un numero indeterminato di fattori ambientali aleatori, che dunque possono non verificarsi. Considerando l'enorme divario sussistente fra le possibilità predittive e quelle terapeutiche, per cui di molte malattie si può prevedere la possibile insorgenza, anche in un futuro remoto, senza che, allo stato attuale della medicina, vi siano però cure che consentano di debellarle, sorge dunque il delicato problema di capire se, accanto al diritto di sapere, ne sia prospettabile anche uno di non sapere[23] e, in caso positivo, come essi vadano bilanciati per stabilire la prevalenza dell'uno sull'altro.

Entrambi i diritti sono esplicitamente sanciti dalla Convenzione di Oviedo, il cui art. 10, comma 2, dispone che «ogni persona ha il diritto di conoscere ogni informazione raccolta sulla propria salute. Tuttavia, la volontà di una persona di non essere informata deve essere rispettata» e nello stesso senso è anche l'art. 5, lett. c, della *Dichiarazione universale sul genoma umano e i diritti umani*.

Proprio la mancanza di eventuali terapie efficaci spinge verso l'astratta desiderabilità di un diritto di "non sapere" di eventuali probabilità di contrarre una determinata patologia[24], poiché alla mera possibilità che essa insorga fa da contraltare un potenziale turbamento del proprio diritto all'autodeterminazione esistenziale, tanto più gravoso quanto più alta è la percentuale risultante dal test. Così alcuni potrebbero subire un profondo stress emotivo e non vivere pienamente la propria vita solo perché, in seguito ad un test, sussiste

---

[23] Sul diritto di non sapere cfr., fra gli altri, G.M. Pizzuti, *Il diritto di non sapere. Lo specifico dell'uomo bioetico*, La città del sole, Napoli, 2006.

[24] «Il diritto a non sapere confligge con il principio di responsabilità, ma è certamente un aspetto del diritto alla libera autodeterminazione nelle proprie scelte di vita (C. Faralli, *Dati genetici e tutela dei diritti*, in F. Lanchester, T. Serra [a cura di], *"Et si omnes…". Scritti in onore di Francesco Mercadante*, Giuffré, Milano, 2008, p. 406).

la possibilità di contrarre patologie assai gravi: il tutto in virtù del fatto stesso di essere "malati di rischio"[25].

La grande eterogeneità ravvisabile nelle condotte umane, tuttavia, può far ipotizzare che alcuni, venendo a conoscenza della futura possibilità, più o meno elevata, dell'insorgenza di determinate malattie, possano modificare anche in senso migliorativo la propria esistenza. In altri termini, vi sarà chi, ad esempio, potrebbe addirittura perdere la voglia di vivere, rinunciando a costituire una famiglia per il timore di doverla abbandonare troppo presto ed in maniera tragica, oppure chi non si lascerà influenzare da un test probabilistico e magari sarà convinto che in futuro saranno sviluppate delle terapie che consentano di debellare quella specifica malattia; ancora, alcuni cercheranno di vivere più intensamente la propria vita, concentrandosi su progetti non a lungo bensì a medio termine.

Tali esemplificazioni rendono palese come a questa problematica sia assai difficoltoso fornire risposte che consentano di cogliere le infinite sfumature che vengono a crearsi ed appare assai difficoltoso riuscire a garantire la libertà e la consapevolezza della scelta circa l'esercizio del diritto di sapere o di non sapere. Oltretutto, bisogna pur considerare che in taluni casi l'esercizio del diritto di non sapere dovrebbe essere limitato qualora l'esito di un test possa riverberarsi su altre persone perché, ad esempio, una determinata patologia potrebbe essere contagiosa, per cui al diritto di non sapere di un soggetto può contrapporsi quello di sapere di un altro, che, nel caso di specie, deve essere ritenuto prevalente perché necessario per tutelare il proprio diritto alla salute.

Le considerazioni sin qui esposte non dovrebbero far ritenere che sia più desiderabile sancire un generalizzato divieto di effettuare test genetici predittivi, in modo da eliminare il conflitto fra i suddetti diritti, qualora non vi siano terapie che consentano di debellare le patologie individuabili mediante i medesimi test. Sarebbe opportuno, comunque, stabilire delle linee guida, dandone ampia conoscibilità alla cittadinanza, che permettano a chiunque di avere il controllo dei propri dati personali in qualsiasi momento, poiché non è det-

[25] Sul punto cfr. M. Tamburini, A. Santosuosso (a cura di), *Malati di rischio. Implicazioni etiche, legali e psicologiche*, Masson, Milano, 1999.

to che chi è gravemente ammalato o chi potrebbe esserlo non voglia conoscere il proprio stato di salute. Il diritto di non sapere dovrebbe essere manifestato esplicitamente o al più mediante procedure di silenzio-assenso, purché esse siano ben note.

Per risolvere le suddette problematiche, a parere dello scrivente si potrebbe prospettare la creazione di un *database* informatizzato, gestito da un soggetto pubblico, nel quale archiviare i risultati dei test qualora essi sanciscano la suscettibilità genetica verso determinate patologie, garantendo in ogni caso la massima riservatezza possibile mediante l'adozione di misure di sicurezza allo stato dell'arte ed opportune garanzie giuridiche affinché tali dati non vengano utilizzati da alcun soggetto pubblico o privato. In tal modo i risultati potrebbero essere comunicati a ciascun interessato solo qualora vengano create terapie efficaci; il processo potrebbe essere automatizzato grazie a sistemi informativi sanitari basati su cartelle cliniche elettroniche. Il tutto potrebbe essere realizzato mediante un sistema costituito da due database generali: l'uno contenente i risultati dei test, l'altro l'elencazione delle patologie curabili ed incurabili. Il sistema potrebbe occuparsi, automaticamente, di effettuare un trattamento incrociato fra i due *database*.

Sino alla creazione di un simile sistema, o di altre soluzioni che consentano di risolvere le delicate problematiche sin qui esposte, appare tuttavia utile far riferimento alla realtà giuridica e fattuale oggi esistente.

In Italia bisogna menzionare il Codice di deontologia medica, approvato dalla Federazione nazionale degli ordini dei medici chirurghi e degli odontoiatri del 16 dicembre 2006, il cui art. 44, commi 1 e 2, dispone che «i test diretti in modo esclusivo a rilevare o predire malformazioni o malattie su base ereditaria, devono essere espressamente richiesti, per iscritto, dalla gestante o dalla persona interessata. Il medico deve fornire al paziente informazioni preventive e dare la più ampia ed adeguata illustrazione sul significato e sul valore predittivo dei test, sui rischi per la gravidanza, sulle conseguenze delle malattie genetiche sulla salute e sulla qualità della vita, nonché sui possibili interventi di prevenzione e di terapia». Tale disposizione denota l'attenzione verso il profilo informativo dei test genetici predittivi, in virtù della loro delicatezza. Essi, infatti, non

possono essere svolti con leggerezza, dal momento che, come si è visto, le loro implicazioni negative sono alquanto delicate.

Degno di menzione è anche il comma 3 del suddetto articolo, ai sensi del quale «il medico non deve eseguire test genetici o predittivi a fini assicurativi od occupazionali se non a seguito di espressa e consapevole manifestazione di volontà da parte del cittadino interessato che è l'unico destinatario dell'informazione». Tale norma, tuttavia, potrebbe essere elusa qualora un datore di lavoro dovesse spingere un proprio dipendente o aspirante tale ad effettuare comunque il test e a comunicargli i risultati. Ovviamente, però, sui medici non potrebbe gravare l'onere di verificare la possibilità che sussistano simili fattispecie.

Bisogna, poi, accennare al comma 4 del medesimo articolo, che così dispone: «è vietato eseguire test genetici o predittivi in centri privi dei requisiti strutturali e professionali previsti dalle vigenti norme nazionali e/o regionali». Tale richiamo appare importante soprattutto qualora venga letto nella prospettiva di una Società dell'informazione nel cui ambito il ricorso a determinati settori della medicina può diventare sin troppo facile: su Internet, infatti, non è "solo" possibile acquistare farmaci senza prescrizione medica, ma addirittura richiedere l'effettuazione di test genetici (per quanto i campioni debbano comunque essere sempre inviati con i mezzi materiali "tradizionali")[26]. Sul punto appare opportuno ribadire che le implicazioni di tali test sono potenzialmente idonee a riverberarsi non solo sul soggetto richiedente, ma anche sulla propria famiglia genetica in virtù delle peculiarità dei dati genetici, essendo gli stessi riferibili a più persone.

Accanto a tale previsione specificatamente relativa allo situazione italiana si pone anche la disciplina di carattere internazionale di cui alla già citata Convenzione di Oviedo. Più specificatamente, l'art. 12 dispone che «si può procedere a test predittivi di malattie genetiche o che permettono di identificare il soggetto come portatore di un gene responsabile di una malattia, ovvero di rivelare una

[26] La dottrina ha ribadito la necessità di adottare la massima cautela possibile nell'invio dei campioni, mediante un'informazione preventiva circa le modalità e le finalità del loro trattamento (P.A. Roche, G.J. Annas, *Dna Testing, Banking, and Genetic Privacy*, in *The New England Journal of Medicine*, 2006, 355, 6, p. 546).

predisposizione o una sensibilità genetica a una malattia, solo a fini medici o di ricerca legata alla tutela della salute, e previa appropriata consulenza genetica».

Tale disposizione, dunque, pone l'attenzione sulla necessità e sull'estrema utilità della consulenza genetica, ossia «il processo di comunicazione consistente nell'aiutare l'individuo o la famiglia colpita da patologia genetica a comprendere le informazioni mediche che includono la diagnosi e il probabile decorso della malattia, le forme di assistenza disponibili, il contributo dell'ereditarietà al verificarsi della malattia e il rischio di ricorrenza esistente per sé e per altri familiari, nonché tutte le opzioni esistenti nell'affrontare il rischio di malattia e l'impatto che tale rischio può avere su scelte procreative; a tale processo partecipano, oltre al medico e/o al biologo specialisti in genetica medica, altre figure professionali competenti nella gestione delle problematiche psicologiche e sociali connesse alla genetica»[27].

La consulenza genetica, dunque, assume un'importanza fondamentale prima e dopo lo svolgimento di test genetici, siano essi predittivi e non[28], e dovrebbe essere «non direttiva» e «assolutamente neutrale»[29]. Secondo la Commissione Europea, essa «è un requisito fondamentale per alcuni test genetici, in particolare per i test genetici altamente predittivi di patologie gravi»[30].

Nella prima fase, preliminare all'effettuazione del test, appare assolutamente necessario, anche da un punto di vista etico, fornire un'informativa che permetta, poi, di esprimere un consenso realmente informato. In particolare, è d'uopo fare riferimento a tutte le

---

[27] Garante per la protezione dei dati personali, *Autorizzazione al trattamento dei dati genetici*, 22 febbraio 2007, 1, lett. g.

[28] Uno studio statunitense ha evidenziato la necessità di una maggiore conoscenza sia dei profili genetici che etici nei reparti delle strutture sanitarie da parte di medici ed infermieri. In particolare è stata osservata una correlazione fra una maggior fiducia da parte dei pazienti nel rispetto delle problematiche relative alla propria privacy nei reparti specializzati ove veniva fornita un'adeguata consulenza genetica rispetto a quelli "generici" (in tal senso T. Nyrhinen *et al.*, *Privacy and Equality in Diagnostic Genetic Testing*, in *Nursing Ethics*, 2007, 14, 3, p. 305).

[29] A. Conti *et al.*, *I test genetici. Etica, deontologia, responsabilità*, cit., p. 125.

[30] Commissione Europea, *25 raccomandazioni concernenti le implicazioni etiche, giuridiche e sociali dei test genetici*, Brussels, 2004, p. 14.

maggiori implicazioni dei test, mettendo in evidenza che i dati così acquisiti possono fornire informazioni anche sulla propria famiglia genetica.

La fase successiva assume importanza solo qualora, una volta effettuato il test, i risultati siano di predisposizione o di suscettibilità. In tali ipotesi, il consulente genetico dovrebbe essere in grado di riuscire a comunicarli nella maniera meno dolorosa possibile, nel tentativo di sostenere anche moralmente coloro i quali hanno ricevuto risultati non confortanti dal test effettuato e poterli indirizzare verso le migliori metodologie terapeutiche, qualora esistano. In ogni caso, appare fondamentale, in linea di principio, garantire un'adeguata assistenza psicologica per poter far accettare una diagnosi infausta senza che le implicazioni negative di carattere psico-fisico connesse alla patologia impediscano di vivere appieno l'esistenza residua.

Assai delicato appare anche il caso in cui i risultati debbano essere poi riferiti alla famiglia genetica, per cui il consulente dovrebbe riuscire ad abbinare alla preparazione medica adeguata al livello del servizio offerto anche una capacità relazionale che consenta di adattare i problemi di ordine medico ed etico alla realtà concreta.

## 3. *I test genetici*

I test genetici consistono nell'analisi «di specifici geni, del loro prodotto o della loro funzione, nonché ogni altro tipo di indagine del Dna o dei cromosomi, finalizzate ad individuare o a escludere modificazioni (del Dna) verosimilmente associate a patologie mediche»[31]. Secondo un'altra definizione, un test genetico è «l'analisi a scopo clinico di uno specifico gene o del suo prodotto o funzione o di altre parti del Dna o di un cromosoma, volta a effettuare una diagnosi o a confermare un sospetto clinico in un individuo già affetto (test diagnostico), oppure a individuare o escludere la presenza di una mutazione associata ad una malattia genetica che possa svilupparsi in un individuo sano (test presintomatico) o, ancora, a valutare la mag-

[31] Comitato Nazionale per la Bioetica, *Orientamenti bioetici per i test genetici*, Roma, 1999.

giore o minore suscettibilità di un individuo a sviluppare patologie comuni (test predittivo)»[32].

Si distingue comunemente fra test genetici individuali e *screenings* in base al fatto che i primi si rivolgono ad un singolo individuo o a membri di famiglie, mentre i secondi ad una popolazione, in tutto o in parte.

Nella pratica medica i test genetici sono utilizzati prevalentemente per fini diagnostici; la diagnosi di una malattia genetica può assumere importanza per il suo controllo ed il suo trattamento[33], ad esempio mediante la modificazione della propria condotta di vita o, ovviamente, dell'attività terapeutica.

Le informazioni genetiche presentano, però, profili problematici etici[34] e giuridici a vari livelli, sia nei confronti della persona sulla quale il test è effettuato che in relazione alla propria famiglia genetica. Inoltre, le diverse tipologie di test pongono problematiche diverse dall'una all'altra, sia in base alla loro natura che delle finalità per le quali possono essere utilizzati, per cui si è scelto, in questa sede, di distinguerli secondo le seguenti categorie allo scopo di mettere in evidenza tematiche ritenute di particolare interesse per la bioetica e per il diritto: test genetici prenatali e sui minori, nonché in ambito assicurativo, lavorativo, giudiziario.

– *Test genetici prenatali*: essi consentono l'identificazione di diverse malformazioni e sindromi prima del parto[35]. Qualora siano presenti alterazioni somatiche è possibile fare ricorso alla chirurgia neonatale, con buone possibilità di ottenere risultati positivi.

---

[32] Garante per la protezione dei dati personali, *Autorizzazione al trattamento dei dati genetici*, 22 febbraio 2007, 1, lett. c.

[33] A. Conti *et al.*, *I test genetici. Etica, deontologia, responsabilità*, cit., p. 11.

[34] Cfr., fra gli altri, D.H. Lea, J. Williams, M.P. Donahue, *Ethical Issues in Genetic Testing*, in *Journal of Midwifery & Women's Health*, 2005, 50, 3, pp. 234-240.

[35] Il Garante per la protezione dei dati personali ha disposto che per le informazioni relative ai nascituri il consenso sia validamente prestato dalla gestante. Nel caso in cui il trattamento effettuato mediante test prenatale possa rivelare anche dati genetici relativi alla futura insorgenza di una patologia del padre, bisogna acquisirne il consenso (Garante per la protezione dei dati personali, *Autorizzazione al trattamento dei dati genetici*, 22 febbraio 2007, 6).

Il problema principale della diagnosi prenatale di tipo genetico, invece, consiste nel sin troppo ampio *gap* tra capacità diagnostiche e possibilità terapeutiche. Ne consegue che, nella maggior parte dei casi, una volta che sia stato accertato un difetto genetico bisogna scegliere fra accettare il nascituro con la sua sindrome o interrompere la gravidanza[36].

Purtroppo la prima ipotesi sarà sempre più frequente se lo stato non si farà promotore di misure assistenziali di vario tipo che consentano una vita dignitosa sia al futuro portatore di handicap che alla sua famiglia. Le problematiche etiche sono accompagnate a quelle economiche e, nel rispetto di valori largamente condivisi, lo stato dovrebbe aiutare la famiglia, sia prima che dopo la nascita.

La seconda ipotesi, invece, consiste, di fatto, in un'operazione eugenetica, poiché viene eliminato fisicamente un soggetto che non risponde al canone comunemente accettato di normalità fisica.

– *Test genetici sui minori*: essi devono essere svolti con prudenza poiché potrebbero turbarne lo sviluppo evolutivo. Presupposto per la loro effettuazione dovrebbe essere la necessità di tutelare la salute del minore da un pericolo attuale, la cui gravità aumenterebbe col passare del tempo, perché altrimenti basterebbe attendere il raggiungimento della maggiore età[37]. Bisogna in ogni caso effettuare una comparazione fra gli effetti benefici e quelli dannosi che potrebbero scaturirne, sia dal punto di vista prettamente fisico che psicologico, poiché qualora gli effetti benefici siano incerti o quelli dannosi siano prevalenti, il test non dovrebbe essere effettuato.

---

[36] «In western countries a woman's informed choice is considered a basic principle in the carrying out of these practices, and prenatal screening and diagnosis are presented as offering new reproductive choices for women and couples […]. Because the possibilities of curing congenital diseases of fetuses are very limited, the choice after detection of an affected fetus is usually whether to continue the pregnancy or to undergo an abortion» (P.I. Santalahti *et al.*, *Women's decision making in prenatal screening*, in *Social Science & Medicine*, 1998, 46, 8, p. 1067).

[37] American Society of Human Genetics, American College of Medicine Genetics, *Point to consider: ethical, legal, and psychosocial implications of genetic testing in children and adolescents*, in *American Journal of Human Genetics*, 1995, 57, p. 1233.

Quanto alla scelta sull'effettuazione del test, sembra opportuno che sia operata congiuntamente con il medico e con il minore, qualora quest'ultimo abbia una sufficiente capacità di intendere e di volere[38].

I vantaggi che potrebbero derivare da tali test sono di vario tipo: in presenza di malattie genetiche con fattori ambientali scatenanti si può modificare lo stile di vita per evitare danni alla salute; minori a rischio possono essere tenuti sotto continuo controllo medico o questo può essere ridotto grazie ai risultati del test; la diagnosi di una malattia può essere perfezionata e così la relativa terapia; nel caso di risultati favorevoli si può eliminare l'incertezza in merito al verificarsi di una futura malattia.

Anche gli svantaggi sono eterogenei: risultati negativi possono portare a discriminazioni del minore sia in ambito familiare che extra-familiare (ad esempio nella scuola); i risultati del test potrebbero riverberarsi sugli altri membri della famiglia, rischiando anche di ampliare l'ambito di una possibile discriminazione; infine, un minore ha, tendenzialmente, la possibilità di subire maggiori danni psicologici di un adulto in presenza di una diagnosi infausta, con probabili shock psicologici che potrebbe non superare per tutta la vita.

Si consideri, però, che la necessità di garantire la riservatezza dei risultati di tali test è ancor maggiore che in altri casi, poiché essi potrebbero successivamente addirittura giungere a precludere al minore, una volta raggiunta la maggiore età, l'ingresso nel mondo del lavoro o la conclusione di polizze sulla salute (con palesi pregiudizi soprattutto in quegli stati ove queste rappresentano la forma comune di previdenza)[39].

A tutela assoluta del minore potrebbe vigere un divieto assoluto ed inderogabile di comunicazione dei risultati a terze parti e di distruzione degli stessi nel momento in cui non siano più necessari a fini terapeutici, con la previsione di sanzioni elevatissime in caso

---

[38] Nello stesso senso è anche il Garante per la protezione dei dati personali: «l'opinione del minore, nella misura in cui lo consente la sua età e il suo grado di maturità, è presa in considerazione» (Garante per la protezione dei dati personali, *Autorizzazione al trattamento dei dati genetici*, 22 febbraio 2007, 6).

[39] Istituto Superiore di Sanità, *Linee guida per i test genetici*, Roma, 1998, p. 42.

di violazione di tali regole. L'immediata utilità terapeutica dovrebbe essere il criterio guida per stabilire la liceità dei test genetici effettuati sui minori; altre finalità non sembrano giustificarne l'effettuazione, non legittimando la lesione della privacy del minore.

Bisogna comunque operare una comparazione fra gli effetti benefici e quelli dannosi che potrebbero scaturirne, sia dal punto di vista prettamente fisico che psicologico, poiché qualora gli effetti benefici siano incerti o quelli dannosi siano prevalenti, il test non dovrebbe essere effettato.

– *Test genetici in ambito assicurativo*: essi, in linea ipotetica, possono essere utilizzati nell'ambito di contratti di assicurazione sulla vita o sulla salute per evidenziare se gli assicurati presentano una probabilità più o meno elevata di contrarre una determinata patologia[40]. Scopo del contratto di assicurazione è, in linea generale, la ripartizione del rischio dei singoli entro la massa degli assicurati, i quali pagano i premi il cui complesso forma un fondo dal quale viene attinto il denaro necessario a coprire gli indennizzi. Di norma, vengono individuate su base statistica determinate categorie che presentano un maggior coefficiente di rischio (solitamente i parametri consistono in età, sesso, luogo di residenza, ecc.).

Le imprese di assicurazione, però, spingono affinché fra tali parametri venga inserita l'analisi del patrimonio genetico. Ovviamente, determinati soggetti non sarebbero più assicurabili qualora dai test effettuati emergesse un'alta possibilità di contrarre diverse malattie genetiche, mentre coloro i quali presentano nulle o ridotte possibilità in tal senso sarebbero dei clienti "perfetti" per le assicurazioni, poiché l'alea del rischio sarebbe assai ridimensionata. La natura dei dati genetici, inoltre, comporta l'idoneità dei risultati dei test a riverberarsi anche sulla famiglia genetica di chi li ha effettuati, per cui interi nuclei familiari potrebbero non essere astrattamente e concretamente assicurabili. Addirittura, mediante il trattamento incro-

[40] Tale problematica assume un particolare rilievo in nazioni, come gli Stati Uniti, dove l'assistenza sanitaria è basata sulle assicurazioni sanitarie ed è in molti casi fornita dai datori di lavoro, per cui si pone il problema di garantire la riservatezza dei dati sanitari di coloro i quali sono, al contempo, lavoratori ed assicurati.

ciato dei dati genetici è, in linea ipotetica, possibile acquisire informazioni relative a più famiglie genetiche (ad esempio, della prole di due soggetti).

In dottrina è stato sostenuto che risulta difficile comparare gli interessi economici e i diritti fondamentali, per cui «il contratto quando si realizza tra soggetti privati altro non è se non uno strumento dell'economia come tale rivolto al perseguimento di fini puramente materiali»[41], dando mero risvolto etico al diritto alla privacy.

Tuttavia, il diritto alla riservatezza è tutelato quale diritto fondamentale sia dalla Costituzione che dalla legge ordinaria, per cui nel bilanciamento fra interessi confliggenti deve essere ritenuto prevalente rispetto alla tutela degli interessi economici delle compagnie di assicurazione. La loro attività, del resto, concretizza un'iniziativa economica privata e dunque «non può svolgersi in contrasto con l'utilità sociale o in modo da recare danno alla sicurezza, alla libertà, alla dignità umana». Appare chiaro che, in tali casi, la libertà di autodeterminazione nonché la dignità dell'individuo e della sua famiglia genetica sarebbero lese dalla possibilità di rendere obbligatoria o altamente desiderabile[42] l'effettuazione di test genetici e la loro comunicazione alle società assicurative.

In linea generale, dunque, sembra corretto sancire un generale divieto di utilizzare test genetici nel corso del rapporto assicurativo, sia per l'elevata potenzialità discriminatoria sia perché consisterebbero in forme di coazione nei confronti di coloro che preferiscono "non sapere" e che invece sarebbero costretti "a sapere" pur di stipulare un determinato contratto di assicurazione.

– *Test genetici in ambito lavorativo*: essi possono essere svolti sia in una fase prodromica all'assunzione che nel corso del rapporto di lavoro. Anche qualora il datore di lavoro adotti tutte le cautele possibili per rendere salubre l'ambiente di lavoro, determinati lavori, in virtù delle condizioni ambientali in cui sono svolti, possono cagionare patologie in soggetti predisposti geneticamente o la cui con-

---

[41] S. Landini, *Assicurazioni sanitarie e privacy genetica*, in *Diritto pubblico*, 2003, 1, p. 241.

[42] Ad esempio, potrebbero essere fissate tariffe proibitive e dissuasive per chi non si sottopone ai test e, al contrario, assai convenienti per chi invece li effettua.

dizione genetica si è modificata durante il periodo di permanenza in ambienti poco salubri.

Tali test possono però cagionare discriminazioni, per cui potrebbero aversi anche in questo caso delle "caste genetiche" di abili o maggiormente idonei al lavoro solo in seguito ad un'analisi probabilistica del loro stato di salute, mentre altri incorrerebbero in maggiori difficoltà nel trovare un posto di lavoro.

Bisogna infatti evitare che i test genetici divengano un'alternativa più economica al risanamento dell'ambiente di lavoro, poiché «l'esclusione del lavoratore risulta in sé eticamente ammissibile solo nel caso di impossibilità di un sufficiente miglioramento delle condizioni di lavoro, ossia se i provvedimenti organizzativi e tecnici sul posto di lavoro non bastano a garantire la sicurezza di terzi»[43].

È quindi opportuna la sussistenza di un generalizzato divieto di richiesta, da parte del datore di lavoro, di effettuazione di test genetici non solo prima dell'assunzione, ma anche nel normale corso del rapporto di lavoro: secondo lo "European Group on Ethics in Science and New Technologies" lo svolgimento di tali test è «eticamente inaccettabile»[44]. La soggezione psicologica ed economica di chi è in cerca di lavoro, o comunque di chi è lavoratore subordinato, potrebbe infatti spingere ad effettuare comunque eventuali test richiesti ed a comunicarne i risultati al datore di lavoro pur di essere assunti o di conservare con certezza il proprio posto di lavoro.

Possono, però, essere previste delle eccezioni specifiche per talune categorie di lavori particolarmente a rischio, il tutto a tutela del diritto alla salute dei lavoratori[45]. In tal caso, nel bilanciamento fra il diritto alla privacy e quello alla salute dovrebbe, ovviamente, prevalere il secondo.

Come si è accennato, la problematica assume maggiore rilievo in quei paesi ove le *health insurances* costituiscono gli strumenti di tutela della salute individuale; nel corso del rapporto di lavoro, i premi vengono solitamente pagati dal datore di lavoro, la cui assicura-

---

[43] A. Conti *et al.*, *I test genetici. Etica, deontologia, responsabilità*, cit., pp. 96-97.

[44] European Group on Ethics in Science and New Technologies, *Opinion on Ethical Aspects of Genetic Testing in the Workplace*, 28 luglio 2003, p. 15.

[45] Ivi, pp. 15-16.

zione sarà tenuta a sostenere i costi delle malattie dei lavoratori. La conoscenza dei test da parte dei datori di lavoro, dunque, potrebbe eventualmente portare alla diffusione dei dati anche nei confronti delle compagnie assicuratrici, in virtù dell'esposta connessione, con la conseguenza che i dati genetici di un soggetto uscirebbero dal suo controllo, in chiara violazione del diritto alla privacy.

– *Test genetici in ambito giudiziario:* essi vengono utilizzati nel corso di procedimenti giudiziari al fine di identificare uno o più soggetti. Gli ambiti principali sono quello penale, per l'identificazione dei rei[46], e quello civile, soprattutto in materia di accertamento della paternità.

Da un punto di vista scientifico ed etico, la problematica più delicata consiste nella certezza circa la correttezza dei risultati dei test, poiché in caso di errore le conseguenze potrebbero essere gravissime sia in sede civile che, soprattutto, in sede penale. Si pensi alle conseguenze di erronee attribuzioni di paternità o di eventuali attribuzioni di responsabilità in sede penale, soprattutto ove vige la pena di morte. Come è stato sottolineato in dottrina, la prova del DNA appare, da un punto di vista scientifico e statistico, maggiormente utile nell'escludere che qualcuno abbia commesso un atto più che nel riferire lo stesso atto ad una determinata persona[47], per cui eventuali usi più generalizzati di tali tecniche dovrebbero, in teoria, richiedere dimostrazioni scientifiche rigorose e provenienti da studi indipendenti[48].

Una volta acclarata la correttezza scientifica dei test, bisogna tuttavia riflettere adeguatamente sulle problematiche inerenti la privacy individuale e collettiva. Così, anche a soggetti non indagati, magari residenti nel medesimo territorio, potrebbe essere chiesto di sottoporsi a test genetici al fine di identificare un criminale. Appare

---

[46] Comitato Nazionale per la Bioetica, *Orientamenti bioetici per i test genetici*, cit., p. 122.

[47] D.J. Solove, M. Rotenberg, P.M. Schwartz, *Information Privacy Law*, Aspen, New York, 2006, p. 441.

[48] M.A. Rothstein, M.K. Talbott, *The Expanding use of DNA in Law Enforcement: What Role for Privacy*, in *The Journal of Law, Medicine & Ethics*, 2006, 34, 2, p. 162.

chiara la coercizione psicologica ad effettuare il test, che andrebbe svolto per non essere sospettati di avere qualcosa da nascondere. Il fine di punire chi ha commesso un delitto non può tuttavia rendere tutti i cittadini presunti imputati. Oltretutto, in tal modo potrebbe essere realizzata una schedatura di massa, creando un archivio contenente le «impronte genetiche» della collettività[49].

Un numero sempre crescente di stati, però, sta creando archivi contenenti campioni di Dna dei criminali assicurati alla giustizia, nei quali non viene inserito l'intero codice genetico degli individui, bensì dei frammenti utili a fini identificativi[50]. Sul punto, bisogna menzionare la Risoluzione del Consiglio dell'Unione Europea del 9 giugno 1997 sullo scambio di risultati di analisi del Dna[51], con la quale gli Stati membri sono stati invitati a prevedere la costituzione di banche dati nazionali relative al Dna. Per quanto tali banche dati possano essere utili per una migliore e più efficace lotta al crimine, il rischio di schedatura di massa sembra, invero, troppo elevato per fornire un giudizio positivo sulla creazione e lo sviluppo di simili banche di dati[52].

Si pensi, del resto, a quanto avvenuto nel Regno Unito, dove un simile database è stato creato già nel 1994 e dove la tendenza sembra «denotare chiaramente l'intenzione di raccogliere progressiva-

---

[49] Comitato Nazionale per la Bioetica, *Orientamenti bioetici per i test genetici*, cit., p. 123. Proprio ad una schedatura di massa sembra riferirsi Lawrence Lessig quando riporta il seguente annuncio che ha letto sui mezzi di trasporto pubblico: «Abuse, Assault, Arrest: Our staff are here to help you. Spitting on DLR staff is classified as an assault and is a criminal offence. Saliva Recovery Kits are now held on every train and will be used to identify offenders against the national DNA database» (L. Lessig, *Code version 2.0*, Basic Books, New York, 2006, p. 208). Sembra opportuno rilevare che, stante la delicatezza dei dati genetici, il mezzo utilizzato sembra eccessivo rispetto al fine perseguito.

[50] D.J. Solove, M. Rotenberg, P.M. Schwartz, *Information Privacy Law*, cit., p. 441.

[51] Risoluzione n. 97/C 193/02.

[52] In dottrina si è sostenuta «la necessità di introdurre nell'ordinamento italiano uno strumento che permetta la raccolta di materiale biologico della persona indagata al fine di *Dna profiling*» ma «il legislatore, nel determinare i casi e i modi del prelievo coattivo, dovrebbe non contemplare, tra i destinatari dell'ordine, i *terzi* e dovrebbe esplicitamente escludere la possibilità di disporre la coazione al fine di realizzare *screening* di massa» (A. Santosuosso, G. Gennari, *Il prelievo coattivo di campioni biologici e i terzi*, in *Diritto penale e processo*, 2007, 3, p. 401).

mente, in *un'unica* banca dati i campioni organici appartenenti ad una più ampia categoria di soggetti che si potrebbero definire «attiva popolazione criminale». In questo novero rientrerebbero sia persone già indagate sia quelle "potenzialmente" suscettibili di divenire tali; di conseguenza, qualunque individuo potrebbe entrare a far parte di quest'ultima classe»[53].

## 4. *Gli "screenings"*

Gli *screenings*, come si è detto, si differenziano dai test genetici poiché essi non sono svolti su scala individuale, bensì su intere popolazioni o su un numero più o meno elevato di persone. Essi si contraddistinguono per la sistematicità, l'obiettivo preciso (consistente nell'identificazione di un rischio determinato per la salute) ed il fatto di riguardare persone che, di norma, non hanno evidenza di aver contratto la malattia per la quale lo *screening* stesso viene effettuato[54].

Di norma sono suddivisi in base all'età del campione di individui[55]:

– prenatali (svolti durante la gravidanza; consentono, ad esempio, di individuare la sindrome di Down);

– neonatali (ad esempio, consentono di individuare la fenilchetonuria);

– in adolescenti (ad esempio, consentono di individuare i portatori di malattia di Tay-Sachs);

– in adulti (ad esempio, sono stati svolti in Sardegna per identificare i portatori della talassemia).

---

[53] C. Fanuele, *Un archivio centrale per i profili del DNA nella prospettiva di un "diritto comune" europeo*, in *Diritto penale e processo*, 2007, 3, p. 387.

[54] S. Gevers, *Population screening: the role of the law*, in *European Journal of Health Law*, 1998, 5, 1, p. 18, ripresi in G. Gambino, *Criteri e metodi per una valutazione etica degli screening genetici*, in *Tendenze nuove*, 2004, 4-5, 2004, p. 426.

[55] Comitato Nazionale per la Bioetica, *Orientamenti bioetici per i test genetici*, cit., p. 52.

L'effettuazione degli *screenings* porta con sé problematiche di diverso carattere. Più specificatamente, essi dovrebbero essere utilizzati solo in ambiti strettamente clinici, non prescindendo in alcun modo dalla considerazione di un'effettiva utilità per i soggetti a rischio[56].

In linea generale, è necessario individuare gruppi di individui che abbiano caratteristiche simili; ciò spiega come, di norma, siano svolti su comunità isolate sia da un punto di vista geografico che storico. Appare chiaro, poi, che le fasi di acquisizione e dei trattamenti dei dati siano assai delicate e rese più complesse dalla notevole mole di dati coinvolti; inoltre, è assolutamente necessario rispettare la privacy degli interessati in tutte le fasi di svolgimento dello *screening* stesso.

Così, già da un punto di vista etico è essenziale fornire un'informazione corretta in ordine allo *screening* ed alle sue implicazioni, al fine di ottenere un consenso esplicito al trattamento dei dati, anche perché alla protezione della riservatezza del gruppo non può che affiancarsi quella del singolo. Il consenso, ovviamente, non può essere presunto e deve essere individualizzato; inoltre, l'informativa dovrebbe rendere edotti gli interessati delle modalità e delle finalità del trattamento.

Dal consenso non dovrebbe mai potersi prescindere, anche qualora i dati siano raccolti in forma anonima, poiché un esame genetico rappresenta un trattamento sanitario e, in linea generale, non può essere imposto. Esso, infatti, potrebbe violare il nucleo più duro del diritto alla privacy, anche se quest'ultimo deve cedere in caso di pericolo grave ed attuale per la salute pubblica, poiché nel bilanciamento degli interessi il diritto alla riservatezza soccombe dinanzi alla necessità di tutelare una o più persone dalla concreta lesione del diritto alla salute.

Del resto, come si è visto, il diritto alla privacy, soprattutto in ambito sanitario, è ormai considerato un diritto fondamentale dell'uomo, sancito in numerosi testi normativi internazionali e nazionali, il cui rispetto è essenziale per impedire che si realizzino invasive for-

[56] G. Gambino, *Criteri e metodi per una valutazione etica degli screening genetici*, cit., p. 429.

me di «controllo sociale» e di discriminazione genetica verso interi gruppi; ad esempio, la presenza di certe mutazioni genetiche in determinati ceppi potrebbe essere assunta a fondamento di nuove teorie razziste, nonostante l'erroneità scientifica di simili ideologie. Ciò nonostante, appare opportuno evitare la creazione di nuove e delicate problematiche, dal momento che nella realtà contemporanea accadono spesso eventi tragici in conseguenza dell'odio razziale[57].

Si consideri, comunque, che addirittura la mancata partecipazione ad uno *screening* di massa potrebbe cagionare discriminazioni, per cui dovrebbe essere sempre fornita la possibilità di rifiutare privatamente di sottoporsi al test, nonostante un'eventuale dichiarazione pubblica di parteciparvi.

Anche principi etici tanto palesi come quelli esposti possono tuttavia essere violati qualora i legislatori tutelino l'iniziativa economica privata ben più dei diritti dei propri cittadini, come avvenuto in Islanda, dove in seguito all'emanazione della legge 17 dicembre 1998 denominata "Act on a Health Sector Database" sono state autorizzate società private a raccogliere ed elaborare i dati sanitari e genetici dell'intera popolazione; successivamente, i diritti di esclusiva sono stati concessi per dodici anni ad un'azienda denominata "deCode Genetics", che dovrebbe far uso di un sistema di decodificazione in grado di offrire un'adeguata garanzia di anonimato e di sicurezza dei dati ottenuti, anche se la protezione offerta è stata fortemente criticata da autorevole dottrina[58].

---

[57] La Commissione Europea ha effettuato le seguenti raccomandazioni qualora si vogliano porre in essere degli *screenings*: «a. adottare delle misure per garantire l'utilità dei test: la patologia deve essere grave e il test altamente predittivo; si raccomanda di prevedere delle azioni di *follow up* in termini di interventi medici (ivi comprese le opzioni riproduttive); b. valutare e regolarmente riesaminare la pertinenza della patologia genetica sottoposta a *screening*, nel contesto della sanità pubblica (che può variare da paese a paese nell'UE); c. istituire l'ambiente medico adeguato per fornire informazioni prima del test e servizi di consulenza dopo il test, prima di avviare lo *screening*; d. attuare programmi pilota prima dell'introduzione generale dello *screening*; e. esaminare attentamente la dimensione economica dei programmi di *screening* previsti» (Commissione Europea, *25 raccomandazioni concernenti le implicazioni etiche, giuridiche e sociali dei test genetici*, cit., p. 13).

[58] R. Anderson, *The DeCODE Proposal for an Icelandic Health Database*, in http://www.cl.cam.ac.uk/~rja14/Papers/iceland.pdf.

Bisogna premettere che il ceppo da cui deriva la popolazione islandese è unico, poiché la posizione geografica dell'isola ha limitato i contatti con le altre popolazioni, e dal punto di vista scientifico uno *screening* generalizzato su tale popolazione è molto interessante perché le popolazioni isolate sono considerate ideali per le loro caratteristiche genetiche, demografiche e ambientali per lo studio dei fattori di rischio, genetici e non, cui consegue lo sviluppo di malattie multifattoriali.

Il caso islandese ha suscitato ampi dibattiti nel mondo scientifico[59]. Si consideri, infatti, che la legge summenzionata ha previsto non il meccanismo dell'*opt-in*, bensì quello dell'*opt-out*: era pertanto necessario un atto di volontà esplicito affinché i propri dati non venissero acquisiti e trattati[60]. Difatti, non solo non era assolutamente previsto il consenso informato, ma vigeva addirittura il principio del silenzio-assenso, "giustificato" dalle difficoltà di ottenere un consenso esplicito.

La violazione della privacy, però, non si arrestava alla fase acquisitiva dei dati, ma poteva potenzialmente andare oltre, dal momento che la popolazione islandese è poco numerosa (circa 300.000 abitanti) e dunque mediante un trattamento incrociato di dati sanitari è possibile identificare i titolari dei numerosi dati acquisiti: di fatto, anche i dati di coloro i quali avrebbero negato il consenso sarebbero, in via indiretta, sarebbero stati memorizzati nella banca dati poiché essa avrebbe contenuto quasi tutte le informazioni genealogiche della popolazione islandese[61].

Nell'enorme *database*, infatti, sarebbero dovuti confluire sia i dati genetici relativi ai defunti (già archiviati nelle strutture pubbliche) che ai viventi (raccolti dai loro medici), gli alberi genealogici conservati nelle chiese ed infine le informazioni raccolte sui campioni di sangue e di tessuti; il trasferimento dei dati viene facilitato dalla

---

[59] M. Enserink, *Opponents Criticize Iceland's Database*, in *Science*, 1998, 5390, 282, p. 859.

[60] Su tale profilo cfr., fra gli altri, V. Arnason, *Coding and Consent: Moral Challenges of the Database Project in Iceland*, in *Bioethics*, 2004, 18, 1, pp. 27-49.

[61] J.F. Merz, G.E. McGee, P. Sankar, *"Iceland Inc."? On the ethics of commercial population genomics*, in *Social Science & Medicine*, 2004, 58, p. 1205.

prevista connessione delle strutture sanitarie in un'unica rete facente capo ad un computer centrale.

L'acquisizione di una mole tanto elevata di dati sensibili sarebbe difficilmente prospettabile già in linea di principio, ma appare di inaudita gravità qualora si consideri che il fine della ricerca non è di interesse generale, bensì risponde alle esigenze di una società privata costituita con capitali privati, che potrebbe lucrare sulla «materia prima» fornita gratuitamente dai cittadini islandesi, senza che a tale sacrificio corrisponda, tuttavia, una effettiva tutela della salute pubblica e individuale in grado di giustificare questa violazione su larga scala del diritto alla riservatezza.

Sul punto, però, il *Chief Executive Officer* della "deCode Genetics" (ossia il genetista islandese Kari Stefansson) è giunto addirittura a sostenere, sulle prestigiose pagine del «New England Journal of Medicine», che i cittadini siano più garantiti dal fatto che i dati genetici siano conservati da un'azienda privata anziché dallo stato poiché esso potrebbe violare i diritti dei singoli in nome dell'avanzamento della società, mentre qualora la medesima azienda violasse in modo grave e ripetuto la privacy dei cittadini potrebbe addirittura essere costretta a cessare la propria attività[62].

Fortunatamente, l'*Act on a Health Sector Database* è stato dichiarato incostituzionale dalla Corte Suprema islandese con sentenza del 27 novembre 2003, perché le tecniche utilizzate per il trattamento dei dati non sono idonee a garantire il rispetto della privacy dei soggetti i cui dati vengono inseriti nel *database*[63].

Tale caso, comunque, rimane assai significativo, in virtù della generalizzata lesione di un diritto fondamentale come quello alla privacy posta in essere da un potere legislativo asservito a quello economico[64]. Nella fattispecie, però, l'espressione del dissenso ed il

---

[62] J.R. Gulcher, K. Stefansson, *The Icelandic Healthcare Database and Informed Consent*, in *New England Journal of Medicine*, 2000, 342, 24, pp. 1827-1830.

[63] Sul punto cfr. G.J. Annas, *Family Privacy and Death. Antigone, War, and Medical Research*, in *The New England Journal of Medicine*, 2005, 352, 5, pp. 503-504.

[64] In dottrina è stato osservato che «se le due prospettive che riescono a dar meglio conto della vicenda islandese sono la violazione delle norme antitrust e il diritto di disobbedienza, vuol dire che la genetica, la sua ricerca e le sue applicazioni,

contributo del potere giudiziario hanno consentito, almeno per ora, di ristabilire il primato della persona sul mercato.

## 5. *La protezione dei dati genetici nella normativa italiana*

La legge n. 675/1996, nella sua formulazione originaria, non faceva specifico riferimento a particolari modalità di gestione dei dati genetici, la cui disciplina, pertanto, era da individuarsi in quella, più generale, relativa ai dati sensibili e, in particolare, ai dati idonei a rivelare lo stato di salute.

Solo con il d.lgs. 11 maggio 1999, n. 135, si è avuta una prima regolamentazione dei dati genetici, che, nella specie, sanciva la necessità di una apposita autorizzazione del Garante per la protezione dei dati personali per trattare informazioni genetiche. Tale autorizzazione presupponeva il parere obbligatorio del Ministro della salute nonché del Consiglio superiore della sanità[65].

Nel cod. priv. è stata seguita la medesima impostazione, tanto che l'art. 90, comma 1, cod. priv., dispone che il trattamento di dati genetici può essere svolto solo nei casi previsti da apposita autorizzazione del Garante, sentito il Ministro della salute che acquisisce, a tal fine, il parere del Consiglio superiore di sanità.

L'all. B al cod. priv., inoltre, detta alcune misure minime di sicurezza specifiche per i dati genetici, che possono essere trattati solo all'interno di locali protetti il cui accesso è ristretto agli incaricati dei trattamenti oppure a chi è in possesso di specifica autorizzazione.

Particolare attenzione viene riservata, poi, al trasporto ed al trasferimento dei dati, avvenga esso utilizzando mezzi "materiali" od

---

sollevano problemi la cui soluzione va cercata nell'economia e nella politica, più che nell'etica o nel diritto: una questione non da poco», A. Santosuosso, *Il diritto alla disobbedienza genetica: il caso dell'Islanda*, in C.M. Mazzoni (a cura di), *Etica della ricerca biologica*, Olschki, Firenze, 2000 (anche in http://www.globius.org/documenti/Islanda.pdf).

[65] Sulla tutela dei dati genetici nella normativa previgente cfr., fra gli altri, J. Monducci, G. Pasetti, *Il trattamento dei dati sanitari e genetici*, in J. Monducci, G. Sartor (a cura di), *Il Codice in materia di protezione dei dati personali*, Cedam, Padova, 2004, pp. 255-282.

"immateriali": nel primo caso, possono essere trasportate solo quelle informazioni conservate in contenitori muniti di serratura o dispositivi equipollenti; nel secondo, i dati possono essere trasferiti in formato elettronico solo se sono previamente cifrati.

Invero, appare abbastanza singolare che in un *corpus* tanto vasto quale il cod. priv. solo queste poche disposizioni si occupino di un settore tanto delicato come quello della protezione dei dati genetici, la cui regolamentazione specifica è stata, di fatto, lasciata ad una *authority*, seppur autorevole, che si è trovata ad assumere una responsabilità che sarebbe stata propria del legislatore.

Il Garante è intervenuto sul punto, da ultimo, con l'Autorizzazione al trattamento dei dati genetici del 22 febbraio 2007, che ha efficacia dal 1° aprile 2007 al 31 dicembre 2008.

Tale autorizzazione è stata rilasciata ad una cerchia abbastanza vasta di soggetti, sia operanti nel settore sanitario che in altri nei quali il trattamento dei dati genetici può consentire l'esercizio di diritti diversi[66], disciplinando minuziosamente anche i casi nei quali

[66] Più specificatamente, essa è stata rilasciata: agli esercenti le professioni sanitarie ed agli organismi sanitari pubblici e privati limitatamente ai dati e alle operazioni indispensabili per esclusive finalità di tutela della salute dell'interessato o di un appartenente alla sua famiglia genetica; ai laboratori di genetica medica limitatamente alle operazioni indispensabili rispetto a dati essenziali da trattare per esclusive finalità di prevenzione e di diagnosi genetica nei confronti dell'interessato, o da utilizzare per lo svolgimento delle indagini difensive o per far valere o difendere un diritto, anche da parte di un terzo, in giudizio o, ad esclusivi fini di ricongiungimento familiare, per l'accertamento della sussistenza di vincoli di consanguineità di cittadini di Stati non appartenenti all'Unione europea, apolidi e rifugiati; alle persone fisiche o giuridiche e a qualsiasi organismo pubblico o privato avente finalità di ricerca, limitatamente ai dati e alle operazioni indispensabili per esclusivi scopi di ricerca scientifica o statistica, finalizzata alla tutela della salute dell'interessato, di terzi o della collettività in campo medico, biomedico ed epidemiologico e antropologico, nell'ambito delle attività di pertinenza della genetica medica; agli psicologi, ai consulenti tecnici e ai loro assistenti, nell'ambito di interventi pluridisciplinari di consulenza genetica, limitatamente ai dati e alle operazioni indispensabili per esclusive finalità di consulenza nei confronti dell'interessato o dei suoi familiari; ai farmacisti, limitatamente ai dati e alle operazioni indispensabili per adempiere agli obblighi derivanti da un rapporto di fornitura di farmaci all'interessato; ai difensori, consulenti tecnici e investigatori privati autorizzati, limitatamente alle operazioni e ai dati indispensabili per esclusive finalità di svolgimento di investigazioni difensive, nonché per far valere o difendere un diritto, anche da parte di un terzo, in sede giudiziaria, sempre che il diritto sia di rango almeno pari a quello dell'interessato e i dati siano trattati esclusivamente

gli stessi soggetti sono legittimati ad effettuare il trattamento medesimo, che deve essere effettuato rendendo una specifica informativa all'interessato (la quale deve contenere elementi ulteriori rispetto a quelli normalmente previsti[67]), affinché questi possa prestare, necessariamente in forma scritta, un consenso realmente informato, che può comunque essere revocato in qualsiasi momento.

Bisogna poi rilevare che il Garante ha altresì disposto l'obbligatorietà della consulenza qualora i test genetici siano effettuati per finalità di tutela della salute o di ricongiungimento familiare. La consulenza deve essere fornita sia prima che dopo lo svolgimento dell'analisi e deve fornire all'interessato informazioni complete e accurate su tutte le possibili implicazioni dei risultati.

---

per tali finalità e per il periodo strettamente necessario al loro perseguimento; agli organismi internazionali ritenuti idonei dal Ministero degli affari esteri e alle rappresentanze diplomatiche o consolari per il rilascio delle certificazioni ad esclusivi fini di ricongiungimento familiare e solo qualora l'interessato non possa fornire documenti ufficiali che provino i suoi vincoli di consanguineità, in ragione del suo *status*, ovvero della mancanza di un'autorità riconosciuta o della presunta inaffidabilità dei documenti rilasciati dall'autorità locale.

[67] Salvo che per i trattamenti non sistematici di dati genetici effettuati dal medico di medicina generale e dal pediatra di libera scelta nell'ambito degli ordinari rapporti con l'interessato per la tutela della sua salute e della sua incolumità fisica, l'informativa evidenzia, oltre agli elementi previsti in base agli artt. 13, 77 e 78 cod. priv.: a) l'esplicitazione analitica di tutte le specifiche finalità perseguite; b) i risultati conseguibili anche in relazione alle notizie inattese che possono essere conosciute per effetto del trattamento dei dati genetici; c) il diritto dell'interessato di opporsi al trattamento dei dati genetici per motivi legittimi; d) la facoltà o meno, per l'interessato, di limitare l'ambito di comunicazione dei dati genetici e il trasferimento dei campioni biologici, nonché l'eventuale utilizzo di questi per ulteriori scopi; e) il periodo di conservazione dei dati genetici e dei campioni biologici. Per i trattamenti effettuati per scopi di ricerca scientifica e statistica l'informativa deve inoltre evidenziare: a) che il consenso è manifestato liberamente ed è revocabile in ogni momento senza che ciò comporti alcuno svantaggio o pregiudizio per l'interessato, salvo che i dati e i campioni biologici, in origine o a seguito di trattamento, non consentano più di identificare il medesimo interessato; b) gli accorgimenti adottati per consentire l'identificabilità degli interessati soltanto per il tempo necessario agli scopi della raccolta o del successivo trattamento; c) l'eventualità che i dati e/o i campioni biologici siano conservati e utilizzati per altri scopi di ricerca scientifica e statistica, per quanto noto, adeguatamente specificati anche con riguardo alle categorie di soggetti ai quali possono essere eventualmente comunicati i dati oppure trasferiti i campioni; d) le modalità con cui gli interessati che ne facciano richiesta possono accedere alle informazioni contenute nel progetto di ricerca.

Anche nel caso di *screenings* finalizzati alla tutela della salute è necessaria un'attività di informazione al pubblico circa la disponibilità dei test effettuati, la loro natura, le loro specifiche finalità e conseguenze. Tale attività può essere svolta anche nell'ambito di pubblicazioni istituzionali e mediante reti di comunicazione elettronica.

I soggetti che rientrano nell'elencazione svolta dal Garante e che effettuano uno o più trattamenti di dati genetici per le stessa finalità individuate dalla medesima *authority* non devono richiedere l'autorizzazione qualora il trattamento che si intende effettuare sia conforme alle prescrizioni dell'autorizzazione. Casi diversi saranno presi in considerazione dal Garante solo qualora ricorrano circostanze eccezionali.

L'Autorità ha altresì individuato le finalità del trattamento di dati genetici, qualora le stesse non possano essere adempiute mediante il trattamento di dati anonimi o di dati personali di natura diversa[68],

[68] Le finalità consistono in: a) tutela della salute, con particolare riferimento alle patologie di natura genetica e alla tutela dell'identità genetica dell'interessato, con il suo consenso, salvo quanto previsto dagli artt. 26 e 82 cod. priv. in riferimento al caso in cui l'interessato non possa prestare il proprio consenso per incapacità d'agire, impossibilità fisica o incapacità di intendere o di volere; b) tutela della salute, con particolare riferimento alle patologie di natura genetica e tutela dell'identità genetica di un terzo appartenente alla stessa linea genetica dell'interessato, nel caso in cui il consenso non sia prestato o non possa essere prestato per impossibilità fisica, per incapacità di agire o per incapacità d'intendere o di volere; ciò, limitatamente ai dati genetici già raccolti e qualora il trattamento sia indispensabile per consentire al terzo di compiere una scelta riproduttiva consapevole o sia giustificato dalla disponibilità, per il terzo, di interventi di natura preventiva o terapeutica; c) ricerca scientifica e statistica, finalizzata alla tutela della salute della collettività in campo medico, biomedico ed epidemiologico (sempre che la disponibilità di dati solo anonimi su campioni della popolazione non permetta alla ricerca di raggiungere i suoi scopi), da svolgersi con il consenso dell'interessato salvo che nei casi di indagini statistiche o di ricerca scientifica previste dalla legge; d) per lo svolgimento da parte del difensore delle investigazioni difensive consentite *ex lege*, anche a mezzo di sostituti, di consulenti tecnici e investigatori privati autorizzati, o, comunque, per far valere o difendere un diritto anche da parte di un terzo in sede giudiziaria, anche senza il consenso dell'interessato salvo che il trattamento presupponga lo svolgimento di test genetici. Il diritto da far valere o difendere deve essere di rango pari a quello dell'interessato, o consistente in un diritto della personalità o in un altro diritto o libertà fondamentale e inviolabile e i dati siano trattati esclusivamente per tali finalità e per il periodo strettamente necessario al loro perseguimento. Devono comunque essere rispettate le autorizzazioni generali del Garante al trattamento dei dati sensibili da parte dei liberi professionisti e da parte degli investigatori privati; e) per adempiere o per esigere l'adempimento di specifici obblighi o per eseguire

ed ha inoltre disciplinato le modalità di trattamento, disponendo che, se è necessario identificare anche temporaneamente gli interessati, i dati identificativi dovrebbero essere tenuti separati già al momento della raccolta dei dati (salvo che ciò risulti impossibile in ragione delle particolari caratteristiche del trattamento o richieda un impiego di mezzi manifestamente sproporzionato).

È stato inoltre disposto un generale divieto di comunicazione[69] e di diffusione[70] dei dati genetici, fatte salve alcune eccezioni. Inoltre, i dati genetici devono essere resi noti di regola direttamente all'interessato o a persone diverse dal diretto interessato sulla base di una delega scritta di quest'ultimo, adottando ogni mezzo idoneo a prevenire la conoscenza non autorizzata da parte di soggetti anche compresenti.

## 6. *La privacy genetica fra problematiche attuali e prospettive future*

La privacy, come si è detto, è progressivamente diventata qualcosa di più di un mero *right to be let alone*, essendo comunemente vista nella prospettiva di un controllo, attivo, sui propri dati personali. Ma vi è di più. Essa, anche in virtù dell'acquisizione di nuovi campi di attività e di nuove zone di intervento, si accentra nella essenziale funzione di tutela della persona e diventa sempre più un

specifici compiti previsti espressamente dalla normativa comunitaria, da leggi o da regolamenti in materia di previdenza e assistenza o in materia di igiene e sicurezza del lavoro o della popolazione, anche senza il consenso dell'interessato, nei limiti previsti dall'autorizzazione generale del Garante al trattamento dei dati sensibili nei rapporti di lavoro e ferme restando le disposizioni del codice di deontologia e di buona condotta di cui all'art. 111 cod. priv.; f) per l'accertamento dei vincoli di consanguineità per il ricongiungimento familiare di cittadini di Stati non appartenenti all'Unione europea, apolidi e rifugiati.

[69] In linea generale, i dati genetici non possono essere comunicati e i campioni biologici non possono essere messi a disposizione di terzi salvo che sia indispensabile per il perseguimento delle finalità indicate dall'autorizzazione del Garante.

[70] In linea di principio, i dati genetici non possono essere diffusi. I risultati delle ricerche non possono essere diffusi se non in forma aggregata, ovvero secondo modalità che non rendano identificabili gli interessati neppure tramite dati identificativi indiretti.

mezzo che tutela altri diritti e libertà fondamentali di singoli e gruppi, che possono operare una reale autodeterminazione della propria esistenza senza il timore di subire discriminazioni originate da valutazioni negative ed arbitrarie di dati dai quali potrebbero emergere profili, significativi e non, della propria personalità[71].

In tal senso, assume già oggi un'importanza fondamentale necessità di tutelare la privacy genetica e, con forti probabilità, tale esigenza sarà ben maggiore nel prossimo futuro, quando la genetica riuscirà ad esprimere ancor di più le sue potenzialità. Torna, quindi «il problema della ricerca scientifica e dei suoi limiti. La storia ci mostra la impossibilità o anche la inutilità di limitare la ricerca, ma ci mostra anche la necessità di aver chiara la differenza tra libertà della ricerca e utilizzo di strumenti ai fini della ricerca. Ci mostra l'importanza di una libertà della ricerca correlata ai fini che essa si pone. Ci mostra la necessità di distinguere tra ricerca e utilizzo delle sue scoperte o invenzioni»[72].

Alle molteplici possibilità delle applicazioni della genetica, dunque, bisogna dunque porre un freno, affinché sia sempre rispettata la dignità della persona, che non può essere ridotta ad un ammasso di informazioni che ne delineano il profilo genetico e comportamentale.

Si ribadisce, infatti, che l'individuo rischia di ridursi ad un ammasso di informazioni che «possono mutare la percezione che ciascuno ha di sé, incidere profondamente sui caratteri democratici delle nostre organizzazioni sociali»[73].

In tal modo, infatti, non solo diventa impossibile coglierne l'individualità, ma si corre il rischio di creare delle nuove caste basate sulla genetica, operando discriminazioni che potrebbero essere erroneamente ritenute come scientificamente fondate. Tali discriminazioni, inoltre, sono potenzialmente idonee a spiegare i propri effetti ben oltre l'ambito individuale, perché potrebbero toccare sia la famiglia genetica che il ceppo di appartenenza.

---

[71] G. Santaniello, *Ricerca genetica e tutela della persona*, in http://www.interlex.it/675/santaniello2.htm.

[72] T. Serra, *L'uomo programmato*, cit., p. 135.

[73] S. Rodotà, *Informazione genetica e diritti umani*, in Aa.Vv., *Lezioni di bioetica*, Ediesse, Roma, 1997, p. 97.

Un'eccessiva fiducia nelle possibilità della tecnica potrebbe altresì portare a fondare decisioni, anche giudiziarie, unicamente sui risultati di test che hanno una complessità tale da rendere l'eventuale prova contraria addirittura una *probatio diabolica*.

Appare chiaro, dunque, che la tutela del diritto alla privacy genetica debba essere sempre garantita e che l'utilizzo di dati tanto sensibili quanto quelli genetici non può essere generalizzato, ad esempio per avere una maggiore certezza di identificare univocamente una persona. Come si è visto, l'acquisizione illecita di informazioni delicate come impronte digitali e altri dati biometrici pone problematiche di assoluto rilievo, ma ancor più pericoloso e deprecabile è l'illecito trattamento di dati genetici, poiché dalla loro conoscenza, si ribadisce, possono essere ottenute informazioni che trascendono i dati considerati singolarmente.

La strategia di tutela delle informazioni genetiche e di limitazione alla creazione di banche dati, dunque, dovrebbe essere operata su scala internazionale, nel tentativo di garantire standard comuni che consentano un pieno rispetto della privacy genetica. Ciò appare di fondamentale importanza perché, come si è detto, la persona nella società contemporanea è sempre meno legata stabilmente ad un singolo territorio e le occasioni di spostamento, virtuale e non, appaiono sempre maggiori.

Inoltre, «l'avvento della società "post-genomica" consegnerà a tutti e a ciascuno il genoma umano, vale a dire una massa crescente di informazioni capace di approfondire l'attuale conoscenza di sé e di orientarla verso il futuro. E da qui, da questa diffusa e profonda possibilità di sapere e di prevedere, ciascuno potrà partire per occupare, con le proprie decisioni, territori prima segnati solo dal caso o dalla necessità. Né natura, né piano, ma il concorso di infinite scelte ci darà l'organizzazione sociale del futuro, segnando profondamente la stessa evoluzione del genere umano. Non un solo potere, d'un Dio lontano o d'uno scienziato, ma molteplici volontà disegneranno il mondo»[74].

[74] Id., *La vita e le regole. Tra diritto e non diritto*, Feltrinelli, Milano, 2006, p. 165.

Compito dei vari legislatori sarà quello di far sì che le volontà di alcuni, ivi compreso lo stato medesimo, non divengano arbitrio a danno delle persone, le quali dovranno avere strumenti efficaci per tutelare quella parte più intima del proprio io costituita proprio dal patrimonio genetico. Ciò richiede, però, una presa di coscienza di quanto esso sia importante, non solo per se stessi, e di quanto facilmente determinati prodotti della ricerca scientifica e tecnologica possano violarne la riservatezza ed acquisirlo. Nel caso di specie, è dunque il diritto alla privacy, nella sua specificazione di privacy genetica, lo strumento che consente di tutelare la persona da ingerenze esterne ed estreme nella propria vita e nella propria intimità. La speranza è che l'involuzione di una privacy sempre più burocratizzata non ingeneri la convinzione che essa sia un inutile orpello anziché un baluardo a difesa della persona, sia nella sua veste individuale che di appartenente a gruppi più o meno estesi.

# BIBLIOGRAFIA


Aa.Vv., *Codice della privacy*, Giuffré, Milano, 2004.

Aa.Vv., *Lezioni di bioetica*, Ediesse, Roma, 1997.

J. Abbate, *Inventing the Internet*, MIT Press, Cambridge, Massachusetts, 1999.

R. Acciai (a cura di), *Il diritto alla protezione dei dati personali*, Maggioli, Santarcangelo di Romagna, 2004.

E. Agazzi, *La filosofia di fronte al problema delle manipolazioni genetiche*, in *Iustitia*, 1985, 1, pp. 159-189.

G. Aiello, *Diritto di cronaca e diritto alla riservatezza*, nota a Pret. Firenze 3 marzo 1986, in *Giustizia civile*, 1986, 9, pp. 2285-2287.

M. Aimo, *I "lavoratori di vetro": regole di trattamento e meccanismi di tutela dei dati personali*, in *Rivista giuridica e della previdenza sociale*, 2002, 1, pp. 45-134.

G. Alpa, G. Resta, *Le persone fisiche e i diritti della personalità*, UTET, Torino, 2006.

A.C. Amato Mangiameli, *Diritto e cyberspace. Appunti di informatica giuridica e filosofia del diritto*, Giappichelli, Torino, 2000.

A.C. Amato Mangiameli (a cura di), *Parola chiave: informazione*, Giuffré, Milano, 2004.

American Society of Human Genetics, American College of Medicine Genetics, *Point to consider: ethical, legal, and psychosocial implications of genetic testing in children and adolescents*, in *American Journal of Human Genetics*, 1995, 57, pp. 1233-1241.

American Society of Human Genetics, American College of Medicine Genetics, *The Human Genome Project: implications for human genetics*, in *The American Journal of Human Genetics*, 1991, 49, pp. 687-691.

R. Anderson, *The DeCODE Proposal for an Icelandic Health Database*, in http://www.cl.cam.ac.uk/~rja14/Papers/iceland.pdf.

G.J. Annas, *Family Privacy and Death. Antigone, War, and Medical Research*, in *The New England Journal of Medicine*, 2005, 352, 5, pp. 501-505.

G. Arcudi, V. Poli, *Il diritto alla riservatezza*, Ipsoa, Milano, 2000.

V. Arnason, *Coding and Consent: Moral Challenges of the Database Project in Iceland*, in *Bioethics*, 2004, 18, 1, pp. 27-49.

Associazione Editori Software Videoludico Italiana, *Quarto rapporto annuale sullo stato dell'industria videoludica in Italia*, 2008, in http://www.aesvi.it/cms/attach/editor/rapporto_2007.pdf.

Associazione Editori Software Videoludico Italiana, *Rapporto annuale sullo stato dell'industria videoludica in Italia*, 2007, in http://www.aesvi.it/cms/attach/editor/Rapporto_Annuale_2006.pdf.

Associazione Editori Software Videoludico Italiana, *Secondo rapporto annuale sullo stato dell'industria videoludica in Italia*, 2006, in http://www.aesvi.it/cms/attach/editor/rapp06previewDEF.zip.

U. Ausiello, *Tutela della privacy e azione inibitoria presso l'Autorità Garante per la protezione dei dati personali*, in *Responsabilità comunicazione impresa*, 2000, 4, pp. 531-561.

J. Balkin, *Come cambiano i diritti: la libertà di espressione nell'era digitale*, in V. Colomba (a cura di), *I diritti nell'era digitale. Libertà di espressione e proprietà intellettuale*, Diabasis, Reggio Emilia, 2004, pp. 1-15.

J.M. Balkin, B.S. Noveck (eds.) *The State of Play. Law, Games and Virtual Worlds*, New York University Press, New York, 2006.

P. Balsamo, *Distribuzione on line di file musicali e violazione del copyright: il caso Napster*, in *Il diritto d'autore*, 2001, 1, pp. 34-59.

A. Bardusco, *Articolo 1 (Diritto alla protezione dei dati personali)*, in Aa.Vv., *Codice della privacy*, Giuffré, Milano, 2004, pp. 12-24.

D.W. Bates, A.A. Gawande, *Improving Safety with Information Technology*, in *The New England Journal of Medicine*, 2003, 348, 25, pp. 2526-2534.

D.W. Bates *et al.*, *Effects of computerized physician order entry and a team intervention on prevention of serious medical errors*, in *Journal of American Medical Association*, 1998, 280, pp. 1311-1316.

R. Bellazzi, A. Abu-Hanna, J. Hunter (ed.), *Artificial Intelligence in Medicine. Proceedings of the 11th Conference on Artificial Intelligence in Medicine*, Springer, Berlin, 2007.

F. Bergadano *et al.*, *Privacy digitale. Giuristi e informatici a confronto*, Giappichelli, Torino, 2005.

T. Berners-Lee, *L'architettura del nuovo Web*, tr. it, Feltrinelli, Milano, 2001.

C.M. Bianca (a cura di), *Tutela della privacy*, in *Le nuove leggi civili commentate*, 1999, 2-3.

C.M. Bianca, F.D. Busnelli (a cura di), *La protezione dei dati personali. Commentario al D.lgs. 30 giugno 2003, n. 196 (Codice della privacy)*, Cedam, Padova, 2007.

B. Blobel, *Analysis, design and implementation of secure and interoperable information systems*, IOS Press, Amsterdam, The Netherlands, 2002.

T. Bodheneimer, K. Grumbach, *Electronic Technology. A Spark to Revitalize Primary Care?*, in *Journal of the American Medical Association*, 2003, 2, pp. 259-264.

A. Bompiani, *Il comitato internazionale di bioetica dell'UNESCO e la redazione della "Dichiarazione universale sul genoma umano e i diritti umani"*, in *Iustitia*, 1998, 1, pp. 62-108.

A. Bompiani, *Una valutazione della "Convenzione sui diritti dell'uomo e la biomedicina" del Consiglio d'Europa*, in *Medicina e morale*, 1997, 1, pp. 37-55.

S. Bono *et al.*, *Security Analysis of a Cryptographically-Enabled RFID Device*, in *Proceedings of the 14th Usenix Security Symposium*, 2005, pp. 1-16 (http://www.usenix.org/events/sec05/tech/bono.html).

G. Boole, *Indagine sulle leggi del pensiero su cui sono fondate le teorie matematiche della logica e della probabilità*, tr. it., Einaudi Torino, 1976.

R. Borruso, *Computer e diritto*, I, *Analisi giuridica del computer*, Giuffré, Milano, 1988.

E. Brovedani, *La decifrazione del genoma umano. Aspetti scientifici e implicazioni etiche*, in *Aggiornamenti sociali*, 2000, 9-10, pp. 659-672.

B.G. Buchanan, E.H. Shortliffe (ed.), *Rule-Based Expert Systems: The MYCIN Experiments of the Stanford Heuristic Programming Project*, Addison Wesley, Reading, Massachusetts, 1984.

G. Buttarelli, *Banche dati e tutela della riservatezza. La privacy nella Società dell'Informazione*, Giuffré, Milano, 1997.

F. Buzzi, P. Danesino (a cura di), *Gli esercenti le professioni sanitarie nel recente riassetto formativo. Interazioni e responsabilità nell'attuale cornice normativa delle aziende sanitarie*, Pavia, 26-27 settembre 2002, Giuffré, Milano, 2003.

S. Cacciaguerra, *Partecipazione a mondi virtuali e utenti mobili*, in *Sistemi intelligenti*, 2007, 1, pp. 9-23.

S. Callens (ed.), *E-Health and the Law*, Kluwer Law International, The Hague, The Netherlands, 2003.

L. Caputi, *Liti bagatellari, dal paradosso al parossismo: il danno da disappunto per illegittima introduzione di volantini pubblicitari nelle cassette della posta*, in *Danno e responsabilità*, 2004, 8-9, pp. 882-887.

V. Caridi, *La tutela dei dati personali in Internet: la questione dei logs e dei cookies alla luce delle dinamiche economiche dei dati personali*, in *Il diritto dell'informazione e dell'informatica*, 2001, 4-5, pp. 763-783.

R. Caso, *Digital rights management. Il commercio delle informazioni digitali tra contratto e diritto d'autore*, Cedam, Padova, 2004.

G. Cassano, I.P. Cimino, *Il nuovo regime di responsabilità dei "providers": verso la creazione di un novello "censore telematico"*, in *I contratti*, 2004, 1, pp. 88-96.

M. Castells, *Galassia Internet*, tr. it., Feltrinelli, Milano, 2001.

G. Catalano, *Di cassette per la corrispondenza piene e danno "esistenziale" derivante*, in *Danno e responsabilità*, 2004, 8-9, pp. 887-889.

G. Cataldi, *Convenzione europea dei diritti dell'uomo e ordinamento italiano: un tentativo di bilancio*, in *Rivista internazionale dei diritti dell'uomo*, 1998, 1, pp. 20-43.

G.A. Cavaliere, *La tutela della proprietà intellettuale e il file-sharing. Il nuovo business delle major*, in *Diritto ed Economia dei Mezzi di Comunicazione*, 2006, 2, pp. 245-266.

G.A. Cavaliere *et al.*, *Manuale breve di informatica per avvocati*, Utet giuridica, Milano, 2007.

P. Ceccoli, *Articolo 14 (definizione di profili e della personalità dell'interessato)*, in Aa.Vv., *Codice della privacy*, Giuffré, Milano, 2004, pp. 191-197.

Centro Nazionale per l'Informatica nella Pubblica Amministrazione, *Linee guida per l'impiego di sistemi RFId nella Pubblica Amministrazione*, in *I Quaderni*, 2007, 30.

P. Cerina, *Il caso Napster e la musica on line: cronaca della condanna annunciata di una rivoluzione tecnologica*, in *Il diritto industriale*, 2001, 1, pp. 48-59.

C. Cevenini, *I servizi della società dell'informazione. Profili informatico-giuridici*, Gedit, Bologna, 2004.

A. Chein, *A practical look at virtual property*, in *St. John's Law Review*, 2006, 80, 3, pp. 1059-1090.

H. Chen *et al.* (eds.), *Medical Informatics. Knowledge Management and Data Mining in Biomedicine*, Springer science, New York, 2005.

R. Chiesa, S. Ciappi, *Profilo hacker. La scienza del Criminal Profiling applicata al mondo dell'hacking*, Apogeo, Milano, 2007.

G. Citarella, *Spamming: interferenze nella sfera privata e violazione del diritto alla privacy*, in *Diritto dell'internet*, 2007, 1, pp. 27-29.

P.L. Cochran, M.V. Tatikonda, J. Manning Magid, *Radio frequency Identification and the Ethics of Privacy*, in *Organizational Dynamics*, 2007, 2, pp. 217-229.

J.E. Cohen, *DRM and Privacy*, in *Berkeley Technology Law Journal*, 2003, 189, pp. 575-617.

F.S. Collins *et al.*, *A vision for the future of genomics research. A blueprint for genomic era*, in *Nature*, 422, 2003, pp. 1-13.

V. Colomba (a cura di), *I diritti nell'era digitale. Libertà di espressione e proprietà intellettuale*, Diabasis, Reggio Emilia, 2004.

G. Comandè, *Al via l'attuazione della direttiva sul commercio elettronico, ma… serve un maggiore coordinamento*, in *Danno e responsabilità*, 2003, 7-8, pp. 809-815.

Comitato Nazionale per la Bioetica, *Etica, salute e nuove tecnologie dell'informazione*, Roma, 2006.

Comitato Nazionale per la Bioetica, *Orientamenti bioetici per i test genetici*, Roma, 1999.

Comitato Nazionale per la Bioetica, *Progetto genoma umano*, Roma, 1994.

Commissione Europea, *25 raccomandazioni concernenti le implicazioni etiche, giuridiche e sociali dei test genetici*, Brussels, 2004.

M. Consalvo, *Cheating. Gaining Advantages in Videogames*, The MIT Press, Cambridge, Massachusetts, 2007.

A. Conti *et al.*, *I test genetici. Etica, deontologia, responsabilità*, Giuffré, Milano, 2007.

P. Costanzo, *Motori di ricerca: un altro campo di sfida tra logiche del mercato e tutela dei diritti?*, in *Diritto dell'Internet*, 2006, 6, pp. 545-549.

P. Cristiani, F. Pinciroli, M. Stefanelli, *I sistemi informativi sanitari*, Pàtron, Bologna, 1996.

D. Crolla, *Cyberlaw: A Potent New Medicine for Health Law on The Internet*, in S. Callens (ed.), *E-Health and the Law*, Kluwer Law International, The Hague, The Netherlands, 2003, pp. 1-27.

V. Cuffaro, R. D'Orazio, V. Ricciuto (a cura di), *Il Codice del trattamento dei dati personali*, Giappichelli, Torino, 2007.

V. Cuffaro, V. Ricciuto, *La disciplina del trattamento di dati personali*, Giappichelli, Torino, 1997.

V. Cuffaro, V. Ricciuto, V. Zeno-Zencovich (a cura di), *Trattamento dei dati e tutela della persona*, Giuffré, Milano, 1998.

M. D'Alberti, *Poteri pubblici, mercati e globalizzazione*, Il Mulino, Bologna, 2008.

M. De Giorgi, A. Lisi, *Guida al codice della privacy: la protezione dei dati personali alla luce del D.Lgs. 196/2003*, Simone, Napoli, 2004.

D. De Kerckhove, A. Tursi (a cura di), *Dopo la democrazia? Il potere e la sfera pubblica nell'epoca delle reti*, Apogeo, Milano, 2006.

F. Di Ciommo, *Il trattamento dei dati sanitari tra interessi individuali e collettivi*, in *Danno e responsabilità*, 2002, 2, pp. 121-134.

A. Di Corinto, T. Tozzi, *Hacktivism. La libertà nelle maglie della rete*, Manifestolibri, Roma, 2002.

A. Di Giandomenico, *La genetica e l'evoluzione del diritto*, in A. Tarantino (a cura di), *Filosofia e politica dei diritti umani nel terzo millennio. Atti del V congresso dei filosofi politici italiani*, Lecce, 13-14-15 aprile 2000, Milano, 2003, pp. 509-515.

F. Di Luciano, *Il messaggio sms quale modalità di commissione del reato di molestie telefoniche*, in *Diritto dell'internet*, 2006, 4, pp. 374-376.

G. Elli, R. Zallone, *Il nuovo Codice della privacy (commento al D.lgs. 30 giugno 2003, n. 196)*, Giappichelli, Torino, 2004.

T.R. Eng, *Population Health Technologies. Emerging Innovations for the Health of the Public*, in *American Journal of Preventive Medicine*, 2004, 3, pp. 237-242.

M. Enserink, *Opponents Criticize Iceland's Database*, in *Science*, 1998, 5390, 282, p. 859.

J.S. Erickson, *Fair Use, DRM and Trusted Computing*, in *Communications of the ACM*, 2003, 4, pp. 34-39.

A. Etzioni, *The Limits of Privacy*, Basic Books, New York, 1999.

European Group on Ethics in Science and New Technologies, *Opinion on Ethical Aspects of Genetic Testing in the Workplace*, 28 luglio 2003.

European Group on Ethics in Science and New Technologies, *Opinion on Ethical issues of healthcare in the Information Society*, 30 luglio 1999.

G. Eysenbach, C. Köhler, *How do consumers search for and appraise health information on the world wide web? Qualitative study using focus groups, usability tests, and in-depth interviews*, in *British Medical Journal*, 2002, 324, pp. 573-577.

G. Eysenbach, E.R. Sa, T.L. Diepgen, *Shopping around the Internet today and tomorrow: towards the millennium of cybermedicine*, in *British Medical Journal*, 1999, 319, p. 1294.

G. Eysenback, J.E. Till, *Ethical issues in qualitative research on internet communities*, in *British Medical Journal*, 2001, 323, pp. 1103-1105.

E. Falletti, *Profili di diritto comparato*, nota a Trib. Aosta 25 maggio 2006, in *Diritto dell'internet*, 2006, 5, pp. 493-498.

C. Fanuele, *Un archivio centrale per i profili del DNA nella prospettiva di un "diritto comune" europeo*, in *Diritto penale e processo*, 2007, 3, pp. 385-394.

C. Faralli, *Dati genetici e tutela dei diritti*, in F. Lanchester, T. Serra (a cura di), *"Et si omnes…". Scritti in onore di Francesco Mercadante*, Giuffré, Milano, 2008, pp. 399-407.

M. Faundez-Zanuy, *Privacy Issues on Biometric Systems*, in *IEEE Aerospace & Electronic Systems Magazine*, 2005, 2, pp. 13-15.

M.R. Ferrarese, *Diritto sconfinato. Inventiva giuridica e spazi nel mondo globale*, Laterza, Roma-Bari, 2006.

M.R. Ferrarese, *Le istituzioni della globalizzazione. Diritto e diritti nella società transnazionale*, Il Mulino, Bologna, 2000.

A. Fici, *Mondo hacker e logica dell'azione collettiva*, Franco Angeli, Milano, 2004.

G. Fioriglio, P. Szolovits, *Copy Fees and Patients' Rights to Obtain a Copy of Their Medical Records: From Law to Reality*, in *Proceedings of American Medical Informatics Association Annual Symposium*, 2005, pp. 251-255.

G. Fioriglio, *La privacy e i sistemi di intercettazione globale: il caso dell'Information Awareness Office*, in *L'ircocervo*, 2003, 1.

G. Fioriglio, *Temi di informatica giuridica*, Aracne, Roma, 2004.

T. Forester, P. Morrison, *Computer Ethics. Cautionary Tales and Ethical Dilemmas in Computing*, MIT Press, Cambridge, Massachusetts, 1994.

G. Francione, *Hacker. I Robin Hood del ciberspazio*, Lupetti, Milano, 2004.

C.P. Friedman, J.C. Wyatt, *Evaluation Methods in Biomedical Informatics*, Springer Science, New York, 2006.

V. Frosini, *I giuristi e la società dell'informazione*, in *Il diritto dell'informazione e dell'informatica*, 1996, 1, pp. 17-20.

V. Frosini, *La protezione della riservatezza nella società informatica*, in *Informatica e diritto*, 1981, 1, pp. 5-14.

J.K. Gable, *An Overview of the Legal Liabilities Facing Manufacturers of Medical Information Systems*, in *Quinnipiac Health Law Journal*, 2001, 5, pp. 127-151.

P. Galdieri, *Profili di diritto penale*, nota a Trib. Aosta 25 maggio 2006, in *Diritto dell'internet*, 2006, 5, pp. 489-493.

F. Galgano, *La globalizzazione nello specchio del diritto*, Il Mulino, Bologna, 2005.

R. Gamberale, *Il settore sanitario*, in R. Panetta (a cura di), *Libera circolazione e protezione dei dati personali*, Giuffré, Milano, 2006, II, pp. 1499-1552.

G. Gambino, *Criteri e metodi per una valutazione etica degli screening genetici*, in *Tendenze nuove*, 2004, 4-5, 2004, pp. 425-441.

S. Gambino, *Trattato che adotta una Costituzione per l'Europa, Costituzioni nazionali, diritti fondamentali*, Giuffré, Milano, 2006.

Garante per la protezione dei dati personali, *Relazione 2006. Diritti dei cittadini, protezione dei dati e attività del Garante*, Roma, 2007.

S.L. Garfinkel, *An RFID Bill of Rights*, in *Technology Review*, 2002, http://www.technologyreview.com/Infotech/12953.

S.L. Garfinkel, A. Juels, R. Pappu, *RFID Privacy: An Overview of Problems and Proposed Solutions*, in *IEEE Security and Privacy*, 2005, 3, pp. 34-43.

R. Gartee, *Electronic Health Records. Understanding and Using Computerized Medical Records*, Prentice Hall, Old Tappan, New Jersey, 2007.

M. Gerosa, *Second Life*, Meltemi, Roma, 2007.

M. Gerosa, A. Pfeffer, *Mondi virtuali*, Castelvecchi, Roma, 2006.

S. Gevers, *Population screening: the role of the law*, in *European Journal of Health Law*, 1998, 5, 1, pp. 7-18.

G. Giacobbe, *Il diritto alla riservatezza: da diritto di elaborazione giurisprudenziale a diritto codificato*, in *Iustitia*, 1999, 2, pp. 91-124.

G. Giacobbe, *Il diritto alla riservatezza nella prospettiva degli strumenti di tutela*, in *DRT – Il diritto delle radiodiffusioni e delle telecomunicazioni*, 1982, 2, pp. 277-314.

G. Giacobbe, G. Giuffrida, *I diritti della personalità*, UTET, Torino, 2000.

E. Giannantonio, M.G. Losano, V. Zeno-Zencovich (a cura di), *Commentario alla legge 31 dicembre 1996, n. 675*, Cedam, Padova, 1997.

D. Goldstein *et al.*, *Medical Informatics 20/20. Quality and Electronic Health Records through Collaboration, Open Solutions and Innovation*, Jones & Bartlett, London, 2007.

M. Granieri, *La tutela dei diritti nella normativa sulla protezione dei dati personali: un bilancio provvisorio*, in *Danno e responsabilità*, 2004, 8-9, pp. 827-831.

M. Grauso, *Radio Frequency Identification Technology e tutela della persona*, in *Diritto dell'internet*, 2005, 6, pp. 623-628.

A. Greenhoug, H. Graham, *Protecting and using patient information: the role of the Caldicott Guardian*, in *Clinical Medicine*, 2004, 4, 3, pp. 246-249.

C. Gubitosa, *La storia di Internet*, Apogeo, Milano, 1999.

J.R. Gulcher, K. Stefansson, *The Icelandic Healthcare Database and Informed Consent*, in *New England Journal of Medicine*, 2000, 342, 24, pp. 1827-1830.

O. Günther, S. Spiekerman, *RFID and the Perception of Control: The Consumer's View*, in *Communications of ACM*, 2005, 9, pp. 73-76.

P. Harrigan, N. Wardrip-Fruin (eds.), *Second Person. Role-Playing and Story in Games and Playable Media*, The MIT Press, Cambridge, Massachusetts, 2007.

P. Himanen, *L'etica hacker e lo spirito dell'età dell'informazione*, tr. it., Feltrinelli, Milano, 2003.

J.S. Horner, *Research, ethics and privacy: the limits of knowledge*, in *Public Health*, 1998, 112, pp. 217-220.

S.J. Horowitz, *Competing Locklean Claims to Virtual Property*, in *Harvard Journal of Law & Technology*, 2007, 20, 2, pp. 443-458.

D. Hunter, *Cyberspace as a place, and the Tragedy of the Digital Anticommons*, in *California Law Review*, 2003, 2, pp. 439-519.

M. Iaselli, *Navigazione anonima in Rete*, in A. Maggipinto, M. Iaselli (a cura di), *Sicurezza e anonimato in rete. Profili giuridici e tecnologici della navigazione anonima*, Nyberg, Milano, 2005, pp. 9-24.

Ri. Imperiali, Ro. Imperiali, *Codice della privacy. Commento alla normativa sulla protezione dei dati personali*, Il Sole 24 ore, Milano, 2005.

Ri. Imperiali, Ro. Imperiali, *La tutela dei dati personali*, Il sole 24 ore, Milano, 1997.

N. Irti, *Norma e luoghi. Problemi di geo-diritto*, Laterza, Roma-Bari, 2001.

Istituto Superiore di Sanità, *Linee guida per i test genetici*, Roma, 1998.

V. Italia, *Articolo 3 (Principio di necessità nel trattamento dei dati)*, in Aa.Vv., *Codice della privacy*, Giuffré, Milano, 2004, pp. 40-46.

S. Kirschner, *Il codice della privacy, fra tradizione e innovazione*, in R. Panetta (a cura di), *Libera circolazione e protezione dei dati personali*, Giuffré, Milano, 2006, I, pp. 3-105.

E.H.W. Kluge, *Secure e-Health: Managing risks to patient health data*, in *International Journal of Medical Informatics*, 2007, 76, pp. 402-406.

L.T. Kohn, J.M. Corrigan, M.S. Donaldson (eds.), *To Err is Human: Building a Safer Health System*, National Academy Press, Washington, DC, 2000.

J. Kumagai, S. Cherry, *Sensors & Sensibility*, in *IEEE Spectrum*, 2004, 7, pp. 22-28.

S. Johnson, *La nuova scienza dei sistemi emergenti. Dalle colonie di insetti al cervello umano, dalle città ai videogame e all'economia, dai movimenti di protesta ai network*, tr. it., Garzanti, Milano, 2004.

M. Lamley, *Luogo e cyberspazio*, in V. Colomba (a cura di), *I diritti nell'era digitale. Libertà di espressione e proprietà intellettuale*, Diabasis, Reggio Emilia, 2004, pp. 77-104.

F. Lanchester, T. Serra (a cura di), *"Et si omnes…". Scritti in onore di Francesco Mercadante*, Giuffré, Milano, 2008.

S. Landini, *Assicurazioni sanitarie e privacy genetica*, in *Diritto pubblico*, 2003, 1, pp. 219-243.

F.G. Lastowka, D. Hunter, *The Laws of the Virtual Worlds*, in *California Law Review*, 2004, 92, 1, pp. 1-73.

D.H. Lea, J. Williams, M.P. Donahue, *Ethical Issues in Genetic Testing*, in *Journal of Midwifery & Women's Health*, 2005, 50, 3, pp. 234-240.

H.P. Lehman *et al.* (eds.), *Aspects of Electronic Health Record Systems*, Springer Science, New York, 2006.

L. Lessig, *Code version 2.0*, Basic Books, New York, 2006.

L. Lessig, *Il futuro delle idee*, tr. it., Feltrinelli, Milano, 2006.

N. Leveson, C.S. Turner, *An Investigation of the Therac-25 Accidents*, *IEEE Computer*, 1993, 7, pp. 18-41.

P. Levy, *Verso la ciberdemocrazia*, in D. De Kerckhove, A. Tursi (a cura di), *Dopo la democrazia? Il potere e la sfera pubblica nell'epoca delle reti*, Apogeo, Milano, 2006, pp. 3-23.

S. Levy, *Crypto. I ribelli del codice in difesa della privacy*, tr. it., Shake, Milano, 2002.

A. Lioy, *Riservatezza e sicurezza nei sistemi informativi sanitari*, in P. Cristiani, F. Pinciroli, M. Stefanelli, *I sistemi informativi sanitari*, cit., pp. 143-155.

L. Loevinger, *Jurimetrics. The Next Step Forward*, in *Minnesota Law Review*, 1949, 33, pp. 455-493.

M.G. Losano, *I progetti di legge italiani sulla riservatezza dei dati personali*, in *DRT. Il diritto delle radiodiffusioni e delle telecomunicazioni*, 1983, 2, pp. 275-283.

M.G. Losano, *La "giuscibernetica" dopo quattro decenni*, in *Il diritto dell'informazione e dell'informatica*, 2005, 4-5, 2005, pp. 727-751.

M.G. Losano (a cura di), *La legge italiana sulla privacy. Un bilancio dei primi cinque anni*, Laterza, Roma-Bari, 2001.

N. Lugaresi, *Internet, privacy e pubblici poteri negli Stati Uniti*, Giuffré, Milano, 2000.

D. Lyon, *La società sorvegliata. Tecnologie di controllo della vita quotidiana*, tr. it., Feltrinelli, Milano, 2002.

G. Maccaboni, *La profilazione dell'utente telematico fra tecniche pubblicitarie online e tutela della privacy*, in *Il diritto dell'informazione e dell'informatica*, 2001, 3, pp. 425-444.

A. Maggipinto, M. Iaselli (a cura di), *Sicurezza e anonimato in rete. Profili giuridici e tecnologici della navigazione anonima*, Nyberg, Milano, 2005.

M. Maglio, *La tutela dei dati personali*, Simone, Napoli, 1999.

R.S. Magnusson, *The Changing Legal and Conceptual Shape of Health Care Privacy*, in *Journal of Law, Medicine & Ethics*, 2004, 4, pp. 680-691.

T. Maldonado, *Reale e virtuale*, Feltrinelli, Milano, 2007.

F. Mantovani, voce *Manipolazioni genetiche*, in *Digesto delle discipline penalistiche*, Utet, Torino, 1995, VII, pp. 540-559.

G. Marazzita, *La Costituzione europea*, Laterza, Roma-Bari, 2006.

T. Margoni, *Il conflitto tra Digital Rights Management e privacy nel caso Sony-rootkit*, in *Diritto dell'internet*, 2006, 5, pp. 519-524.

A. Mascia, *Lo spamming telefonico e i pregiudizi alla vita privata dell'utente*, in *Responsabilità civile e previdenza*, 2006, 7-8, pp. 1321-1336.

A. Masters, K. Michael, *Lend me your arms: the use and implications of humancentric RFID*, in *Electronic Commerce Research and Applications*, 2007, 6, pp. 29-39.

F. Mastropaolo, voce *Ingegneria genetica*, in *Digesto delle discipline privatistiche*, sezione civile, UTET, Torino, 1999, IX, pp. 427-453.

V. Mathieu, *Privacy e dignità dell'uomo. Una teoria della persona*, Giappichelli, Torino, 2004.

R. Mazza, *Recenti sviluppi nella repressione internazionale dei crimini informatici: la Convenzione di Budapest del 2001*, in *La comunità internazionale*, 2004, 1, pp. 91-117.

S. Mazzamuto, *Il principio del consenso e il problema della revoca*, in R. Panetta (a cura di), *Libera circolazione e protezione dei dati personali*, Giuffré, Milano, 2006, I, pp. 991-1067.

C.M. Mazzoni (a cura di), *Etica della ricerca biologica*, Olschki, Firenze, 2000.

E.A. McGlynn, *Health Information Systems: design issues and analytic applications*, RAND Health, Santa Monica, California, 1998.

F. McMenamin, *Risks for E-Health*, in S. Callens (ed.), *E-Health and the Law*, Kluwer Law International, The Hague, The Netherlands, 2003, pp. 45-56.

J.F. Merz, G.E. McGee, P. Sankar, *"Iceland Inc."? On the ethics of commercial population genomics*, in *Social Science & Medicine*, 2004, 58, pp. 1201-1209.

M. Mezzanotte, *La memoria conservata in internet ed il diritto all'oblio telematico: storia di uno scontro annunciate*, in *Diritto dell'internet*, 2007, 4, pp. 398-405.

V. Milana, *La cartella clinica*, in F. Buzzi, P. Danesino (a cura di), *Gli esercenti le professioni sanitarie nel recente riassetto formativo. Interazioni e responsabilità nell'attuale cornice normativa delle aziende sanitarie*, Pavia, 26-27 settembre 2002, Giuffré, Milano, 2003, pp. 215-218.

R.A. Miller, K.F. Schaffner, A. Meisel, *Ethical and Legal Issues Related to the Use of Computer Programs in Clinical Medicine*, in *Annals of Internal Medicine*, 1985, 102, pp. 529-536.

T. Minella, *La privacy*, Simone, Napoli, 2001.

K.D. Mitnick, *L'arte dell'inganno. I consigli dell'hacker più famoso del mondo*, tr. it., Feltrinelli, Milano, 2003.

J. Monducci, G. Pasetti, *Il trattamento dei dati sanitari e genetici*, in J. Monducci, G. Sartor (a cura di), *Il Codice in materia di protezione dei dati personali*, CEDAM, Padova, 2004, pp. 255-282.

J. Monducci, G. Sartor (a cura di), *Il codice in materia di protezione dei dati personali*, CEDAM, Padova, 2004.

A. Monti, *Codici deontologici: se chi ruba i dati può scrivere le regole*, in http://www.interlex.it/675/amonti68.htm.

A. Monti, *Il caso "Le Iene" e le funzioni del Garante*, in http://www.interlex.it/675/amonti87.htm.

G. Morbidelli, F. Donati, *Una costituzione per l'Unione Europea*, Giappichelli, Torino, 2006.

L. Mormile, *I diritti dell'interessato*, in R. Panetta (a cura di), *Libera circolazione e protezione dei dati personali*, Giuffrè, Milano, 2006, II, pp. 1197-1241.

National Institute of Health, *Human Genome Project. Fact Sheet*, in http://www.nih.gov/about/researchresultsforthepublic/HumanGenomeProject.pdf.

National Research Council, *For the Record. Protecting Electronic Health Information*, National Academy Press, Washington, DC, 1997.

N. Negroponte, *Essere digitali*, Sperling & Kupfer, Milano, 1996.

S. Nespor, *Internet e la legge. Come orientarsi negli aspetti giuridici della rete*, Hoepli, Milano, 1999.

A. Nicoll, *Protecting health and patient confidentiality, ethics and surveillance*, in *Current Pediatrics*, 2005, 15, pp. 581-589.

S. Niger, *Il diritto alla protezione dei dati personali*, in J. Monducci, G. Sartor (a cura di), *Il codice in materia di protezione dei dati personali*, Cedam, Padova, 2004, pp. 1-17.

S. Niger, *Le nuove dimensioni della privacy: dal diritto alla riservatezza alla protezione dei dati personali*, Cedam, Padova, 2006.

T. Nyrhinen *et al.*, *Privacy and Equality in Diagnostic Genetic Testing*, in *Nursing Ethics*, 2007, 14, 3, pp. 295-308.

M. Ohkubo, K. Suzuki, S. Kinoshita, *RFID Privacy Issues and Technical Challenges*, in *Communications of the ACM*, 2005, 9, pp. 66-71.

M. O'Rourke, *Property Rights and Competition on the Internet: in Search of an Appropriate Analogy*, in *Berkeley Technology Law Journal*, 2001, 1, pp. 561-630.

G. Orwell, *1984*, Mondadori, Milano, 1989.

R. Panetta (a cura di), *Libera circolazione e protezione dei dati personali*, Giuffrè, Milano, 2006.

E. Pariotti, *Prospettive e condizioni di possibilità per un biodiritto europeo a partire dalla Convenzione di Oviedo sui diritti dell'uomo e la biomedicina*, in *Studium juris*, 2002, 5, pp. 561-570.

T. Perfetti, *Spamming e comunicazioni indesiderate*, in *Rivista di diritto, economia e gestione delle nuove tecnologie*, 2006, 2, pp. 148-160.

PEW/Internet, *Online Health Search 2006*, Washington, DC, 2006, in http://www.pewinternet.org.

S. Piazza, *Il progetto genoma umano e la responsabilità del genetista*, in C.M. Mazzoni (a cura di), *Etica della ricerca biologica*, Olschki, Firenze, 2000, pp. 23-37.

A. Pierucci, *La responsabilità del provider per i contenuti illeciti della Rete*, in *Rivista critica del diritto privato*, 2003, 1, pp. 143-165.

F. Piraino, *Il codice della privacy e la tecnica del bilanciamento di interessi*, in R. Panetta (a cura di), *Libera circolazione e protezione dei dati personali*, Giuffrè, Milano, 2006, I, pp. 693-741.

G.M. Pizzuti, *Il diritto di non sapere. Lo specifico dell'uomo bioetico*, La città del sole, Napoli, 2006.

E.O. Policella, *Il danno da "spamming"*, nota a Giudice di Pace di Napoli 10 giugno 2004, in *Diritto dell'internet*, 2005, 6, pp. 660-675.

J. Powell, R. Fitton, C. Fitton, *Sharing electronic health records: the patient view*, in *Informatics in primary care*, 2006, 14, pp. 55-57.

S. Prabhakar, S. Pankanti, A.K. Jain, *Biometric Recognition: Security and Privacy Concerns*, in *IEEE Security & Privacy*, 2003, 2, pp. 33-42.

A. Pradelli, *Nuove tecnologie: privacy e controlli del datore*, in *Diritto & pratica del lavoro*, 2007, 7, pp. 471-476.

S. Praduroux, *L'attualità del contributo della Convenzione europea di salvaguardia dei diritti dell'uomo e delle libertà fondamentali nell'evoluzione del diritto privato italiano e francese*, in *Rivista critica del diritto privato*, 2003, 4, pp. 705-744.

Privacy International, *A Race to the Bottom: Privacy Ranking of Internet Service Companies*, in http://www.privacyinternational.org/issues/internet/interimrankings.pdf.

W.L. Prosser, *Privacy [a legal analysis]*, in *California Law Review*, 1960, 48, pp. 338-423.

A. Proto Pisani, *La tutela giurisdizionale dei diritti della personalità: strumenti e tecniche di tutela*, in *Foro italiano*, 1990, V, cc. 1-19.

E.S. Raymond (ed.), *The New Hacker's Dictionary*, The MIT Press, Cambridge, Massachusetts, 1999.

Q. Renzong, *Human genome and philosophy: What ethical challenge will human genome studies bring to the medical practices in the 21st century?*, in *Life Sciences*, 2001, 324, pp. 1097-1102.

G. Riem, *Privacy e sicurezza*, Simone, Napoli, 2000.

P.A. Roche, G.J. Annas, *DNA Testing, Banking, and Genetic Privacy*, in *The New England Journal of Medicine*, 2006, 355, 6, pp. 545-546.

S. Rodotà, *Informazione genetica e diritti umani*, in Aa.Vv., *Lezioni di bioetica*, Ediesse, Roma, 1997.

S. Rodotà, *La privacy tra individuo e collettività*, in *Politica del diritto*, 1974, pp. 545-563.

S. Rodotà, *La vita e le regole. Tra diritto e non diritto*, Feltrinelli, Milano, 2006.

S. Rodotà, *Persona, riservatezza, identità. Prime note sistematiche sulla protezione dei dati personali*, in *Rivista critica di diritto privato*, 1997, 4, pp. 583-609.

S. Rodotà, *Privacy e costruzione della sfera privata*, in *Politica del diritto*, 1991, 4, pp. 521-546.

S. Rodotà, *Proprietà, Privacy e Pornografia, le tre "P" di Internet*, in *Problemi dell'informazione*, 2001, 2-3, pp. 238-243.

S. Rodotà, *Sul buon uso del diritto e i dilemmi della clonazione*, in *Rivista critica del diritto privato*, 1999, 4, pp. 561-569.

S. Rodotà, *Tecnologie e diritti*, Il Mulino, Bologna, 1995.

S. Rodotà, *Tecnopolitica*, Laterza, Roma-Bari, 1997.

S. Rodotà, *Trasformazioni del corpo*, in *Politica del diritto*, 2006, 1, pp. 3-24.

B. Roemer, *Trusted Computing, Digital Rights Management, and the Fight for Copyright Control on Your Computer*, in *UCLA Journal of Law and Technology*, 2003, 8 (http://www.lawtechjournal.com/articles/2003/08_040223_roemer.php).

M.A. Rothstein, M.K. Talbott, *The Expanding use of DNA in Law Enforcement: What Role for Privacy*, in *The Journal of Law, Medicine & Ethics*, 2006, 34, 2, pp. 153-164.

S.J. Russell, P. Norvig, *Intelligenza artificiale. Un approccio moderno*, tr. it., Pearson Education, Milano, 2005.

M. Russinovich, *More on Sony: Dangerous Decloaking Patch, EULAs and Phoning Home*, in http://blogs.technet.com/markrussinovich/archive/2005/11/04/more-on-sony-dangerous-decloaking-patch-eulas-and-phoning-home.aspx.

M. Russinovich, *Sony, Rootkits and Digital Rights Management Gone Too Far*, in http://blogs.technet.com/markrussinovich/archive/2005/10/31/sony-rootkits-and-digital-rights-management-gone-too-far.aspx.

M. Salvi, *Biotecnologie e bioetica, un ritorno alla metafisica? Terapia genica in utero, clonazione umana e lo statuto morale dell'embrione*, in *Rivista critica del diritto privato*, 1999, 4, pp. 587-597.

P. Sammarco, *Il motore di ricerca, nuovo bene della società dell'informazione: funzionamento, responsabilità e tutela della persona*, in *Il diritto dell'informazione e dell'informatica*, 2006, 4-5, pp. 621-634.

P.I. Santalahti *et al.*, *Women's decision making in prenatal screening*, in *Social Science & Medicine*, 1998, 46, 8, pp. 1067-1076.

G. Santaniello, *I fattori evolutivi della codificazione concernente i dati personali*, in http://www.interlex.com/675/santaniello11.htm.

G. Santaniello, *Le nuove garanzie nell'era del diritto alla protezione dei dati personali*, in http://www.interlex.it/675/santaniello9.htm.

G. Santaniello, *Ricerca genetica e tutela della persona*, in http://www.interlex.it/675/santaniello2.htm.

A. Santosuosso, *Il diritto alla disobbedienza genetica: il caso dell'Islanda*, in C.M. Mazzoni (a cura di), *Etica della ricerca biologica*, Olschki, Firenze, 2000 (anche in http://www.globius.org/documenti/Islanda.pdf).

A. Santosuosso, G. Gennari, *Il prelievo coattivo di campioni biologici e i terzi*, in *Diritto penale e processo*, 2007, 3, pp. 395-401.

R. Sapienza, *La convenzione europea sui diritti dell'uomo e la biomedicina*, in *Rivista di diritto internazionale*, 1998, 2, pp. 457-470.

G. Sartor, *Gli agenti software e la disciplina giuridica degli strumenti cognitivi*, in *Il diritto dell'informazione e dell'informatica*, 2003, 1, pp. 55-87

G. Sartor, *Il diritto della rete globale*, in G. Scorza, *Il diritto dei consumatori e della concorrenza in Internet. Pubblicità, privacy, contratti, concorrenza e proprietà intellettuale nel cyberspazio*, Cedam, Padova, 2006, pp. 1-33.

G. Sartor, *Intelligenza artificiale e diritto. Un'introduzione*, Giuffrè, Milano, 1996.

G. Sartor, *Privacy, reputazione, affidamento: dialettica e implicazioni per il trattamento dei dati personali*, in F. Bergadano *et al.*, *Privacy digitale. Giuristi e informatici a confronto*, Giappichelli, Torino, 2005, pp. 81-97.

W.B. Schwartz, *Medicine and the computer: the promise and problema of change*, in *The New England Journal of Medicine*, 1970, 283, pp. 1257-1264.

W.B. Schwartz, R.S. Patil, P. Szolovits, *Artificial Intelligence in Medicine. Where Do We Stand?*, in *The New England Journal of Medicine*, 1987, 316, pp. 685-688.

S. Scoglio, *Privacy. Diritto, filosofia, storia*, Editori Riuniti, Roma, 1994.

G. Scorza, *Il diritto dei consumatori e della concorrenza in Internet. Pubblicità, privacy, contratti, concorrenza e proprietà intellettuale nel cyberspazio*, Cedam, Padova, 2006.

T. Serra, *La democrazia redenta. Il cammino senza fine della democrazia*, Giappichelli, Torino, 2001.

T. Serra, *La disobbedienza civile. Una risposta alla crisi della democrazia?*, Giappichelli, Torino, 2002.

T. Serra, *Lo stato e la sua immagine*, Giappichelli, Torino, 2005.

T. Serra, *L'uomo programmato*, Giappichelli, Torino, 2003.

E. Sgreccia, *La Convenzione sui diritti dell'uomo e la biomedicina*, in *Medicina e morale*, 1997, 1, pp. 9-13.

K.I. Shine, *Technology and health*, in *Technology in Society*, 2004, 26, pp. 137-148.

E.H. Shortliffe, J.C. Cimino (ed.), *Biomedical Informatics. Computer Applications in Health Care and Biomedicine*, Spinger science, New York, 2006.

D. Silber, *The Case for eHealth*, European Institute for Public Administration, Maastricht, The Netherlands, 2003.

S. Simitis, *Crisi dell'informazione giuridica ed elaborazione elettronica dei dati*, tr. it., Giuffrè, Milano, 1977.

M. Sirimarco, *Tra apocalittici ed integrati: spunti di riflessione sul rapporto uomo-internet*, in A.C. Amato Mangiameli (a cura di), *Parola chiave: informazione*, Giuffrè, Milano, 2004, pp. 271-291.

A. Sirotti Gaudenzi, *Il nuovo diritto d'autore. La tutela della proprietà intellettuale nella società dell'informazione*, Maggioli, Santarcangelo di Romagna, 2005.

D.J. Solove, M. Rotenberg, P.M. Schwartz, *Information Privacy Law*, Aspen, New York, 2006.

G. Spoto, *I diritti dei consumatori*, in R. Panetta (a cura di), *Libera circolazione e protezione dei dati personali*, Giuffrè, Milano, 2006, I, pp. 385-439.

F. Stajano, *RFID Is X-Ray Vision*, in *Communications of the ACM*, 2005, 9, pp. 31-33.

P. Szolovits, *Artificial Intelligence and Medicine*, in Id. (ed.), *Artificial Intelligence in Medicine*, Westview Press, Boulder, Colorado, 1982, pp. 1-19.

P. Szolovits (ed.), *Artificial Intelligence in Medicine*, Westview Press, Boulder, Colorado, 1982.

M. Tamburini, A. Santosuosso (a cura di), *Malati di rischio. Implicazioni etiche, legali e psicologiche*, Masson, Milano, 1999.

A. Tarantino (a cura di), *Filosofia e politica dei diritti umani nel terzo millennio. Atti del V congresso dei filosofi politici italiani*, Lecce, 13-14-15 aprile 2000, Milano, 2003.

T.L. Taylor, *Play Between Worlds: Exploring Online Game Culture*, The MIT Press, Cambridge, Massachusetts, 2006.

D. Thomas, *Hacker Culture*, University of Minnesota Press, Minneapolis, Minnesota, 2002.

E. Tosi, *Diritto privato dell'informatica e di Internet. I beni – I contratti – Le responsabilità*, Giuffrè, Milano, 2006.

S. Tosoni, *Identità virtuali. Comunicazione mediata da computer e processi di costruzione dell'identità personale*, Franco Angeli, Milano, 2004.

A. Valeriani, *La tutela della privacy in ambito assicurativo*, in *Il diritto dell'informazione e dell'informatica*, 2004, 3, pp. 505-520.

A. Viterbo, A. Codignola, *La rete: tecnologia di libertà?*, in *Il diritto dell'infromazione e dell'informatica*, 2003, 2, pp. 219-246.

V. Viti, *Il danno da "spamming" e la tutela della riservatezza*, nota a Giudice di Pace di Napoli 29 settembre 2005, in *Il corriere del merito*, 2006, 2, pp. 170-175.

J.M. Walker, E.J. Bieber, F. Richards (eds.), *Implementing an Electronic Health Record System*, Springer science, New York, 2005.

S.D. Warren, L.D. Brandeis, *The Right to Privacy*, in *Harvard Law Review*, 1890, 5, pp. 193-220.

J.D. Watson, F.H. Crick, *A structure for desoxyribose nucleic acids*, in *Nature*, 1953, 171, pp. 737-738.

D.J. Weitzner *et al.*, *Information Accountability*, MIT Computer Science and Artificial Intelligence Technical Report, MIT-CSAIL-TR-2007-034, 2007.

A.F. Westin, *Privacy and freedom*, Atheneum, New York, 1967.

J. Wickins, *The ethics of biometrics: the risk of social exclusion from the widespread use of electronic identification*, in *Science and Engineering Ethics*, 2007, 1, pp. 45-54.

P. Wilson, *Sealing in the Quality: A Classification of Quality Assurance Initiatives for Health-Related Information on the Internet*, in S. Callens (ed.), *E-Health and the Law*, Kluwer Law International, The Hague, The Netherlands, 2003, pp. 57-65.

P.H. Winston, *Artificial Intelligence*, Addison Wesley, Reading, Massachusetts, 1993.

C. Woodford, *Trusted Computing or Big Brother? Putting the Rights Back in Digital Rights Management*, in *University of Colorado Law Review*, 2004, 75, pp. 253-300.

B. Wooley, *Mondi virtuali*, tr. it., Bollati Boringhieri, Milano, 1999.

World Health Organization, *Building foundations for eHealth. Progress of Member States. Report of the WHO Global Observatory for eHealth*, WHO Press, Geneva, 2006.

V.L. Yu *et al.*, *An Evaluation of MYCIN's ADVICE*, in B.G. Buchanan, E.H. Shortliffe (eds.), *Rule-Based Expert Systems: The MYCIN Experiments of the Stanford Heuristic Programming Project*, Addison Wesley, Reading, Massachusetts, 1984, pp. 589-596.

P. Zagnoni, *Sulla tutela penale del diritto alla riservatezza*, in *Rivista italiana di diritto e procedura penale*, 1982, 3, pp. 970-1003.

V. Zambrano, *Dati sanitari e tutela della sfera privata*, in *Il diritto dell'informazione e dell'informatica*, 1999, 1, pp. 1-28.

T. Zarsky, *Privacy and Data Collection in Virtual Worlds*, in J.M. Balkin, B.S. Noveck (eds.) *The State of Play. Law, Games and Virtual Worlds*, New York University Press, New York, 2006, pp. 217-223.

V. Zeno-Zencovich, *I diritti della personalità dopo la legge sulla tutela dei dati personali*, in *Studium Juris*, 1997, 5, pp. 466-469.

V. Zeno-Zencovich, *Il "diritto ad essere informati" quale elemento del rapporto di cittadinanza*, in *Il diritto dell'informazione e dell'informatica*, 2006, 1, pp. 1-10.

V. Zeno-Zencovich, *Informatica ed evoluzione del diritto*, in *Il diritto dell'informazione e dell'informatica*, 2003, 1, pp. 89-94.

V. Zeno-Zencovich, voce *Personalità (diritti della)*, in *Digesto delle discipline privatistiche*, sezione civile, Torino, 1997, XIII, pp. 430-444.

V. Zeno-Zencovich, *Telematica e tutela del diritto all'identità personale*, in *Politica del diritto*, 1983, 2, pp. 345-355.

V. Zeno-Zencovich, *Una lettura comparatistica della l. n. 675/96 sul trattamento dei dati personali*, in *Rivista trimestrale di diritto e procedura civile*, 1998, 3, pp. 733-745.

D. Zolo, *Globalizzazione*, in *Digesto delle discipline pubblicistiche*, Aggiornamento, UTET, Torino, 2005, pp. 378-398.

A. Zucchetti, *Privacy*, Giuffrè, Milano, 2005.

# INDICE DEI NOMI

# SOMMARIO

Capitolo III
TECNOLOGIE E METODOLOGIE DI CONTROLLO INDIVIDUALE E COLLETTIVO



Capitolo IV
IL DIRITTO ALLA PRIVACY NELL’AMBITO DELL’INFORMATICA MEDICA



Capitolo V
LA PRIVACY GENETICA FRA BIOETICA E DIRITTO

# PUBBLICAZIONI DEL SEMINARIO GIURIDICO DELLA UNIVERSITÀ DI BOLOGNA

1. Coli U., *Collegia et sodalitates*, 1913.
2. Donatelli I., *La "consortia" di Avesa*, 1914.
3. Valenza P., *Il diritto di usufrutto nelle leggi sulle tasse del registro*, 1915.
4. Zingali G., *La statistica della criminalità*, 1916.
5. Tumedei C., *La separazione dei beni ereditari*, 1917.
6. Albertoni A., *L'"Apokeryxis"*, 1923.
7. Salvi F., *La cessione dei beni ai creditori*, 1947.
8. Milani F., *Distinzioni delle servitù prediali*, 1948.
9. Fassò G., *I "quattro autori" del Vico*, 1949.
10. Ferri L., *La trascrizione degli acquisti "mortis causa" e problemi connessi*, 1951.
11. Rossi G., *La "Summa arboris actionum" di Ponzio da Ylerda*, 1951.
12. Poggeschi R., *Le associazioni e gli altri gruppi con autonomia patrimoniale nel processo*, 1951.
13. Matteucci N., *Antonio Gramsci e la filosofia della prassi*, 1951.
14. Forchielli P., *I contratti reali*, 1952.
15. Salvi F., *Il possesso di stato familiare*, 1952.
16. Fassò G., *La storia come esperienza giuridica*, 1953.
17. Palazzini Finetti L., *Storia della ricerca delle interpolazioni nel Corpus iuris giustinianeo*, 1953.
18. Rossi G., *Consilium sapientis iudiciale*, 1958.
19. Mancini G.F., *La responsabilità contrattuale del prestatore di lavoro*, 1957.
20. Ferri L., *L'autonomia privata*, 1959.
21. Torelli P., *Scritti di storia del diritto italiano*, 1959.
22. Santini G., *I Comuni di Valle del medioevo. La Costituzione federale del "Frignano"*, 1960.
23. Gianniti F., *I reati della stessa indole*, 1959.
24. Ghezzi G., *La prestazione di lavoro nella comunità familiare*, 1960.
25. Nardi E., *Case "infestate da spiriti" e diritto romano e moderno*, 1960.
26. Ferri L., *Rinunzia e rifiuto nel diritto privato*, 1960.
27. Ghezzi G., *La responsabilità contrattuale delle associazioni sindacali*, 1963.
28. Bonsignori A., *Espropriazione della quota di società a responsabilità limitata*, 1961.
29. Redenti E., *Scritti e discorsi giuridici di un mezzo secolo*, vol. I, *Intorno al diritto processuale*, 1962.
30. Redenti E., *Scritti e discorsi giuridici di un mezzo secolo*, vol. II, *Intorno al diritto sostanziale*, 1962.
31. Gualandi A., *Spese e danni nel processo civile*, 1962.
32. Bonsignori A., *Assegnazione forzata e distribuzione del ricavato*, 1960.
33. Mancini G.F., *Il recesso unilaterale e i rapporti di lavoro*, vol. I, *Individuazione della fattispecie. Il recesso ordinario*, 1962.
34. Nardi E., *Rabelais e il diritto romano*, 1962.
35. Romagnoli U., *Il contratto collettivo di impresa*, 1963.
36. Santini G., *I "comuni di pieve" nel medioevo italiano*, 1964.
37. Rudan M., *Il contratto di tirocinio*, 1966.
38. Bonini R., *I "libri de cognitionibus" di Callistrato. Ricerche sull'elaborazione giurisprudenziale della "cognitio extra ordinem"*, 1964.
39. Colliva P., *Ricerche sul principio di legalità nell'amministrazione del Regno di Sicilia al tempo di Federico II*, 1964.
40. Mengozzi P., *L'agenzia di approvvigionamento dell'Euratom*, 1964.
41. *Scritti minori di Antonio Cicu*, tomi I e II, *Scritti di teoria generale del diritto - Diritto di famiglia*, 1965.
42. *Scritti minori di Antonio Cicu*, *Successioni e donazioni. Studi vari*, 1965.
43. Sacchi Morsiani G., *Il potere amministrativo delle Comunità europee e le posizioni giuridiche dei privati*, I, 1965.
44. Ghezzi G., *La mora del creditore nel rapporto di lavoro*, 1965.
45. Roversi Monaco F.A., *Enti di gestione. Struttura, funzioni, limiti*, 1967.
46. Gianniti F., *L'oggetto materiale del reato*, 1966.

47. Mengozzi P., *L'efficacia in Italia di atti stranieri di potestà pubblica su beni privati*, 1967.
48. Romagnoli U., *La prestazione di lavoro nel contratto di società*, 1967.
49. Montuschi L., *I limiti legali nella conclusione del contratto di lavoro*, 1967.
50. Ranieri S., *Scritti e discorsi vari*, vol. I, *Scritti di diritto penale*, 1968.
51. Ranieri S., *Scritti e discorsi vari*, vol. II, *Scritti di procedura penale*, 1968.
52. Bonini R., *Ricerche di diritto giustinianeo*, 1968.
53. Santini G., *Ricerche sulle "Exceptiones legum romanorum"*, 1969.
54. Lo Castro G., *La qualificazione giuridica delle deliberazioni conciliari delle fonti del diritto canonico*, 1970.
55. Sacchi Morsiani G., *Il potere amministrativo delle Comunità europee e le posizioni giuridiche dei privati*, II, 1970.
56. Roversi Monaco F.A., *La delegazione amministrativa nel quadro dell'ordinamento regionale*, 1970.
57. Gianniti F., *Studi sulla corruzione del pubblico ufficiale*, 1970.
58. De Vergottini G., *Indirizzo politico della difesa e sistema costituzionale*, 1971.
59. Mengozzi P., *Il regime giuridico internazionale del fondo marino*, 1971.
60. Carinci F., *Il conflitto collettivo nella giurisprudenza costituzionale*, 1971.
61. Osti G., *Scritti giuridici*, voll. I e II, 1973.
62. Zuelli F., *Servizi pubblici e attività imprenditoriale*, 1973.
63. Pergolesi F., *Sistema delle fonti normative*, 1973.
64. Montuschi L., *Potere disciplinare e rapporto di lavoro*, 1973.
65. Pattaro E., *Il pensiero giuridico di L.A. Muratori tra metodologia e politica*, 1974.
66. Pini G., *Arbitrato e lavori pubblici*, 1974.
67. Carpi F., *L'efficacia "ultra partes" della sentenza civile*, 1974.
68. De Vergottini G., *Lo "Shadow cabinet"*, 1973.
69. Paolucci L.F., *La mutualità nelle cooperative*, 1974.
70. De Gennaro A., *Crocianesimo e cultura giuridica italiana*, 1974.
71. Stortoni L., *L'abuso di potere nel diritto penale*, 1978.
72. Gianniti F., *Prospettive criminologiche e processo penale*, 1977.
73. Bonvicini D., *Le "joint ventures": tecnica giuridica e prassi societaria*, 1977.
74. De Vergottini G., *Scritti di storia del diritto italiano*, voll. I, II, III, 1977.
75. Lambertini R., *I caratteri della Novella 118 di Giustiniano*, 1977.
76. Dalla D., *L'incapacità sessuale in diritto romano*, 1978.
77. Di Pietro A., *Lineamenti di una teoria giuridica dell'imposta sull'incremento di valore degli immobili*, 1978.
78. Mazzacuva N., *La tutela penale del segreto industriale*, 1979.
79. Romanelli G., *Profilo del noleggio*, 1979.
80. Borghesi D., *Il contenzioso in materia di eleggibilità*, 1979.
81. Dalla Torre G., *L'attività assistenziale della Chiesa nell'ordinamento italiano*, 1979.
82. Carpi F., *La provvisoria esecutorietà della sentenza*, 1979.
83. Alleva P., *Il campo di applicazione dello statuto dei lavoratori*, 1980.
84. Puliatti S., *Ricerche sulla legislazione "regionale" di Giustiniano*, 1980.
85. Fassò G., *Scritti di filosofia del diritto*, voll. I, II, III, 1982.
86. Sgubbi F., *Uno studio sulla tutela penale del patrimonio*, 1980.
87. Lambertini R., *Plagium*, 1980.
88. Dalla D., *Senatus consultum Silanianum*, 1980.
89. Vandelli L., *L'ordinamento regionale spagnolo*, 1980.
90. Nardi E., *L'otre dei parricidi e le bestie incluse*, 1980.
91. Pellicanò A., *Causa del contratto e circolazione dei beni*, 1981.
92. Giardini D., *Politica e amministrazione nello Stato fondato sul decentramento*, 1981.
93. Bortolotti D., *Potere pubblico e ambiente*, 1981.
94. Roffi R., *Contributo per una teoria delle presunzioni nel diritto amministrativo*, 1982.
95. Alessi R., *Scritti minori*, 1981.
96. Bassanelli Sommariva G., *L'imperatore unico creatore ed interprete delle leggi e l'autonomia del giudice nel diritto giustinianeo*, 1983.
97. Zanotti A., *Cultura giuridica del Seicento e* jus publicum ecclesiasticum *nell'opera del cardinal Giovanni Battista De Luca*, 1983.
98. Illuminati G., *La disciplina processuale delle intercettazioni*, 1983.
99. Toniatti R., *Costituzione e direzione della politica estera negli Stati Uniti d'America*, 1983.
100. Nardi E., *Squilibrio e deficienza mentale in diritto romano*, 1983.

101. Dalla D., *Praemium emancipationis*, 1983.
102. Mazzacuva N., *Il disvalore di evento nell'illecito penale - L'illecito commissivo doloso e colposo*, 1983.
103. *Studi in onore di Tito Carnacini*. I. *Studi di diritto costituzionale, civile, del lavoro, commerciale*, 1983.
104. Caia G., *Stato e autonomie locali nella gestione dell'energia*, 1984.
105. Baratti G., *Contributo allo studio della sanzione amministrativa*, 1984.
106. Bortolotti D., *Attività preparatoria e funzione amministrativa*, 1984.
107. Puliatti S., *Ricerche sulle novelle di Giustino II. La legislazione imperiale da Giustiniano I a Giustino II*, 1984.
108. Lambertini R., *La problematica della commorienza nell'elaborazione giuridica romana*, 1984.
109. Zuelli F., *Le collegialità amministrative*, 1985.
110. Pedrazzoli M., *Democrazia industriale e subordinazione*, 1985.
111. Zanotti M., *Profili dogmatici dell'illecito plurisoggettivo*, 1985.
112. Ruffolo U., *Interessi collettivi o diffusi e tutela del consumatore*, I, 1985.
113. Biagi M., *Sindacato democrazia e diritto*, 1986.
114. Insolera G., *Problemi di struttura del concorso di persone nel reato*, 1986.
115. Malagù L., *Esecuzione forzata e diritto di famiglia*, 1986.
116. Ricci G.F., *La connessione nel processo esecutivo*, 1986.
117. Zanotti A., *Il concordato austriaco del 1855*, 1986.
118. Selmini R., *Profili di uno studio storico sull'infanticidio*, 1987.
119. Dalla D., *"Ubi venus mutatur"*, 1987.
120. Zunarelli S., *La nozione di vettore*, 1987.
121. Zoli C., *La tutela delle posizioni "strumentali" del lavoratore*, 1988.
122. Cavina M., *Dottrine giuridiche e strutture sociali padane nella prima età moderna*, 1988.
123. Califano L., *Innovazione e conformità nel sistema regionale spagnolo*, 1988.
124. Sarti N., *Gli statuti della società dei notai di Bologna dell'anno 1336 (contributo allo studio di una corporazione cittadina)*, 1988.
125. Scarponi S., *Riduzione e gestione flessibile del tempo di lavoro*, 1988.
126. Bernardini M., *Contenuto della proprietà edilizia*, 1988.
127. La Torre M., *La "lotta contro il diritto soggettivo". Karl Larenz - la dottrina giuridica nazionalsocialista*, 1988.
128. Garcia De Enterria J., *Le obbligazioni convertibili in azioni*, 1989.
129. Biagi Guerini R., *Famiglia e Costituzione*, 1989.
130. Caia G., *Arbitrati e modelli arbitrali nel diritto amministrativo*, 1989.
131. Magagni M., *La prestazione caratteristica nella Convenzione di Roma del 19 giugno 1980*, 1989.
132. Petroni L., *La disciplina pubblicistica dell'innovazione tecnologica in Francia*, 1990.
133. Zanotti A., *Le manipolazioni genetiche e il diritto della Chiesa*, 1990.
134. Sartor G., *Le applicazioni giuridiche dell'intelligenza artificiale*, 1990.
135. Rossi L.S., *Il "buon funzionamento del mercato comune". Delimitazione dei poteri fra CEE e Stati membri*, 1990.
136. Luchetti G., *La legittimazione dei figli naturali nelle fonti tardo imperiali e giustinianee*, 1990.
137. Sarti N., *Un giurista tra Azzone e Accursio*, 1990.
138. Gustapane A., *La tutela globale dell'ambiente*, 1991.
139. Bottari C., *Principi costituzionali e assistenza sanitaria*, 1991.
140. Donini M., *Illecito e colpevolezza nell'imputazione del reato*, 1991.
141. Perulli A., *Il potere direttivo dell'imprenditore*, 1992.
142. Vandelli L. (a cura di), *Le forme associative tra enti territoriali*, 1992.
143. Gasparri P., *Institutiones iuris publici*, 1992.
144. Capuzzo E., *Dal nesso asburgico alla sovranità italiana*, 1992.
145. Biavati P., *Accertamento dei fatti e tecniche probatorie nel processo comunitario*, 1992.
146. Ferrari F., *Atipicità dell'illecito civile. Una comparazione*, 1992.
147. Gustapane A., Sartor G., Verardi C.M., *Valutazione di impatto ambientale. Profili normativi e metodologie informatiche*, 1992.
148. Orlandi R., *Atti e informazioni della autorità amministrativa nel processo penale. Contributo allo studio delle prove extracostituite*, 1992.
149. Carpani G., *Le aziende degli enti locali. Vigilanza e controlli*, 1992.

150. Musso A., *Concorrenza ed integrazione nei contratti di subfornitura industriale*, 1993.
151. Donini M., *Il delitto contravvenzionale. "Culpa iuris" e oggetto del dolo nei reati a condotta neutra*, 1993.
152. Califano Placci L., *Le commissioni parlamentari bicamerali nella crisi del bicameralismo italiano*, 1993.
153. Fornasari G., *Il concetto di economia pubblica nel diritto penale. Spunti esegetici e prospettive di riforma*, 1994.
154. Manzini P., *L'esclusione della concorrenza nel diritto antitrust italiano*, 1994.
155. Timoteo M., *Le successioni nel diritto cinese. Evoluzione storica ed assetto attuale*, 1994.
156. Sesta M. (a cura di), *Per i cinquant'anni del codice civile*, 1994.
157. Tullini P., *Contributo alla teoria del licenziamento per giusta causa*, 1994.
158. Rescigno F., *Disfunzioni e prospettive di riforma del bicameralismo italiano: la camera delle regioni*, 1995.
159. Lugaresi N., *Le acque pubbliche. Profili dominicali, di tutela, di gestione*, 1995.
160. Sarti N., *Maximum dirimendarum causarum remedium. Il giuramento di calunnia nella dottrina civilistica dei secoli XI-XIII*, 1995.
161. Colliva P., *Scritti minori*, 1996.
162. Dugato M., *Atipicità e funzionalizzazione nell'attività amministrativa per contratti*, 1996.
163. Gardini G., *La comunicazione degli atti amministrativi. Uno studio alla luce della legge 7 agosto 1990, n. 241*, 1996.
164. Manzini P., *I costi ambientali nel diritto internazionale*, 1996.
165. Mittica M.P., *Il divenire dell'ordine. L'interazione normativa nella società omerica*, 1996.
166. Luchetti G., *La legislazione imperiale nelle Istituzioni di Giustiniano*, 1996.
167. La Torre M., *Disavventure del diritto soggettivo. Una vicenda teorica*, 1996.
168. Camon A., *Le intercettazioni nel processo penale*, 1996.
169. Mancini S., *Minoranze autoctone e Stato. Tra composizione dei conflitti e secessione*, 1996.
170. Zanobetti Pagnetti A., *La non comparizione davanti alla Corte internazionale di giustizia*, 1996.
171. Bricola F., *Scritti di diritto penale*. Vol. I, *Dottrine generali, Teoria del reato e sistema sanzionatorio*. Vol. II, *Parte speciale e legislazione complementare, Diritto penale dell'economia*, 1997.
172. Graziosi A., *La sentenza di divorzio*, 1997.
173. Mantovani M., *Il principio di affidamento nella teoria del reato colposo*, 1997.
174. Biavati P., *Giurisdizione civile, territorio e ordinamento aperto*, 1997.
175. Rossi G. (1916-1986), *Studi e testi di storia giuridica medievale*, a cura di Giovanni Gualandi e Nicoletta Sarti, 1997.
176. Pellegrini S., *La litigiosità in Italia. Un'analisi sociologico-giuridica*, 1997.
177. Boni G., *La rilevanza del diritto dello Stato nell'ordinamento canonico. In particolare la canonizatio legum civilium*, 1998.
178. *Scritti in onore di Giuseppe Federico Mancini*. Vol. I, *Diritto del lavoro*, 1998.
179. *Scritti in onore di Giuseppe Federico Mancini*. Vol. II, *Diritto dell'Unione europea*, 1998
180. Rossi A., *Il GEIE nell'ordinamento italiano. Criteri di integrazione della disciplina*, 1998.
181. Bongiovanni G., *Reine Rechtslehre e dottrina giuridica dello Stato. H. Kelsen e la Costituzione austriaca del 1920*, 1998.
182. Caputo G., *Scritti minori*, 1998.
183. Garrido J.M., *Preferenza e proporzionalità nella tutela del credito*, 1998.
184. Bellodi Ansaloni A., *Ricerche sulla contumacia nelle* cognitiones extra ordinem, I, 1998.
185. Franciosi E., *Riforme istituzionali e funzioni giurisdizionali nelle Novelle di Giustiniano. Studi su nov. 13 e nov. 80*, 1998.
186. Cattabriga C., *La Corte di giustizia e il processo decisionale politico comunitario*, 1998.
187. Mancini L., *Immigrazione musulmana e cultura giuridica. Osservazioni empiriche su due comunità di egiziani*, 1998.
188. Gustapane A., *L'autonomia e l'indipendenza della magistratura ordinaria nel sistema costituzionale italiano. dagli albori dello Statuto Albertino al crepuscolo della bicamerale*, premessa di Giuseppe De Vergottini, 1999.
189. Ricci G.F., *Le prove atipiche*, 1999.
190. Canestrari S., *Dolo eventuale e colpa cosciente. Ai confini tra dolo e colpa nella struttura delle tipologie delittuose*, 1999.
191. Fassò G., *La legge della ragione*. Ristampa, a cura di Carla Faralli, Enrico Pattaro, Giampaolo Zucchini, 1999.

192. Fassò G., *La democrazia in Grecia*. Ristampa, a cura di Carla Faralli, Enrico Pattaro, Giampaolo Zucchini, 1999.
193. Scarciglia R., *La motivazione dell'atto amministrativo. Profili ricostruttivi e analisi comparatistica*, 1999.
194. Briguglio F., *"Fideiussoribus succurri solet"*, 1999.
195. Maltoni A., *Tutela dei consumatori e libera circolazione delle merci nella giurisprudenza della Corte di giustizia, profili costituzionali*, prefazione di Augusto Barbera, 1999.
196. Fondaroli D., *Illecito penale e riparazione del danno*, 1999.
197. Rossi L.S., *Le convenzioni fra gli Stati membri dell'Unione europea*, 2000.
198. Gragnoli E., *Profili dell'interpretazione dei contratti collettivi*, 2000.
199. Boni G., *La rilevanza del diritto secolare nella disciplina del matrimonio canonico*, 2000.
200. Lugaresi N., *Internet, privacy e pubblici poteri negli Stati Uniti*, 2000.
201. Lalatta Costerbosa M., *Ragione e tradizione. Il pensiero giuridico ed etico-politico di Wilehlmvon Humboldt*, 2000.
202. Semeraro P., *I delitti di millantato credito e traffico di influenza*, 2000.
203. Verza A., *La neutralità impossibile. Uno studio sulle teorie liberali contemporanee*, 2000.
204. Lolli A., *L'atto amministrativo nell'ordinamento democratico. Studio sulla qualificazione giuridica*, 2000.
205. Busetto M.L., *Giudice penale e sentenza dichiarativa di fallimento*, 2000.
206. Campanella P., *Rappresentatività sindacale: fattispecie ed effetti*, 2000.
207. Bricola F., *Scritti di diritto penale. Opere monografiche*, 2000.
208. Lassandari A., *Il contratto collettivo aziendale e decentrato*, 2001.
209. Bianco A., *Il finanziamento della politica in Italia*, 2001.
210. Raffi A., *Sciopero nei servizi pubblici essenziali. Orientamenti della Commissione di garanzia*, 2001.
211. Piergigli V., *Lingue minoritarie e identità culturali*, 2001.
212. Cafaro S., *Unione monetaria e coordinamento delle politiche economiche. Il difficile equilibrio tra modelli antagonisti di integrazione europea*, 2001.
213. Morrone A., *Il custode della ragionevolezza*, 2001.
214. Masutti A., *La liberalizzazione dei trasporti in Europa. Il caso del trasporto postale*, 2002.
215. Zanotti A., Orlando F., *L'itinerario canonistico di Giuseppe Caputo*, 2002.
216. Lupoi M.A., *Conflitti transnazionali di giurisdizioni*. Vol. I, *Policies, metodi, criteri di collegamento*. Vol. II, *Parallel proceedings*, 2002.
217. Lolli A., *I limiti soggettivi del giudicato amministrativo. Stabilità del giudicato e difesa del terzo nel processo amministrativo*, 2002.
218. Curi F., *Tertium datur. Dal Common Law al Civil Law per una scomposizione tripartita dell'elemento soggettivo del reato*, 2003.
219. Cottignola G., *Studi sul pilotaggio marittimo*, 2003.
220. Gardini G., *L'imparzialità amministrativa tra indirizzo e gestione. Organizzazione e ruolo della dirigenza pubblica nell'amministrazione contemporanea*, 2003.
221. Cevenini C., *Virtual enterprises. Legal issues of the on-line collaboration between undertakings*, 2003.
222. Monducci J., *Diritto della persona e trattamento dei dati particolari*, 2003.
223. Villecco Bettelli A., *L'efficacia delle prove informatiche*, 2004.
224. Zucconi Galli Fonseca E., *La convenzione arbitrale rituale rispetto ai terzi*, 2004.
225. Brighi R., *Norme e conoscenza: dal testo giuridico al metadato*, 2004.
226. Luchetti G., *Nuove ricerche sulle istituzioni di Giustiniano*, 2004.
227. *Studi in memoria di Angelo Bonsignori*, voll. I, II, 2004.
228. Piperata G., *Tipicità e autonomia nei servizi pubblici locali*, 2005.
229. Canestrari S., Foffani L. (a cura di), *Il diritto penale nella prospettiva europea. Quali politiche criminali per l'Europa?* Atti del Convegno organizzato dall'Associazione Franco Bricola (Bologna, 28 febbraio-2 marzo 2002), 2005.
230. Memmo D., Miconi S. (a cura di), *Broadcasting regulation: market entry and licensing. Regolamentazione dell'attività radiotelevisiva: accesso al mercato e sistema di licenze. Global Classroom Seminar*, 2006.
230. bis Briguglio F., *Studi sul procurator*, 2008.
231. Querzola L., *La tutela anticipatoria fra procedimento cautelare e giudizio di merito*, 2006.
232. Tarozzi S., *Ricerche in tema di registrazione e certificazione del documento nel periodo postclassico*, 2006.
233. Botti F., *L'eutanasia in Svizzera*, 2007.

234. Fondaroli D., *Le ipotesi speciali di confisca nel sistema penale*, 2007.
235. Alagna R., *Tipicità e riformulazione del reato*, 2007.
236. Giovannini M., *Amministrazioni pubbliche e risoluzione alternativa delle controversie*, 2007.
237. Montalti M., *Orientamento sessuale e costituzione decostruita. Storia comparata di un diritto fondamentale*, 2007.
238. Tordini Cagli S., *Principio di autodeterminazione e consenso dell'avente diritto*, 2008.
239. Legnani Annichini A., *La mercanzia di Bologna. Gli statuti del 1436 e le riformagioni quattrocentesche*, 2008.
240. Lolli A., *L'amministrazione attraverso strumenti economici*, 2008
241. Vaccarella M., *Titolarità e funzione nel regime dei beni civici*, 2008
242. Tubertini C., *Pubblica amministrazione e garanzia dei livelli essenziali delle prestazioni*, 2008
243. Fioriglio G., *Il diritto alla privacy. Nuove frontiere nell'era di Internet*, 2008

Finito di stampare nel mese di settembre 2008
presso Editografica – Rastignano (BO)