PROBLEMI E INIZIATIVE IN TEMA DI TUTELA DEI DATI PERSONALI, CON PARTICOLARE RIGUARDO AI DATI SANITARI

di Gianluigi Ciacci

Sommario: 1. La nuova informazione. – 2. I nuovi sistemi di informazione e le banche dati. – 3. La tutela dell'individuo nei confronti del potere informatico. – 3.1. La protezione dell'individuo mediante un'attività ermeneutica. – 3.2. La protezione dell'individuo mediante un'attività legislativa apposita. La situazione internazionale. – 4. L'attività degli organismi internazionali, in particolare della CEE. – 4.1. Le principali iniziative degli organismi internazionali. Loro finalità. – 4.2. La proposta di direttiva della Commissione delle Comunità europee del 24 settembre 1990. – 4.2.1. Campo di applicazione e norme sulla legittimità del trattamento dei dati. – 4.2.2. Disciplina del trattamento dei dati sensibili e dei rapporti con i Paesi terzi. – 5. La situazione in Italia, in particolare il nuovo progetto di legge all'esame del Parlamento (c. d. Mirabelli/bis). – 5.1. I motivi del ritardo italiano. – 5.2. Le disposizioni applicabili nell'ordinamento italiano in assenza di una legge organica sulla protezione dei dati. – 5.3. I progetti di legge. – 5.3.1. Il progetto Accame (21 aprile 1981). – 5.3.2. Il progetto Picano (24 febbraio 1982). – 5.3.3. Il progetto Seppia (27 gennaio 1984). – 5.3.4. Il progetto Martinazzoli (5 maggio 1984). – 5.4. Il secondo progetto Mirabelli (1989). – 6. Analisi specifica della disciplina di una particolare categoria di dati sensibili: la tutela dei dati sanitari. – 6.1. La disciplina dei dati sensibili. – 6.2. I dati sanitari. Nozione e caratteristiche particolari. – 6.3. Disciplina dei dati sanitari a livello degli organismi internazionali. – 6.4. La disciplina dei dati sanitari nei due maggiori disegni di legge italiani.

1. Oggi informarsi ed informare sono sempre più presupposti indefettibili di ogni attività intellettuale e sociale dell'uomo. Si può inoltre affermare che esiste un rapporto diretto tra grado di democraticità di un sistema politico e massa di informazioni rilevanti che circolano al suo interno: a conferma di ciò i drammatici avvenimenti verificatisi negli ultimi tempi in tutto il mondo, e specialmente in seguito al crollo dei sistemi comunisti. Nello stesso senso si esprime la Raccomandazione 854 emessa nel 1979 dal

Il presente scritto fa parte di una più ampia ricerca sugli «Aspetti giuridici del trasferimento elettronico dei dati» finanziata dal CNR (contratto 90.00269ST74) e diretta dal prof. Ettore Giannantonio.

Parlamento europeo, la quale afferma che «soltanto una società informatizzata può essere una società democratica»[1].

Quanto detto finora mantiene la sua validità anche su un piano più prettamente economico-giuridico.

Infatti nell'ambito dell'economia dei mercati occidentali, l'informazione può considerarsi oggi come un fattore di produzione, analogo e per certi versi più importante di altri; può considerarsi come la nuova materia prima degli ultimi anni del XX secolo, con ormai lo stesso peso, se non maggiore, del fattore lavoro[2].

Le imprese hanno infatti crescenti problemi di competitività sul piano interno ed internazionale, e cercano di recuperare produttività ed efficienza attraverso tutti quei mezzi che la tecnologia mette a disposizione per produrre, immagazzinare, trasferire, distribuire ed elaborare informazioni. Essa diventa fattore primario della produzione, merce privilegiata.

Così, dopo la società agricola, la società industriale e la società post-industriale, si può parlare oggi di società dell'informazione[3].

Nell'ambito di questo processo hanno svolto un ruolo fondamentale le nuove tecnologie informatiche. L'avvento e la vastissima diffusione dell'elaboratore elettronico, con le infinite possibilità di memorizzazione e trattamento delle informazioni, ma soprattutto la sua applicazione alle telecomunicazioni, con la nascita della telematica, e quindi la possibilità di trasmettere a distanza le informazioni elaborate, hanno profondamente rivoluzionato l'intero settore.

L'informazione cambia, diventa informazione automatica, informatica: viene ora intesa come un bene, che si produce, si vende, si acquista e si consuma, generando così il sorgere di una vera e propria industria, di un vero e proprio mercato di essa.

E proprio i bisogni del mercato oggi si orientano sempre più verso la necessità di accedere in maniera semplice e veloce, con minima spesa, ad un gran numero di informazioni di vario genere, elaborate ed aggiornate.

2. Per soddisfare tali esigenze nascono nuovi sistemi di informazione, «nuovi» perché resi possibili dalla più recente tecnologia. Volendo procedere ad una classificazione di questi nuovi sistemi informativi, e per fornire un quadro esauriente di essi, occorre distinguere a seconda che l'applicazione dell'informatica avvenga sui mezzi trasmissivi o sulla fornitura di informazioni.

Nel primo caso, in cui non si considera la fonte dei dati, ma solo il modo in cui avviene la loro diffusione, l'elaboratore elettronico ha reso possibile nuovi sistemi di comunicazione che hanno accelerato ulteriormente la velocità di circolazione delle informazioni. Si pensi al *telefax*, oramai diventato di uso comune, almeno nell'utenza affari, quasi quanto il telefono; si pensi ai servizi di messaggistica elettronica.

Qualora l'applicazione informatica avvenga invece nella fornitura di informazioni, prendendo quindi in considerazione la fonte di queste, occorre operare una distinzione a seconda che i dati vengano forniti *on line*, cioè quasi in tempo reale e attraverso una rete di telecomunicazione, oppure *off line*, cioè non attraverso una rete di telecomunicazione e con un aggiornamento periodico. La seconda ipotesi è quella della tecnologia dei *compact-disk*, o CD-ROM, supporto multimediale totale che permette di memorizzare, e quindi di accedere, non solo testi, ma anche immagini e commenti sonori: tecnologia che, almeno in Italia, sta avendo una larga diffusione, anche a livello giuridico[4].

Nel caso in cui le informazioni vengano fornite *on line*, cioè ripetiamo attraverso una rete di telecomunicazione e con aggiornamento in tempo reale, si verificano le ipotesi del *teletext*, del *videotext* e dei servizi di accesso a banche dati. Forma televisiva di lettura il primo, che consente agli utenti televisivi di avere una serie di servizi informativi di vario genere (dalle ultime notizie di attualità, alle previsioni del tempo e alle ricette di cucina) attraverso uno speciale decodificatore che viene oggi venduto con la maggior parte degli apparecchi video. Tipico esempio di servizio telematico il secondo che, attraverso questa volta la rete telefonica, permette di usufruire di vari servizi i quali, a differenza del *teletext*, si svolgono in maniera interattiva: si svolgono cioè mediante una sorta di colloquio tra utente e computer. Anche in questo caso i servizi sono di vario genere, tra i quali quelli di accesso a banche dati, che ora verranno esaminati[5].

Le banche dati, o *data bases*, sono raccolte elettroniche di informazioni, non duplicate, in correlazione reciproca ed utilizzabili per più applicazioni e da più utenti, sulle quali agiscono sistemi di ricerca automatizzati che permettono di operare una selezione di documenti in maniera efficace secondo le esigenze del ricercatore[6], consentendo così di operare una vera e propria trasformazione qualitativa degli effetti derivati dai tradizionali archivi

cartacei[7]. Le banche dati possono essere di informazione primaria, o fattuali, oppure di informazione secondaria. Le prime (*source data bases*) forniscono direttamente l'informazione stessa, il documento completo, quella cioè elaborabile per produrre nuova conoscenza. Le seconde (*reference data bases*) consentono invece di avere accesso ad informazioni di riferimento, poiché contengono dati che permettono di identificare e descrivere la fonte informativa atta a soddisfare le esigenze dell'utente; nella maggior parte dei casi forniscono anche un sommario del contenuto di tali fonti.

L'utente telematico ha quindi attualmente la possibilità, e si potrebbe dire la necessità, di consultare «in linea» grandi archivi nazionali ed internazionali di informazioni, ottenendo in modo quasi istantaneo risposte ai suoi quesiti sui più differenti argomenti e settori dello scibile umano.

Ma, nonostante il generico apprezzamento per questa evoluzione che si è verificata nel settore del trattamento e dell'utilizzo delle informazioni, si è da più parti avvertita l'esigenza di non lasciarsi trasportare da facili entusiasmi. Si è cercato quindi di sollecitare una riflessione attenta circa le implicazioni non solo sociali, ma anche giuridiche, attinenti a questa nuova «rivoluzione». Infatti è stato rilevato come oggi la capacità propria dell'elaboratore di confrontare e aggregare i dati più diversi tra loro in modo di trasformare informazioni disperse in una informazione organizzata e risalire così dagli atti più banali dell'individuo ai suoi più intimi segreti, e la possibilità di reperire immediatamente e di comunicare le informazioni così ottenute a chiunque le richieda, abbiano creato un nuovo potere di dominio sociale sull'individuo, il c. d. potere informatico[8].

3. Parallelamente alla creazione di questa nuova forma di potere, nasce e diventa sempre più pressante l'esigenza di protezione della persona di fronte al processo di informatizzazione di ogni aspetto della vita sociale.

Tale esigenza si è esplicata attraverso due indirizzi. Da una parte quello che cerca di proteggere l'individuo mediante gli strumenti già esistenti nell'ordinamento giuridico, quindi essenzialmente attraverso un'attività ermeneutica[9]. Dall'altra quello che tende alla protezione mediante la creazione di nuovi strumenti, in seguito all'emanazione di leggi apposite, quindi attraverso un'attività legislativa.

La seconda soluzione è quella adottata dai Paesi maggiormente informatizzati, atteso l'ormai pacifico riconoscimento circa la opportunità di risolvere a livello legislativo il problema, mentre la prima sussiste in quei Paesi ancora in attesa di emanare una normativa.

Entrambe le soluzioni comunque prendono le mosse da una base comune, il tradizionale sistema di protezione dell'individuo dalle ingerenze esplicate dall'esercizio del diritto all'informazione, salvo poi differenziarsi circa il metodo per ovviare ai limiti di tale tradizionale sistema di tutela.

Infatti il primo bene della persona che viene protetto dall'ordinamento giuridico è tradizionalmente la sua immagine, la cui diffusione è vietata senza il consenso dell'interessato, o in ogni caso se tale fatto rechi pregiudizio all'onore, alla reputazione o al decoro dell'individuo. Questa disciplina del diritto all'immagine è stata oggetto di un'interpretazione ampiamente analogica da parte di dottrina e giurisprudenza, tanto da farlo considerare l'aspetto più appariscente e pacifico di un più vasto diritto alla riservatezza o alla *privacy*[10].

Ne risulta un sistema complesso, ove coesistono e vengono tutelati contrapposti interessi e diritti: da una parte il diritto dell'informazione, e tra le sue espressioni il c.d. diritto di cronaca (i cui limiti sono stati affermati nella veridicità, interesse pubblico ed obiettività della notizia pubblicata), che ha raggiunto oggi la sua massima estensione ed estensibilità, grazie alle ricordate applicazioni informatiche; dall'altra il diritto alla riservatezza, i cui limiti corrispondono a quelli del diritto all'immagine (e quindi notorietà, pubblico interesse, informazione collegata a fatti pubblici), che deve essere oggi potenziato al massimo, vista la notevole estensione del diritto all'informazione.

Si può fin da ora rilevare che i mezzi tradizionali di protezione dell'individuo, brevemente analizzati nel loro precario equilibrio, di fronte ai nuovi sistemi di informazione risultano in genere insufficienti ed inadeguati.

Rilevata tale inadeguatezza, le due correnti di cui si è parlato in precedenza propongono soluzioni diverse.

3.1. Coloro infatti che si basano sugli strumenti già esistenti nell'ordinamento giuridico, tendono a potenziare tali strumenti.

Secondo tale indirizzo, il diritto alla riservatezza oggi non può

più essere considerato il diritto «ad essere lasciato solo», ma in una nuova dimensione sociale, e non più solo individuale, deve essere ora inteso come il potere di controllare l'uso che altri faccia delle informazioni riguardanti un determinato soggetto[11]. Questo soprattutto per cercare di porre un limite alla nuova società dell'informazione, un limite che tenga conto non solo dell'esigenza dell'individuo ad essere informato, ma anche dell'altrettanto basilare esigenza di questo a non subire discriminazioni illecite a causa delle informazioni raccolte.

Inoltre si è cercato di agire non solo sui poteri azionabili dall'individuo per reagire alle violazioni della propria riservatezza, ma anche preventivamente, disciplinando cioè l'attività connessa alla gestione di una banca dati[12].

Volendo disciplinare tale attività con gli strumenti già esistenti nell'ordinamento giuridico, riferendosi in particolare all'ordinamento giuridico italiano, occorre innanzitutto distinguere il momento di raccolta e memorizzazione delle informazioni da quello dell'elaborazione e diffusione delle stesse.

I limiti che si potrebbero porre nella prima ipotesi sono ricavabili in particolare, anche in questo caso, dalle leggi che tutelano l'immagine dell'individuo, intesa questa in senso ampio. Ma, più in generale, permettendoci di farvi rientrare un numero maggiore di fattispecie, da una norma costituzionale, l'art. 41, comma 2, che limita l'esercizio dell'attività economica, la quale non può svolgersi in contrasto con la libertà e dignità della persona umana. Applicando tale norma alla banca dati, se ne ricava che un'impresa di elaborazione dati va considerata legittima solo nella misura in cui essa operi in modo da non incidere sulla dignità della persona umana. Pur essendo un principio che sicuramente necessita di un ulteriore svolgimento da parte del legislatore ordinario, è principio che riguarda anche, e immediatamente, il giudice, chiamato a risolvere eventuali controversie sul punto.

Per quanto riguarda poi l'attività di diffusione delle informazioni elaborate, oltre a confermare l'applicazione dell'art. 41, comma 2, della Costituzione, è stato ipotizzato da una parte della dottrina[13] la possibilità di disciplinare l'attività di gestione di una banca dati come attività pericolosa, mediante l'applicazione delle norme sulla responsabilità civile (quindi l'art. 2055 del cod. civ.)[14].

3.2. Invece coloro che propongono l'esplicazione di un'attività

legislativa apposita per tutelare la persona dalle ingerenze dei nuovi sistemi informativi, pur recependo il nuovo modo di intendere il diritto alla riservatezza dell'indirizzo precedente, vanno oltre, suggerendo la creazione di strumenti *ad hoc*.

Quest'ultima soluzione è stata recepita in tutti i Paesi maggiormente informatizzati, ed è quella che, anche a livello internazionale, è consigliata dagli organismi delle principali organizzazioni internazionali[15]. Anche l'Italia, nonostante sia tuttora sprovvista di una normativa specifica, sembra muoversi in tal senso, attraverso i vari progetti di legge presentati in Parlamento[16].

La scelta di creare strumenti di tutela appositi sembra sicuramente di maggiore efficacia rispetto a quella che preferiva un'attività ermeneutica sulle fonti già esistenti, ma anche in questo caso sorgono alcuni problemi che diminuiscono notevolmente tale efficacia. Si pensi alla rapida evoluzione cui sono sottoposte le tecnologie informatiche e telematiche, alla complessa realtà dell'elaborazione dei dati: e quindi alla estrema facilità con cui una norma diventa vetusta e superata, o alla grande probabilità per cui possa risultare incompleta. Costituisce, secondo una parte della dottrina[17], un esempio di tale incompletezza, difetto comune alla maggioranza delle legislazioni in materia, il modo in cui vengono disciplinate le banche dati giornalistiche: in genere, infatti, nelle varie normative che tutelano la riservatezza si prevedono numerose eccezioni a favore dei *network* informativi, non rendendosi conto che in questo modo si frustra l'operatività dell'intera disciplina. Così, ai dati raccolti nell'esercizio legittimo dell'attività giornalistica non si applicano le disposizioni previste a garanzia della riservatezza dell'individuo: per i dati acquisiti in questo modo è infatti in genere permessa anche l'elaborazione di quelli raccolti segretamente o aventi natura di dati sensibili, talvolta senza addirittura l'obbligo di comunicazione all'interessato[18], equiparando in tal modo i dati provenienti dalla stampa a quelli pubblici per legge. È chiaro che previsioni di questo genere, pur soddisfacendo il diritto all'informazione della collettività, portano però a togliere efficacia alla normativa posta a protezione dell'individuo, poiché infatti, stando al nostro esempio, basterebbe filtrare le notizie attraverso la stampa per rendere lecita qualsiasi tipo di banca dati[19].

Comunque le direttive delle soluzioni legislative adottate nei vari Paesi, che hanno seguito la seconda corrente di pensiero, possono essere schematizzate in due posizioni contrapposte, in due differenti

indirizzi, ai quali corrispondono due diverse generazioni di leggi. Uno, di carattere più restrittivo, vieta qualsiasi raccolta di dati personali non espressamente e specificamente autorizzata con legge o provvedimento amministrativo: ad esso corrisponde la prima generazione di leggi sulla riservatezza, alla base delle quali vi è un profondo timore del legislatore nei confronti dell'elaboratore[20]. L'altra, più liberale, sancisce il principio di libertà di raccolta dei dati, senza necessità di alcuna autorizzazione, salvo l'obbligo di darne notificazione ad un particolare organo o ufficio, che controlla la liceità della raccolta delle informazioni: a tale indirizzo corrispondono le leggi di seconda generazione[21].

Anche per le normative che si rifanno all'indirizzo più liberale, una particolare attenzione viene comunque prestata alla tutela dei dati personali «sensibili», cioè a quelle notizie sull'individuo riguardanti l'origine razziale, la fede religiosa, le opinioni politiche, le informazioni sanitarie. Su questo punto, in particolare sui dati sanitari, ci si soffermerà oltre, in un apposito capitolo.

Altro elemento comune alle varie legislazioni è in ogni caso, come si è già detto, una rilettura del diritto alla riservatezza, inteso in senso più ampio, e delle facoltà ad esso connesse. Così si parla del diritto dell'individuo ad essere informato delle raccolte dei dati che concernono la propria persona; del diritto di accedere a tali dati; del diritto di chiedere la rettifica, la cancellazione o comunque la cessazione dell'abuso nel caso di dati erronei o illeciti. Più sinteticamente, del diritto di controllo, di accesso e di rettifica concessi all'individuo quale esplicazione di un più vasto diritto alla riservatezza di fronte all'ingerenza delle banche dati.

Oltre a tali facoltà riconosciute alla persona e da questa esercitabili singolarmente, in molte normative viene anche prevista la presenza di un organo pubblico che permetta un'ulteriore forma di tutela. Chiamato in differenti modi, Ufficio di controllo, Ispettorato dei dati, *Data protection registar*, o Garante, gli vengono affidati dalle varie legislazioni differenti compiti: dal semplice controllo della liceità degli scopi e delle modalità della raccolta dei dati, fino ad avere un vero e proprio potere di autorizzazione. Si unisce così alla forma di tutela affidata all'esercizio dei poteri del singolo individuo, che potremmo definire atomistica, un'ulteriore e diversa forma di tutela affidata ad un organo pubblico: garanzia di una maggiore imparzialità e di un più efficace contemperamento degli interessi delle parti, non ultimo quello del gestore della banca dati

a non essere esposto all'esercizio indiscriminato dei nuovi poteri concessi al singolo per proteggere la propria riservatezza.

Se queste sono le direttive delle soluzioni legislative adottate nei vari Paesi, analizzate in maniera sintetica, può risultare interessante soffermarsi ad esaminare l'attività di coordinamento svolta dagli organismi delle maggiori organizzazioni internazionali, in particolare della Comunità europea, e quindi la situazione nel nostro Paese. Successivamente si analizzerà in maniera specifica la disciplina di una particolare categoria di dati sensibili, quella dei dati sanitari.

4. L'esigenza di cui si è parlato all'inizio del presente scritto, cioè quella da parte di ognuno di informare e di essere informato, non è circoscrivibile ad un determinato ambito territoriale, ma comune ad ognuno in qualsiasi parte del mondo.

Anzi, sono proprio le peculiarità del nuovo bene informazione e della sua trasferibilità[22] che sembrano rendere obsoleta e non più adatta la tradizionale disciplina del commercio internazionale. È proprio nel campo dell'informatica, e specificamente in quello del trasferimento elettronico dei dati (Electronic Data Interchange, o E.D.I.), che maggiormente si avverte la necessità di nuove regole coordinate tra loro e valide per tutti i soggetti componenti la comunità internazionale[23]. Ed in particolare per ciò che riguarda il flusso transnazionale di dati personali, con il preciso fine di proteggere l'individuo anche nell'ambito sovranazionale.

4.1. Si vuole cioè evitare che i dati riguardanti una determinata persona, ed in qualche modo discriminanti, possano essere trasferiti da uno Stato munito di una normativa efficace e funzionante, ad un altro Stato che potrebbe addirittura essere sprovvisto di una disciplina a protezione dei dati personali, vero e proprio «paradiso informatico». Si vuole anche evitare che le varie legislazioni nazionali, pur perseguendo lo stesso obiettivo (la protezione della persona interessata), adottino soluzioni diverse, non coordinate tra loro, a causa delle molteplici scelte possibili. Questo specificamente per ciò che riguarda, ad esempio, la disciplina applicabile agli archivi manuali, la protezione delle persone giuridiche, le procedure preventive alla creazione degli archivi, la portata dell'obbligo di notifica, il trattamento dei dati sensibili, il trasferimento verso altri Paesi, tutti temi suscettibili di essere affrontati in maniera diversa[24].

Fondamentale funzione in tal senso hanno svolto gli organismi internazionali, mediante le numerose iniziative adottate allo scopo di suggerire ai singoli Stati l'emanazione di norme a garanzia della vita privata e della riservatezza nei confronti dei pericoli derivanti da un uso scorretto dei sistemi automatici di elaborazione di dati a carattere personale, e allo scopo di coordinare le normative, già esistenti, tra loro[25].

Specificamente hanno seguito tale direzione il Consiglio d'Europa[26], in particolare con la Convenzione del 28 gennaio 1981 sulla protezione delle persone relativamente al trattamento automatizzato dei dati personali, attualmente unico strumento di diritto internazionale applicabile in materia; inoltre l'Organizzazione per la Cooperazione e lo Sviluppo Economico (OCSE)[27], la Fondazione Europea della Scienza (ESF)[28], e le Comunità europee[29].

Particolarmente significativa risulta essere la Raccomandazione adottata il 29 luglio 1981 dalla Commissione delle Comunità europee, che esordisce così: «con l'introduzione dell'elaborazione automatica dei dati e il suo crescente uso in molti campi della vita privata, aumenta il pericolo di un abuso nell'utilizzo di tali dati (...)». E siccome «la sfera della vita privata ha bisogno di un'ampia protezione per quanto riguarda i dati (...) è auspicabile che si operi all'interno della Comunità un'armonizzazione del livello di protezione dei dati» affinché venga fornito in tal modo un importante contributo alla realizzazione dei diritti dei cittadini su scala europea.

4.2. Di grande attualità e di rilevante importanza è inoltre la recente proposta di direttiva concernente la protezione delle persone relativamente al trattamento dei dati personali, emanata dalla Commissione delle Comunità europee il 24 settembre 1990, attualmente all'esame del Parlamento. L'importanza di tale proposta risiede non solo nell'atto in sé, tentativo di disciplina esaustiva della materia dei rapporti tra individuo e banca dati, ma anche nel fatto che, una volta approvata dal Parlamento, essa diventerebbe immediatamente esecutiva, con forza e valore di legge, in tutti gli Stati membri. Ed anzi, in particolare, nei Paesi ancora privi di una normativa interna, come l'Italia, diventerebbe l'unica disciplina applicabile.

La proposta di direttiva ha per oggetto la predisposizione di una protezione equivalente, di elevato livello, in tutti gli Stati membri della Comunità, al fine di eliminare gli ostacoli agli scambi

di dati necessari al funzionamento del mercato interno[30]. L'approccio proposto dalla Commissione mira a raggiungere e garantire questo elevato livello di protezione mediante un sistema comunitario che si basa su una gamma di misure fra loro complementari, che verranno esaminate più avanti. In ogni caso i principi della direttiva potranno comunque essere completati: vengono previste infatti numerose disposizioni alle quali gli Stati membri possono apportare precisazioni per gli archivi soggetti alla loro legislazione. Viene anche prevista la possibilità di adottare misure complementari da parte del singolo Stato per l'applicazione di taluni principi generali a settori che presentano peculiarità importanti.

Nonostante le numerose critiche alle proposte di direttiva della Commissione, sollevate da esperti ed operatori del settore[31], risulta comunque interessante analizzare, anche se in maniera sintetica e limitatamente agli articoli più rilevanti, alcuni degli aspetti della disciplina stabilita in tale atto.

4.2.1. *Campo di applicazione e norme sulla legittimità del trattamento dei dati.* Innanzitutto per il campo di applicazione della futura normativa, esteso non solo agli archivi automatizzati, ma anche a quelli che si basano su un trattamento manuale di dati, purché «strutturati ed accessibili in una raccolta organizzata secondo criteri tali da facilitarne l'utilizzazione e l'interconnessione» (art. 2): non solo agli archivi del settore pubblico, ma anche a quelli del settore privato (art. 3)[32].

Una distinzione nella disciplina tra questi ultimi settori nei quali si svolge l'attività di gestione della banca dati, in genere più rigida per gli archivi del settore privato, viene prevista per ciò che riguarda la legittimità del trattamento dei dati, in particolare per la comunicazione dei dati personali.

Infatti, la creazione di un archivio relativo al settore pubblico è legittima se necessaria per lo svolgimento dei compiti dell'autorità pubblica, oppure, anche per finalità diverse, nel caso la persona interessata vi acconsenta o non abbia interessi legittimi contrastanti, o qualora il trattamento abbia una base giuridica, o ancora nel caso di minaccia imminente all'ordine pubblico o di rischio di violazioni del diritto di terzi (art. 5). Per quanto riguarda la comunicazione di dati personali a terzi, rilevata la necessità di una disposizione specifica per disciplinare questo aspetto del trattamento dei dati, si distingue a seconda che il *destinatario* appartenga a sua volta

al settore pubblico o a quello privato. Nel primo caso, la comunicazione deve essere necessaria all'esercizio delle funzioni dell'amministrazione che domanda o che comunica i dati; nel secondo, si impone una valutazione degli interessi in causa onde determinare la fondatezza dell'interesse legittimo del richiedente ad evitare che prevalga quello della persona interessata (art. 6).

La creazione poi di un archivio relativo al settore privato è legittima se basata sul consenso dell'interessato, o, in mancanza di tale consenso, nel caso in cui: esista una relazione di tipo contrattuale tra responsabile dell'archivio e persona interessata, purché il trattamento sia necessario all'esecuzione del contratto; i dati provengano da fonti generalmente accessibili al pubblico, se il trattamento sia destinato alla corrispondenza; il responsabile dell'archivio abbia un interesse legittimo, o comunque l'interesse della persona interessata non sia preminente. La comunicazione dei dati è poi legittima solo se compatibile con la finalità dell'archivio, quale notificata all'autorità di controllo[33], e non contraria all'ordine pubblico (art. 8). Deve comunque essere informata la persona interessata «in occasione della prima comunicazione o dell'apertura di una possibilità di consultazione in linea»: a meno che i dati provengano da fonti generalmente accessibili al pubblico e il loro trattamento sia unicamente destinato alla corrispondenza[34]. In caso contrario se l'interessato si oppone alla comunicazione o a qualsiasi altro trattamento, il responsabile dell'archivio deve porre termine al trattamento contestato (art. 9, possibilità di esercizio concreto del diritto di accesso da parte della persona interessata).

4.2.2. *Disciplina del trattamento dei dati sensibili e dei rapporti con i Paesi terzi.* È opinione generalmente riconosciuta che il diritto alla vita privata può essere compromesso non tanto dal contenuto di un archivio, quanto dal contesto in cui si opera un trattamento di dati personali. Tuttavia è altrettanto genericamente ammesso che alcuni tipi di dati, per il loro solo contenuto, a prescindere dal contesto in cui sono elaborati, possono violare il diritto alla vita privata dell'individuo. Per quanto riguarda quindi la disciplina del trattamento automatizzato di queste categorie di informazioni personali, c.d. «dati sensibili»[35], l'art. 17, al paragrafo 1, ne vieta il trattamento automatizzato, salvo consenso libero, esplicito e scritto dell'interessato.

Si può fin da ora rilevare, prima di esaminare la deroga stabilita

nel paragrafo 2 dello stesso articolo alla disciplina appena esaminata, che il campo di applicazione della norma è comunque limitato, poiché riguarda i soli trattamenti «automatizzati» dei dati sensibili, e non anche quelli tradizionali[36]. Gli Stati membri possono però derogare alla regola stabilita nel paragrafo 1 dell'art. 17 per consentire l'elaborazione dei dati sensibili, qualora lo richieda un importante interesse generale[37].

Ha suscitato invece notevoli critiche la previsione dell'art. 24 della proposta, circa i rapporti con i Paesi terzi, secondo cui «gli Stati membri dispongono nella loro legislazione che il trasferimento temporaneo o definitivo, verso un Paese terzo, di dati personali che formano oggetto di un trattamento, oppure raccolti a tal fine, può aver luogo soltanto a condizione che detto Paese garantisca un livello di protezione adeguato». È soprattutto la parte della norma che parla di protezione «adeguata», e non «equivalente» (come previsto nella Convenzione del Consiglio d'Europa 28 gennaio 1981), a provocare le maggiori perplessità. Infatti viene rilevato che in questo modo si corre «il rischio di un totale isolamento della Comunità dal resto del mondo»[38]. La lettura completa dell'articolo in esame, ed in particolare della complessa ed esaustiva procedura per stabilire l'«inadeguatezza» di una normativa, e degli strumenti per porvi rimedio (possibilità di avviare negoziati con il Paese terzo interessato), sembra in realtà minimizzare i pericoli connessi al trasferimento di dati personali verso Paesi terzi.

A prescindere comunque dalle differenti opinioni circa l'adeguatezza della proposta di direttiva a disciplinare il trattamento dei dati personali, in ogni caso rimane integra l'importanza di tale atto: tra l'altro quale esempio per gli ultimi orientamenti internazionali della materia. Particolarmente utile quindi nel caso di Paesi ancora in attesa di una normativa, situazione che si registra oggi in Italia.

5. In Italia il problema della tutela della riservatezza in relazione all'uso degli elaboratori è oggetto di discussione già da molti anni, ma, nonostante ciò, la regolamentazione giuridica della materia è ancora agli albori.

Infatti è sopratutto nel nostro Paese che maggiormente si rispecchiano i due indirizzi di cui si è parlato all'inizio del presente scritto, le due correnti di pensiero che sostengono differenti approcci per la tutela dell'individuo (attività ermeneutica o attività legislativa apposita). In Italia il dibattito sul punto si è svolto in un

nel paragrafo 2 dello stesso articolo alla disciplina appena esaminata, che il campo di applicazione della norma è comunque limitato, poiché riguarda i soli trattamenti «automatizzati» dei dati sensibili, e non anche quelli tradizionali[36]. Gli Stati membri possono però derogare alla regola stabilita nel paragrafo 1 dell'art. 17 per consentire l'elaborazione dei dati sensibili, qualora lo richieda un importante interesse generale[37].

Ha suscitato invece notevoli critiche la previsione dell'art. 24 della proposta, circa i rapporti con i Paesi terzi, secondo cui «gli Stati membri dispongono nella loro legislazione che il trasferimento temporaneo o definitivo, verso un Paese terzo, di dati personali che formano oggetto di un trattamento, oppure raccolti a tal fine, può aver luogo soltanto a condizione che detto Paese garantisca un livello di protezione adeguato». È soprattutto la parte della norma che parla di protezione «adeguata», e non «equivalente» (come previsto nella Convenzione del Consiglio d'Europa 28 gennaio 1981), a provocare le maggiori perplessità. Infatti viene rilevato che in questo modo si corre «il rischio di un totale isolamento della Comunità dal resto del mondo»[38]. La lettura completa dell'articolo in esame, ed in particolare della complessa ed esaustiva procedura per stabilire l'«inadeguatezza» di una normativa, e degli strumenti per porvi rimedio (possibilità di avviare negoziati con il Paese terzo interessato), sembra in realtà minimizzare i pericoli connessi al trasferimento di dati personali verso Paesi terzi.

A prescindere comunque dalle differenti opinioni circa l'adeguatezza della proposta di direttiva a disciplinare il trattamento dei dati personali, in ogni caso rimane integra l'importanza di tale atto: tra l'altro quale esempio per gli ultimi orientamenti internazionali della materia. Particolarmente utile quindi nel caso di Paesi ancora in attesa di una normativa, situazione che si registra oggi in Italia.

5. In Italia il problema della tutela della riservatezza in relazione all'uso degli elaboratori è oggetto di discussione già da molti anni, ma, nonostante ciò, la regolamentazione giuridica della materia è ancora agli albori.

Infatti è sopratutto nel nostro Paese che maggiormente si rispecchiano i due indirizzi di cui si è parlato all'inizio del presente scritto, le due correnti di pensiero che sostengono differenti approcci per la tutela dell'individuo (attività ermeneutica o attività legislativa apposita). In Italia il dibattito sul punto si è svolto in un

dati personali, che in genere nel settore informatico è mancata una politica di coordinamento e di controllo, nonché di promozione e di indirizzo, di cui altri Paesi ci hanno fornito l'esempio[43]. Questo ha portato ad una presa di coscienza un po' tardiva del fenomeno (con l'eccezione dell'ambiente assai ristretto nel quale il dibattito sulla tutela della riservatezza si è svolto).

Inoltre, per molto tempo, si è teso a minimizzare il problema, considerandolo prematuro (nonostante il diffondersi degli elaboratori elettronici nell'apparato pubblico e nelle imprese private), nella sfiduciata consapevolezza che il perdurare di una situazione di inefficienza e di mancanza di coordinamento nei vari settori della pubblica amministrazione costituiva un efficace presidio contro l'evocato pericolo[44].

Vi sono state anche delle resistenze specifiche alle normative previste dai vari disegni di legge, frutto di una tendenza al rifiuto dell'intervento legislativo, di cui si è già parlato e che non ha avuto molto seguito: gli si preferiva un'autoregolamentazione o codice di comportamento, destinato d'altra parte a valere per il solo settore privato, dato che i comportamenti della pubblica amministrazione, come è noto, sono regolati dalla legge. Una soluzione siffatta, proposta dal mondo imprenditoriale[45], era motivata dalla preoccupazione che un sistema di controlli amministrativi e di imposizione di numerosi adempimenti risultasse paralizzante e fortemente pregiudizievole per lo svolgimento dell'attività economica. Dal punto di vista economico, infatti, le leggi sulla tutela della riservatezza impongono in genere un rilevante onere alle imprese e agli enti che gestiscono banche di dati personali, onere che era ritenuto eccessivo in rapporto al valore del bene da tutelare.

Resistenze si ebbero anche dal mondo scientifico, preoccupato dal fatto che una legge potesse, nel campo della ricerca, precludere o comunque limitare le possibilità di accesso a fonti di informazione indispensabili, e per giunta divenute di uso comune. Non bisogna poi dimenticare che tra gli esperti del settore vi era chi asseriva l'opportunità di disciplinare la materia mediante le fonti già esistenti nell'ordinamento.

Dal punto di vista politico, infine, ci si chiedeva se le esigenze di controllo democratico non imponessero il contrario della riservatezza, e cioè la pubblicità, almeno in specifici campi (si pensi alle polemiche sul segreto di Stato). Un'ulteriore estensione della riservatezza era considerata da taluni come incompatibile con le

esigenze di una società democratica, visto che certi riserbi sono tanto più gelosi, quanto più sono turpi i traffici che essi celano. Da non sottovalutare anche l'ignoranza della classe politica, totalmente disinformata circa la natura, l'oggetto e la sostanza del problema delle banche dati e della tutela della riservatezza.

Questi quindi alcuni dei motivi del ritardo italiano rispetto agli altri Paesi che, oltre a provocare la già ricordata situazione di inadempienza internazionale, corre il rischio di porre l'Italia a livello degli Stati sottosviluppati, nonostante la posizione di preminenza nell'ambito tecnologico. Risulta interessante a questo punto analizzare come si supplisce alla situazione appena analizzata, cioè su quali basi nel nostro ordinamento si svolge l'attività ermeneutica degli operatori del diritto per disciplinare la realtà qui esaminata.

5.2. Le disposizioni applicabili nell'ordinamento italiano in assenza di una legge organica sulla protezione dei dati. Occorre inizialmente rilevare che in Italia, pur in assenza di una legge organica sulla protezione dei dati, non si ha però una situazione di totale vuoto normativo. Anzi, più volte il legislatore ha anticipato alcune forme di tutela della riservatezza in una serie di disposizioni riferibili, direttamente o meno, al settore dell'informatica, che sono però prive di uno sviluppo e di una sistematica normativa organica. Si è parlato di «legislazione sommersa»[46] per il fatto che in genere manca, in tali norme, un riferimento diretto all'informatica.

I due interventi legislativi più significativi in tal senso sono rappresentati dalla legge 20 maggio 1970, n. 300, c.d. Statuto dei lavoratori, e dalla legge 1° aprile 1981, n. 121, concernente il nuovo ordinamento della Amministrazione della Pubblica Sicurezza. Per ciò che riguarda il primo dei due atti citati, due sono gli articoli che interessano, e precisamente l'art. 8, che vieta al datore di lavoro di effettuare indagini, ai fini dell'assunzione del prestatore d'opera, su fatti non rilevanti per la valutazione della sua attività professionale; e l'art. 4[47], che vieta al datore di lavoro di usare impianti audiovisivi ed altre apparecchiature per finalità di controllo a distanza dell'attività del lavoratore, salvo eccezioni (ad esempio per motivi di sicurezza). La legge sul nuovo ordinamento dell'Amministrazione della Pubblica Sicurezza[48] contiene invece una serie di disposizioni che interessano la tutela dei dati, e precisamente gli articoli da 6 a 12: tanto da presentarla come una vera e propria «mini-legge» sulla protezione dei dati personali. In realtà, essa ha

esigenze di una società democratica, visto che certi riserbi sono tanto più gelosi, quanto più sono turpi i traffici che essi celano. Da non sottovalutare anche l'ignoranza della classe politica, totalmente disinformata circa la natura, l'oggetto e la sostanza del problema delle banche dati e della tutela della riservatezza.

Questi quindi alcuni dei motivi del ritardo italiano rispetto agli altri Paesi che, oltre a provocare la già ricordata situazione di inadempienza internazionale, corre il rischio di porre l'Italia a livello degli Stati sottosviluppati, nonostante la posizione di preminenza nell'ambito tecnologico. Risulta interessante a questo punto analizzare come si supplisce alla situazione appena analizzata, cioè su quali basi nel nostro ordinamento si svolge l'attività ermeneutica degli operatori del diritto per disciplinare la realtà qui esaminata.

5.2. Le disposizioni applicabili nell'ordinamento italiano in assenza di una legge organica sulla protezione dei dati. Occorre inizialmente rilevare che in Italia, pur in assenza di una legge organica sulla protezione dei dati, non si ha però una situazione di totale vuoto normativo. Anzi, più volte il legislatore ha anticipato alcune forme di tutela della riservatezza in una serie di disposizioni riferibili, direttamente o meno, al settore dell'informatica, che sono però prive di uno sviluppo e di una sistematica normativa organica. Si è parlato di «legislazione sommersa»[46] per il fatto che in genere manca, in tali norme, un riferimento diretto all'informatica.

I due interventi legislativi più significativi in tal senso sono rappresentati dalla legge 20 maggio 1970, n. 300, c.d. Statuto dei lavoratori, e dalla legge 1° aprile 1981, n. 121, concernente il nuovo ordinamento della Amministrazione della Pubblica Sicurezza. Per ciò che riguarda il primo dei due atti citati, due sono gli articoli che interessano, e precisamente l'art. 8, che vieta al datore di lavoro di effettuare indagini, ai fini dell'assunzione del prestatore d'opera, su fatti non rilevanti per la valutazione della sua attività professionale; e l'art. 4[47], che vieta al datore di lavoro di usare impianti audiovisivi ed altre apparecchiature per finalità di controllo a distanza dell'attività del lavoratore, salvo eccezioni (ad esempio per motivi di sicurezza). La legge sul nuovo ordinamento dell'Amministrazione della Pubblica Sicurezza[48] contiene invece una serie di disposizioni che interessano la tutela dei dati, e precisamente gli articoli da 6 a 12: tanto da presentarla come una vera e propria «mini-legge» sulla protezione dei dati personali. In realtà, essa ha

derarsi una normativa particolarmente completa: prevede infatti i mezzi di tutela amministrativa e giurisdizionale, un sistema di sanzioni penali e la disciplina relativa alla trasmissione dei dati oltre frontiera[54].

Nel progetto vengono tutelati sia i dati relativi alle persone fisiche, sia quelli delle persone giuridiche, accogliendo così una concezione ampia di tutela da attuare. Viene quindi affermato il principio di libertà di raccolta dei dati senza limitazioni aprioristiche. Viene anche affermato il principio di libertà di conservazione e di diffusione dei dati, con l'individuazione di alcuni limiti relativi agli aspetti intimi della personalità, alle idee politiche, sindacali, religiose, ecc. Il progetto non prevede poi soltanto un potere di controllo da parte del soggetto interessato, ed un conseguente diritto di accesso, ma anche un potere di controllo pubblico esercitato da un apposito ufficio che viene posto alle dirette dipendenze della Presidenza del Consiglio dei Ministri.

Tratteggiate le linee essenziali della disciplina stabilita nel disegno di legge, occorre però dire che, appena conosciuto, il testo redatto dalla Commissione Mirabelli è stato oggetto di vivace contestazione, specialmente da parte del mondo imprenditoriale[55]. Le critiche riguardavano soprattutto il suo carattere di normativa generale, cioè il fatto che sottoponesse ad una stessa disciplina qualsiasi tipo di banca dati. Non si condivideva poi, in particolare, la scelta attuata nel progetto di legge circa la natura dei dati protetti (si richiedeva una tutela più elastica e limitata alle sole persone fisiche), la composizione dell'ufficio di controllo (considerato troppo legato alle strutture governative), il diritto di accesso (ritenuto fonte di eccessivi oneri per le aziende) e il sistema sanzionatorio (troppo rigido, data anche la complessità della materia).

5.4. I vari disegni di legge presentati agli organi legislativi del nostro Paese, ed esaminati sinteticamente nelle pagine precedenti, non sono stati approvati dal Parlamento, e lo scadere della nona legislatura ne ha comportato la decadenza. Nel corso della decima legislatura il Ministro di Grazia e Giustizia, con decreto in data 4 febbraio 1988, ha quindi istituito un gruppo di studio con l'incarico di procedere alla revisione e all'aggiornamento del disegno di legge n. 1657 (il primo progetto Mirabelli). Il 30 settembre il gruppo ultimava i suoi lavori e rimetteva al Ministro Vassalli il testo

definitivo della relazione e dello schema del disegno di legge concernente la disciplina delle banche di dati personali ad elaborazione informatica [*secondo progetto Mirabelli* (1989)][56].

Tale progetto sembra differenziarsi dai precedenti, e dalla maggioranza delle soluzioni legislative adottate a livello internazionale[57], per l'originalità di alcune soluzioni adottate.

Innanzitutto per la precisa affermazione del principio di libertà informatica, inteso in senso nuovo: non tanto come libertà di non essere assoggettati al potere informatico altrui, quanto come libertà di adoperare senza vincoli ingiustificati i mezzi informatici per le proprie personali esigenze[58]. Ma soprattutto per la differenziazione della disciplina da applicarsi alle singole banche dati a seconda dello scopo perseguito da esse: evitando così di assoggettare ai medesimi oneri ed alle medesime sanzioni realtà diverse quali quelle di banche dati gestite da grandi enti e quelle di archivi elettronici gestite da singoli privati su comuni personal computer.

In particolare, il nuovo disegno di legge si muove lungo linee direttrici ben definite, ispirate ai seguenti principi fondamentali: a) esonero dall'obbligo della notificazione per le raccolte destinate a scopi privati e professionali; b) obbligo di notificazione e normativa di controllo solamente per le banche di dati destinate alla comunicazione a terzi; c) normativa particolare per i c.d. dati sensibili; d) disciplina rigorosa per le banche pubbliche di dati; e) indipendenza dell'organo di controllo dal Governo; f) esclusione dell'obbligo di comunicazione preventiva all'interessato[59].

Un progetto di disciplina particolarmente valido, che però non è riuscito a risolvere l'attuale situazione di carenza legislativa in cui versa il nostro Paese. Anzi, sembra molto più probabile che tra i due progetti esposti alle lungaggini dei rispettivi Parlamenti, quello europeo per la proposta di direttiva 24 settembre 1990, e quello italiano per il nuovo Mirabelli, sia la normativa europea a prevalere, con conseguenze facilmente immaginabili. In attesa di qualcosa apparentemente inevitabile, l'interprete deve utilizzare gli strumenti già esistenti nell'ordinamento e, come già detto, affidarsi ad un'attività prettamente ermeneutica. Risulta allora particolarmente interessante procedere ad un esame di come in pratica vengono tutelati i dati personali nel nostro Paese, e quindi ad un'analisi della disciplina di una categoria di dati sensibili, i dati sanitari, per la tutela dei quali la drammaticità della situazione raggiunge i livelli più alti.

6. L'analisi svolta fino ad ora delle principali fonti normative in materia di tutela della riservatezza già in vigore o ancora a livello di progetto (come nel caso dell'Italia), permette di rilevare che le considerazioni svolte in generale sulla protezione dell'individuo nei confronti del nuovo potere informatico sono valide in particolar modo per la disciplina delle banche dati sanitarie, cioè per quelle raccolte di informazioni relative alla salute dell'individuo. Costituendo i dati sanitari una delle principali categorie di dati c.d. sensibili, ne verrà esaminata ora la disciplina.

6.1. La tendenza delle ultime generazioni di leggi in materia di banche dati, come già detto nei precedenti paragrafi, è nel senso dell'affermazione del principio di libertà informatica, anche se concepito con accezioni diverse[60]. Tuttavia anche a tale principio vengono posti svariati limiti, tra i quali quello più importante, e comune alle varie legislazioni, è il divieto dell'elaborazione dei c.d. «dati sensibili».

Individuati nelle varie normative in modo abbastanza uniforme sono quei dati che hanno una particolare capacità di incidere sulla riservatezza dei singoli individui e di determinare discriminazioni sociali particolarmente rilevanti. Dei dati sensibili sono state effettuate in dottrina varie classificazioni[61], e nell'art. 17 della proposta di Direttiva 24 settembre 1990 della Commissione delle Comunità europee, in precedenza esaminata, vengono così enumerati: a) origine razziale (comprese le informazioni sul colore della pelle); b) le opinioni politiche, comunicazioni religiose e filosofiche (comprese quella secondo cui la persona non ha convinzioni religiose) e informazioni sulle attività della persona interessata connessa a convinzioni politiche, religiose o filosofiche; c) informazioni sull'adesione a sindacati; d) informazioni riguardanti la salute della persona interessata (comprese quelle sullo stato fisico e mentale passato, presente o futuro della persona interessata e le informazioni sull'abuso di droga o alcool); e) le informazioni concernenti la vita sessuale.

Individuate quindi le varie categorie di dati sensibili, deve rilevarsi che, nonostante sia generico il riconoscimento della necessità di previsioni apposite per la loro disciplina, questo non è pacifico. Infatti parte della dottrina afferma che non è corretto differenziare la disciplina a seconda della categoria di dati che vengono trattati, poiché nessun tipo di dato è, in assoluto, contrario

alla riservatezza dell'individuo, ma soltanto in relazione all'uso che si faccia del dato stesso. A tale proposito basti riportare quanto affermato dalla Commissione delle Comunità europee nella proposta di direttiva del settembre 1990. Infatti, se da un lato si dice che è opinione generalmente riconosciuta che il diritto alla vita privata può essere compromesso non tanto dal contenuto di un archivio, quanto dal contesto in cui si opera un trattamento di dati personali; dall'altro si deve però riportare l'affermazione precisa che «è altrettanto genericamente ammesso che alcuni tipi di dati, per il loro solo contenuto, a prescindere dal contesto in cui sono elaborati, possono violare il diritto alla vita privata dell'individuo»[62]. Da qui il riconoscimento della necessità di norme specifiche sulla materia.

La disciplina dei dati sensibili, nella quasi totalità delle legislazioni, prevede in genere il divieto di trattamento di tali dati, tranne nel caso in cui il soggetto interessato presti il suo consenso[63]: a causa delle perplessità sollevate circa l'efficacia di tale requisito[64], in alcune legislazioni si è costruito anche un sistema autorizzatorio, che si aggiunge o si sostituisce al consenso dell'individuo[65]. Stabilita quindi questa regola generale, il divieto di trattamento dei dati sensibili, vengono normalmente previste anche alcune regole particolari, come per le eccezioni a tale divieto, ad esempio in materia di informazioni acquisite nel legittimo esercizio dell'attività giornalistica, o per le norme in materia di dati sanitari, che si esamineranno nel prossimo paragrafo.

6.2. Come si è già detto, la categoria più importante di dati sensibili è costituita dai dati sanitari[66], cioè dalle informazioni relative alla salute pregressa, attuale e futura, fisica o mentale, di un individuo, nonché le informazioni amministrative e sociali associate (quali domicilio, professione, stato di famiglia, fattori psicologici, ecc.)[67]. Le banche dati che permettono la elaborazione di tali particolari informazioni presentano peculiari caratteristiche: esse devono infatti trattare numerosi dati di vario genere, per consentire di fornire al meglio prevenzione, cure e servizi medici, ma allo stesso tempo, a causa dell'estrema delicatezza delle notizie a cui accedono, questo deve avvenire rispettando dignità e *privacy* della persona interessata[68]. E le normative emanate nella presente materia devono cercare di adottare discipline appropriate che permettano di trovare e raggiungere un saldo punto di incontro tra i diversi interessi

implicati, tenendo in particolare considerazione quelli del soggetto interessato. Devono cioè tendere a realizzare, attraverso sottili equilibri, una tutela della salute e non un potere sulla salute.

Ma nella ricerca di una disciplina della materia in esame occorre tenere presenti non solo gli obblighi al rispetto della vita privata del malato, ma anche il fatto che la qualità e la certezza delle informazioni rivestono un'importanza sempre crescente nel campo della salute: in un'epoca di sempre maggiore mobilità delle persone, lo scambio rapido di informazioni esatte e pertinenti è una necessità per la sicurezza dell'individuo[69].

La complessità della materia trattata si evince quindi anche dalle esigenze che i sistemi informatici medicali devono soddisfare, che sono, come già rilevato, spesso contraddittorie. Si pensi al fatto che soprattutto in questo campo la velocità e la completezza delle informazioni sono caratteristiche basilari, talvolta addirittura vitali; e, allo stesso tempo, che maggiore è la necessità che l'utilizzazione dei dati sanitari avvenga in modo da rispettare la dignità e la riservatezza della persona interessata. Si pensi al difficile rapporto tra l'obbligo al rispetto della vita privata del malato, che pone rilevanti limiti alla registrazione e diffusione dei dati medici, con il diritto alla salute di ciascun individuo, che esige che tutti possano approfittare dei progressi della scienza medica realizzati grazie all'utilizzazione intensiva dei dati sanitari. Si pensi ancora al fatto che l'accesso alle banche dati sanitarie non è limitato al solo personale medico, tenuto al rispetto della deontologia professionale, ma implica l'ausilio tecnico ed organizzativo di numerosi altri soggetti (ad esempio degli esperti informatici), rendendo ancora più difficoltoso il compito del giurista che deve disciplinare l'intero settore.

Risulta quindi interessante analizzare come, a livello internazionale e nazionale, è stato risolto il problema del contemperamento dei vari interessi implicati nel settore delle banche dati sanitarie.

6.3. Nella quasi totalità delle legislazioni europee sulla protezione dei dati personali vengono previste specifiche norme sui dati sensibili in genere, su quelli sanitari in particolare. Evitando di soffermarsi sulle soluzioni adottate nei vari Paesi, risulta particolarmente interessante, anche in questa specifica materia, esaminare quanto disposto, con finalità di indirizzo e di coordinamento, dai principali organismi internazionali, e poi, nel paragrafo successivo,

quanto previsto nei due maggiori progetti italiani sull'argomento.

Chi tempestivamente ha recepito l'importanza del problema della tutela dei dati sanitari è stato il Consiglio d'Europa che, non solo genericamente nell'art. 6 della Convenzione del 28 gennaio 1981[70], di cui si è già parlato[71], ma anche specificamente con una Raccomandazione *ad hoc* nello stesso anno[72], ha tentato di stimolare l'adozione di una legislazione uniforme nei vari Stati della Comunità.

La disciplina stabilita nella specifica Raccomandazione del 1981[73] si caratterizza soprattutto riguardo a determinati settori e problematiche, quali ad esempio quelle dell'utilizzazione e dell'accesso ai dati sanitari.

Stabilito che per dati sanitari si intende, come già detto, quelle informazioni relative alla salute pregressa, attuale e futura, fisica o mentale, di un individuo, nonché le informazioni amministrative e sociali associate (quali domicilio, professione, stato di famiglia, fattori psicologici, ecc.), la Raccomandazione individua come proprio oggetto soltanto le informazioni attribuibili ad individui identificati o identificabili, restandone escluse le informazioni anonime, aggregate o statistiche (paragrafo 1.1 dell'allegato alla Raccomandazione).

Essendo il paziente la fonte delle informazioni, il suo consenso riveste in questo settore una particolare importanza, e viene infatti posto alla base dell'utilizzazione, specificamente della comunicazione a terzi (vedi par. 5.4) e della conservazione delle informazioni che lo riguardano. Per evitare che si tolga ogni efficacia a tale consenso, deve quindi essere circondata di cautele l'utilizzazione dei dati per fini diversi da quelli originariamente previsti e propri della specifica banca dati: a tale proposito viene effettuata una distinzione tra le persone che hanno accesso alle informazioni nell'esercizio delle loro funzioni, e le altre. Le prime, principalmente gli esercenti la professione medica, possono utilizzare i dati anche ad altri fini, purché ciò avvenga in forma anonima, oppure con l'autorizzazione delle persone o dell'organo di controllo a tal fine designati dal regolamento della banca dati. Per quanto riguarda gli altri soggetti, l'utilizzazione è possibile, come già detto, solo con il consenso della persona interessata (par. 5.4).

Presenta varie peculiarità, rispetto alla disciplina generale della tutela dei dati personali, l'esercizio di uno dei diritti connessi al diritto alla riservatezza, il c.d. diritto di accesso alla banca dati, e cioè il diritto di ogni persona di conoscere le informazioni che

lo concernono e che sono trattate in un archivio automatizzato. In campo sanitario, varie sono le difficoltà che ostacolano l'esercizio di tale diritto: si pensi alla difficile comprensibilità per il non iniziato delle informazioni mediche; si pensi ancora all'eventualità che si dimostri dannoso per il malato che gli siano comunicate tutte le informazioni sul suo caso. La Raccomandazione del Consiglio d'Europa prevede in proposito, come regola generale, che ogni persona abbia la possibilità di conoscere l'esistenza di dati che la concernono in una banca dati sanitaria. La conoscenza di tali dati deve però avvenire, in particolare, per evitare possibili riflessi negativi sull'interessato, attraverso il filtro del suo medico (par. 6.1).

Un'altra peculiarità della disciplina delle banche dati sanitarie riguarda poi una delle facoltà che in genere viene riconosciuta alla persona i cui dati sono oggetto di un trattamento automatizzato: è generalmente stabilito, infatti, nella quasi totalità delle legislazioni sulla materia, che le informazioni sulla persona non debbano essere conservate oltre il tempo strettamente necessario (c.d. diritto all'oblio), poiché in caso contrario potrebbe verificarsi una minaccia alla vita privata dell'individuo. Per quanto riguarda lo specifico settore qui esaminato, l'interesse alla sanità pubblica e quello della ricerca scientifica possono giustificare la conservazione di lunga durata dei dati medici, anche dopo la morte della persona. Secondo la Raccomandazione ciò deve essere consentito, sacrificando così il diritto all'oblio dell'individuo, ma a condizione che siano adottate le misure adeguate di sicurezza e di tutela della vita privata(par. 7).

Infine, l'esattezza e l'aggiornamento dei dati memorizzati, nonché il rispetto del carattere riservato delle informazioni e il loro corretto utilizzo, devono essere garantiti dalla responsabilità sia del medico nella fase di raccolta dei dati, sia dell'informatico nella fase di concezione ed esecuzione del programma (par. 8).

Fin qui la disciplina europea della protezione dei dati sanitari, che per i suoi stessi scopi e la sua natura non può che essere di carattere generale, e che presuppone le regolamentazione adottate dai singoli Paesi membri del Consiglio d'Europa in conformità ad essa, ma con le più particolari e specifiche disposizioni adeguate alla situazione sociale, economica, scientifica, culturale di ciascun Paese.

6.4. Anche in questo specifico settore il nostro Paese deve registrare una situazione di assoluta carenza legislativa. Può comun-

que dimostrarsi utile esaminare come, nei due maggiori progetti di legge italiani, viene disciplinata la materia trattata in questa sede.

Premettendo che tra i due disegni di legge è il secondo Mirabelli quello che prevede un sistema abbastanza completo ed organico per la tutela dei dati sanitari, nel primo progetto Mirabelli sono essenzialmente due le norme che si riferiscono direttamente al trattamento di tali dati, e cioè gli artt. 11 e 15. Il primo dei due articoli in commento, immediatamente successivo alla norma che regola la «Raccolta dei dati» (art. 10), e intitolato «Dati sanitari», dispone che tali dati possono essere assoggettati ad elaborazione informatica solo ad opera di organismi sanitari ed unicamente per il trattamento sanitario dell'interessato o dei suoi consanguinei o del coniuge; il secondo comma prevede la possibilità di eccezioni a tale regola a favore della Pubblica Amministrazione, disposte con legge, e sempre con adeguate garanzie. Anche in questo caso si pongono quindi delle limitazioni alla possibilità di trattare i dati sanitari, questa volta mediante la precisa affermazione del soggetto che può sottoporre ad elaborazione tale categoria di informazioni personali e del fine dell'elaborazione stessa. L'art. 15 del primo progetto Mirabelli riguarda invece la loro comunicazione, specificamente all'interessato (mentre la comunicazione a terzi rientra nelle regole generali, cioè gli artt. 16 ss.), che deve avvenire obbligatoriamente se richiesta da questo, e mediante il tramite del personale medico.

Nel secondo disegno di legge invece la disciplina è strutturata in tre diverse parti, previste rispettivamente all'art. 3, comma 4, all'art. 13 e agli artt. 18 e 19, che riguardano il trattamento di tali dati quale limite al principio di libertà informatica affermato in generale nel progetto di legge, il diritto di accesso dell'interessato, la loro comunicazione e diffusione.

Il quarto comma dell'art. 3, intitolato ai limiti alla libertà informatica (principio affermato nel precedente articolo), subordina la liceità della raccolta dei dati sanitari al consenso dell'interessato, ammette il loro trattamento informatico senza tale consenso soltanto da parte di sanitari o di imprese assicurative e previdenziali, non ne consente invece l'elaborazione nonostante siano stati acquisiti nell'esercizio legittimo dell'attività giornalistica[74].

Il diritto di accesso[75] alle informazioni sanitarie viene, anche in questo disegno, disciplinato secondo soluzioni tradizionali: così l'art. 13 dispone che l'interessato può chiedere di conoscere i dati

sanitari che lo concernono alla struttura che li detiene, che li comunica per il tramite del proprio personale medico, tenendo conto delle particolarità del caso e delle condizioni psicofisiche del soggetto richiedente.

Infine, la comunicazione e diffusione dei dati sanitari a terzi[76] sono disciplinate in due articoli, rispettivamente il 18 che pone la regola e il 19 che prevede l'eccezione. Tali due norme si pongono nell'ambito di un sistema complesso, stabilito in sette articoli, che regolano la comunicazione e diffusione dei dati in genere (art. 14), i divieti (art. 15), e tre particolari tipi di trasmissione: quelle aventi ad oggetto dati delle banche dati della Pubblica Amministrazione (art. 16), quelle aventi ad oggetto dati sensibili in genere (art. 17), e i dati sanitari in particolare (art. 18). L'art. 19 pone poi delle eccezioni ai divieti affermati in precedenza, e l'art. 20 disciplina infine l'ipotesi di trasmissione dei dati oltre frontiera. Per quanto riguarda in particolare la comunicazione e diffusione dei dati sanitari, l'art. 18 stabilisce la necessità del consenso dell'interessato (comma 1), anche se sono ammesse ipotesi in cui la trasmissione può essere effettuata senza tale requisito: è il caso in cui la comunicazione sia necessaria per il trattamento sanitario dell'interessato stesso, o di suoi consanguinei o del convivente (sempre art. 18, comma 1); inoltre quando a ciò vi autorizzi il Garante[77], sentito il parere del Consiglio Superiore di Sanità, per esigenze di prevenzione o di cura. Infine, la comunicazione e diffusione dei dati sanitari sono ammesse, così come la diffusione di altri dati personali, se fatte in forma anonima per scopi di studio o di ricerca (art. 19, lett. a), oppure per scopi concernenti la sicurezza dello Stato e l'accertamento di reati (art. 19, lett. b); la diffusione dei dati sanitari non è invece ammessa neppure nell'esercizio del diritto di cronaca (art. 18, comma 3).

Questa appena esaminata è dunque la disciplina progettata in materia di banche dati sanitarie in Italia. Nell'attesa dell'approvazione di una legge sulla materia si registra allora la già rilevata situazione di carenza di regole precise per gli operatori del settore, fatto drammatico in particolare per la materia in questa sede esaminata. Per ora quindi il rispetto dell'individuo, i cui dati riguardanti le sue condizioni sanitarie formano oggetto di elaborazione informatica in archivi magnetici, rimane affidato unicamente alla correttezza di chi gestisce tali informazioni, e in questo caso alla deontologia professionale della categoria medica.

Note

[1] Così E. Giannantonio, *Introduzione all'informatica giuridica*, Milano, 1984, p. 212.

[2] In Italia oltre il 50% dei 20 milioni di occupati è legato, direttamente o indirettamente, al trattamento dell'informazione.

[3] Con l'avvento della società dell'informazione, inoltre, per la prima volta l'economia si basa su una risorsa chiave che non è solo rinnovabile, ma che si riproduce da sé. Acquista allora particolare valore l'affermazione «conoscere è decidere». Se in passato si parlava infatti di «civiltà del capitale», in quanto il potere risiedeva nelle mani di coloro che lo possedevano, oggi si può parlare di «civiltà della conoscenza», in quanto il potere si sta sempre più accentrando su coloro che «hanno» le informazioni, e la capacità e la conoscenza per utilizzarle.

[4] Sui CD-ROM e le sue applicazioni al mondo giuridico, vedi M.G. Losano, *Scritto con la luce. Il disco compatto e la nuova editoria elettronica*, Milano 1988, p. 198, e M.G. Losano e L. Philipps, *Diritto e CD-ROM. Esperienze italiane e tedesche a confronto*, Milano, pp. XI-118; per le recenti applicazioni e gli sviluppi dei dischi ottici, dell'editoria elettronica e della multimedialità vedi «Media 2000», anno IX, n. 7, luglio-agosto 1991.

[5] Per un quadro relativo ai nuovi servizi telematici ed ai problemi giuridici ad essi afferenti v. R. Speciale, *Sulla configurazione giuridica dei servizi telematici. Appunti e problemi*, in «Dir. Inf. Inf.», 1988, pp. 359-374, e G. Ciacci, *I contratti per la fornitura dei servizi telematici*, in «Economia e diritto del terziario avanzato», 1990, 1, pp. 73-119.

[6] Così R. Borruso e C. Tiberi, *L'informatica per il giurista*, Milano, 1990, p. 190. Nello stesso testo vengono poste cinque regole che devono essere soddisfatte affinché si possa dire di essere in presenza di una banca dati. Tali regole sono: a) libertà e causalità della ricerca (...); b) libera combinazione delle chiavi di ricerca in *and*, *or*, *not* secondo le regole della logica *booleana*; c) libera mascherabilità di caratteri alfanumerici di un dato chiave (...); d) possibilità di estrarre automaticamente informazioni dai documenti registrati ed ottenerne la prospettazione in forma sintetica; e) possibilità di interagise con l'elaboratore svolgendo la ricerca con una serie successiva di ordini e dati (...).

[7] Il Borruso parla a tale proposito di una conoscenza più veloce di quella normale, tanto da essere qualcosa di diverso, una «superconoscenza» (Borruso, *Computer e diritto*, vol. II, Milano, 1988, p. 383).

[8] Così V. Frosini, *Banche dati e tutela della persona*, nel volume omonimo edito dalla Camera dei Deputati, II, Roma, 1983, p. 4.

[9] Ed è la situazione nel nostro Paese, come si vedrà oltre, al paragrafo 3.1. e in genere al capitolo 5.

[10] Tale ultimo diritto, nato concettualmente alla fine del secolo scorso negli USA, e tradizionalmente contrapposto al diritto all'informazione quale suo contrappeso e limite, sarebbe costituito dal diritto di ciascuno di escludere dall'altrui conoscenza tutto quanto ha riferimento alla persona stessa: non solo alla figura fisica, ma anche a certi avvenimenti e allo sviluppo della propria vita. Nato come diritto «ad essere lasciato solo» (*to be let alone*), viene inteso via via in modo sempre più esteso, tanto da arrivare a comprendere tutti i diritti della personalità, tutti quei valori dell'individuo che devono essere protetti contro le ingerenze esterne. La bibliografia sul tema è vastissima, si citano solo alcuni autori: A. De Cupis, *Le persone celebri e il diritto alla riservatezza*, in «Foro Pad.», 1953, I, pp. 1341 ss.; Id., *Il diritto alla riservatezza esiste*, in «Foro It.», 1954, IV, pp. 89 ss., Id., *Riservatezza e segreto (diritto a)*, in «Noviss. dig. it.» XVI, Torino, 1969, pp. 115 ss.; G. Giacobbe, *Riservatezza (diritto alla)*, in «Enc. dir.», XL, Milano, pp. 1243 ss., Sgroi V, *Il diritto alla riservatezza ancora in Cassazione*, in «Giust. Civ.», 1963, I, pp. 1280 ss.; M. Giorgianni, *La tutela della riservatezza*, in «Riv. trim. dir. proc. civile», 1970, I, pp. 13 ss.; per la riservatezza in relazione alle banche di dati personali, rilevata nuovamente l'ampiezza delle fonti sulla materia, valgano i richiami fatti nel testo a seconda degli argomenti trattati.

[11] Così Giannantonio, *Introduzione all'informatica giuridica*, cit., p. 218.

[12] Sul punto vedi G. Giacobbe, *Problemi civilistici dell'era informatica*, in AA.VV., *Banche dati e diritti della persona*, Atti del convegno in Sciacca, 9-10 novembre 1984, Milano, pp. 25-41.

[13] Così Giacobbe, *op. cit.*, p. 39.

[14] Ipotesi non del tutto azzardata se si pensa alle varie fattispecie verificatesi, in particolare al caso dell'imprenditore fallito perché, a causa di una negligenza del gestore della banca dati, erroneamente ritenuto protestato.

[15] Sul punto vedi oltre, paragrafo 4.1.

[16] Un esame dei principali progetti di legge è svolto al paragrafo 5.3.

[17] Così Borruso, *Computer e diritto*, vol. II., cit., pp. 372-374.

[18] Così ad esempio gli artt. 10 e 13, 2 comma, del primo disegno di legge Mirabelli.

[19] Così Borruso, *op. cit.*, p. 374, che tra l'altro sottolinea che «non si può pretendere la massima tutela del diritto alla riservatezza nei confronti dell'informatica e il suo più ampio sacrificio invece nei confronti del diritto di stampa».

[20] Appartengono a questa generazione la prima legge svedese (*Datalag* dell'11 maggio 1973), la *Bundesdaten Schutzgesetz* (BDSG) tedesca, la *Datenschtzgesetz* (DSG) austriaca, le leggi danese, norvegese ed islandese.

[21] Appartengono a questa generazione la legge statunitense, la seconda legge svedese, in parte quella francese, quella israeliana e quella britannica; vi aderisce anche il disegno di legge Martinazzoli. Per un quadro completo delle varie fonti internazionali, anche se purtroppo non particolarmente aggiornato, si faccia riferimento al volume *Banche dati e tutela della persona*, a cura del Servizio per la documentazione della Camera dei Deputati, Roma, 1983; si veda anche N. Catania, *Dossier Privacy*, 1983.

[22] Tra queste la possibilità di accedere alle varie fonti informative ovunque ubicate da qualsiasi posto (unica condizione la presenza di una rete di telecomunicazione, intesa in senso ampio), senza alcun vincolo determinato dalle distanze o dalle frontiere.

[23] La Commissione delle Comunità europee si è iniziata ad occupare della materia fin dal 1977, (decisione del Consiglio 27 settembre 1977, n. 377D0617), sviluppando tre programmi diversi: il programma CD (*Coordinated Development of Computerised Administrative Procedures*, istituito con la Risoluzione del Consiglio 15 aprile 1984, n. 384Y0524(01)), il programma CADDIA (*Cooperation on Automatation of Documentation and Data for Imports, Exports and Agricolture*, Decisione 26 marzo 1985, n. 385D0214), ed infine il programma TEDIS (*Trade Electronic Data Interchange*), in materia di *EDI* per uso commerciale (Decisione 5 ottobre 1987, n. 387D0499).

[24] L'integrazione europea prevista dal mercato unico comporta lo sviluppo sempre maggiore degli archivi di dati personali e sopratutto la necessità di fare «viaggiare» i dati in essi contenuti. Se merci, capitali, servizi e persone potranno spostarsi liberamente, ne consegue che una grande quantità di operazioni avrà bisogno di ricevere informazioni su *partners*, clienti, corrispondenti, ecc. Per non parlare delle Amministrazioni Pubbliche. L'abbattimento delle frontiere (esempio più classico) sarà possibile solo grazie al massimo scambio di informazioni tra le autorità fiscali, se si vuole evitare un'evasione delle imposte nazionali di proporzioni tali da mettere in ginocchio i bilanci pubblici di mezza Europa. I controlli incrociati si faranno sempre più spesso lungo le direttive del c.d. «sistema nervoso europeo», cioè la rete telematica ramificata in tutto il Continente. E per ottenere tutto ciò occorre che le condizioni giuridiche siano uguali in ciascun Paese (così M. Cavalli, *Privacy cercasi per banca dati. Ma l'euroregola piace a pochi*, in «Il Sole-24 ore», 6 giugno 1991).

[25] Per un approfondimento sul tema dell'attività degli organismi internazionali, vedi C. Sarzana, *L'attività delle istituzioni internazionali in materia di tutela della privacy*, in *Banche dati e tutela della persona*, cit., pp. 498 ss., e, con particolare riferimento all'opera svolta dal Consiglio d'Europa, G. Buquicchio, *Aspetti internazionali della protezione dei dati: il ruolo svolto dal Consiglio d'Europa*, in *Privacy e banche dati*, Bologna, 1982, pp. 67-85.

[26] Risoluzione 26 settembre 1973 n. (73)22 e Risoluzione 20 settembre 1974 n. (74)29 del Comitato dei Ministri agli Stati membri, relativa alla protezione della vita privata delle persone fisiche nei confronti delle banche dati elettroniche nel settore privato (1973) e nel settore pubblico (1974); Raccomandazioni del Comitato dei Ministri agli Stati membri del 13 settembre 1980 (*«relativa allo scambio di informazioni giuridiche in materia di protezione dei dati»*), del 23 gennaio 1981 (*«relativa alla regolamentazione applicabile alle banche dati sanitarie autorizzate»*), del 23 settembre 1983, del 25 ottobre 1985 e

del 23 gennaio 1986 (relative alla protezione dei dati a carattere personale utilizzati rispettivamente a fini di ricerca scientifica e statistica la prima, a fini di marketing diretto la seconda, e a fini di previdenza sociale la terza), del 17 settembre 1987 (volta a regolare l'utilizzo dei dati a carattere personale nel campo della pubblica sicurezza, in «Dir. Inf. Inf.», 1990, p. 241); Convenzione del Consiglio d'Europa del 28 gennaio 1981 per *La protezione delle persone in relazione all'elaborazione automatica di dati a carattere personale* (la maggioranza dei testi di tali atti, tranne dove diversamente indicato, sono riportati nel volume *Banche dati e tutela della persona*, cit.).

[27] Raccomandazione del 23 settembre 1980 *«concernente le linee direttive riguardanti la protezione della vita privata e i flussi transfrontiera di dati di carattere personale»* (in *Banche dati e tutela della persona*, cit., pp. 527 ss.).

[28] Dichiarazione del 12 novembre 1980 su *La protezione della vita privata e l'uso di dati a carattere personale a fini di ricerca* (in *Banche dati e tutela della persona*, cit., pp. 568 ss.).

[29] Risoluzione del Parlamento europeo emessa l'8 maggio 1979 su *La tutela dei diritti dell'individuo di fronte al crescente progresso tecnico nel settore dell'informatica* (in G.U. 5 giugno 1979, n. 140); Raccomandazione Commissione delle Comunità europee del 29 luglio 1981, concernente la *Convenzione del Consiglio d'Europa sulla protezione delle persone per quanto riguarda l'elaborazione dei dati a carattere personale* (in *Banche dati e tutela della persona*, cit., pp. 566-567).

[30] «Una protezione equivalente di livello elevato è indispensabile per il completamento del mercato interno» (allegato alla proposta di direttiva della Commissione delle Comunità europee 24 settembre 1990, esaminate nel testo).

[31] Vedi, tra gli altri, M. Cavalli, *Pioggia di critiche su Bruxelles*, in «Il Sole-24 Ore», 6 giugno 1991.

[32] Nel secondo paragrafo dello stesso articolo vengono previste due eccezioni: per gli archivi detenuti da persona fisica per fini esclusivamente privati (è il caso ad esempio dell'agenda elettronica personale); o per gli archivi detenuti da associazioni senza scopo di lucro, nel quadro del loro scopo legittimo, e solo nel caso riguardino i membri consenzienti e non siano trasmessi a terzi (è ad esempio il caso dei registri dei membri di un'associazione).

[33] L'organo pubblico, garanzia di una tutela non solo atomistica dell'individuo, è rappresentato, nella proposta di direttiva, da un Comitato denominato «Gruppo per la protezione dei dati personali», e da un'«Autorità di controllo». Costituito da un rappresentante delle varie Autorità di controllo dei singoli Stati membri, presieduto da un membro della Commissione, e caratterizzato per la sua indipendenza, il primo svolge essenzialmente funzioni di tipo consultivo. L'Autorità di controllo, invece, sempre indipendentemente, controlla la protezione dei dati personali: questo mediante «mezzi investigativi e poteri effettivi di intervento contro la creazione e lo sfruttamento di archivi non conformi alle disposizioni della presente direttiva» (art. 26, par. 3). A tale ultima Autorità può rivolgersi qualsiasi persona interessata a presentare denunce o reclami (artt. 26-28).

[34] Altre deroghe particolari all'obbligo di informare la persona interessata si trovano nell'art. 10 della proposta di Direttiva.

[35] In particolare le informazioni riguardanti l'origine razziale, le opinioni politiche, le convinzioni religiose o filosofiche, quelle sull'adesione a sindacati, quelle riguardanti la salute della persona o la sua vita sessuale. Sul punto vedi paragrafo 6.1.

[36] Ne rimarrebbero quindi escluse ad esempio le procedure giornalistiche, anche se ormai sono quasi interamente automatizzate (si parla sempre più comunemente di «editoria elettronica»): la norma sembra quindi costituire un'ulteriore discriminazione, e quindi conseguente perdita di efficacia della normativa esaminata, a favore dei *network* informativi, come già rilevato al paragrafo 3.2.

[37] Ai fini della deroga è comunque necessaria l'adozione di uno specifico atto giuridico.

[38] In M. Cavalli, *Così protetti da leggi altrui*, in «Il Sole-24 Ore», 6 giugno 1991.

[39] «I problemi da essi prospettati hanno rappresentato per lungo tempo piuttosto un'esperienza culturale tratta dalla realtà dei Paesi informaticamente più avanzati che una reale esigenza nazionale» (così R. Pagano, *Informatica e diritto*, Milano, 1986, p. 85).

[40] L'art. 4 della Convenzione infatti dispone che ciascuno Stato aderente ha l'obbligo di porre in essere i mezzi necessari per rendere operanti nel proprio ordinamento i principi fondamentali per la protezione dei dati stabiliti nella Convenzione stessa, e che l'adempimento di tale obbligo deve essere attuato al più tardi al momento dell'entrata in vigore dell'accordo. Sul punto vedi R. Lattanzi, *La tutela dei dati personali dopo la ratifica della Convenzione europea sulle banche dati*, in «Dir. Inf. Inf.» 1990, pp. 220-240.

[41] Il c.d. progetto Accame, presentato il 21 aprile 1981, su cui vedi oltre, paragrafo 5.3.1.

[42] Secondo il Ministero dell'Interno le banche dati computerizzate nel 1981 erano 105739 (ricordiamo che la legge del 1° aprile 1981, n. 121, concernente il nuovo ordinamento della Amministrazione della Pubblica Sicurezza, primo esempio in Italia di tutela normativa della riservatezza nei confronti dei trattamenti automatizzati dei dati, stabilisce, all'art. 8, l'obbligo di notificare al Ministero dell'Interno l'esistenza di banche di dati personali presso le amministrazioni pubbliche e private). Alla fine del 1982, al già cospicuo numero di archivi notificati, se ne aggiunsero altri 21019, nel 1983 altri 18759, senza contare poi quelle non denunciate. Un totale, quindi, secondo stime approssimative del Ministero, di circa 150000 banche dati (i primi risultati dell'indagine sono stati pubblicati negli Atti Parlamentari della Camera dei Deputati, Doc. XXIII, n. 9, 1983).

[43] Ad esempio, volendo rimanere nell'ambito dell'esperienza europea, la Francia ed il Belgio; per un'approfondita analisi della situazione in materia di banche di dati personali e tutela della riservatezza dell'individuo in questi due Paesi, vedi B.M. Tommasi, *Banche dati e tutela della riservatezza in Italia, Francia e Belgio: tre esperienze a confronto*, Tesi di laurea, L.U.I.S.S., Roma, 1990.

[44] Per un'analisi delle cause del persistente vuoto legislativo vedi anche R. Pagano, *Informatica e diritto*, cit., pp. 48 ss.

[45] «Si opponevano sopratutto gli entusiasmi tecnocratici dei managers pubblici e privati, che ritenevano l'intervento istituzionale poco più che un impaccio, e quindi chiedevano piuttosto un vuoto di diritto che non una nuova istituzionalizzazione adeguata dei bisogni della nuova tecnologia» (così S. Rodotà, *Progresso tecnico e problemi istituzionali nella gestione delle informazioni*, in AA.VV., *Privacy e banche di dati*, a cura di N. Matteucci, Bologna, 1981, p. 26).

[46] Così V. Frosini, *Legislazione sommersa*, in «Il Tempo», 12 ottobre 1985.

[47] L'articolo 24 della legge 29 marzo 1983, n. 93, ha esteso al settore del pubblico impiego il divieto previsto all'art. 4 in esame.

[48] Il testo legislativo deve essere integrato con il decreto del Presidente della Repubblica del 3 maggio 1982, n. 378, intitolato «Regolamento concernente le procedure di raccolta, accesso, comunicazione, correzione, cancellazione ed integrazione dei dati e delle informazioni registrate negli archivi magnetici del centro di elaborazione dati di cui all'art. 8 della l. 1° aprile 1981, n. 121».

[49] Si possono ancora ricordare l'art. 17 della l. 11 luglio 1978, n. 32, concernente le «norme di principio nella disciplina militare», che ha stabilito il divieto «di fare uso delle schede informative ai fini di discriminazione politica dei militari», e le norme a tutela della riservatezza, libertà e segretezza delle comunicazioni, stabilite con legge 8 aprile 1974, n. 98 (sono diritti già garantiti dalla nostra Costituzione, ma con questa ultima legge vengono specificati e viene previsto un rigido sistema di sanzioni). Rinviamo infine al paragrafo 3.1. per le teorie di una parte della dottrina sull'applicabilità alla materia in esame di alcune norme costituzionali e del codice civile (ad esempio gli artt. 41, comma 2, Cost. e 2055 cod. civ.).

[50] Camera dei Deputati n. 2553, proposta di legge d'iniziativa del deputato Accame, presentata il 21 aprile 1981: «Norme per la salvaguardia del diritto al rispetto della vita privata nei confronti dei sistemi di trattamento ed elaborazione automatica dei dati e delle informazioni».

[51] Camera dei Deputati, n. 3195, progetto di legge d'iniziativa dei deputati Picano ed altri, presentata il 24 febbraio 1982: «Norme per la tutela del diritto alla riservatezza delle persone fisiche nel trattamento automatizzato dei dati e delle informazioni».

[32] Camera dei Deputati, n. 1210, proposta di legge d'iniziativa dei deputati Seppia ed altri, presentata il 27 gennaio 1984: «Disciplina sull'uso dei sistemi informativi personali».

[33] Camera dei Deputati, n. 1657, disegno di legge presentato dal Ministero di Grazia e Giustizia (Martinazzoli) il 5 maggio 1984: «Costituzione ed esercizio delle banche dati personali ad elaborazione automatica».

[34] Vedi Giannantonio, *Il progetto di legge sulle banche di dati personali e le normative straniere*, in «Giur. It»., 1985, IV, p. 168.

[35] Le critiche sono state tali da portare a degli aggiustamenti nella successiva stesura del testo, quella presentata al Parlamento il 5 maggio 1984: gli articoli sono passati da 37 a 38, e le variazioni di maggior rilievo riguardano la norma che istituisce l'organo di controllo (art.5). Una raccolta sistematica delle critiche rivolte al disegno di legge è contenuta in G. Mirabelli, *Osservazioni e rilievi allo schema di DDL sulle banche di dati*, in «Quaderni della giustizia», n. 31, p. 25.

[36] Gli aspetti principali del disegno di legge vengono descritti in R. Foglia, *Tutela della riservatezza del lavoratore e controllo informatico dell'attività lavorativa*, in *Questioni attuali di diritto del lavoro*, Collana di ricerche, studi e dibattiti del lavoro, Notiziario di Giurisprudenza del lavoro, Roma, 1989, p. 28; e, specialmente, Giannantonio, *Il nuovo disegno di legge sulle banche di dati personali*, in «Dir. Inf. Inf.», 1991, pp. 67-69.

[37] Per un'analisi comparata del nuovo disegno di legge con le principali normative internazionali vedi sempre Giannantonio, *op. ult. cit.*

[38] L'art. 2 del nuovo disegno di legge così dispone: «Chiunque ha il diritto di raccogliere dati, assoggettarli ad elaborazione informatica e utilizzare i dati raccolti ed elaborati allo scopo di soddisfare interessi personali, nell'ambito della propria vita privata e della propria attività professionale e imprenditoriale». Il testo completo del disegno di legge può essere trovato nella rivista «Dir. Inf. Inf.», I, 1991, p. 267.

[39] Così Giannantonio, *op. cit.*, p. 68.

[40] Sia essa intesa come libertà di non essere assoggettati al potere informatico altrui, o, come nel nuovo progetto Mirabelli (di cui si è già parlato al paragrafo 5.4.), libertà di adoperare senza vincoli ingiustificati i mezzi informatici per le proprie esigenze.

[41] In Italia Rodotà ha proposto di distinguere le informazioni in: a) informazioni obiettivamente neutre, la cui conoscenza non può in alcun modo arrecare pregiudizio alla persona; b) informazioni che l'interessato potrebbe voler tenere riservate, ma la cui divulgazione è resa opportuna da finalità sociali; c) informazioni la cui diffusione non è desiderata dall'interessato e non è socialmente necessaria (come quelle sulle opinioni politiche o religiose). Queste ultime costituiscono i dati di maggiore sensibilità o, come si esprimono alcuni autori, il «nucleo duro della riservatezza» (da Giannantonio, *Il nuovo disegno di legge sulle banche dati personali*, cit., p.81).

[42] Dall'allegato alla proposta di direttiva della Commissione delle Comunità europee 24 settembre 1990, esaminata nel testo al paragrafo 4.2.

[43] Che deve avere particolari requisiti, come ad esempio quello di essere «libero, esplicito, scritto» (così nell'art. 17 della proposta di direttiva della Commissione delle Comunità europee, su cui v. par. 4.2.).

[44] Si è parlato a tal proposito di «mito del consenso», poiché molto spesso il consenso dell'individuo è apparente e del tutto necessitato; infatti basare la liceità del trattamento dei dati su questo requisito vuol dire accettare ogni elaborazione a scapito dei soggetti più deboli ed a vantaggio di quelli più forti (così Giannantonio, *Introduzione all'informatica giuridica*, cit., p. 218).

[45] Discipline autorizzatorie con riferimento ai dati sensibili sono previste nella legislazione svedese del 1982 ed in quella francese.

[46] In materia di dati sanitari vedi S. Piccinini Graziani, *Diritto alla riservatezza, elaboratori e informazioni sanitaria*, in «Giustizia civile», 1980, II, pp. 243-251; Y. Poullet, *Aspetti legali della protezione dei dati nell'informatica medica. La tessera dei dati sanitari*, in questa «Rivista», 1990, pp. 443-475; O. Fanelli, *Banche di dati sanitari e tutela della riservatezza*, Corso di dispense, Fac. Scienze Poltiche, 1991.

[47] Così Fanelli, *op. cit.*

[48] E questa volta non solo nei confronti dei terzi, che non devono essere informati

delle notizie personali che riguardano l'individuo, ma anche nei confronti dell'interessato stesso, che talvolta, in questo specifico settore, può risultare danneggiato dall'apprendere informazioni sulla sua salute (si pensi ai soggetti cardiopatici).

[69] Così Fanelli, *op. cit.*

[70] Intitolato «Categorie particolari di dati», così dispone: «I dati di carattere personale rilevanti l'origine razziale, le opinioni politiche, le convinzioni religiose o altre convinzioni, così come i dati di carattere personale relativi alla salute o alla vita sessuale, non possono essere trattati automaticamente a meno che il diritto interno non preveda garanzie appropriate» (in *Banche dati e tutela della persona*, cit., p. 509).

[71] Vedi paragrafo 4.1.

[72] Raccomandazione n.R. (81) 1 del 23 gennaio 1981, in AA.VV., *Banche dati in Italia*, a cura di V. Zeno-Zencovich, Napoli, 1985; vedi inoltre, ancora più specifica, la Raccomandazione n.R. (86) 1 del 23 gennaio 1986, relativa alla «Protezione dei dati a carattere personale utilizzati a fini di sicurezza sociale», che disciplina i dati sanitari contenuti nelle banche dati degli istituti di previdenza sociale, in maniera non dissimile da quella più estesa dei dati sanitari in genere.

[73] Analizzata in particolare in Fanelli, *op. cit.*

[74] Tale limitazione del diritto di cronaca può essere dedotta dal terzo comma dell'art. 3 e confermata, per un aspetto diverso (quello della comunicazione e diffusione dei dati sanitari), dal terzo comma dell'art. 18.

[75] Sul diritto di accesso nel nuovo disegno di legge italiano ed in genere vedi Giannantonio, *Il nuovo disegno di legge sulle banche dati personali*, cit., pp. 88-93.

[76] La lettera f) e la lettera g) dell'art. 1 del disegno di legge definiscono rispettivamente la comunicazione e la diffusione dei dati come il «dare conoscenza dei dati elaborati a soggetto determinato diverso dall'interessato» la prima, mentre come il «dare conoscenza dei dati elaborati a soggetti indeterminati» la seconda.

[77] Nel nuovo Mirabelli è l'organo pubblico per l'attuazione della legge e per rendere più efficace la tutela dell'individuo, disciplinato agli artt. 9 e 10 (sul punto v. Giannantonio, *op. ult. cit.*, p. 84).