GIANLUIGI FIORIGLIO

TEMI DI INFORMATICA GIURIDICA

www.dirittodellinformatica.it
www.informaticagiuridica.com

L'edizione cartacea della presente opera è stata già pubblicata da Aracne Editrice, Roma, 2004.

Ai miei genitori

L'edizione cartacea della presente opera è stata già pubblicata da Aracne Editrice, Roma, 2004.

PREMESSA 7

CAPITOLO 1 10
L'INFORMATICA GIURIDICA: ASPETTI GENERALI 10
1. Le origini: elaboratore elettronico, cibernetica e giurimetria 10
2. Verso il superamento della giurimetria 25
3. La giuritecnica e l'informatica giuridica nell'ambito dello sviluppo tecnologico 31
4. Il diritto dell'informatica 40
5. L'informatica giudiziaria 44
6. L'insegnamento dell'informatica giuridica 49

CAPITOLO 2 54
L'INFORMATICA GIURIDICA METADOCUMENTARIA 54
1. Legistica e legimatica 54
2. La fabbrica delle leggi e i loro difetti 59
3. Le regole e raccomandazioni sulla formulazione dei testi legislativi 67
4. I sistemi esperti 69
5. Gli agenti *software* 75

CAPITOLO 3 77
L'INFORMATICA GIURIDICA DOCUMENTARIA 77
1. Aspetti generali 77
2. Cenni sugli ipertesti 82
3. Cenni sull'algebra booleana 85
4. I principi delle ricerche documentarie e gli operatori logici 87
5. I thesauri 92
6. Le banche dati giuridiche 98
7. Informazioni *on line* ed *off line* 101

CAPITOLO 4 105
IL WEB SEMANTICO 105
1. Dal *world wide web* al *web* semantico 105
2. La rappresentazione della conoscenza e il linguaggio 107
3. Le ontologie 111
4. Le applicazioni giuridiche 112

CAPITOLO 5 116
LA CRITTOGRAFIA 116
1. Origini ed evoluzione 116
2. Cenni sulla regolamentazione delle tecniche di crittografia 121
3. Il PGP (Pretty Good Privacy) e il caso Zimmermann 124

CAPITOLO 6 127
INTERNET E PROBLEMATICHE GIURIDICHE 127
1. Aspetti generali 127
2. Nascita ed evoluzione di Internet 131

3. Internet: aspetti tecnici 141
4. I motori di ricerca su Internet 149
5. L'immaterialità e l'a-territorialità del Cyberspace 153
6. Il ruolo del diritto nella regolamentazione del Cyberspazio 161
7. Il provider 166
8. Hackers e crackers 177
9. Cenni su diritto d'autore, Internet e duplicazione abusiva del *software* 188

CAPITOLO 7 193
IL DIRITTO ALLA PRIVACY 193
1. Origine del diritto alla privacy 193
2. L'evoluzione del diritto alla privacy in Italia 197
3.1 Il c.d. «codice della privacy»: aspetti generali 208
3.2 I soggetti del codice della privacy 213
3.3 Il trattamento di dati personali (informativa, consenso, notificazione) 217
3.4 I diritti dell'interessato 227
3.5 Le misure di sicurezza 231
3.6 Il Garante per la protezione dei dati personali 235
3.8 Le sanzioni previste dal codice della privacy 243

CAPITOLO 8 244
IL DOCUMENTO INFORMATICO E LA FIRMA DIGITALE 244
1. Cenni preliminari 244
2. Il documento informatico nella evoluzione (o involuzione) della normativa italiana e comunitaria 246
3. La firma digitale 258

CAPITOLO 9 269
IL COMMERCIO ELETTRONICO 269
1. Aspetti generali 269
2. Business to Business (B2B), Business to Consumer (B2C), Person to Person (P2P) 273
3. La regolamentazione del commercio elettronico: in particolare il d.lgs. 70/03 276
4. I sistemi di pagamento 286
5. Aspetti problematici della sicurezza delle transazioni elettroniche 303
6. Questioni fiscali 305
7. I Meta Tags 308
8.1 Il nome di dominio e la tutela del marchio. Aspetti generali 309
8.2 La giurisprudenza in tema di nome di dominio 314

BIBLIOGRAFIA ESSENZIALE 324

PREMESSA

Questo volume nasce, in primo luogo, da una personale passione per l'informatica giuridica, materia nuova ed affascinante, ricca di numerosi stimoli e di molteplici problemi; in secondo luogo, per fornire sia una ricostruzione, per grandi linee, dell'evoluzione storica della materia, sia una analisi delle tematiche attuali anche in prospettiva futura. Soprattutto nasce, su suggerimento della prof.ssa Serra, per far fronte all'esigenza di fornire uno strumento per la didattica**,** utile per una preparazione di carattere generale, senza trascurare l'approfondimento di talune problematiche di particolare interesse. Il presente lavoro costituisce, tuttavia, la prima parte di un'opera più completa, che comprenderà le tematiche che non vi hanno trovato compiuta trattazione, in special modo i crimini informatici, il processo telematico, la sicurezza informatica, nonché i complessi rapporti fra pubblica amministrazione ed informatica e fra diritto d'autore e nuove tecnologie. Si è però avvertita l'esigenza di fornire un primo strumento interpretativo sia per fenomeni di particolare interesse (come Internet, *hackers*, *crackers*, ecc.) che per discipline di diritto positivo di particolare rilevanza e di recentissima emanazione, come il codice della *privacy*, i decreti legislativi in tema di commercio elettronico, di documento elettronico e firma digitale, ed altri ancora. Il completamento della seconda parte dell'opera consentirà, pertanto, di delineare un quadro generale dell'informatica giuridica con tutte le sue sfaccettature.

Ovviamente, ciascun argomento trattato può trovare maggiore approfondimento in opere di carattere monografico, per la molteplicità

di spunti che sorgono dall'analisi di ciascuno di essio; nondimeno, un'analisi, talvolta rapida, può risultare assai proficua sia per un primo accostamento alla materia che per un aggiornamento di discipline che sono soggette a continue variazioni.

Così, alla storia dell'informatica giuridica ed all'analisi delle sue branche, si è affiancata la trattazione di problematiche specifiche, con particolare riferimento ad Internet (approfondendone, soprattutto, le caratteristiche strutturali), al diritto alla *privacy*, al commercio elettronico, al documento informatico ed alla firma digitale. Ciascuna di esse comprende numerose altre tematiche e tocca più campi del diritto, per cui in taluni casi si è fatto un largo utilizzo di note, che per quanto potrebbero apparire invasive, hanno consentito di approfondire alcuni punti o di chiarire certi aspetti che avrebbero solo tediato il lettore più avveduto, ma che per alcuni potrebbero risultare essenziali per una corretta comprensione del testo od anche per soddisfare la mera curiosità di conoscere quegli aspetti specifici delle varie problematiche affrontate che non sempre sono recepiti a livello generale. Basti pensare alla *vexata quaestio* degli *hackers*, raramente distinti dai *crackers*; oppure alle nuove ed eterogenee implicazioni derivanti dalla diffusione del cyberspazio, relative sia a questioni che investono i principi fondamentali delle moderne democrazie rappresentative, sia a problematiche inerenti la tutela dei diritti fondamentali dell'uomo, a volte agevolandone la lesione, più spesso consentendone l'esercizio.

L'incidenza dell'informatica sul mondo e sul diritto è del resto innegabile, tanto da far comunemente definire la società odierna come la «società dell'informazione». In questo ambito a tutti noi spetta una

grande responsabilità: non far mai dimenticare la centralità dell'uomo in un mondo sempre più «artificiale».

Desidero ringraziare la prof.ssa Teresa Serra, le cui straordinarie doti umane e scientifiche non possono essere compiutamente espresse con queste poche parole, così come la mia gratitudine nei suoi confronti. Ringrazio inoltre i professori Donato Limone, per aver avuto la pazienza di discutere con me queste pagine e per le preziose indicazioni fornitemi, Agata C. Amato Mangiameli, per aver letto il manoscritto, e Serenella Armellini, che mirabilmente coniuga generosità e professionalità.

Rivolgo un ringraziamento particolare ai dottori Mario Sirimarco, Giuseppe Croari e Stefano Pratesi, all'avv. Iolanda Giordanelli ed a Fabrizio Totera, Gerardo Antonio Cavaliere, Giuseppe Contissa ed Antonio Fioriglio, per la loro amicizia ed il loro sincero affetto.

L'edizione cartacea della presente opera è stata già pubblicata da Aracne Editrice, Roma, 2004.

CAPITOLO 1

L'INFORMATICA GIURIDICA: ASPETTI GENERALI

1. LE ORIGINI: ELABORATORE ELETTRONICO, CIBERNETICA E GIURIMETRIA

L'elaboratore elettronico è uno strumento polifunzionale, che si presta agli usi più diversi: difatti è la prima macchina cibernetica finalizzata a coadiuvare l'uomo non nello svolgimento di attività fisiche, bensì intellettuali, grazie ad un'ampiezza di memoria, una velocità di elaborazione ed una capacità di comunicazione per alcuni aspetti di gran lunga superiori a quelle della mente umana ed, anzi, talvolta neppure immaginabili da parte di questa[1].

Uno schema di funzionamento di un moderno computer è stato predisposto già negli anni quaranta da **Norbert Wiener**, il creatore della cibernetica[2]. Nella sua opera fondamentale, intitolata C*ybernetics, or control and communication in the animal and the machine*, pubblicata nel 1948, egli sostiene che la macchina calcolatrice ideale dovrebbe in una prima fase (*input*) ricevere tutti i dati necessari per l'elaborazione richiesta, dunque grazie all'intervento umano, e in una seconda fase (*output*) procedere all'elaborazione stessa senza interferenze esterne. Ne consegue che nella

[1] E. GIANNANTONIO, *Introduzione all'informatica giuridica*, Milano, 1984, p. 4.

[2] "Il termine cibernetica è oggi passato ad indicare l'impiego dei metodi dell'analisi scientifica nella soluzione dei problemi di controllo, in relazione soprattutto al vertiginoso sviluppo contemporaneo della tecnologia" (R. BIN – N NAUCCHI, *Informatica per le scienze giuridiche*, Padova, 2003, p. 9).

prima fase dovrebbero essere inseriti non solo i dati numerici, ma anche le regole per la loro combinazione, sotto forma di istruzioni idonee a coprire qualsiasi situazione che potrebbe verificarsi nello svolgimento del calcolo. La macchina calcolatrice, pertanto, deve essere al contempo una macchina logica ed aritmetica e deve combinare le alternative secondo un algoritmo sistematico[3], utilizzando la logica booleana, la quale è caratterizzata da una rigida dicotomia, ossia dalla scelta fra due condizioni antitetiche, come il vero e il falso o l'appartenere ad una classe e il non appartenervi[4]. Sul punto vi è un parallelismo fra le macchine e gli animali (ivi comprendendo l'uomo) nello studio dei problemi della comunicazione e del controllo: l'analisi della struttura fisiologica consente una migliore comprensione del comportamento umano o animale, ma, al tempo stesso, la riproduzione in termini elettromeccanici o elettrici d'un fenomeno in senso intellettuale suggerisce nuove soluzioni interpretative del suo funzionamento. A sostegno della tesi sta la considerazione che le cellule nervose (i neuroni) hanno, in condizioni normali, un'attività fisiologica conforme al principio dicotomico di cui alla logica booleana, per cui o sono in posizione di riposo oppure, quando scattano, attraversano una serie di cambiamenti semidipendenti dalla natura e dall'intensità dello stimolo[5].

---

[3] Con riferimento a tale aspetto è doveroso menzionare A. M. TURING, *Calcolatori e intelligenza*, tr. it., in D. R. HOFSTADTER – TADTER ENNETT, *L'io della mente*, Milano, 1985, pp. 61-74, e ID., *On Computable Numbers with an Application to the Entscheidungsproblem*, in *Proceedings of the London Mathematical Society*, 1936, 42, pp. 230-265.

[4] N. WIENER, *La cibernetica. Controllo e comunicazione nell'animale e nella macchina*, tr. it., Milano, 1968, pp. 161-162.

[5] "Vi è una prima fase attiva, trasmessa dall'uno all'altro capo del neurone con velocità definita, alla quale fa seguito un periodo di refrattarietà durante il quale il neurone è insensibile agli stimoli, o almeno a stimoli connessi con normali processi

Un'altra similitudine fra il sistema nervoso animale e le macchine calcolatrici è data dalla necessarietà della memoria, ossia della capacità di conservare i risultati di operazioni già fatte per adoperarle in quelle da farsi. Wiener evidenzia la molteplicità di usi cui si presta la memoria: così, in alcuni casi sarà necessaria la presenza di una memoria che costituisce la base per il comportamento futuro della macchina (potrebbero farsi rientrare in questa categoria il BIOS ed il sistema operativo dei computer[6]); in altri occorrerà una grande rapidità in lettura, scrittura e cancellazione di dati (come oggi avviene con la memoria volatile dei computer, ossia la RAM)[7]; ovviamente sullo sfondo si pone il problema dei sistemi di immagazzinamento dei dati, negli anni quaranta ben diversi da quelli odierni. Il sistema nervoso animale e le macchine si differenziano, comunque, per un aspetto fondamentale: il primo non può

---

fisiologici. Alla fine di questo periodo, il nervo rimane inattivo, ma può venire di nuovo stimolato. Il nervo può quindi essere considerato un relé essenzialmente a due stati: scatto e riposo. A parte quei neuroni che ricevono i loro segnali da terminazioni libere o organi sensoriali terminali, in ogni neurone i segnali sono immessi da altri neuroni in punti di contatto chiamati *sinapsi*. Per un dato neurone di uscita questi variano da molto pochi a parecchie centinaia. È lo stato degli impulsi in ingresso alle varie sinapsi, combinato con il precedente stato dello stesso neurone, a determinare lo scatto o meno di questo. Se esso non è già attivo o refrattario, e se il numero di sinapsi in ingresso entro un certo brevissimo intervallo di fusione supera una certa soglia, allora il neurone scatterà con un ritardo sinaptico noto e abbastanza costante. La descrizione […] è forse troppo semplificata [ma chiarisce che] alcune definite combinazioni di impulsi sui neuroni aventi connessioni sinaptiche con un dato neurone determineranno lo scattare di questo, mentre altre non lo determineranno" (N. WIENER, *ivi*, p. 164).

[6] Le informazioni del BIOS sono assolutamente necessarie per l'avvio di ciascun elaboratore, poiché forniscono quelle funzioni di base che coordinano le varie periferiche presenti nel computer e ne consentono il funzionamento. Tali informazioni sono contenute in una tipologia di memoria detta ROM (*Read Only Memory*) e vengono lette ad ogni avvio dell'elaboratore; oggi sono generalmente contenute in memorie del tipo *Flash ROM* e sono aggiornabili via *software*. Le informazioni contenute nella ROM permangono anche dopo lo spegnimento del computer, al contrario di quelle contenute nella RAM (*Random Access Memory*).

[7] N. WIENER, *ivi*, p. 165.

autonomamente cancellare le proprie registrazioni (ciò può avvenire solo in seguito a determinate patologie o a forti traumi), mentre nelle seconde ogni ciclo operativo può essere totalmente autonomo, per cui il funzionamento del sistema nervoso risulta paragonabile ad un unico ciclo operativo di una macchina.

Un altro punto centrale della riflessione cibernetica è poi il concetto di *retroazione* (*feedback*), in base al quale il soggetto adatta il proprio comportamento all'ambiente circostante ed agisce anche in base alle modificazioni cagionate dalle proprie azioni, per cui l'azione non è vista in sé e per sé ma è analizzata anche alla luce delle conseguenze da essa provocate. L'interazione con l'ambiente e la modificazione dinamica del comportamento in base alle circostanze fattuali non è assolutamente semplice da realizzare e non è alla portata delle tecnologie attuali, che al riguardo sono ancora ad uno stato primordiale. La percezione e l'analisi dell'infinita varietà delle situazioni concrete costituiscono attività assai complesse, ma, secondo **Ettore Giannantonio**, "il «robot» del futuro sarà una "macchina" incredibile, capace di fare cose che l'uomo non è in grado di fare o, addirittura, di concepire. Sarà in grado di captare suoni che l'orecchio umano non può sentire e luci che l'occhio umano non è in grado di vedere; riprodurrà la complessità del sistema nervoso umano; sarà in grado di comportarsi come se vedesse o sentisse, «come se» pensasse. Ma non sarà in grado di pensare, di compiere cioè, quell'atto naturale ed elementare, proprio del genere umano, pel quale solamente possediamo il mondo, anzi pel quale solamente il mondo è"[8].

La considerazione dell'attuale livello tecnologico dell'informatica

[8] E. GIANNANTONIO, *op. cit.*, p. 6.

consente di accettare quanto sostenuto da Giannantonio, né sembra che nei prossimi anni si possa giungere alla costruzione di un sistema dotato di una intelligenza artificiale paragonabile a quella biologica dell'uomo, per quanto già oggi gli elaboratori elettronici riescano a svolgere molte operazioni, come l'esecuzione di calcoli complessi, in maniera di gran lunga più efficiente di quanto non possa fare l'uomo. Più specificatamente, "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"[9]. La complessità della mente umana rappresenta però la conseguenza di una lunghissima evoluzione e difficilmente potrà essere imitata da un computer, che invece coadiuverà l'uomo in un sempre crescente numero di attività. Anzi, lo sviluppo dell'intelligenza artificiale

[9] G. SARTOR, *Intelligenza artificiale e diritto. Un'introduzione*, Milano, 1996, p. 9. In materia si è progressivamente affermato anche un "paradigma ispirato al tentativo di rappresentare formalmente, e trasferire in sistemi di elaborazione, entità capaci di comportarsi in modo intelligente, anziché teorie del contesto e degli scopi dell'attività intelligente. Un'entità siffatta viene normalmente ottenuta costruendo un modello astratto di alcune caratteristiche del cervello umano. Così, una *rete neurale (neural network)* è composta di unità, chiamate *neuroni*, il cui comportamento è specificato da funzioni statistiche e matematiche. Ogni neurone è connesso con altri neuroni e interagisce con questi: riceve segnali (valori numerici) dai neuroni collegati o dal mondo esterno, applica una funzione di attivazione, e, eventualmente (se viene superata la soglia che caratterizza il neurone), invia il risultato della funzione ad altri neuroni o all'esterno. Alle connessioni tra i neuroni vengono assegnati pesi, che sono applicati ai segnali che attraversano tali connessioni, in modo da amplificare o ridurre quei segnali. Nell'architettura di una rete neurale, si distingue solitamente un livello di input, composto dai neuroni che comunicano esclusivamente con altri neuroni, un livello nascosto, composto dai neuroni che comunicano esclusivamente con altri neuroni, un livello di output composto dai neuroni che trasmettono all'esterno il risultato dell'elaborazione compiuta dalla rete" (*ivi*, pp. 19-21). Una rete neurale può essere addestrata, mediante la proposizione di un esempio di comportamento corretto da applicare in una determinata ipotesi, in modo da essere in grado di affrontare correttamente situazioni simili.

quale supporto all'intelligenza biologica consentirà una crescente interconnessione tra la stessa mente umana e gli apparati elettronici, con risultati eccezionali ed oggi inimmaginabili[10]. Probabilmente gli studi sull'intelligenza artificiale dovrebbero essere finalisticamente orientati ed incentrati non tanto sull'imitazione del pensiero umano, ma piuttosto sulla ricerca di nuove metodologie che consentano la creazione di sistemi finalizzati al supporto delle attività umane.

Da un altro punto di vista, Pierre Lévy afferma che, "di fatto, il punto di fuga ideale dell'informatica non è più l'intelligenza artificiale (rendere una macchina altrettanto, anzi, più intelligente dell'uomo), ma l'*intelligenza collettiva*, vale a dire la valorizzazione, l'utilizzazione ottimale e la messa in sinergia delle competenze, delle immaginazioni e delle energie intellettuali, qualunque sia la loro diversità qualitativa e ovunque si attui. Questo ideale d'intelligenza collettiva passa evidentemente attraverso una messa in comune della memoria, dell'immaginazione e dell'esperienza, attraverso una pratica semplificata dello scambio di conoscenze, attraverso nuove forme di organizzazione e coordinamento flessibile in tempo reale"[11].

Come afferma Giannantonio, del resto, le teorie cibernetiche volte

---

[10] A. VITERBO – TERBODIGNOLA, *L'informazione e l'informatica nella società della conoscenza*, in *Dir. inf.*, 2002, 1, p. 8. Autorevole dottrina ha poi osservato che "l'enorme difficoltà del progetto di «meccanizzare» l'intelligenza – e l'ambiguità dello stesso concetto di intelligenza – ha fatto dell'intelligenza artificiale il campo di battaglia tra programmi di ricerca alternativi, spesso ispirati da opposte «filosofie», da contrastanti concezioni del comportamento e della mente umana. Questa discussione vivace e continua, nel ricordare la natura sempre provvisoria e problematica dei risultati dell'intelligenza artificiale, fa sì che questa disciplina non sia un settore tecnologico isolato e asettico, ma l'ambito nella quale vengono discusse tematiche fondamentali di natura scientifica, epistemologica, etica, e sociale, spesso in relazione a problemi concreti e a quesiti formulati con precisione" (SARTOR G., *op. cit.*, p. 11).

[11] P. LÉVY, *Cybercultura. Gli usi sociali della nuova tecnologia*, tr. it, Milano, 2001, p. 163.

alla creazione di sistemi che si comportino come l'uomo mostrano la loro fragilità nel preconcetto che tutta l'attività dell'uomo, ed in particolare il pensiero, sia algoritmizzabile. Per algoritmo si intende "la prescrizione precisa dell'esecuzione in un certo ordine di un certo sistema di operazioni per la soluzione di tutti i problemi di un certo tipo. A questo fine, un problema complesso viene analizzato nelle sue diverse componenti più semplici, che vengono a loro volta analizzate sinché non vengano ridotte alle componenti elementari. La soluzione del problema originario può venire allora raggiunta per mezzo di una serie di operazioni in fasi successive. Per ogni fase, il sottoproblema consiste nello scegliere una fra due sole alternative possibili, cioè a dire, la risposta può essere solo «sì» o «no», «più» o «meno», «zero» o «uno». L'esecuzione di ogni fase successiva è determinata dai risultati di quella precedente. Lo svolgimento degli algoritmi appropriati è la condizione decisiva per ottenere la trasposizione in forma di automazione di un dato tipo di attività mentale umana, compresa la giurisprudenza. Si tratta cioè di una riduzione di ogni problema in termini binari, conforme all'esigenza base del meccanismo di ogni calcolatore elettronico"[12].

L'algoritmo non può avere ad oggetto l'infinita varietà dei singoli atti di conoscenza, ma solo gli schemi concettuali, le classi o le categorie create arbitrariamente dall'uomo, i fatti o gli atti già raggruppati e distinti ai quali va riservato il nome di dati. "Se è vero quindi che l'elaboratore può fare tutto ciò che fa l'uomo purché algoritmizzabile, ne consegue che l'elaboratore non potrà pensare, ma soltanto "elaborare", ossia confrontare i dati per rilevarne le somiglianze e le differenze e

[12] V. FROSINI, *Cibernetica diritto e società*, Milano, 1968, ora in ID., *Informatica diritto e società*, Milano, 1988, (cui si fa riferimento) pp. 20-21.

trasformarli da una classe in un'altra. Il dato da elaborare, così come il dato elaborato, non sarà costituito mai dal concreto atto di conoscenza, ma da un atto di conoscenza strutturato. E l'elaboratore permette il confronto e lo scambio dei dati entro le strutture; non conosce, ma stabilisce formule di eguaglianza e non serve a conoscere, ma a elaborare, ossia, contare, confrontare, trasformare il già conosciuto. L'elaborazione può, pertanto, essere definita come la trasformazione di certi dati (detti dati di ingresso) in altri dati (detti dati di uscita) che costituiscono i risultati dell'elaborazione. Per fare ciò l'elaboratore procede, in sostanza, ad un confronto tra dati diversi per affermarne l'identità. […] Di qui l'importanza dell'elaboratore in tutti i campi nei quali vi siano notevoli masse di dati da elaborare; e, al contrario, gli insuccessi dei tentativi di far compiere all'elaboratore anche i più banali atti concreti e particolari di conoscenza o di giudizio"[13].

Bisogna infatti considerare che il vero pensiero, che è attività percettiva della realtà, non è mai algoritmizzabile perché ogni atto di pensiero è diverso da qualsiasi altro. Difatti, l'atto di conoscenza avente ad oggetto una medesima cosa varia non solo da persona a persona, ma anche da un periodo all'altro da parte della stessa persona. Dunque, non è l'attività umana di conoscenza ad essere algoritmizzabile, ma lo è quell'altra, pratica e successiva, con la quale l'uomo ordina l'infinita varietà degli atti di conoscenza in gruppi o categorie o classi, raggruppando sotto una sola denominazione tutti gli atti di conoscenza simili e distinguendoli da quelli dissimili. Tuttavia, dal momento che qualunque atto di conoscenza è per sua natura diverso da ogni altro, per

[13] E. GIANNANTONIO, *op. cit.*, p. 9.

potere considerare simili, raggruppando sotto un solo concetto atti diversi, bisogna prescindere dalle differenze, seppur esistenti, e tenere fermi solo i caratteri comuni[14].

La creazione di un «giudice elettronico», dunque, non sembra possibile con le attuali tecnologie, perché nessuna macchina elettronica si avvicina, oggi, alla capacità di pensare dell'uomo, e, del resto, un elaboratore applica una determinata regola seguendo una rigida consequenzialità, ma non può cogliere le infinite sfumature della realtà. La regola, inoltre, è stabilita a priori dall'uomo, per cui si porrebbe l'ulteriore problema di giungere alla fissazione di regole oggettivamente certe. Come afferma **Vittorio Frosini**, "il vero problema è se il ricorso alla regola sia sempre necessario, o se non convenga talora invece commisurare il giudizio alla situazione concreta; e vera disumanità non è quella della macchina, che esegue senza sentire e capire, ma è bensì quella di integerrimi magistrati e di zelanti funzionari, che conoscono e praticano il rispetto della legge, costi quel che costi"[15].

L'applicazione automatica delle leggi ha, in ogni caso, destato l'interesse degli studiosi del diritto ed ha costituito uno dei tre punti principali di una disciplina che si è sviluppata a partire dal 1949, quando sulle pagine del *Minnesota Law Review* viene pubblicato un saggio di **Lee Loevinger** intitolato *Jurimetrics. The Next Step Forward*[16], nel quale per la prima volta si parla di **giurimetria**. L'autore evidenzia, primariamente, un grave paradosso dell'epoca moderna: la legge, che dovrebbe costituire il modello di condotta dei consociati, è divenuta un così recondito

[14] E. GIANNANTONIO, *ivi*, pp. 7-8.
[15] V. FROSINI, *op. cit.*, p. 55.
[16] L. LOEVINGER, *Jurimetrics. The Next Step Forward*, in *Minnesota Law Review*, 1949, 33, pp. 455-493

mistero da risultare *normalmente* incomprensibile. La crescente complessità della legge confonde, dunque, i cittadini e la società diventa meno coesa, con l'ulteriore conseguenza che i primi non rispettano leggi che non comprendono e che non vengono attuate, mentre i giuristi lamentano la mancanza di considerazione nei loro confronti e nei confronti della professione che svolgono. Sul punto, qualsiasi rimedio astrattamente proponibile si dimostra viziato già in partenza, ove non si tenga presente che è necessaria una evoluzione che porti al cambiamento del diritto stesso, il cui principale problema non è dato dai cittadini ma dai giuristi[17].

Secondo Loevinger, che riprende il pensiero di Julius Stone, i principi di diritto possono incorrere in cinque *logical fallacies*, riassumibili nelle seguenti categorie:

a) *meaningless reference*, quando i principi non rispondono alla logica;

b) *concelead multiple reference*, quando i concetti sembrano univoci nella loro espressione, ma in realtà si applicano a numerose fattispecie che hanno ben pochi elementi in comune;

[17] Come afferma Loevinger, "Many remedies are proposed: We must have better law enforcement – that is, more policemen to make the people obey the laws they do not understand. We must have a great moral renascence – presumably some sort of mystical process which will enable people intuitevely to apprehend the mysteries of law. We need better education – catch'em young, and teach them to respect the law while they're still credulous and uncritical. We ought to pass a new law to make people respect the old laws – ignorance of the law is no excuse, even for the lawyers. We need better "public relations" between the lawyers and the public – which simply means that the lawyers want to advertise like everybody else. There is a school of support for every proposal except the one that is the law itself which needs to be changed" (*ivi*, p. 455).

c) *competing reference*, quando ad un singolo caso concreto risultano applicabili più norme che tuttavia portano a conseguenze diverse;

d) *concelead circuitous reference*, quando la definizione di un principio è data dalla presupposizione dello stesso concetto che si intende definire;

e) *indeterminate reference*, quando un termine giuridico è tanto ambiguo da poter significare tutto o niente[18].

Gli sviluppi della cibernetica potrebbero consentire il superamento di tali fallacie, dal momento che possono essere costruiti dispositivi che, imitando il pensiero umano, riescono a risolvere equazioni con qualsiasi numero di variabili. Al riguardo si pongono però difficoltà di ordine pratico, poiché, a differenza dei numeri e dei simboli utilizzati dagli scienziati, caratterizzati da univocità, i termini legali costituiscono per lo più vaghe verbalizzazioni che hanno solo un significato ritualistico e che rappresentano la conseguenza della mancata evoluzione del diritto, nel cui ambito non sono stati elaborati nuovi metodi significativi nel corso di venti secoli di storia.[19] Tale evoluzione potrebbe essere possibile passando dalla giurisprudenza (basata sulla speculazione, sull'ipotesi e sulla superstizione) alla giurimetria, ossia all'investigazione scientifica dei problemi giuridici, utilizzando quegli stessi approcci e quelle stesse metodologie di carattere scientifico che hanno portato al progresso attraverso l'ampliamento della conoscenze in tutti i campi dello scibile

[18] L. LOEVINGER, *ivi*, pp. 470-471.
[19] L. LOEVINGER, *ivi*, pp. 471-473.

umano[20].

In particolare, Loevinger individua alcuni problemi oggetto d'indagine da parte della giurimetria[21], fra i quali bisogna primariamente menzionare la questione dell'analisi del comportamento del legislatore e dei giudici, prendendo pertanto in considerazione la legge sia nella fase della sua creazione che in quella della sua applicazione; tali momenti, comunque, presuppongono anche le ulteriori questioni della terminologia utilizzata nell'ambito giuridico nonché delle procedure da seguirsi in caso di lite giudiziaria.

Giurisprudenza e giurimetria non sono, comunque, concetti coincidenti; i problemi della prima non hanno un fine ultimo, perché possono essere oggetto di dibattito ma mai risolti né investigati, al contrario di quelli inerenti la giurimetria; inoltre, se la giurisprudenza ha carattere filosofico e ben pochi risvolti pratici, la giurimetria si caratterizza per un approccio eminentemente pratico[22].

Ciononostante, lo stesso Loevinger sostiene che la giurimetria non rappresenti la panacea di tutti i mali: *"jurimetrics promises no more than an opportunity for law to move forward along the same rocky road that all the other disciplines have already travelled. It is not an easy nor an inviting road (except for*

[20] L. LOEVINGER, *ivi*, p. 483.

[21] Essi consistono in: A. The behaviour of witnesses; B. The behaviour of judges; C. The behaviour of legislators; D. Legal language and communication; E. Legal procedure and recordation; F. Non-aberrant personal maladjustments; G. Aberrations of behaviour; H. Unintentional personal injury; I. Macrolegal techniques of investigation.

[22] Inoltre, "the problems of jurisprudence are formally "static" problems which presuppose the existence of one final authoritative answer, while the question of jurimetrics "are dynamic" in form in that they allow for changing answers as our knowledge increases. Indeed, in jurimetrics the questions themselves change as the body of knowledge grows, since the problems are constantly reformulated in terms of prior data" (L. LOEVINGER, *ivi*, p. 489).

those hardy souls who enjoy pioneering), but the grim and inescapable fact is that there is no other road running in the same direction"[23].

Le idee espresse dal giurista statunitense, considerate nel contesto temporale nel quale sono state espresse, sono dunque rivoluzionarie ed è pertanto evidente l'importanza del suo saggio, il quale non ha, tuttavia, una solida base teorica, perché, tra l'altro, non fornisce neanche una definizione di giurimetria. Del resto Loevinger non era solo un giurista, ma era anche il responsabile della Divisione Antitrust degli U.S.A., dunque un manager, non un teorico interessato alla creazione di una nuova disciplina secondo rigorosi presupposti logici. La giurimetria trova una compiuta sistemazione teorica quasi quindici anni dopo, quando nel 1963 viene pubblicato un volume collettivo intitolato **Jurimetrics**[24], curato da **Hans Baade**.

Baade afferma che il termine giurimetria "*signifies the scientific investigation of legal problems*": tale ambito è dunque vastissimo, al punto di coincidere con il diritto inteso nella sua totalità. Ciononostante, la ricerca in questo settore in quegli anni è stata svolta in tre aree principali:

a) applicazione dell'elaboratore elettronico in campo giuridico, con riferimento all'archiviazione e al reperimento elettronico delle informazioni legali (*electronic data storage and retrieval*);

b) previsione delle future sentenze dell'autorità giudiziaria, mediante l'analisi dei precedenti giurisprudenziali (*behavioral analysis of judicial decisions*);

[23] L. LOEVINGER, *ivi*, p. 490.
[24] H. W. BAADE (edited by), *Jurimetrics*, New York – London, 1963.

c) applicazione di criteri logici a questioni giuridiche (*use of symbolic logic*)[25].

Tali aree sono eterogenee, sia con riferimento all'oggetto che al metodo, ma presentano un denominatore comune costituito dalla tecnologia informatica; la tematica citata *sub b)* è stata da subito considerata il punto fondamentale della giurimetria e ciò si spiega chiaramente ove si consideri che questa disciplina è stata teorizzata in un ordinamento di *common law*, ove i precedenti giurisprudenziali hanno forza di legge e sono basati sul principio dello *stare decisis*, cioè del rispetto delle pronunce precedenti. Negli ordinamenti di *civil law*, come quello italiano, le leggi scritte costituiscono formalmente il diritto vigente, mentre i precedenti giurisprudenziali non sono vincolanti[26]. Pertanto, poter prevedere in anticipo le sentenze avrebbe portato benefici sia agli operatori economici ed amministrativi che allo stesso legislatore: ai primi, perché avrebbero potuto regolare le proprie azioni evitando le incertezze di eventuali (e costosi) procedimenti giudiziari; al secondo, perché sarebbe potuto intervenire in presenza di uno scarto fra le posizioni affermate dalle sentenze e le esigenze del sistema economico e sociopolitico[27].

Agli evidenti interessi economici coinvolti si accompagnava dunque una interessante progressione teorica e il consolidamento del

[25] H. W. BAADE, *Foreword*, in ID. (edited by), *op. cit.*, p. 1.

[26] Le tendenze evolutive del diritto hanno tuttavia portato ad una contaminazione dei suddetti modelli di ordinamento giuridico: come la produzione legislativa è in aumento anche nei paesi di *common law*, nei paesi di *civil law* si osserva che i precedenti giurisprudenziali hanno, di fatto, importanza fondamentale nell'applicazione del diritto. A ciò si aggiunge, inoltre, una sempre più corposa produzione legislativa extranazionale.

[27] E. FERRI – G. GIACOBBE – G. TADDEI ELMI, *Informatica e ordinamento giuridico*, Milano, 1988, p. 7.

principio della «retroazione anticipata». Tuttavia, le applicazioni pratiche delle teorie in materia non si sono dimostrate soddisfacenti a causa di più fattori, fra cui lo stato primordiale degli strumenti informatici dell'epoca, poco potenti e di difficile utilizzo, che non hanno consentito un facile svolgimento di operazioni connotate comunque da una notevole complessità. Già la mera archiviazione delle sentenze si è dovuta scontrare con le ridotte capacità di memorizzazione dei computer di quegli anni, nei quali è stato immagazzinato un numero tanto ridotto di sentenze da inficiare il calcolo di prevedibilità, che si è dimostrato poco attendibile anche perché non è stato effettuato su un numero di casi abbastanza vasto da risultare statisticamente attendibile.

In realtà, il problema più grande è di carattere ben più generale e coinvolge l'essenza stessa del diritto, che non costituisce una realtà statica e dunque prevedibile in base ad assiomi determinati, ma è invece una realtà viva ed in continua trasformazione, sulla quale incide una molteplicità di fattori astrattamente imprevedibili, coincidenti con le infinite situazioni che si presentano quotidianamente al giudice nel momento in cui deve applicare il diritto.

La possibilità di prevedere le sentenze dei giudici si è così risolta in un fallimento, ma tale settore della giurimetria non ha mai suscitato un fortissimo interesse negli ordinamenti di *civil law*, a causa della differente impostazione di tali sistemi giuridici rispetto a quello statunitense alla quale si è fatto cenno.

Al contrario, le metodologie di cui all'approccio informativo, che hanno poi dato vita al *legal information retrieval*, e quelle di cui all'approccio logico, in seguito denominate *legal expert systems*, hanno trovato ampia

diffusione ed hanno inoltre suscitato l'interesse degli studiosi appartenenti ad ordinamenti di *civil law*, anch'essi interessati da fenomeni di inflazione normativa, sia con riferimento a norme legislative che a precedenti giurisprudenziali.

La giurimetria non esaurisce il campo delle proposte avanzate negli anni sessanta di definizione terminologica della nuova disciplina: difatti, Paul S. Hoffmann nel 1963 conia il termine di *lawtomation*[28], che rappresenta l'unione dei termini *law* e *automation* e che indica con una sola parola le indicazioni delle provenienze giuridiche e tecnologiche. L'ambito disciplinare della *lawtomation*, o automazione giuridica, non coincide con quello della giurimetria, atteso che l'obiettivo di Hoffmann consiste nella semplificazione, razionalizzazione ed unificazione del criterio di classificazione dei testi giuridici al fine di facilitarne la memorizzazione ed il reperimento.

2. VERSO IL SUPERAMENTO DELLA GIURIMETRIA

Negli anni sessanta anche la dottrina italiana inizia ad interessarsi ai problemi e alle prospettive di quella disciplina allora denominata giurimetria, senza tuttavia conoscerne l'esatto ambito e dunque affrontando tematiche oltremodo eterogenee. Per mettere ordine nella disciplina, **Mario G. Losano** propone la sostituzione del termine «giurimetria» col termine «**giuscibernetica**», abbandonando al contempo la tripartizione utilizzata in giurimetria, ormai non più attuale in ragione, soprattutto, del fallimento degli esperimenti di previsione delle sentenze

[28] P. HOFFMANN, *Lawtomation in Legal Research: Some indexing Problems*, in *MULL*, 1963.

future, che non hanno comunque mai destato un vero interesse nei giuristi di *civil law*. La giuscibernetica, invece, dovrebbe essere divisa in quattro settori, corrispondenti ai quattro modi di accostarsi ai rapporti tra diritto e cibernetica, riassumibili in altrettanti approcci[29]:

a) la considerazione del *diritto come un sottosistema di quello sociale*. In tale concezione, propria della filosofia sociale, la società viene concepita come un insieme di sistemi (economico, religioso, giuridico) che interagiscono l'uno con l'altro. Fra essi assume particolare rilevanza il sistema giuridico, il quale fornisce le regole per poter operare nel sistema generale;

b) la considerazione del *diritto come un sistema autoregolantesi*. Tale prospettiva trova origine nella tradizione europea, ove lo studio del diritto ha assunto valenza autonoma, ed esso è stato rielaborato in chiave cibernetica, considerandolo un sistema cibernetico a retroazione, nel quale la commissione di un reato turba l'equilibrio sociale e l'irrogazione della sanzione al reo ristabilisce l'equilibrio sociale originariamente turbato;

c) l'*applicazione della logica e di altre tecniche di formalizzazione al diritto*, allo scopo di giungere ad un concreto uso dell'elaboratore;

d) l'*uso dell'elaboratore*, ossia l'apprendimento delle tecniche necessarie per il suo utilizzo nell'ambito giuridico.

I primi due approcci hanno un ambito puramente teorico e gli studi compiuti in tali settori sono finalizzati alla costruzione di modelli formalizzati, per cui essi costituiscono la modellistica giuscibernetica, al

[29] M. G. LOSANO, *Corso di informatica giuridica*, 1, *L'elaborazione dei dati non numerici*, Milano, 1984, p. 44.

cui interno si può inoltre distinguere fra una "modellistica astratta" e una "modellistica a fini pratici": più precisamente, la modellistica è astratta quando viene affrontato il discorso astratto sul diritto inteso nella sua totalità, mentre è pratica quando si affronta uno specifico settore del diritto, cui viene applicato il procedimento cibernetico di modellizzazione. In quest'ultimo caso si pongono le basi per un uso avanzato dell'elaboratore nel diritto, trasferendo all'elaboratore una serie di attività sino a quel momento svolte dall'uomo[30].

Più specificatamente, la modellistica giuscibernetica pratica pone il fondamentale problema della definizione della forma che un'attività giuridica deve assumere per essere svolta dall'elaboratore elettronico. Tale attività, concretizzantesi in una serie di atti miranti al raggiungimento di un certo fine, deve essere formalizzabile e, in particolare, traducibile in algoritmo, ossia in "un sistema di regole di trasformazione dei dati di entrata (problema) in altri dati di uscita (soluzione)". La definizione di algoritmo rende tuttavia palese i limiti principali della modellistica, dovuti al fatto che non tutti i problemi sociali sono riducibili in algoritmi e che non tutti gli algoritmi possono essere affidati proficuamente al computer. Inoltre, l'algoritmizzazione dei vari settori del diritto necessita di modifiche legislative che elidano la discrezionalità dei soggetti decidenti, adattando i testi normativi all'approccio della modellistica, per cui l'applicazione automatica della legge da parte di un elaboratore elettronico richiederebbe la riscrittura dell'intero impianto normativo e dunque la disumanizzazione della

[30] M. G. LOSANO, *ivi*, pp. 45-46.

giustizia costituisce un problema ben lontano dal venire[31].

L'ambito degli altri due approcci è invece immediatamente pratico, perché essi consistono nell'uso della logica applicata al diritto e nel passaggio dalla formalizzazione logica a tutte le altre formalizzazioni necessarie per giungere all'uso dell'elaboratore. Tali approcci costituiscono i due settori tradizionali oggetto di studio da parte della giurimetria e Losano afferma che essi rientrano nella più ampia definizione di "informatica giuridica", le cui tecniche consentono in primo luogo la memorizzazione in forma elettronica di informazioni giuridiche e in secondo luogo il loro reperimento mediante l'utilizzo dei computer. Tale settore coincide oggi con la c.d. informatica giuridica documentaria, per cui non esaurisce il più ampio ambito dell'informatica giuridica intesa in senso lato.

Del 1970 è *Informationskrise des Rechts und Datenverarbeitung*, tradotto in italiano col titolo di "Crisi dell'informazione giuridica ed elaborazione elettronica dei dati", nel quale **Spiros Simitis** supera le originarie concezioni della giurimetria, soprattutto con riferimento all'aspetto della previsione delle future sentenze dei giudici. L'illustre autore, infatti, dubita delle necessità di siffatte prognosi, poiché se la previsione non è effettuata soltanto a fini statistici, essa costituisce il controllo dell'attività giudiziaria, consentendo di accertare se i giudici si sono attenuti, anche incondizionatamente, alle norme vigenti. In tal modo si potrebbero "eliminare parecchi fattori spiacevoli e così tracciare la cornice della decisione giudiziaria molto più precisamente che finora. Ma il prezzo di un tale risultato è di palmare evidenza: la rigidità della giurisprudenza. In

[31] M. G. LOSANO, *ivi*, pp. 51-54.

nome di una certezza del diritto, ad ogni altra cosa preposta, ci si dichiara pronti a rinunziare ad ogni flessibilità"[32].

Infatti, come si è accennato in precedenza, il diritto è una realtà dinamica, in continua evoluzione, e dunque non è sussumibile entro criteri rigidi: esso nasce con la società e cammina con essa, misurandosi non con dati fissati una volta per tutti, ma piuttosto con la concreta situazione degli interessi. L'incertezza della decisione giudiziaria viene vista, forse paradossalmente, non come un fattore destabilizzante della società, ma piuttosto come un fattore di adeguamento continuo dell'ordinamento giuridico all'evoluzione della società. Se viene invece formalizzata e positivizzata la prevedibilità del comportamento giudiziale, il giudice viene costretto a tenere una posizione fissa senza la possibilità di rivederla[33]. In tal modo non c'è spazio né per la riflessione

[32] S. SIMITIS, *Crisi dell'informazione giuridica ed elaborazione elettronica dei dati*, tr. it., Milano, 1977, p. 110.

[33] Sul punto, Gianfranco Caridi osserva che "il passaggio all'applicazione automatica di una norma comporta un ridimensionamento della discrezionalità e un aumento dell'omogeneità del trattamento di destinatari della norma stessa, anche se esiste il pericolo di irrigidimento, di scarsa capacità di adattamento ai vari casi. Il ridimensionamento della discrezionalità comporta infatti conseguenze positive e negative: positive nella misura in cui rende rigidi, perché quantificabili, criteri di valutazione vaghi che consentono applicazioni arbitrarie: negative perché, operando a partire da una sola interpretazione, preclude o almeno complica notevolmente la possibilità di reinterpretare la norma nel tempo. In termini informatici, quando viene meno l'univocità dell'interpretazione del disposto normativo, bisogna modificare l'algoritmo costruito su quell'interpretazione" (*L'applicazione della legge mediante procedure automatizzate*, in AA.VV., *Liber amicorum in onore di Vittorio Frosini*, II, *Studi giuridici*, Milano, 1999, p. 61). Bisogna inoltre considerare che l'attività interpretativa di un testo giuridico viene svolta presupponendo un elevatissimo numero di dati "che non sono direttamente contenuti nei testi normativi [, … per cui] il diritto non è nelle leggi più di quanto non sia nella loro interpretazione" (F. ROMEO, *Il diritto artificiale*, Torino, 2002, p. 2), senza comunque dimenticare che l'analisi della realtà fattuale è operazione ancor più complessa ove si consideri la molteplicità dei singoli fattori che la compongono, i quali, a loro volta, devono essere, in alcuni casi, presi in considerazione dal diritto al momento della sua applicazione: questa fase,

né per la dialettica, ma si realizza solo una meccanica ripetizione del già dato. Perciò, le casualità e gli elementi irrazionali nell'ambito del reperimento del verdetto da parte del giudice, per quanto possano essere preoccupanti, non sono sufficienti a giustificare l'avvio di uno sviluppo che finirebbe per mettere in questione la stessa vigenza del diritto[34].

Simitis non ha tuttavia una visione pessimistica delle conseguenze provocate dallo sviluppo degli strumenti informatici e dal loro utilizzo in ambito giuridico, perché ritiene che essi avranno un ruolo prioritario anche nell'ambito applicativo del diritto[35]. L'illustre studioso, dunque, non estremizza le concezioni sostenibili nell'ambito della diffusione e dell'utilizzo degli elaboratori elettronici, ma analizza in maniera equilibrata i pro e i contro derivanti da essi, non cadendo, dunque, né in facili allarmismi né in altrettanto facili speranze. "In verità, gli apparecchi elettronici permettono di rendere palesi le contraddizioni alle premesse del diritto vigente, ma non possono affatto sostituire l'abile governo di quelle aperture dell'ordinamento giuridico che sempre consentono di superare la rigidità dei limiti esterni e con ciò permettono l'evoluzione delle norme considerate. In altre parole: il calcolo e l'assiomatizzazione sono, in verità, soltanto un'apoteosi dell'esistente ed una negazione radicale della trasformazione della disciplina giuridica, che a volte è con la legge appena compatibile ma che tuttavia è inevitabile"[36].

---

ovviamente, è preceduta dalla ricostruzione del fatto e dalla sua sussunzione entro le norme giuridiche, attività, pertanto, caratterizzate da una complessità intrinseca.

[34] S. SIMITIS, *ivi*, p. 111.

[35] S. SIMITIS, *ivi*, p. 116.

[36] S. SIMITIS, *ivi*, p. 120.

3. LA GIURITECNICA E L'INFORMATICA GIURIDICA NELL'AMBITO DELLO SVILUPPO TECNOLOGICO

La materia prima detta giurimetria e giuscibernetica va oggi sotto il nome di «**informatica giuridica**», con un'espressione ormai comunemente accettata, coniata nel 1962 da Philippe Dreyfus come contrazione di *information automatique juridique*. L'utilizzo di tale espressione è stato tuttavia criticato da **Vittorio Frosini**, perché "essa designa un settore specifico (quello giuridico) della scienza e della tecnica dell'informazione, che comprende un campo di indagini e di manipolazioni ormai reso vastissimo dallo sviluppo dell'informatica, ma non designa un modello nuovo di procedimento operativo giuridico: quello che si è cercato di definire come "diritto artificiale", e che consiste in un trattamento tecnicizzato, ossia oggettuale ed automatico, dei dati giuridici come metodologia logico-operativa. Secondariamente, e sia pure in subordine, l'espressione si presta malamente all'uso linguistico, non potendosi adoperare in forma aggettivale con la consueta flessibilità"[37].

L'illustre autore propone, dunque, un nuovo termine: «**giuritecnica**», contrazione di «tecnologia giuridica», espressione con la quale si designa la produzione in atto delle metodologie operative nel campo del diritto risultanti dall'applicazione di procedimenti e di strumenti tecnologici, senza che esso sia finalizzato alla sostituzione degli altri termini sino ad allora utilizzati per indicare la nuova disciplina. Esso rappresenta un nuovo simbolo semantico, di facile fungibilità e riassuntivo delle istanze emergenti nell'ambito dell'evoluzione del diritto.

[37] V. FROSINI, *La giuritecnica: problemi e proposte*, in *Informatica e diritto*, 1975, 1, pp. 26-35, e in ID., *Informatica diritto e società*, Milano, 1988, (cui si fa riferimento) pp. 163-164.

I problemi della giuritecnica sono anche problemi di tecnica giuridica, nel senso che condizionano i processi tecnologici della convivenza sociale e da questi sono condizionati. In tale ambito assumono primaria importanza le questioni inerenti l'automazione elettronica della ricerca giurisprudenziale nonché quelle relative all'automazione delle procedure amministrative: le prime realizzano una sintesi nuova fra diritto e tecnologia in un ambito interdisciplinare perché caratterizzato dagli apporti di varie scienze (lessicografia, logica simbolica, linguistica operativa, teoria dei sistemi), mentre le seconde prospettano un nuovo modo di amministrare, per cui assumono un ulteriore e duplice rilievo, sociologico e politico[38].

Nella ricostruzione di Frosini, dunque, la giuritecnica rappresenta la nuova frontiera nell'ambito dello studio del diritto ed è una disciplina caratterizzata da una intrinseca dinamicità perché legata all'inarrestabile progresso tecnologico, per cui giustamente si coglie la necessità di evitare la progressiva instaurazione di un insanabile iato fra lo sviluppo dell'informatica e l'evoluzione del diritto, evoluzione che può essere tale solo ove la legge colga i mutamenti di quella medesima società che deve regolamentare. Frosini, dunque, "avvia, con una felice intuizione, una sistematica e rigorosa riflessione filosofico-giuridica sul rapporto «macchina-diritto», con ampio anticipo sui giuristi"[39] e "il suo merito intellettuale consiste nella capacità di rappresentare in prospettiva lo scenario dei diritti e dei valori nell'era tecnologica, in cui stiamo cominciando a vivere, e che sarà il contesto diretto dell'esperienza

[38] V. FROSINI, *ivi*, p. 172.
[39] D. A. LIMONE., *Introduzione*, in ID. (a cura di), *Dalla giuritecnica all'informatica giuridica. Studi dedicati a Vittorio Frosini*, Milano, 1995, p. VII.

giuridica del futuro"[40].

Nonostante la persuasività e la modernità delle tesi di Losano e Frosini, non si impose nessuno dei due termini da loro suggeriti; tuttavia, le dispute riguardo al nome col quale designare l'informatica giuridica non devono essere considerate meri dibattiti formali e terminologici, poiché ogni diversa definizione sottende una diversa concezione sostanziale dell'ambito della materia che è ormai pacificamente detta «informatica giuridica». Secondo Frosini, essa rappresenta "una specificazione metodologica, se riferita ai suoi principi costitutivi, ed una applicazione particolare della nuova dimensione acquistata dal settore dell'informazione con l'avvento dei mezzi di comunicazione di massa o *mass-media*. Essa ha infatti consentito anzitutto una crescita concettuale ed una conferma sperimentale della «logica giuridica» o logica deontica, come viene chiamata la ricerca logica applicata al calcolo razionale delle relazioni fra le norme (ed in ispecie di quelle giuridiche). Ciò è dovuto al fatto, che una ricerca documentaria nel campo dei testi giuridici di legge richiede una trascrizione del linguaggio giuridico in linguaggio elettronico (che è propriamente un metalinguaggio simbolico) e perciò il ricorso a tecniche di omogeneizzazione e di standardizzazione linguistica nei collegamenti sintattici"[41].

Oggi l'**informatica giuridica** ha per oggetto l'applicazione della tecnologia dell'informazione al diritto. "È una disciplina bifronte nella quale si intrecciano una metodologia tecnologica con il suo oggetto

[40] A. E. PÉREZ-LUÑO, *Vittorio Frosini ed i nuovi diritti della società tecnologica*, in AA.VV., *Liber amicorum in onore di Vittorio Frosini*, II, *Studi giuridici*, Milano, 1999, p. 197.
[41] V. FROSINI, *Diritto e informatica negli anni ottanta*, in *Riv. trim. dir. pubbl.*, 1984, 2, pp. 390-400, ora in ID., *Informatica diritto e società*, Milano, 1988, (cui si fa riferimento) p. 231.

giuridico, che a sua volta condiziona le stesse possibilità o modalità di applicazione"[42]. Questa espressione ha prevalso sulle altre perché nel suo ambito rientrano tutti gli aspetti (molteplici e distinti) del rapporto fra computer e diritto, secondo una terminologia diversa da quella utilizzata negli Stati Uniti, ove è per lo più indicata con l'espressione di «*computer and law*»[43].

La differenza terminologica fra i paesi europei e gli Stati Uniti si accompagna ad un altrettanto differenziato sviluppo dell'informatica giuridica: il diritto europeo è infatti profondamente diverso da quello statunitense, con la citata prevalenza del materiale legislativo rispetto a quello giurisprudenziale. Ne consegue un diverso interessamento alle tecnologie informatiche, che negli anni settanta sono state primariamente finalizzate alla costruzione di banche dati. Ciò ha portato alcuni Stati ad emanare, in quegli anni, normative di regolamentazione delle banche dati, anche a tutela della *privacy* informatica. A tali primi interventi ha fatto seguito una normazione di carattere internazionale, cui l'Italia si è adeguata solo nel 1996[44].

Com'è evidente, gli sviluppi legislativi e dottrinali sono stati legati, e lo sono tuttora all'evoluzione tecnologica, in quanto gli elaboratori elettronici sono profondamente mutati nel corso di pochi decenni: infatti, inizialmente la diffusione di tali sistemi è stata limitata alla presenza di pochi *mainframe*, i quali contenevano le informazioni cui si poteva accedere utilizzando dei terminali collegati all'elaboratore

[42] A. E. PÉREZ-LUÑO, *Saggi di informatica giuridica*, cit., p. 39.
[43] R. BORRUSO, *Informatica giuridica* (voce), in *Enc. dir.*, Agg., I, Milano, 1997, p. 640.
[44] Il 31 dicembre 1996 è stata infatti emanata la legge n. 675 (la c.d. legge sulla *privacy*), oggi abrogata e sostituita dal d. lgs. 30 giugno 2003, n. 196 (Codice in materia di protezione dei dati personali, già detto «codice della *privacy*»).

centrale. L'utilizzo di tali sistemi è sempre risultato assai difficoltoso, a causa della mancanza di interfacce grafiche fra l'utente e la macchina, mentre i sistemi di interrogazione richiedevano conoscenze specifiche per ciascun sistema.

Successivamente è cresciuta la capacità elaborativa dei singoli *computers*, che dunque sono progressivamente diventati indipendenti e successivamente anche interconnessi (conservando comunque la propria autonomia) per poter condividere le proprie risorse. Negli anni ottanta, infatti, è iniziata l'informatizzazione di massa e in alcuni sistemi operativi[45] sono state implementate le interfacce grafiche a finestre, che hanno reso assai più semplice l'utilizzo dei *computers*. Se il lancio del Macintosh nel 1984 da parte della Apple ha rappresentato una rivoluzione in questo ambito, poiché per la prima volta i sistemi dotati di interfaccia grafica (già creati negli anni settanta) possono conquistare il mercato di massa[46], il vero *boom* avviene però negli anni novanta, quando l'informatizzazione ha iniziato a crescere a ritmo esponenziale, anche grazie alla diffusione di Internet e all'avvento del *World Wide Web* (WWW), che ha reso assai semplice la navigazione in Rete. Si è così realizzata l'interconnessione globale dei sistemi ed Internet è diventata una sorta di mondo «virtuale», al contempo parallelo, sovrapposto e

[45] Il sistema operativo è un *software* che gestisce l'*hardware* del *computer* e i programmi eseguiti su di esso. Costituisce un'interfaccia fra la macchina e l'utente e gestisce le risorse (*hardware* e *software*) dell'elaboratore.

[46] L'anno successivo la Commodore presenta l'Amiga 1000, dotato di interfaccia grafica nonché capace di svolgere più operazioni (*task*) ed eseguire più applicazioni in parallelo (*multitasking pre-emptive*), mentre la Microsoft rilascia la prima versione di Windows, ancora allo stato di ambiente operativo (difatti Windows, sino alla versione 3.11 inclusa, richiedeva che sulla macchina fosse presente il sistema operativo MS-DOS (della stessa Microsoft). Solo nel 1995 il colosso di Seattle lanciava la prima versione *stand-alone* di Windows, un vero e proprio sistema operativo che tuttavia includeva ancora una versione, seppur aggiornata, di MS-DOS.

contrapposto al mondo «reale».

I *computers* si sono così diffusi nella maggior parte dei luoghi di lavoro nonché nei luoghi domestici, diventando in breve uno strumento insostituibile sia per fini professionali che ludico-ricreativi. La polifunzionalità che da sempre caratterizza gli elaboratori elettronici ha assunto nuove caratteristiche, trasformando ogni singolo computer in una stazione multimediale adattabile alle esigenze più diverse.

Come afferma Giancarlo Taddei Elmi, a seconda della funzione svolta o del fine perseguito le applicazioni informatiche possono essere suddivise in cinque **ambiti applicativi funzionali**: informativo, conoscitivo, redazionale, gestionale, didattico[47].

A questi cinque ambiti corrispondono i sistemi informatici:

a) *informativi*: costituiscono lo sviluppo dell'ambito informativo della giurimetria, poiché sono sistemi che memorizzano informazioni, consentendone il reperimento. Sono isomorfi, in quanto le informazioni in entrata sono uguali a quelle in uscita e sussiste corrispondenza morfologica fra i dati registrati e i dati ricercati. Inizialmente tali sistemi erano *adialogici* o *batch*, dunque non consentivano il dialogo fra l'utente e il sistema, e le loro prime implementazioni di una certa importanza risalgono agli anni sessanta[48], ma presentavano il problema, strutturale, di dover procedere a ricerche sull'intera banca dati senza consentire l'affinamento di ricerche già effettuate. Negli anni settanta questo problema viene superato dai sistemi informativi *dialogici*, tuttavia

[47] G. TADDEI ELMI, *Origine e sviluppo dell'informatica giuridica*, in N. PALAZZOLO (a cura di), *Corso di informatica giuridica*, Catania, 1998, p. 5 e ss.
[48] Come il sistema *LITE* dell'*Air Force Accounting and Finance Center*, sviluppato nel 1963.

caratterizzati da una elevata difficoltà nell'utilizzo, dovendosi utilizzare linguaggi di interrogazione *ad hoc* sempre per mezzo di interfacce testuali (le c.d. CLI, *command line interface*[49]). Negli anni ottanta fanno la loro comparsa le prime interfacce grafiche (le c.d. GUI, *graphical user interface*[50]) ed inoltre i sistemi informativi divengono *ipertestuali*: l'informazione non viene indicizzata ma organizzata in maniera non lineare, per cui l'approccio conoscitivo è di tipo associativo e non sequenziale. L'individualità di tali sistemi viene meno con l'evoluzione delle reti telematiche e soprattutto di Internet, che, come detto, consente l'interconnessione globale di praticamente tutti i computer anche se basati su *hardware* e *software* completamente diversi, per cui tali sistemi sono anche detti *integrali* o *telematici*;

b) *cognitivi*: producono conoscenza, poiché a partire da una conoscenza di base forniscono una nuova conoscenza diversa da quella di partenza, per cui sono sistemi eteromorfi. Costituiscono lo sviluppo dell'ambito logico della giurimetria e sono detti sistemi esperti. L'informazione viene così trattata non in maniera meramente formale, come nei sistemi informativi, ma piuttosto in maniera sostanziale, cercando di cogliere il significato dei dati immessi nel sistema e successivamente di elaborarli per poterne fornire di nuovi, esprimendo contenuti e producendo ragionamenti sulla conoscenza. I primi esperimenti in materia

[49] Il sistema operativo MS-DOS è un tipico esempio di interfaccia di tipo CLI: le funzioni vengono svolte mediante comandi testuali digitati sulla tastiera del computer.

[50] Come nei già ricordati sistemi Apple Macintosh (col suo MacOS) e Commodore Amiga (con i suoi AmigaOS e Workbench).

risalgono alla fine degli anni sessanta ed agli inizi degli anni settanta (come il sistema *Taxman*, nel settore del diritto fiscale societario[51]), ma il loro sviluppo continua a proseguire, nonostante l'estrema complessità di tale profilo, ed oggi suscitano un forte interesse le tecniche di *semantic web*, che dunque segnerebbero un enorme salto qualitativo per gli elaboratori elettronici: il reale passaggio da una conoscenza formale ad una sostanziale delle informazioni *on line*;

c) *redazionali*: producono atti giuridici, siano essi documenti negoziali, processuali, decisionali e normativi. Di base, tali sistemi si concretizzano nei *word processor*, ossia in quei programmi di *editing* del testo, utilizzabili per la redazione di qualsiasi scritto. L'evoluzione tecnologica ha interessato anche tali programmi, che assommano oramai numerosissime funzioni (vocabolari, controllori ortografici, thesauri) e si dimostrano sempre più potenti e flessibili. Sono stati creati anche programmi specifici per la redazione di atti giuridici, basati sulla considerazione che i singoli atti rientranti nelle categorie generali presentano un contenuto minimo comune; dunque, alle funzioni linguistiche, che già i normali *editor* di testo offrono, si accompagnano funzioni strutturali, che accompagnano l'utente nell'ambito della struttura formale e di quella funzionale, in altri

[51] Su di esso v. L. T. MCCARTHY, *Reflections on TAXMAN: An experiment in Artificial Intelligence and Legal Reasoning*, in *Harv. Law Rev.*, 1977, pp. 837-893. Questo progetto, iniziato negli Stati Uniti nel 1972, era finalizzato alla creazione di un sistema in grado di stabilire se una riorganizzazione societaria rientrasse in una delle fattispecie esente da imposte di cui all'*Internal Revenue Code*.

termini sia nella redazione delle componenti formali del singolo atto che nella composizione di quelle componenti contenutistiche;

d) *gestionali* o *manageriali*: producono procedure di gestione, automatizzando l'attività burocratico-amministrativa degli uffici giudiziari e legali; in tale caso specifico si parla, propriamente, di informatica giudiziaria;

e) *didattici*: producono processi di apprendimento, agevolando l'apprendimento delle nozioni giuridiche, e possono costituire applicazioni specifiche di sistemi esperti[52].

Ovviamente, la grande diffusione dei computer non comporta che sia la loro invenzione in sé e per sé a giustificare la nascita dell'informatica giuridica o la sua considerazione quale disciplina autonoma[53], perché, come afferma Vincenzo Zeno-Zencovich, non è "l'invenzione in sé che fa evolvere il diritto, quanto una serie di

[52] Fra i sistemi elettronici per la didattica giuridica si possono ricordare i sistemi tutoriali (realizzati dai docenti e contenenti materiali di esercitazione integrativi delle lezioni) ed esplorativi (manuali elettronici, sostitutivi dei tradizionali manuali cartacei). Accanto ad essi si pongono le simulazioni (come videogiochi che simulano, ad esempio, l'attività di uno studio legale) nonché una fonte di apprendimento virtualmente illimitata, come Internet. Come è risultato dai lavori della *3rd International Conference on Substantive Technology in Legal Education*, tenutasi a Parigi nel 1994, questi sistemi costituiscono uno strumento stimolante per l'apprendimento del diritto, indipendentemente dal loro livello di complessità tecnica (R. M. DI GIORGI – R. NANNUCCI, *Informatica e didattica del diritto*, in N. PALAZZOLO (a cura di), cit., pp. 205-216).

[53] Sul punto, tenendo presente la suddivisione in ambiti applicativi funzionali di cui si è detto, si può ricordare la posizione di Taddei Elmi, secondo il quale "il termine *informatica giuridica* indica solo un vasto campo di competenze interdisciplinari, distinte da *diversi oggetti primari dell'esperienza* (la documentazione, la teoria della conoscenza, del ragionamento e della decisione, l'organizzazione dell'ufficio, la redazione del documento e la didattica) e legate da un comune oggetto dell'esperienza primario costituito dal calcolatore e da un comune oggetto dell'esperienza secondario costituito da una nozione molto generica di diritto" (*Corso di informatica giuridica*, Napoli, 2003, p. 94).

interazioni più complesse fra la diffusione dell'invenzione ed i processi sociali e fra questi ed il diritto"[54]. Tali interazioni si sono verificate e continuano a verificarsi, perché solo l'informatizzazione di massa ha inciso tanto profondamente e in maniera tanto repentina sulle dinamiche della società. La rivoluzione informatica si è potuta realizzare grazie alla continua applicazione pratica degli studi compiuti in tale settore, con un progressivo rafforzamento del nesso fra la creazione dell'innovazione ed il suo utilizzo[55], che, come si è visto, ha superato ben presto gli ambiti applicativi delle discipline di riferimento per estendersi anche al diritto, caratterizzato da ambiti e ritmi evolutivi assai diversi.

4. IL DIRITTO DELL'INFORMATICA

Il passaggio dall'informatica giuridica al diritto dell'informatica è avvenuto con la regolamentazione legislativa della gestione degli elaboratori elettronici. L'informatica è, al contempo, la linea che divide e che unisce l'informatica giuridica e il **diritto dell'informatica**, il quale rappresenta una nuova forma dell'esperienza propriamente giuridica, anche se riferita ad elementi tecnologici, per cui si propone in un'ottica complementare e corrispettiva rispetto all'informatica giuridica[56]. Il diritto dell'informatica riguarda le questioni connesse all'impiego dell'informatica non come strumento ausiliario, ma come oggetto esso

[54] V. ZENO-ZENCOVICH, *Informatica ed evoluzione del diritto*, in *Dir. inf.*, 2003, 1, p. 90.
[55] A. VITERBO – TERBODIGNOLA, *La rete: tecnologia di libertà?*, in *Dir. inf.*, 2003, 2, p. 227.
[56] V. FROSINI, *op. ult. cit.*, p. 232.

stesso di disposizioni normative e di indagini dottrinarie[57].

L'informatica giuridica e il diritto dell'informatica rappresentano, comunque, una realtà unica caratterizzata dalla trasversalità: non c'è un settore del diritto che non sia stato investito dalla rivoluzione informatica, dalla filosofia del diritto al diritto privato, dal diritto pubblico al diritto penale[58]. Nel diritto dell'informatica il *trait d'union* fra le varie discipline è costituito dalla "omogeneità degli argomenti trattati e dall'esistenza di principi e criteri che la regolano e che trovano il loro fulcro nell'individuazione dell'oggetto di studio rappresentato dall'attività informatica. Questa non è né un bene materiale, né un'attività propria dell'uomo, né tantomeno un'energia umana dovendo invero riferire più correttamente detta attività all'elaboratore, il quale, benché costruito dall'uomo, ha una sua propria capacità elaborativa e decisionale pur nei limiti dell'*hardware* e del *software* che ne comandano l'attività"[59]. Ciò

[57] Antonio-Enrique Pérez Luño definisce il diritto dell'informatica come "il settore normativo dei sistemi giuridici contemporanei, integrato dall'insieme delle disposizioni volte a regolare le nuove tecnologie della informazione e della comunicazione, l'informatica e la telematica" (*Saggi di informatica giuridica*, tr. it., Milano, 1998, p. 6).

[58] Come sottolinea Pietro Rescigno, "le materie 'nuove', quale è certamente quella che appartiene al diritto dell'informatica, presentano in modo costante, o almeno frequente, un carattere ulteriore. Esse si collocano fuori o al di là delle usuali partizioni scolastiche, a cominciare dalla elementare distinzione tra diritto pubblico e privato: vuoi nel senso che per taluni istituti la separazione è intollerabile o fuor di luogo, vuoi nel senso che nel settore confluiscono discipline collocate nei due settori in cui si continua ad ordinare l'esperienza giuridica (anche quando del criterio si sottolinea la storica relatività)" (*Prefazione*, in E. GIANNANTONIO, *Manuale di diritto dell'informatica*, Padova, 2001, p. XVI).

[59] M. BARBARISI, *Diritto e informatica*, Napoli, 1997, p. 13. Sul punto, Ettore Giannantonio osserva che il computer "è la prima macchina cibernetica dotata della capacità di distinguere e di connettere e di reagire al verificarsi di predeterminate situazioni; una macchina capace, quindi, di svolgere un'attività molto simile a quella ritenuta propria dell'uomo. L'introduzione dell'informatica nella vita sociale ha comportato, dunque, la configurazione di un nuovo tipo di bene, l'attività automatica, che non è possibile inquadrare nella tradizionale distinzione dei beni

costituisce, da un lato, il punto più dolente della nuova disciplina, ma, dall'altro, anche la nota più peculiare, caratterizzante e, soprattutto, unificante della nuova materia[60].

L'informatica, del resto, ha messo in crisi i concetti sui quali sono basate interi settori del diritto: oggi, ad esempio, non è più possibile tutelare il diritto d'autore seguendo le metodologie classiche che sono oramai obsolete, perché la normativa di riferimento è stata e continua ad essere oggetto di interventi che pretendono di disciplinare fattispecie nuove con strumenti all'uopo inadatti, i cui principi presuppongono la materialità dei supporti contenenti le opere dell'ingegno. L'informatica ha, infatti, smaterializzato l'informazione, che diviene progressivamente il bene più importante, tanto che la società odierna è comunemente detta «società dell'informazione»: questo carattere si riverbera non solo sul diritto d'autore, ma su una molteplicità di fattispecie, oggetto delle discipline più eterogenee. Una delle nuove forme di criminalità, infatti, è quella informatica, che pone, fra l'altro, i difficili problemi dell'individuazione del *locus commissi delicti*, in ragione del carattere di a-territorialità di Internet, oltre al problema dell'individuazione del luogo ove si verificano gli effetti della condotta illecita, rilevanti nell'ambito del diritto privato con riferimento, fra l'altro, alla regole di responsabilità civile. Ancora, si registrano sperimentazioni in tema di processo telematico che potrebbero snellire un *iter* procedimentale spesso lento e

giuridici e degli oggetti del diritto" (*Manuale di diritto dell'informatica*, cit., p. 3).

[60] A. TRAVERSI, *Il diritto dell'informatica*, Milano, 1990, p. 42. In senso contrario si pone Giancarlo Taddei Elmi, il quale ritiene che, "nonostante proliferino opere dedicate al diritto dell'informatica nel suo complesso, al momento non si [può] parlare di una disciplina autonoma ma solo di sviluppi del diritto costituzionale, del diritto privato, del diritto penale e del diritto processuale" (*op. ult. cit.*, p. 114).

farraginoso, che si svolge, oltretutto, in aule di tribunale sempre più affollate nelle quali spesso non c'è la possibilità materiale di analizzare le singole cause nel tempo che sarebbe necessario.

Gli esempi potrebbero continuare a lungo, ma anziché soffermarsi ancora su tale elencazione, bisogna puntualizzare un aspetto che costituisce una conseguenza comune nelle varie discipline e che è relativo all'incidenza dell'informatica sul diritto: la maggior parte delle nuove problematiche non è sussumibile entro le regole già dettate per fattispecie diverse, proprio per una troppo profonda eterogeneità di fondo. Si evidenzia, inoltre, la necessità di giungere alla fissazione (quantomeno) di principi generali a livello internazionale, perché l'interconnessione globale dei sistemi informatici posta in essere per mezzo di Internet impone (o imporrebbe) regole altrettanto globali, anche se è doveroso ammettere che tale necessità potrebbe rimanere una mera utopia, ma l'inadeguatezza delle singole legislazioni è, in tali casi, di lapalissiana chiarezza[61]. Il problema è che si realizza un vero e proprio «scontro» fra un diritto positivo che vuole imporre delle regole ed una realtà che le rifiuta ma che avrebbe comunque bisogno di una regolamentazione, che dovrebbe però essere flessibile e dinamica perché questi caratteri sono propri del settore informatico, il cui sviluppo avviene in tempi ben più celeri di quelli del diritto. Il diritto dovrebbe adattarsi all'informatica perché non può essere slegato dalla realtà, ma deve prenderla in considerazione e regolarla secondo i principi generali dell'ordinamento giuridico, come dovrebbe avvenire per ogni settore della società. Se si realizza un insanabile iato fra la realtà e il diritto,

[61] Sul carattere di a-territorialità della rete Internet v. *infra*, cap. 6.

questo perde la sua ragion d'essere perché regolamenta qualcosa che o non esiste oppure esiste ma in maniera diversa da quanto presupposto nella sua regolamentazione.

Come è stato evidenziato in dottrina, non si è ancora giunti, tuttavia, ad una piena comprensione fra il mondo dei giuristi e il mondo dell'informatica. "Il problema […] è quello di un cambio di mentalità dei giuristi, di una nuova "cultura" che stenta a penetrare nel mondo del diritto. […] Questo cambio di mentalità da parte dei giuristi è assolutamente essenziale per lo stesso progredire dell'informatica giuridica: non si può pensare che la ricerca negli svariati settori in cui ormai si articola l'informatica giuridica possa farsi solo nel chiuso di istituti di ricerca che, per quanto prestigiosi possano essere, non saranno apprezzati se non riusciranno a realizzare prodotti concretamente applicabili alla pratica del diritto. Dire che il futuro del diritto stia tutto nell'informatica è certamente eccessivo. È vero però che le modificazioni che si potranno avere nella conoscenza e nella pratica del diritto per effetto delle applicazioni informatiche sono di grandissimo rilievo, ed in gran parte ancora inesplorate"[62].

5. L'INFORMATICA GIUDIZIARIA

L'**informatica giudiziaria** consiste nell'applicazione della tecnologia informatica e telematica all'attività giudiziaria, nel cui ambito gli elaboratori elettronici possono essere utilizzati a fini diversi. In senso stretto, con tale espressione "suole intendersi l'automazione del lavoro

[62] N. PALAZZOLO, *Informazione pubblica e informatica per il diritto*, Firenze, 2001, p. 52.

degli uffici giudiziari"[63], in senso lato anche l'automazione degli studi legali e notarili, anche se in tal caso si parla più propriamente di **informatica legale**. Questa disciplina assume progressivamente maggiore importanza, parallelamente alla diffusione degli strumenti informatici, i quali, ad esempio, facilitano la memorizzazione delle informazioni nonché la relativa attività di reperimento. Del resto, nella sempre crescente mole di norme, sentenze, atti processuali, divengono man mano evidenti i limiti intrinseci dei tradizionali metodi basati sull'archiviazione cartacea e sulla successiva consultazione necessariamente effettuata direttamente sulla documentazione così prodotta, cui l'informatica consente di porre rimedio.

Lo svolgimento delle attività giudiziarie risulta dunque semplificato dalla creazione di archivi informatici, che concretizzano dunque la fase documentaria di quella branca specifica dell'informatica giuridica che è l'informatica giudiziaria. Bisogna poi considerare che il procedimento giudiziario non ha solo carattere conoscitivo, ma anche operativo, che si esplica nella fase procedurale e consiste nello svolgimento del processo in una successione di fasi temporali, a partire dagli atti introduttivi del processo per giungere poi all'atto conclusivo, costituito dalla sentenza. Appare dunque evidente che tale settore dell'informatica giuridica si rivolge agli operatori del diritto inseriti nell'ambito del sistema giudiziario, ossia magistrati e soggetti inseriti nel settore amministrativo.

L'informatica giudiziaria può pertanto essere suddivisa in quattro aree:

[63] R. CORTESE – C. JACOBAZZI – D. A. LIMONE (a cura di), *Manuale di informatica giudiziaria*, Rimini, 1985, p. 145.

a) *gestionale*, se è relativa ai procedimenti giudiziali, nella fase della gestione degli atti posti in essere dal giudice e dalle parti. Il processo telematico è pertanto il campo d'elezione dell'informatica giudiziaria gestionale[64];

b) *documentaria*, con riferimento alle banche dati inerenti l'attività giudiziaria;

c) *amministrativa*, finalizzata all'amministrazione del personale e dei servizi di supporto di amministrativo degli uffici giudiziari;

d) *decisionale*, per la soluzione di vere e proprie questioni giuridiche[65].

Soprattutto con riferimento al processo penale, la verbalizzazione automatizzata delle fasi dibattimentali consente di superare i limiti della corrispondente attività umana, soggetta ad errori. Inoltre, la possibilità di effettuare testimonianze anche in videoconferenza si dimostra assai utile, perché evita il trasferimento di soggetti lontani dal luogo ove si svolge il dibattimento, con un considerevole risparmio temporale ed economico, soprattutto nel caso in cui chi debba rendere le dichiarazioni sia detenuto in una casa circondariale oppure sia sottoposto a regime di protezione: i relativi trasferimenti sarebbero infatti assai onerosi oltreché rischiosi per la pubblica incolumità.

---

[64] Sul processo telematico v., fra gli altri, G. DI BENEDETTO – NEDEELLANO, *I linguaggi del processo. La forma degli atti e il processo informatico,* Milano, 2002; M. JACCHIA (a cura di), *Il Processo Telematico. Nuovi ruoli e nuove tecnologie per un moderno processo civile*, Bologna, 2000; A. VILLECCO BETTELLI, *Processo telematico* (voce), in *Dig. disc. priv. – sez. civ.*, Agg., II, Torino, 2003, pp. 1028-1035. Per una proposta di processo civile telematico v., fra gli altri, V. DI CATALDO – TA GIRLANDO, *Appunti per l'informatizzazione del processo civile,* in *Dir. inf.*, 1997, 1, pp. 53-60.

[65] M. IASELLI, *Informatica giuridica*, Napoli, 2002, p. 101.

In tale ambito, un grande contributo all'evoluzione delle attuali procedure può giungere dall'ulteriore sviluppo dei c.d. sistemi esperti, i quali sono costituiti da una base di dati che rappresenta la base di conoscenza, cui si accompagna un insieme di regole di ragionamento[66]. Essi applicano le regole ai dati che vengono forniti, analizzando tutti i possibili aspetti di un problema giuridico. Tali sistemi possono automatizzare l'attività di redazione dei documenti legali, simulare procedure processuali, calcolare le conseguenze dell'applicazione di una norma, e così via.

L'informatica giudiziaria ha dunque un duplice carattere, conoscitivo ed operativo, per cui essa riguarda non la *law in books* ma piuttosto la *law in action*[67]. I suoi sviluppi ovviamente sono legati alla progressiva informatizzazione della società, ancora non del tutto metabolizzata e realizzata, per quanto pochi anni di progresso dell'informatica l'abbiano ormai irrimediabilmente mutata. L'automatizzazione degli uffici giudiziari dovrebbe realizzarsi in seguito ad una riforma organica e ragionata di modifica dell'odierno processo, soprattutto del processo civile, che è, notoriamente, un processo scritto. La tecnologia informatica, del resto, grazie alle moderne tecniche di crittografia, consente una elevatissima sicurezza delle informazioni trattate, requisito indispensabile per il trattamento di dati tanto delicati quanto sono quelli giudiziari.

Nell'ambito dei progetti intrapresi per l'informatizzazione dell'attività giudiziaria è doveroso menzionare il progetto «Polis», svolto

[66] Sui sistemi esperti v. *infra*, cap. 2 par. 4.
[67] V. FROSINI, *Sviluppi e prospettive dell'informatica giudiziaria*, in *Quad. giust.*, 1987, 7, pp. 1-4, e in ID., *Informatica diritto e società*, Milano, 1988, (cui si fa riferimento) p. 276.

presso il Tribunale di Bologna e volto alla realizzazione di un sistema di gestione documentale al fine di creare un diritto giurisprudenziale bolognese e di gestire gli adempimenti connessi alla formazione e alla pubblicazione delle decisioni giudiziali. La conoscenza dell'orientamento del Tribunale sarebbe di ausilio sia agli avvocati che ai giudici: i primi avrebbero delle remore a promuovere liti dall'esito presumibilmente negativo, i secondi potrebbero agevolmente accedere ai precedenti giurisprudenziali, eventualmente riprendendone le motivazioni, senza doverle rielaborare *ex novo* anche per casi identici a quelli già decisi. Il sistema così predisposto offre il supporto alla stesura, all'archiviazione e alla gestione dei testi dei provvedimenti, ne consente la trasmissione, permette la ricerca e la consultazione delle sentenze, crea elaborati di sintesi, provvede automaticamente agli adempimenti conseguenti la decisione del giudice[68].

Bisogna poi ricordare il sistema Re.Ge., un sistema di supporto alle attività delle Procure e dei Tribunali, che consente il collegamento e lo scambio di dati con le Corti d'Appello, la Corte di Cassazione e la Procura Generale, oltre alla gestione automatizzata dei registri generali penali e alla possibilità di interscambio delle informazioni di competenza fra i vari uffici giudiziari. Il *software* svolge varie funzioni, che spaziano dall'anzidetta gestione informatizzata dei registri, che allevia il lavoro delle cancellerie, all'effettuazione di ricerche e all'elaborazione dei calendari di udienza, in modo da concentrare in una stessa udienza i processi seguiti da un determinato pubblico ministero e di evitarne l'abbinamento, fisso o ricorrente, con un determinato giudice. Una

[68] P. GUIDOTTI, *Informatica e attività giudiziaria*, in N. PALAZZOLO (a cura di), cit., pp. 164-165.

estensione del sistema Re.Ge è costituita dal progetto della istituzione, presso ciascuna Procura Generale, di una banca dati delle sentenze e dei provvedimenti impugnabili, anche allo scopo di fornire la conoscenza e la verifica dei dati sull'amministrazione della giustizia nel distretto[69].

6. L'INSEGNAMENTO DELL'INFORMATICA GIURIDICA

I primi insegnamenti di informatica giuridica sono stati organizzati nell'Università di Milano da Mario Losano e nell'Università di Catania da Vittorio Frosini, nell'ambito di corsi già preesistenti. Nel 1982 la LUISS di Roma ha invece istituito la prima cattedra di informatica giuridica (presso la Facoltà di Giurisprudenza), inserendo l'insegnamento di "informatica giuridica e amministrativa" nell'ambito delle lezioni del primo anno. Nel 1985 l'Università di Camerino ha poi deliberato l'attivazione dell'insegnamento di informatica giuridica e la sua messa a statuto, nella cui Facoltà di Giurisprudenza Donato A. Limone è diventato il primo docente di ruolo di informatica giuridica.

Fra le questioni inerenti la tematica in oggetto, bisogna menzionare il dibattito relativo alla collocazione dell'insegnamento dell'informatica giuridica nei primi o negli ultimi anni dell'insegnamento della facoltà di giurisprudenza. Chi sostiene la prima tesi afferma che l'informatica giuridica rappresenta un nuovo modo di pensare del giurista e deve dunque formare il nuovo giurista, educandolo al nuovo linguaggio

[69] P. GUIDOTTI, *ivi*, pp. 169-172.

e ai nuovi problemi[70]. Chi sostiene la seconda, invece, ritiene che, in virtù del carattere di generalità dell'informatica giuridica, si presuppone una conoscenza globale del sistema giuridico che può aversi solo negli ultimi anni della formazione.

Qualunque sia la tesi scelta, non si può comunque negare l'importanza di tale insegnamento nel settore degli studi umanistici in generale e della giurisprudenza in particolare, perché, in una società sempre più informatizzata, l'evoluzione tecnologica incide sempre più sui rapporti sociali ed è necessario, quindi, disporre l'obbligatorietà dello studio di una disciplina che comprenda tutte le fattispecie aventi rilievo nell'ambito del computer e del diritto. L'informatica giuridica è, del resto, da considerarsi "destinata ad essere studiata e applicata più dai giuristi che dai tecnici dell'informatica"[71]. Difatti essa presuppone una conoscenza di concetti propri della scienza informatica e tuttavia finalizzati all'applicazione giuridica ed ha, inoltre, carattere generale, comprendendo non singoli rami del diritto, ma piuttosto tutto il diritto, per cui se l'eventuale trattazione dei vari argomenti di pertinenza dell'informatica giuridica fosse svolta nell'ambito di insegnamenti di carattere generale, come diritto civile, penale od amministrativo, non verrebbero adeguatamente approfonditi molti argomenti di massima importanza, come il diritto di Internet, la *privacy*, l'*information retrieval*, e così via, perché bisogna considerare non solo che tali tematiche assumono una complessità vieppiù crescente, e dunque mal si prestano all'inserimento in materie già sin troppo vaste, ma anche che spesso la

[70] E. GIANNANTONIO, *L'insegnamento dell'informatica giuridica nell'università. L'esperienza della LUISS*, in V. FROSINI – OSINI OIMONE (a cura di), *L'insegnamento dell'informatica giuridica*, Napoli, 1990, p. 91.
[71] E. GIANNANTONIO, *Manuale di diritto dell'informatica*, cit., p. 2.

regolamentazione di ciascuna di esse tocca aspetti dei vari rami del diritto, insieme sostanziali e procedurali.

Nel 1988 **Renato Borruso**, nel suo *Computer e diritto*, individua cinque ragioni che giustificano il trattamento dell'informatica giuridica come disciplina particolare e unitaria di studio:

1) l'applicabilità automatica della legge;
2) la ricerca automatica della documentazione giuridica;
3) l'informatica giudiziaria;
4) il diritto dell'informatica;
5) la dipendenza della normativa dalle possibilità tecnico-scientifiche.

Secondo l'illustre autore, il giurista deve conoscere il computer, deve capirne l'intima essenza, osservarne i molteplici usi ed utilizzarla quotidianamente nell'esercizio della sua professione: a distanza di più di un decennio da tali parole, l'elaboratore elettronico è effettivamente divenuto uno strumento insostituibile per il giurista, sia per i teorici che per i pratici del diritto (avvocati, magistrati, notai) [72]. Oggi, del resto, "può ritenersi che uno dei compiti principali dell'Informatica giuridica debba consistere nello sforzo continuo – parallelo, comunque, al suo sviluppo tecnologico e metodologico – di riflettere su sé stessa, allo scopo di pervenire gradualmente a una soddisfacente autocomprensione, nella progressiva, costante ridefinizione dei suoi obiettivi e dei suoi metodi: non solo la validità scientifica delle scelte che in essa si operano, ma anche la consapevolezza della politica di ricerca che per essa si

[72] R. BORRUSO, *Computer e diritto*, Tomo II, *Problemi giuridici dell'informatica*, Milano, 1988, p. 1 e ss; sulle applicazioni dell'informatica legale v. G. TADDEI ELMI, *Informatica e professioni legali*, in N. PALAZZOLO (a cura di), cit., pp. 217-221

conduce, determinano nel tempo il suo configurarsi e consolidarsi come disciplina autonoma"[73].

Accanto a tale insegnamento risulta inoltre necessaria la predisposizione, sempre obbligatoria ed estesa a tutte le facoltà, di corsi di alfabetizzazione informatica, che forniscano una preparazione di base agli studenti necessaria all'apprendimento delle funzioni elementari dei moderni elaboratori elettronici. La mancata conoscenza degli strumenti informatici, infatti, equivale ad una nuova forma di analfabetismo e limita fortemente l'accesso al mondo del lavoro, poiché la conoscenza, quanto meno di base, del computer e dei programmi maggiormente diffusi è richiesta per l'accesso ad un numero sempre più rilevante di professioni.

Oggi l'informatica giuridica è inserita nel settore scientifico-disciplinare IUS/20 (filosofia del diritto), che "comprende gli studi relativi alla dimensione ontologica, assiologica, deontologica ed epistemologica del diritto. Gli studi si riferiscono, altresì, alla teoria generale del diritto e dello Stato, nonché alla sociologia giuridica, ai profili giuridici della bioetica ed all'informatica giuridica", mentre il diritto dell'informatica rientra nel settore IUS/01 (diritto privato), il quale "comprende gli studi relativi al sistema del diritto privato quale emerge dalla normativa del codice civile e dalle leggi ad esso complementari. Gli studi attengono, altresì, al diritto civile, ai diritti delle persone, della famiglia, al diritto dell'informatica e al biodiritto"[74].

Accanto agli insegnamenti predisposti nell'ambito delle facoltà universitarie, sono stati creati alcuni centri di ricerca nell'ambito

[73] E. FAMELI, *Teoria, definizione e sistematica dell'Informatica giuridica*, in R. NANNUCCI (a cura di), *Lineamenti di informatica giuridica*, Napoli, 2002, p. 5.
[74] D.m. 4 ottobre 2000, Allegato B, pubblicato su G.U. n. 249 del 24 ottobre 2000 - supplemento ordinario 175.

dell'informatica giuridica. Fra essi bisogna ricordare:

a) l'Istituto di Teoria dell'interpretazione e di informatica giuridica presso la Facoltà di Giurisprudenza dell'Università di Roma "La Sapienza" (http://www.infogiu.uniroma1.it). L'aggiunta "di informatica giuridica" venne fatta nel 1986, difatti il centro era prima denominato "Istituto di teoria dell'interpretazione" e suo primo direttore era stato Emilio Betti nel 1955;

b) il Centro Interdipartimentale di Ricerca in Storia del Diritto, Filosofia e Sociologia del Diritto e Informatica Giuridica (CIRSFID, http://www.cirfid.unibo.it) presso l'Università di Bologna, prima diretto da Enrico Pattaro. Le linee di ricerca del Centro comprendono l'informatica giuridica, il diritto dell'informatica e delle nuove tecnologie, la storia del diritto, e la filosofia, la teoria e la sociologia del diritto;

c) l'Istituto di Teoria e Tecniche dell'Informazione Giuridica (ITTIG), istituito nell'ambito del Consiglio Nazionale delle Ricerche (CNR) ed avente sede a Firenze ed a Roma; esso risulta dalla fusione fra lo storico Istituto per la Documentazione Giuridica (IDG) di Firenze ed il Centro per gli Studi sul Diritto Romano e Sistemi Giuridici (CSDRSG) di Roma, ed è diretto da Nicola Palazzolo.

CAPITOLO 2

L'INFORMATICA GIURIDICA METADOCUMENTARIA

1. LEGISTICA E LEGIMATICA

L'informatica giuridica ha ambito documentario quando è finalizzata all'archiviazione e al reperimento di dati e dunque ha carattere isomorfo, in quanto i dati in entrata corrispondono a quelli in uscita. La medesima disciplina è invece detta metadocumentaria quando il suo obiettivo è la creazione di nuovi dati, diversi da quelli di partenza, come avviene nei sistemi eteromorfi. In questo ambito, un settore specifico di interesse per l'informatica giuridica, è costituito dalla **legistica**, ossia da quella disciplina che si occupa dell'aspetto redazionale di un testo normativo[1], al fine di renderlo tecnicamente e formalmente corretto[2]. La **legimatica**, invece, si occupa della modellizzazione del ragionamento e

[1] L'attività di redazione legislativa "non va confusa con l'esercizio della funzione legislativa e al tempo stesso va tenuta distinta dalle attività di informazione e conoscenza che molto spesso uffici delle assemblee parlamentari svolgono in funzione di supporto dell'attività legislativa in senso stretto" (S. BARTOLE, *Introduzione allo studio della tecnica di redazione dei testi legislativi*, in IDEM (a cura di), *Lezioni di tecnica legislativa*, Padova, 1988, p. 5). Il compito della legistica, dunque, "non ha nulla da dire sopra i fini che la legislazione, o la normazione in genere, dovrebbe perseguire. Suo compito è solo investigare quali siano i mezzi idonei a conseguire le finalità proprie della legislazione in generale. I fini della legislazione in quanto tale, si badi, e non i fini di questa o quella singola legge, che è problema diverso, di politica legislativa" (R. GUASTINI, *Redazione e interpretazione dei documenti normativi*, in S. BARTOLE (a cura di), *op. cit.*, p. 37).

[2] Quindi "tutto ciò che è percepito come difetto è potenzialmente oggetto dell'intervento correttivo cui tende la legistica" (R. PAGANO, *Introduzione alla legistica. L'arte di preparare le leggi*, Milano, 1999, p. 32).

delle procedure relative alla produzione legislativa, utilizzando metodologie logiche, linguistiche e pragmatiche per l'analisi dei testi normativi, ed è finalizzata all'informatizzazione delle conoscenze elaborate dalle tecniche legislative[3].

La legistica e la legimatica possono contribuire a risolvere una parte dei problemi che oggi vessano il diritto, oramai in crisi a seguito di una molteplicità di fattori[4], fra i quali bisogna ricordare, indubbiamente, la scarsa qualità di molti testi normativi, con riferimento sia all'aspetto formale che a quello sostanziale[5]. Il testo di ciascuna norma dovrebbe infatti essere chiaro e preciso perché questa possa essere applicata e rispettata dai potenziali destinatari; per garantire la comprensibilità strutturale, linguistica e comunicativa sarebbe dunque necessaria una corretta redazione dei testi normativi, attività che può essere agevolata dall'utilizzo degli strumenti informatici[6], in modo da assicurare un controllo in primo luogo formale dei testi legislativi affinché tutti, e non solo il giurista, possano comprenderli. Legistica e legimatica sono dunque discipline complementari, perché i modelli proposti dalla legistica

[3] P. MERCATALI, *Informatica e attività legislativa*, in R. NANNUCCI (a cura di), *Lineamenti di informatica giuridica*, Napoli, 2002, pp. 294-295.

[4] Sulla crisi del diritto v. T. SERRA, *Il disagio del diritto. "Stato punitivo" e disobbedienza civile*, Torino, 1993.

[5] "La *disposizione* sarebbe l'aspetto formale, la veste esteriore, l'involucro della legge. […] Disposizione è ciò che viene «disposto», «positum», da parte del legislatore, la forma, la «littera», contrapposta allo «spirito», alla «ratio», alla «ragione», della legge. La *norma*, invece, sarebbe il *contenuto* della legge stessa, il nucleo che contraddistingue il comando, il precetto che è inserito, incapsulato, nella disposizione stessa, o in talune disposizioni" (V. ITALIA, *La fabbrica delle leggi. Leggi speciali e leggi di principio*, Milano, 1994, p. 6).

[6] "L'informatica può essere uno dei fili per riannodare connessioni e rapporti tra i centri della mappa istituzionale e rendere fattibile ed applicabile una produzione legislativa senza sovrapposizioni e ambiguità indesiderate, dominabile dagli esperti ed accessibile a tutti i cittadini" (C. BIAGIOLI – AGIOERCATALI – RCATARTOR, *Elementi di legimatica*, Napoli, 1995, p. 5).

possono essere gestiti con maggiore proficuità con l'ausilio di strumenti informatici. Sono stati così realizzati numerosi sistemi informatici sperimentali finalizzati ad agevolare l'attività di redazione di testi normativi: Lexedit, Lexeditor[7], Lexeditor 2[8], IRI-AL[9], Norma-System[10],

[7] Ispirato a Lexedit, è stato sviluppato per contro della Regione Friuli-Venezia Giulia; fra l'altro, consente la visualizzazione simultanea del testo del provvedimento modificante e di quello modificato.

[8] "È un ambiente *software* finalizzato alla redazione di testi normativi. È costituito da un insieme di programmi che da una parte integrano le funzioni di *word processing* con funzionalità specifiche di aiuto alla scrittura di testi normativi, dall'altra consentono all'utente la navigazione all'interno di banche dati documentali" (G. MARZANO – E. SILLI, Lexeditor 2: *un approccio integrato alla redazione di testi normativi*, in E. PATTARO – TTARANNOTTI (a cura di), *Applicazione e tecnica legislativa*, Atti del convegno – Bologna 9-10 maggio 1997, Milano, 1998, p. 383)

[9] Realizzato nell'ambito del CIRFID (oggi CIRSFID), è un sistema d'aiuto alla redazione dei testi normativi realizzato in collaborazione con la Regione Emilia-Romagna (P. BALDINI – LDINAPELLI – PELLARTOR – RTORURA, *Prototipo di ambiente informatizzato per la redazione di testi legislativi*, in C. BIAGIOLI – AGIOERCATALI – RCATARTOR (a cura di), *Legimatica. Informatica per legiferare*, Napoli, 1995, pp. 185-199).

[10] Norma-System è, invero, un sistema più complesso, perché non consente solo una mera attività di *drafting*. Sviluppato nell'ambito del CIRSFID, esso è composto di sei moduli base: manuale per la redazione dei testi normativi, modulo *software* di redazione degli atti, modulo *software* per la produzione di testi consolidati, modulo per l'archiviazione dei documenti in un *database server*, modulo per la pubblicazione e navigazione in Internet dei documenti, modulo per le ricerche; sono inoltre presenti due moduli accessori, l'uno di amministrazione di sistema, l'altro per la definizione delle strutture dei documenti normativi (M. PALMIRANI, *Norma-System: un sistema informatico per la gestione del ciclo di produzione normativa*, in A. ARTOSI – G. BONGIOVANNI – NGIOIDA (a cura di), *Problemi della produzione e dell'attuazione normativa*, III, *Analisi del linguaggio giuridico, legistica e legimatica*, Bologna, 2001, p. 222). Sul progetto Norma v. anche: P. BALDINI – LD COPPARI – PPARALMIRANI – S. SOLA, *La seconda generazione: Norma SQL*, in A. ARTOSI – TOSIONGIOVANNI – S. VIDA (a cura di), *op. cit.*, pp. 235-259; M. PALMIRANI, *Laboratorio legistico attraverso progetti legimatici. Il caso Norma*, in ARTOSI A. – TONGIOVANNI G. – NGIOIDA (a cura di), *op. cit.*, pp. 215-219; M. PALMIRANI, *Norma-System*, Bologna, 2000; M. PALMIRANI, Norma-System: software *per la consolidazione e la pubblicazione di testi normativi*, in E. PATTARO – TTARANNOTTI (a cura di), *Applicazione e tecnica legislativa*, Atti del convegno – Bologna 9-10 maggio 1997, Milano, 1998, pp. 407-413; M. PALMIRANI – G. SARTOR, *NORMA: un progetto integrato per la redazione, archiviazione e consolidazione dei testi normativi comunali*, in *Inf. Dir.*, 1996, 2, pp. 173-201).

LEDA[11]. In particolare, Lexedit è stato progettato presso l'Istituto per la Documentazione Giuridica (IDG), introducendo un programma di videoscrittura specialistico per testi legislativi, nonché un ambiente di normazione, al fine di rendere meno complessa l'attività redazionale, mediante la predisposizione, fra l'altro, di funzioni di strutturazione e di controllo del testo nonché di controllo ortografico, simulando inoltre alcuni aspetti dell'impatto normativo[12]. In questo ambito un ruolo centrale è rivestito dal concetto di ambiente di normazione: esso consiste in un unico ambiente informatico che integra tutti gli strumenti di ausilio all'attività normativa; esprime una nozione "giuridica", individuando un'area di utilizzo, ma non imponendo specifiche funzionalità o determinate tecnologie[13].

Questi strumenti hanno tuttavia riguardato essenzialmente il *drafting* normativo, il quale "non è che una fase, quella più tecnica e formalizzata dell'intero processo di produzione normativa", mentre il campo d'intervento potenziale della legimatica è l'intero processo legislativo, se si prendono in considerazione la decisione politica da cui scaturisce il progetto, l'analisi di quest'ultimo e la verifica della legge. "In termini funzionali, occorrerà prendere in considerazione le valutazioni degli impatti reale, normativo e giuridico. […] Mentre la valutazione dell'impatto reale (sia preventivo (valutazione della fattibilità) che

[11] Creato nell'Università di Tilburg, offre supporto metodologico e al *drafting*, nonché attività di *information retrieval* e di consulenza legislativa (su di esso v. W. VOERMANS, *Modelling the draughtman's craft: the LEDA-project. Legimatics and legimatica-project in the Netherlands*, in C. BIAGIOLI – AGIOERCATALI – RCATARTOR (a cura di), *op. cit.*, pp. 109-132).

[12] P. MERCATALI, *Legimatica e redazione delle leggi*, in C. BIAGIOLI – AGIOERCATALI – G. SARTOR (a cura di), *op. cit.*, p. 41.

[13] G. SARTOR, *La legimatica: un modello per l'informatica giuridica?*, in C. BIAGIOLI – P. MERCATALI – RCATARTOR (a cura di), *op. cit.*, p. 95.

consuntivo (valutazione dell'efficacia)), e quindi soprattutto il processo di decisione politica, richiedono analisi, metodi e strumenti totalmente diversi rispetto alla legimatica per il drafting e ne rappresentano quindi una espansione per così dire orizzontale, viceversa le valutazioni degli impatti normativo e giuridico presentano grande contiguità con il drafting, in quanto l'oggetto trattato è esclusivamente la norma"[14], la quale, dopo la sua emanazione, fa necessariamente parte di un sistema, potendo apportarvi cambiamenti anche notevoli, abrogando, ad esempio, disposizioni che regolano intere materie. Essa va dunque in relazione con altre norme, di rango inferiore, pari o superiore, per cui, in fase di progettazione, sarebbe necessario prendere in considerazione le conseguenze derivanti dalla sua vigenza, prevedibili con un certo margine di errore riguardo al mondo materiale, ma con certezza rispetto all'ordinamento giuridico sul quale va ad incidere con riferimento alle leggi vigenti sino a quel momento, perché astrattamente conoscibili senza margine di errore. Tuttavia ciò vale solo in linea di principio, dal momento che il fenomeno dell'inflazione legislativa ha portato ad una inconoscibilità *de facto* dell'intero sistema normativo. Prima dell'emanazione di qualsiasi testo legislativo sarebbe dunque necessaria l'effettuazione di una seria analisi di fattibilità, ossia della valutazione *ex ante* delle probabilità di successo del testo legislativo, seguita, dopo la sua

[14] C. BIAGIOLI, *Legimatica: verso una seconda generazione di strumenti informatici*, in C. BIAGIOLI – AGIOERCATALI – RCATARTOR (a cura di), *op. cit.*, p. 75. La tesi sostenuta dall'a. è che "una analitica strutturazione funzionale dei testi normativi, inserita all'interno di strumenti di supporto al drafting, costituisca il centro di qualunque intervento informatico sulla norma, nonché uno strumento efficace ed economico, che avrà effetti positivi sia sul drafting stesso, che sulla documentazione automatica legislativa, che sulla valutazione normativa, nonché, in qualche misura, sull'interpretazione normativa, quindi su tutti gli interventi diagnostici sulla norma, nonché sulla decisione giudiziale e sulla progettazione di supporti ad essa" (*ivi*, p. 91).

emanazione, da una valutazione *ex post* dello stato di fatto susseguente all'intervento di normazione[15]. Inoltre, riprendendo il c.d. «principio di cooperazione» di Paul Grice, la norma non dovrebbe dare più informazioni di quante ne siano richieste (categoria della quantità), dovrebbe enunciare solo cose di comprovate verità ed utilità (categoria della quantità), dovrebbe essere pertinente all'essenza della legge (categoria della relazione), ed infine dovrebbe essere formulata in modo chiaro (categoria della modalità)[16].

2. LA FABBRICA DELLE LEGGI E I LORO DIFETTI

La produzione normativa cresce col passare del tempo, anche in virtù della moltiplicazione delle fonti del diritto. Gli strumenti di *information retrieval* facilitano il reperimento dei testi normativi nonché la loro consultazione, per quanto il rimedio migliore sarebbe costituito da una legiferazione meno prolifica e più chiara: Vittorio Italia afferma che "oggi le leggi si presentano come un *prodotto industriale*. Esse sono quindi «fabbricate» secondo regole diverse da quelle del passato. Il prodotto: *«legge»* deriva dalla *«fabbrica delle leggi»*, e si tratta di un prodotto più complesso ed articolato delle leggi antiche"[17], che, pertanto, dovrebbe innanzi tutto essere «prodotto» da un legislatore cosciente sia della situazione di fatto che va a regolamentare che del quadro normativo

[15] La legistica viene pertanto intesa in due sensi: nel più ristretto, "come scienza (sapere) delle tecniche legislative e del loro uso appropriato, ed in un senso più ampio come scienza della progettazione legislativa, inclusiva sia degli aspetti formali che di quelli sostanziali" (R. PAGANO, cit., p. 34).
[16] P. GRICE, *Logica e conversazione. Saggi su intenzione, significato e comunicazione*, tr. it., Bologna, 1993, pp. 60-62.
[17] V. ITALIA, *op. cit.*, p. 3.

vigente[18].

Un primo problema, di carattere generale, è costituito dal fenomeno dell'**inflazione legislativa**, ossia di un numero eccessivo di leggi, a scapito della certezza del diritto[19]; tale fenomeno rappresenta la conseguenza del concorso di più fattori, consistenti nella moltiplicazione delle fonti del diritto[20], nella sempre crescente complessità della società odierna (cui consegue un aumento delle situazioni da regolamentare)[21], nonché, a volte, nell'incapacità o nella mancanza di volontà del

[18] Nella pratica, non sempre si verifica la coincidenza fra le figure del legislatore e del *draftsman* o legista (esperto nella redazione di regole giuridiche). Il legista non è uno "scrivano sotto dettatura", ma ha un ruolo più complesso, in quanto, "prima di iniziare a stendere un testo in forma di articolato secondo le indicazioni del committente (se non è, come sovente accade, egli stesso il titolare dell'azione legislativa), dovrà circoscrivere il problema da risolvere, precisarne gli obiettivi, raccogliere i dati giuridici e fattuali necessari, procedere a consultazioni, accertarsi della compatibilità dell'intervento che viene proposto, esplorare le possibili alternative". Il suo compito è invece simile a quello del restauratore quando si limita a ritoccare una disciplina già vigente ma bisognosa di aggiustamenti dovuti all'evoluzione della realtà fattuale oggetto di regolamentazione (R. PAGANO, *op. cit.*, p. 32).

[19] Rodolfo Pagano osserva che "la certezza, come possibilità di prevedere le conseguenze giuridiche della propria condotta, è un valore che sembra scomparso, sebbene ripetutamente richiamato" (*Introduzione*, in IDEM (a cura di) Le *direttive di tecnica legislativa in Europa*, Roma, 1997, p. XXIX).

[20] All'attività di normazione statuale, infatti, sempre più spesso si sovrappone o si affianca quella internazionale, soprattutto con riferimento alle norme emanate nell'ambito dell'Unione Europea; inoltre, si registra una crescente autonomia della legislazione degli enti locali, in particolar modo delle regioni. Addirittura, il decentramento e la delegificazione "corrono il rischio di produrre effetti perversi, inquinando ed inflazionando vieppiù l'intero sistema" (M. RAVEIRARA, *Linguaggio della progettualità normativa, inflazione e inquinamento: aspetti di un'unica patologia del sistema dei fenomeni produttivi del diritto e delle regole? Spunti di riflessione*, in A. ARTOSI – G. BONGIOVANNI – NGIOIDA (a cura di), *Problemi della produzione e dell'attuazione normativa*, III, *Analisi del linguaggio giuridico, legistica e legimatica*, Bologna, 2001, p. 7).

[21] "La presenza, sempre più penetrante ed incisiva, dello Stato determina una *giuridificazione* di scelte e di momenti di vita, prima affidati all'accordo delle parti od a norme extrastatuali. Il processo di giuridificazione, svolgendosi mediante leggi, finisce per modificarne l'intrinseca struttura e per renderle appunto regole di specifiche e determinate attività" (N. IRTI, *L'età della decodificazione*, Milano, 1999, p. 36).

legislatore di riorganizzazione e riordinare determinate materie, eventualmente procedendo ad una parziale delegificazione. Questa esigenza, del resto, è "fondata sulla insostituibilità di una legislazione parlamentare alluvionale, incontrollata e contraddittoria, la cui espansione elefantiaca oltre ad essere in contrasto con qualsiasi canone di efficienza e speditezza, sta gradualmente portando ad un […elevatissimo] grado di inconoscibilità dell'ordinamento. L'esistenza di una galassia di leggi e di leggine non coordinate *allarga invece di restringere* i poteri dell'esecutivo e del giudiziario, in quanto aumenta i margini dell'ambiguità e lascia maggiore spazio ad interpretazioni abroganti o additive: la concentrazione di funzioni normative nel Parlamento si rovescia nel suo contrario, offrendo maggiori possibilità ad un processo di implementazione gestito da soggetti deresponsabilizzati sul piano politico e spesso – per la farraginosità dei procedimenti – anche su quello giuridico. L'esito è oggi più che mai *l'eterogenesi dei fini*, con danni veramente gravi per gli interessi protetti dalla legge e per la credibilità del sistema democratico"[22].

Un altro problema generale è quello del c.d. **inquinamento legislativo**[23]. Secondo Antonio A. Martino, esso consiste nella "rottura dell'equilibrio del sistema delle leggi dovuto alla crescita incontrollata di norme legislative e alla difficoltà di eliminare i rifiuti (norme abrogate)"[24]. Il problema è strutturale, quando i difetti derivano dalla struttura

[22] G. SILVESTRI, *La ridefinizione del sistema delle fonti: osservazioni critiche*, in *Pol. dir.*, 1987, 1, pp. 153-154. In argomento v. anche F. PIZZORUSSO, *Delegificazione e sistema delle fonti*, in *Foro it.*, 1995, V, cc. 233-240.

[23] Il termine è stato utilizzato da A. A. MARTINO, *La progettazione legislativa nell'ordinamento inquinato*, in *Studi parl. pol. cost.*, 1977, 38, pp. 1-21.

[24] A. A. MARTINO, *Ivi*, p. 4.

dell'ordinamento giuridico, come nell'ipotesi della compresenza di più fonti normative concorrenti le cui competenze e i cui rapporti reciproci non sono chiaramente definiti. I difetti sono invece soggettivi quando sono legati ad un'attività di redazione normativa caratterizzata da imperizia, negligenza o insufficiente o mancato coordinamento con il contesto normativo di collocazione del nuovo testo[25].

A volte le leggi vengono infatti emanate senza aver riguardo né alle preesistenti normative né, a volte, alle regole del senso comune, costituendo «prodotti difettosi» di una «fabbrica» la cui «attività» è improntata a meri principi quantitativi e non, purtroppo, qualitativi. Un esempio da citare per la sua lapalissiana assurdità ci è fornito, in particolare, non da un legge dello Stato, ma dal d.p.c.m. 22 ottobre 1999, n. 437 ("Regolamento recante caratteristiche e modalità per il rilascio della carta di identità elettronica e del documento di identità elettronico, a norma dell'articolo 2, comma 10, della legge 15 maggio 1997, n. 127, come modificato dall'articolo 2, comma 4, della legge 16 giugno 1998, n. 191"), il cui art. 4 comma 1 dispone che "*la carta di identità elettronica può contenere* le informazioni e le applicazioni occorrenti per la firma digitale secondo quanto stabilito dalle regole tecniche di cui al decreto del Presidente della Repubblica 10 novembre 1997, n. 513, nonché *gli elementi necessari per generare la chiave biometrica*"[corsivo dell'a.]. Il «problema» è che la chiave biometrica è costituita dalla sequenza di codici informatici utilizzati nell'ambito di meccanismi di sicurezza che impiegano metodi di verifica dell'identità personale basati su *specifiche caratteristiche fisiche*

[25] R. PAGANO, *Introduzione alla legistica*, cit., p. 14.

dell'utente[26]; in altri termini è basata sull'analisi delle impronte digitali, o della retina, o addirittura del volto, e dunque, rispettivamente, le dita, gli occhi, il volto, costituiscono gli "elementi necessari per generare la chiave biometrica" di cui al citato art. 4, che dunque dovrebbero essere contenuti nella carta di identità elettronica: l'assurdità della situazione rende superfluo qualsiasi commento in merito.

Questo esempio è tanto paradossale da far capire la drammaticità dell'attuale quadro normativo con riferimento all'aspetto sostanziale, ma bisogna ora soffermarsi su quello formale, che assume un'importanza fondamentale al fine della comprensione delle norme, a sua volta requisito necessario al fine della sua applicazione, perché non si può applicare ciò che non si conosce, né si può rispettare una disposizione se non si capisce quale condotta debba essere considerata illecita, a volte a causa della successione di leggi che disciplinano la stessa materia o situazioni simili, per cui non si capisce quale debba trovare applicazione. Difatti, un principio comunemente vigente in tutti gli ordinamenti, fra cui il nostro, è rappresentato dall'abrogazione di una legge ad opera di una successiva dello stesso rango. L'abrogazione può essere esplicita, quando il legislatore espressamente la dispone nei confronti di norme determinate, oppure implicita, quando il legislatore tace sul punto oppure utilizza espressioni prive di qualsiasi valore (ad esempio, «sono abrogate tutte le norme incompatibili con la presente legge»). Le **abrogazioni**

[26] Questa è la definizione di cui all'art. 22 lett. e) del Decreto del Presidente della Repubblica 28 dicembre 2000, n. 445 ("Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa"). Il problema posto da questa «cruenta» disposizione è stato messo in luce da M. CAMMARATA – E. MACCARONE, *La firma digitale sicura. Il documento informatico nell'ordinamento italiano*, Milano, 2003, p. 214.

innominate costituiscono, pertanto, uno dei principali fattori di inflazione legislativa, perché lasciano all'interprete il difficile compito di stabilire l'eventuale abrogazione di una legge, ma ciò avviene necessariamente nell'analisi di singoli casi concreti e, in linea generale, un'attività siffatta non può certo essere caratterizzata da univocità, perché solo il legislatore può stabilire l'effettiva abrogazione di una norma, fatti salvi i casi di illegittimità costituzionale. L'espressione prima citata, inoltre, è perfettamente inutile, perché è espressione di un principio generale già vigente nel nostro ordinamento e serve solo a rendere ancor più palese che neanche il legislatore è consapevole del quadro normativo sul quale interviene.

Le **antinomie**, del resto, non dovrebbero sussistere in un ordinamento giuridico coerente, che non può contraddire sé stesso, per cui il legislatore non dovrebbe emanare norme incompatibili con altre norme del sistema. Se ciò si verifica comunque, si possono utilizzare i criteri gerarchico (*lex superior derogat inferiori*), cronologico (*lex posterior derogat priori*) e di specialità (*lex specialis derogat generali*). Ne consegue che la norma di rango superiore prevale su quella di rango inferiore, quella successiva su quella precedente e quella speciale su quella generale. Se tali criteri non risultano sufficienti, in caso di antinomie derivanti da norme di eguale livello gerarchico e di generalità ed emanate contemporaneamente, si tende a conservarle entrambe mediante una interpretazione correttiva o parzialmente abrogante di una norma o di tutte e due[27].

La **norma intrusa** è una disposizione che regola un aspetto di una

[27] E. GIANNANTONIO, *Introduzione all'informatica giuridica*, Milano, 1984, p. 204.

certa materia, ma anziché essere inserita in un testo legislativo che disciplina quel settore, viene inserita in un testo che si occupa di un argomento affatto diverso. Ciò è espressione della mancanza di sistematicità degli odierni testi legislativi, ben lontani da quelli contenuti all'interno dei codici, la cui lettura consente di desumerne i principi generali nonché di interpretare sistematicamente le singole disposizioni. Un chiaro esempio ci è fornito dal codice in materia di protezione dei dati personali, che, nonostante dovesse essere caratterizzato proprio dalla sistematicità, ha disposto la trasformazione dell'AIPA (Autorità per l'Informatica nella Pubblica Amministrazione) da una *authority* ad un centro di diretta emanazione del Ministero per l'innovazione e le tecnologie[28]. Le norme intruse pongono problemi di varia tipologia. In primo luogo, è evidente la scarsa qualità di un testo legislativo che disciplina un determinato settore, ma che contiene anche norme che al settore medesimo non ineriscono. In secondo luogo, si dimostra ben più grave il problema del reperimento di quella disposizione, proprio perché inserita nella regolamentazione di un ambito disciplinare che con essa non ha nulla da spartire, impedendone oltretutto una seria sistematizzazione. Pertanto, "ci si trova di fronte a qualcosa di simile ad una carta geografica errata, ed in tal caso è ben difficile stabilire l'«*itinerarium mentis*» del giurista"[29]. L'utilizzo degli elaboratori a fini

[28] Art. 176 comma 3 d.lgs. 30 giugno 2003, n. 196: «L'articolo 4, comma 1, del decreto legislativo 12 febbraio 1993, n. 39, e successive modificazioni, è sostituito dal seguente: "È istituito il Centro nazionale per l'informatica nella pubblica amministrazione, che opera presso la Presidenza del Consiglio dei ministri per l'attuazione delle politiche del Ministro per l'innovazione e le tecnologie, con autonomia tecnica, funzionale, amministrativa, contabile e finanziaria e con indipendenza di giudizio"».

[29] V. ITALIA, *op. cit.*, p. 14.

documentari consente, quanto meno, di alleviare il problema da ultimo citato, mediante il ricorso a ricerche *full-text* eseguite sull'intero *database* legislativo. La creazione di norme intruse è ancor più inspiegabile, ove si consideri l'enorme numero di leggi attualmente in vigore e di leggi che vengono man mano approvate, per cui, oltretutto, non mancherebbero neanche le occasioni per inserire le norme in un contesto più appropriato. Difatti, un ulteriore problema è dato dal **numero eccessivo di leggi di dettaglio**, che perdono gli essenziali caratteri della generalità e dell'astrattezza al fine di regolamentare settori troppo specifici, giungendo ad una stratificazione disarmonica, in contrasto con la tendenza alla delegificazione, ossia lasciando alla legge la determinazione dei soli caratteri essenziali di una disciplina e al regolamento la disciplina di dettaglio[30].

Tali problemi sono inoltre aggravati dall'**imperfetta stesura delle**

[30] V. ITALIA, *op. cit.*, p. 18. In realtà dovrebbe parlarsi di delegificazioni, perché il termine «delegificazione» può, innanzi tutto, essere inteso in senso lato, come "dismissione della disciplina dettata da norme di diritto pubblico" e, in tal caso, può esplicarsi come deregolazione (o *deregulation*, "cioè l'attribuzione all'autonomia privata del potere di dettare parte della disciplina di determinate materia, con eventuale riserva ai pubblici poteri del compito d'indirizzare e coordinare, con norme di principio, la produzione normativa dei privati"), denazionalizzazione ("ossia il ritirarsi della disciplina statale da certi settori e la copertura di essi con norme dettate da soggetti privati"), deburocratizzazione ("cioè la soppressione di norme che appesantiscono le attività ed i procedimenti amministrativi"). La delegificazione può essere intesa in senso stretto, "quale trasformazione della fonte di diritto pubblico abilitata a porre una certa disciplina, o, più precisamente, quale sostituzione della legge con una fonte secondaria", ed esplicarsi come decentramento normativo ("ossia il trasferimento della disciplina di una determinata materia dalla legge statale ad atti normativi di enti pubblici") o come delegificazione in senso tecnico ("cioè il trasferimento della, o di parte della, disciplina di una certa materia della legge statale al regolamento governativo"). Pertanto, "il termine «delegificazione» racchiude due significati fondamentali: il superamento dell'eccesso di vincoli che limitano le attività private nonché pubbliche ed il superamento dell'uso massiccio della legge" (P. VIPIANA, *La delegificazione: profili teorici e esperienze pratiche*, in G. VISINTINI, (a cura di), *Analisi di leggi-campione. Problemi di tecnica legislativa*, Padova, 1995, pp. 699-700).

leggi, spesso scritte utilizzando termini giuridicamente non corretti o inopportuni sinonimi, rendendo difficile l'interpretazione del testo, spesso vessato anche da errate suddivisioni o da disposizioni tanto estese, nel senso della loro lunghezza, da rendere difficile proprio riuscire a «carpirne» il significato[31].

3. LE REGOLE E RACCOMANDAZIONI SULLA FORMULAZIONE DEI TESTI LEGISLATIVI

La considerazione dello scarso livello qualitativo dei testi legislativi ha spinto, nel 1986, i Presidenti delle Camere ed il Presidente del Consiglio dei Ministri ad emanare, d'intesa fra loro, tre circolari di identico testo contenenti una serie di regole e raccomandazioni di carattere tecnico al fine di migliorare la comprensibilità dei testi legislativi.

Queste circolari sono state aggiornate nel 2001[32], ed i Presidenti delle Camere ed il Presidente del Consiglio dei Ministri hanno

[31] L'ultima legislazione sul documento informatico e la firma digitale (sulla quale v. *infra*, cap. 9) evidenzia una molteplicità terminologica e concettuale che si scontra con la basilare esigenza dell'astratta possibilità di comprensione sostanziale della normativa: difatti, oggi è arduo capire quale sia la condotta da seguire per adempiere alle prescrizioni del t.u. *in subiecta materia*. Nel caso di specie, ciò è dovuto anche al problema della moltiplicazione delle fonti del diritto, poiché l'impianto originale, predisposto dal d.p.r. 513/97, è stato modificato per dare attuazione alla relativa normativa europea.

[32] Ciò è avvenuto in seguito ad una elaborazione tecnica svolta dagli Uffici del Senato e della Camera dei deputati unitamente agli Uffici del Governo, successivamente all'attività svolta in tale ambito dalla Commissione istituita presso il Dipartimento per i rapporti con il Parlamento della Presidenza del Consiglio dei Ministri il 7 aprile 2000.

congiuntamente adottato in data 20 aprile 2001 una "Lettera circolare sulle regole e raccomandazioni per la formulazione tecnica dei testi legislativi".

Le nuove "regole e raccomandazioni" disciplinano minuziosamente il modo in cui le leggi dovrebbero essere strutturate, ispirandosi a principi di omogeneità, chiarezza, completezza. L'atto legislativo dovrebbe dunque disciplinare materia omogenea, sia in termini generali che con riferimento a ciascuna partizione in cui è diviso, per evitare la possibilità di introdurre norme intruse[33], e già il titolo dovrebbe esplicitare almeno l'oggetto principale della disciplina normativa. Si vuole pertanto rendere conoscibile la legge anche a soggetti diversi dagli operatori del diritto, utilizzando una terminologia appropriata al contesto in cui si opera ed evitando in ogni modo possibili ambiguità di carattere semantico e sintattico, rispettando, per quanto possibile, sia il principio della semplicità che quello della precisione. Si afferma, pertanto, l'opportunità di ricorrere a definizioni qualora i termini utilizzati non siano di uso corrente, non abbiano un già chiaro significato giuridico o siano utilizzati con significato diverso sia da quello corrente sia da quello giuridico.

Il problema principale è tuttavia dovuto alla impossibilità pratica, oggi, di garantire l'efficacia delle suddette regole, non potendone garantire la coattività, ma dovendo piuttosto fare affidamento sulla speranza che il legislatore svolga la propria attività metodicamente e con serietà, anche se bisogna obiettivamente considerare che i rapidi mutamenti della società odierna rendono più difficoltosa l'attività di

[33] Ma l'esempio di cui all'art. 176 comma 4 d. lgs. 196/03 (v. *supra*), purtroppo, mette in evidenza che tali regole non sempre vengono rispettate.

normazione, senza tuttavia renderla impossibile.

4. I SISTEMI ESPERTI

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[34]. In linea di principio, un **sistema esperto** è composto da due elementi essenziali: una «base di conoscenza» (*knowledge base*), che contiene una rappresentazione esplicita della conoscenza come un insieme di asserzioni o dichiarazioni che descrivono il dominio del problema[35], e un «motore inferenziale», ossia

[34] In questo senso G. SARTOR, *Intelligenza artificiale e diritto. Un'introduzione*, Milano, 1996, p. 22. "Essi non solo offrono le informazioni, ma le valutano: un'argomentazione irrilevante viene segnalata allo stesso modo di un'argomentazione significativa e eventualmente non compare affatto nel sistema" (J. W. GOEBEL – R. SCHMALZ, *Problemi dell'applicazione del sistema esperto giuridico nella pratica legale*, in A. A. MARTINO – RTINOCCI NATALI (a cura di), *Analisi automatica dei testi giuridici. Logica, informatica, diritto*, Milano, 1998, p. 785).

[35] Nella *knowledge base* la conoscenza "è rappresentata in un linguaggio ad alto livello, cioè in un formalismo relativamente vicino ai linguaggi usati nella comunicazione umana" (G. SARTOR, *Le applicazioni giuridiche dell'intelligenza artificiale. La rappresentazione della conoscenza*, Milano, 1990, p. 58). La base di conoscenza dovrebbe includere anche dati di tipo sociale ed economico, poiché "solo un atteggiamento di acritico positivismo, inutilmente teso a sottrarre le norme al fluire della storia, può disconoscere la necessità di collegare la dimensione giuridica con la prospettiva sociale nell'agire dell'uomo. L'elaborazione consente finalmente un riscontro con la realtà dei comportamenti individuali e delle prassi sociali; mai prima d'ora era stato possibile manipolare in tempi brevi così ingenti masse di dati. Vuote supposizioni o ipotesi inconsistenti, in un contesto in cui la tecnologia dell'informazione non sia stata introdotta invano, possono essere subito individuate e confutate in maniera irrevocabile, contrapponendo il valore concreto dei fatti all'astrattezza delle speculazioni" (E. FAMELI– MELIERCATALI, *Sistemi esperti e modelli di decisione giuridica*, in A. A. MARTINO – RTINOCCI NATALI (a cura di), *Analisi automatica dei testi giuridici. Logica, informatica, diritto*, Milano, 1998, p. 760). Della costruzione e della manutenzione della *knowledge base* si occupa il c.d. ingegnere della conoscenza (*knowledge engineer*).

"un programma in grado di compiere operazioni inferenziali, di effettuare deduzioni usando la base di conoscenza"[36]. Un terzo elemento è costituito da interfacce "che agevolano l'interrogazione e la preparazione della base della conoscenza. Talvolta, l'utente può usare un sottoinsieme del linguaggio naturale nell'interazione con il sistema"[37].

La realizzazione di un simile sistema presuppone la modellizzazione di un settore del diritto, ossia l'individuazione dei contenuti giuridicamente rilevanti e la determinazione delle loro strutture fondamentali.

Essi dovrebbero essere caratterizzati da trasparenza, ossia dalla capacità di motivare le loro conclusione ripercorrendo il ragionamento da cui sono scaturite, e da flessibilità, cioè dalla possibilità di un aggiornamento continuo della base di conoscenza[38].

I sistemi esperti dovrebbero essere in grado di agire anche in un ambiente destrutturato, con la possibilità di fronteggiare situazioni non definite a priori, come fa l'uomo. Se i dati sui quali si vuole operare sono

---

[36] G. SARTOR, *op. ult. cit.*, p. 58. Bisogna sottolineare che i sistemi esperti sono normalmente strutturati come sistemi basati sulla conoscenza, anche se in taluni casi si è fatto uso di reti neurali al fine di automatizzare determinate funzioni percettive. Con riferimento ai sistemi basati sulla conoscenza, si rileva che esistono tre principali approcci, basati: a) "su regole, che comprende il ragionamento basato su regole e la programmazione logica applicata alla legge"; b) "sui casi, che rappresenta la legge come casi e usa le tecniche di ragionamento basate sui casi per ragionare con essi"; c) "sulla logica, che comprende tutte le applicazioni di logica in generale, deontica [costituisce la formalizzazione logica dei concetti dentici: permesso, proibito, obbligatorio] e non-monotona in particolare [in base ad essa le conclusioni possono essere revocate con l'aggiunta di nuova conoscenza] per la rappresentazione della legge" (F. TURCHI, *Prefazione*, in IDEM (a cura di), *Rappresentazione della conoscenza e ragionamento giuridico*, Bologna, 1995, p. 7).

[37] G. SARTOR, *op. ult. cit.*, p. 59.

[38] D. I. GOLD – LD RO IUSSKIND, *I sistemi esperti nel diritto. Un approccio giuridico nella pratica legale*, in A. A. MARTINO – RTINOCCI NATALI (a cura di), *Analisi automatica dei testi giuridici. Logica, informatica, diritto*, Milano, 1998, p. 797.

rilevabili per mezzo di particolari sensori, con periodi di prova e di apprendimento più o meno lunghi e complessi, è possibile ottenere buoni risultati, ma se i dati sono costituiti da espressioni linguistiche (come nel diritto) o da modelli di comportamento non uniformi, la cui intrinseca ambiguità può essere superata solo mediante l'interpretazione, i risultati conseguibili attraverso sistemi esperti sono connotati da un'affidabilità ridotta o nulla in mancanza di una strategia di controllo predefinita[39].

I sistemi esperti vengono utilizzati anche in ambito giuridico e in tal caso sono detti **sistemi esperti legali**. Essi "nascono dalla convergenza tra formalizzazione logica del diritto e modellizzazione giuridica, da un lato, ed elaborazione informatica dei dati giuridici, dall'altro [e] sono realizzati, il più delle volte, sotto forma di colloquio tra utente e computer secondo le tecniche classiche dell'*istruzione programmata*, che i computer più recenti rendono sempre più ricca di possibilità creando una connessione, di fondamentale valore per l'evoluzione del diritto, tra la logica, l'informatica e il diritto"[40]. In altri termini, sono meccanismi diretti alla riproduzione di attività intellettuali proprie dell'uomo in macchine automatiche ed, in particolare, per il reperimento intelligente di una documentazione, parere, consulenza o decisione oltre che per la produzione di un documento amministrativo, giudiziario o professionale o di ausilio della decisione. In essi il procedimento è, per così dire, inverso rispetto a quello seguito nell'ambito dell'informatica giuridica documentaria. Mentre in

[39] G. CARIDI, *Sistemi esperti e pubblica amministrazione*, in D. A. LIMONE (a cura di), *Dalla giuritecnica all'informatica giuridica. Studi dedicati a Vittorio Frosini*, Milano, 1995, p. 107.
[40] M. IASELLI, *Informatica giuridica*, Napoli, 2002, p. 63.

quest'ultima è l'operatore che pone interrogazioni al sistema informatizzato, nei sistemi esperti è il calcolatore che interroga l'operatore e che, sulla base delle sue risposte, sfrutta le «conoscenze» di cui dispone nelle sue banche dati.

Il diritto, tuttavia, difficilmente può rientrare nella logica di funzionamento dei sistemi esperti, ove si consideri che le conoscenze giuridiche potenzialmente utilizzabili derivano sia dall'ambito giuridico formale che dalla realtà concreta, per cui "il ragionamento logico, facilmente algoritmizzabile, deve coesistere con dati incerti, incompleti, a volte contrastanti fra di loro. Il modello con cui si deducono, a partire da alcuni fatti e determinate norme, considerate come premesse, una o più decisioni giuridiche, configurate come conseguenze, non funziona sempre allo stesso modo per l'intervento delle componenti empirica e soggettiva, quindi l'uso di un sistema esperto nell'ambito delle decisioni giuridiche è possibile solo in alcune situazioni, ma non è generalizzabile"[41]. Tali decisioni, inoltre, andrebbero sempre vagliate dalla mente umana, al fine di stabilire se la macchina abbia preso in considerazione tutti i dati fattuali e giuridici (anche alla luce della comprensione intuitiva) del caso di specie necessari per la decisione e, dunque, i sistemi informatici potrebbero avere, più che altro, una sorta di ruolo «consultivo» nell'ambito decisionale umano.

Ciononostante, oggi i sistemi esperti coprono un settore dell'attività giuridica finora non toccato dall'automazione; se originariamente ogni attività giuridica era attività umana, successivamente certe attività apparentemente decisionali ma in realtà esclusivamente

[41] G. CARIDI, *op. cit.*, p. 113.

ripetitive (ad esempio, le attività fiscali) sono state almeno in parte automatizzate, realizzando modelli informatizzati di alcuni settori dell'ordinamento giuridico[42]. In tal modo l'attività umana può essere coadiuvata o sostituita anche nella fase decisionale, perché il sistema può proporre la soluzione da adottare dinanzi ad un caso specifico, fornendo la relativa motivazione; in base all'esito, comunque di pertinenza dell'uomo, il sistema potrà apprendere dalla sua attività decisionale.

Le **applicazioni giuridiche** dei sistemi esperti possono concretizzarsi nella realizzazione di banche dati concettuali (i cui contenuti sono compresi dall'elaboratore non solo dal punto di vista formale ma anche da quello sostanziale), di sistemi di generazione automatica di documenti (la cui complessità è proporzionale a quella del documento) e di sistemi automatici di insegnamento del diritto (che comprende le nozioni della materia oggetto di insegnamento e la scelta della metodologia da seguire).

In Italia sono stati già realizzati alcuni sistemi esperti legali, fra i quali bisogna ricordare il ben noto «Re Mida», in materia di rivalutazione monetaria e di calcolo degli interessi, ma alcuni servizi tipici di tale tipologia di sistemi esperti sono stati resi disponibili anche *on line*, come nel caso del sito «Cyberdiritto» (http://www.cyberdiritto.it), che offre servizi in tema di rivalutazione monetaria, calcolo di parcelle, computo di termini, calcolo dei tassi usurari, ecc.

---

[42] Essi, infatti, "potrebbero essere particolarmente utili in quei settori in cui ricorrono situazioni tipiche dando luogo a problemi di tipo analogo: basti pensare alla materia tributaria, delle locazioni e del lavoro. E diventano particolarmente efficaci qualora dispongano anche della capacità di elaborare i dati forniti dal ricercatore: ad esempio, per calcolare l'ammontare dovuto a titolo di imposta, di equo canone o di liquidazione" (E. GIANNANTONIO, *op. cit.*, p. 177).

I sistemi esperti legali hanno, comunque, un enorme potenziale nel settore giuridico, ma affinché esso possa esprimersi al meglio, è necessario analizzare sia le norme giuridiche in sé e per sé, sia la loro interazione con la realtà, al fine di giungere ad una migliore comprensione del diritto stesso, che è intrinsecamente complesso. Sarebbe pertanto riduttivo fermarsi al modello del "*rule and fact*", per cui la ricerca e l'analisi della realtà giuridica consentono, o consentiranno, di capire sia il suo funzionamento che la sua corrispondenza alla realtà fattuale. Sino a quando ciò non avviene, le tecniche di intelligenza artificiale non possono essere adoperate nella costruzione di sistemi esperti legali che incidono pienamente sulla realtà materiale, per cui il loro ruolo necessariamente si riduce a quello di semplici strumento che coadiuvano lo svolgimento di determinate attività"[43].

Bisogna osservare inoltre che la realizzazione di sistemi esperti finalizzati allo studio del diritto in senso ampio si scontra con la disomogeneità dei testi legislativi, per cui la comprensione e la sistematizzazione dei testi normativi in base a criteri predefiniti è assai difficile da raggiungere, perché i testi vigenti sono organizzati a volte in maniera diversa proprio dal punto di vista, strutturale, della divisione ivi disposta, per cui un elaboratore difficilmente potrebbe essere in grado di «ragionare» caso per caso. Sarebbe pertanto necessario non solo stabilire le regole per la redazione dei testi legislativi, ma anche vigilare sulla loro effettuazione, eventualmente sanzionando le condotte in contrasto.

[43] Così A. MITRAKAS, *A Role for Legal Expert Systems*, in *Inf. dir.*, 1996, 2, p. 226.

5. GLI AGENTI *SOFTWARE*

In questa sede si può solo accennare agli agenti *software* (o agenti elettronici), in quanto essi sono ancora allo stadio sperimentale, nonostante siano disponibili già numerose applicazioni pratiche, e costituiscano una realtà in continua evoluzione. Essi sono sistemi informatici la cui esecuzione avviene senza un controllo diretto da parte dell'uomo, che non deve così preoccuparsi di una continua supervisione del loro operato. Gli agenti elettronici eseguono compiti specifici, previamente determinati dall'utilizzatore, e costituiscono delle entità computazionali che agiscono in via autonoma in un ambiente, che essi percepiscono mediante i propri organi sensori e che modificano attraverso i propri organi effettori.

Gli agenti *software* possono operare sia nel monde reale (*robot*) che in quello virtuale (*software*), sia singolarmente che collettivamente. I secondi vengono utilizzati in vari settori dell'informatica, per sviluppare sistemi informativi, coordinare applicazioni distribuite, realizzare interfacce, gestire attività complesse e situazioni critiche. La loro attività può realizzarsi nella sfera del loro utilizzatore, ma essi possono entrare in contatto con altri soggetti, sia quando sono finalizzati alla raccolta di informazioni che quando svolgono attività contrattuale[44].

L'utilizzatore di un agente *software* gli delega quelle funzioni cognitive che altrimenti dovrebbe svolgere in proprio. La complessità insita in tali sistemi implica, necessariamente, l'imprevedibilità teorica del

[44] G. SARTOR, *Gli agenti software e la disciplina giuridica degli strumenti cognitivi*, in *Dir. inf.*, 2003, 1, p. 55, cui si rinvia per un'ottima ricostruzione della problematica nonché per le indicazioni bibliografiche ivi contenute.

loro comportamento, perché esso si adatta alla molteplicità delle variabili ambientali.

CAPITOLO 3

L'INFORMATICA GIURIDICA DOCUMENTARIA

1. ASPETTI GENERALI

L'**informatica giuridica documentaria** è quella disciplina che si occupa della raccolta, selezione, organizzazione e reperimento attraverso strumenti elettronici delle informazioni necessarie per la conoscenza e l'applicazione del diritto. In altri termini, "l'informatica giuridica documentaria consiste nella memorizzazione, nella ricerca e nella trasmissione delle informazioni relative a fatti giuridici diversi da quelli che costituiscono le fonti dell'ordinamento e degli atti processuali e soprattutto nella automazione degli archivi e dei procedimenti di pubblicità legale. Il termine "documentario" è suggerito dall'importanza che in questo campo hanno il documento che attesta l'esistenza del fatto giuridico stesso ed i problemi della sua forma ed efficacia"[1].

Questo settore dell'informatica giuridica assume una sempre crescente importanza, di pari passo con il fenomeno dell'inflazione legislativa, dovuto a vari fattori. In primo luogo, il progressivo ampliamento delle competenze di alcuni organismi internazionali e soprattutto il processo di unificazione europea, oltre all'attribuzione di nuove potestà agli enti locali, costituiscono tutti fattori di moltiplicazione delle fonti del diritto, cui necessariamente consegue l'aumento della

[1] E. GIANNANTONIO, *Introduzione all'informatica giuridica*, Milano, 1984, p. 16.

produzione normativa, già eccessiva a causa di un legislatore sin troppo prolifico. Questo problema non è nuovo e non riguarda solo l'ordinamento giuridico italiano, ma assume connotati quasi drammatici in ogni stato moderno: "nessun uomo sa precisamente quali norme in quest'ora siano attualmente in vigore, nessun legislatore, nessuna autorità e nessun giudice, nessuno del popolo"[2].

Come ritiene **Spiros Simitis**, dove l'attività dello Stato cresce continuamente in importanza ed estensione, muta anche il panorama delle norme. Difatti, alle norme di legge si accompagna un numero infinito di disposizioni di ovvia utilità, con la conseguenza di rendere la già intricata selva di norme ancor più impenetrabile. La pubblicazione diventa semplicemente un'occasione per osservare con quale vertiginosa velocità aumenti la produzione normativa, giungendo al punto di non poterne neanche stimare con precisione la misura[3]. Il comune cittadino si trova pertanto spaesato dinanzi ad una produzione legislativa tanto vasta, non riuscendo a conoscere effettivamente il diritto, per cui si trova costretto, in caso di bisogno, a fare ricorso agli specialisti dei vari settori, paradossalmente sperando solo che gli siano detratte le spese necessarie alla sua informazione[4].

Una simile situazione snatura l'essenza stessa del diritto, che dovrebbe orientare la condotta dei consociati senza che questi in molti casi sappiano quali comportamenti debbano tenere. In ossequio al principio *ignorantia legis non excusat*, lo Stato talvolta esercita la propria potestà punitiva prescindendo dall'effettiva conoscenza del diritto da

[2] La frase, di Jahrreis, è riportata da Spiros Simitis nel suo *Crisi dell'informazione giuridica ed elaborazione elettronica dei dati*, tr. it., Milano, 1977, p. 15.
[3] *Ibidem.*
[4] S. SIMITIS, *ivi*, p. 34.

parte del reo: in Italia ciò è accaduto in maniera generalizzata sino alla nota sentenza 24 marzo 1998, n. 364 della Corte Costituzionale, che ha stabilito che l'ignoranza inevitabile della norma elide l'eventuale antigiuridicità del fatto[5]. Se già il diritto penale ha comunque un ambito assai vasto, il diritto civile e il diritto amministrativo rappresentano quelle selve impenetrabili di cui parla Simitis: la produzione normativa, di vario rango, sembra inarrestabile, e ad essa si aggiungono gli apporti di giurisprudenza e dottrina, difficilmente caratterizzati da univocità a causa di svariati fattori, come l'ambiguità di alcune disposizioni ed il frenetico susseguirsi di normative contrastanti anche a brevissima distanza di tempo.

Anche l'operatore del diritto non riesce a gestire una mole tanto enorme di materiale, tant'è vero che "la crisi dell'informazione avvolge nelle tenebre l'ordinamento giuridico. Da una trasparenza almeno potenziale l'ordinamento passa ad una crescente imperscrutabilità e diviene inaccessibile perfino allo specialista"[6]. Di certo, la crescente maggiore complessità della società moderna implica, necessariamente, un maggior numero di situazioni concrete di pertinenza del diritto, perché aumentano progressivamente le occasioni di inter-relazionalità, sia con riferimento ai rapporti fra soggetti privati (che siano persone fisiche o giuridiche, professionisti o consumatori, ecc.) che fra pubblici e privati.

[5] "È illegittimo l'art. 5 c.p. nella parte in cui non esclude dall'inescusabilità dell'ignoranza della legge penale l'ignoranza inevitabile, atteso il combinato disposto del comma 1 e 3 dell'art. 27 cost., nel quadro delle fondamentali direttive del sistema costituzionale desunte soprattutto dagli artt. 2, 3, 25 comma 2, 73 comma 3 cost., le quali pongono l'effettiva possibilità di conoscere la legge penale quale ulteriore requisito minimo d'imputazione, che viene ad integrare e completare quelli attinenti alle relazioni psichiche tra soggetto e fatto, consentendo la valutazione e, pertanto, la rimproverabilità del fatto complessivamente considerato".

[6] S. SIMITIS, *op. cit.*, p. 35.

Ciò non comporta, comunque, una crescita eccessiva del numero delle disposizioni legislative, atteso che in molti casi basterebbe fornire una regolamentazione organica di determinate materie che abroghi le disposizioni precedenti al fine di eliminare dubbi interpretativi relativi, fra l'altro, alla scelta della norma da applicare al caso di specie.

Nella situazione cui si è accennato, sinora legata ad una produzione fissata su supporti cartacei, bisogna considerare che l'utilizzo di sistemi informatici permette di superare svariati problemi legati alla memorizzazione su tali supporti, spaziando da problemi di carattere meramente materiale, come l'occupazione fisica dei testi, a questioni, ben più gravi, inerenti il reperimento e la consultazione delle informazioni. In particolare, le relative tecniche sono state sviluppate inizialmente nell'ambito delle scienze chimiche, fisiche e biologiche, discipline nelle quali i risultati raggiunti dai vari ricercatori necessariamente trovano spazio nelle pubblicazioni effettuate sulle varie riviste scientifiche, il cui numero si è tuttavia incrementato esponenzialmente, rendendo difficoltosa l'informazione tempestiva sui risultati raggiunti dai vari scienziati. Lo spoglio di tutte le riviste effettuato senza strumenti informatici, infatti, è subito risultato compito improbo, con l'ulteriore ed assurda conseguenza che talvolta si dimostrava meno costoso ripetere una ricerca di laboratorio già effettuata da altri piuttosto che reperirne il resoconto nel *mare magnum* delle pubblicazioni scientifiche[7]. Le tecnologie informatiche consentono il superamento di tali problemi, rendendo ben più celere e proficua qualsiasi attività di ricerca, per cui già nella metà

[7] "Si calcola che il numero delle riviste scientifiche, che nel 1950 si aggirava nel mondo intorno alle 100 mila unità, si raddoppia ogni 15 anni" (N. PALAZZOLO, *Strumenti per l'accesso all'informazione giuridica*, in ID. (a cura di), *Corso di informatica giuridica*, Catania, 1998, p. 24).

degli anni cinquanta esse sono state utilizzate anche nel settore delle scienze giuridiche, nel quale il sempre crescente numero di pubblicazioni scientifiche ha progressivamente posto il problema della difficoltà di reperimento delle informazioni. L'estensione delle tecniche utilizzate nelle scienze sperimentali al diritto è stata semplificata dal fatto che esso è espresso in proposizioni che non presentano differenze linguistiche rispetto al riassunto di un articolo inerente, ad esempio, la medicina, e negli anni cinquanta ciò ha portato i giudici statunitensi a memorizzare in forma elettronica le sentenze dei tribunali statali e federali[8].

Ovviamente, il ricorso a strumenti di *information retrieval* non sostituisce il lavoro di analisi dei testi, che viene poi compiuto dall'operatore del diritto, ma risulta integrativo della fase preliminare dell'indagine e dunque gli elaboratori elettronici in tali casi svolgono una funzione ausiliaria nell'ambito dello studio e dell'applicazione del diritto[9], che assume sempre maggiore importanza col passare del tempo a causa della sempre più prolifica produzione normativa, giurisprudenziale e dottrinale. In tal modo il giurista può dedicare meno tempo alla mera attività di ricerca, potendo così concentrarsi sull'aspetto prettamente

[8] M. G. LOSANO, *Corso di informatica giuridica*, 1, *L'elaborazione dei dati non numerici*, Milano, 1984, p. 48. Una delle più dibattute questioni sorte proprio negli anni cinquanta riguardava la scelta fra l'archiviazione dei testi in forma integrale oppure in forma di riassunti; ciò era dovuto alle ridotte capacità di memorizzazione degli strumenti informatici dell'epoca, posto che "memorizzare il testo integrale significa perforare molte schede, occupare molta memoria ed usare molto tempo-macchina, cioè aumentare i costi del sistema informativo. I primi esperimenti di informatica giuridica, proprio per limiti tecnologici e per difficoltà finanziarie, dovettero invece ripiegare sulle tecniche più economiche, le quali non sempre si rivelarono idonee al reperimento ottimale dell'informazione giuridica, specie se di tipo europeo continentale" (p. 50).

[9] V. FROSINI, *Cibernetica diritto e società*, Milano, 1968, ora in ID., *Informatica diritto e società*, Milano, 1988, (cui si fa riferimento) p. 41.

concettuale dei problemi giuridici[10].

2. CENNI SUGLI IPERTESTI

I sistemi informatici consentono inoltre di organizzare le informazioni in maniera non lineare, grazie agli *ipertesti*[11], nei quali l'approccio conoscitivo non è di tipo sequenziale bensì associativo, rendendo assai celere la consultazione dei documenti. Un ipertesto consiste nella presentazione di informazioni sotto la veste di una rete di nodi[12] collegati fra di loro, nella quale il fruitore è libero di scegliere il percorso di consultazione. Proprio la struttura ipertestuale ha consentito quell'enorme espansione del *World Wide Web* avvenuta negli anni novanta, anche se la teorizzazione degli ipertesti e il loro utilizzo nell'ambito informatico sono dovuti soprattutto alle pionieristiche idee di **Vannevar Bush**, espresse, fra l'altro, in un articolo intitolato *As we may think*, apparso nel 1945 sulle pagine della rivista *The Atlantic Monthly*[13]. L'illustre studioso mette in evidenza che alla prodigiosa evoluzione della ricerca umana del mondo moderno, cui ha fatto seguito l'aumento del numero delle produzioni scientifiche, si contrappone il mancato progresso degli strumenti di reperimento e consultazione di questo

[10] In questo senso anche: G. ALPA, *L'applicazione delle tecnologie informatiche nel campo del diritto*, in *Dir. inf.*, 1996, 4-5, p. 534; R. DICKERSON, *Some Jurisprudential Implications of Electronic Data Processing*, in H. W. BAADE (edited by), *Jurimetrics*, New York – London, 1963, p. 65.

[11] Sugli ipertesti v., fra gli altri, R. NANNUCCI, *Ipertesti, ipermedialità e diritto*, in ID. (a cura di), *Lineamenti di informatica giuridica*, Napoli, 2002, pp. 157-184.

[12] Un nodo è un elemento di informazione completo ed auto-sufficiente, non esteso se considerato nell'economia dell'intero documento.

[13] V. BUSH, *As we may think*, in *The Atlantic Monthly*, 1945, 176, 1, pp. 101-108

grande numero di informazioni[14]. Ciò è dovuto all'artificiosità dei sistemi di organizzazione e di indicizzazione delle informazioni cartacee, in base ai quali i testi sono disposti in ordine alfabetico o numerico, con la conseguenza di poter trovare il dato che interessa solo cercandolo nelle varie sottoclassi, anche perché ciascun dato è generalmente unico, a meno di non far uso di duplicati (fra l'altro, con i relativi problemi di costi).

La mente umana è diversa: essa opera per associazione, e dunque permette di passare inconsciamente da un concetto all'altro, seguendo un intricato e misterioso percorso delle cellule cerebrali, con un'azione caratterizzata da una così estrema celerità, nonostante la complessità dei pensieri e delle rappresentazioni mentali, che fa emergere la maestosità del pensiero umano. Per quanto l'uomo non possa sperare (almeno attualmente) di replicare artificialmente il proprio pensiero, egli può comunque imparare da esso nell'ambito della riorganizzazione delle informazioni, le quali, anziché essere indicizzate possono essere disposte per associazione e successivamente consultabili in maniera non sequenziale. A tal fine, Bush propone l'utilizzo di una macchina all'uopo costruita, denominata «memex». Essa è un dispositivo, esteticamente simile ad una scrivania, nella quale sono contenuti i propri testi e le proprie informazioni cartacee, cui si può accedere per mezzo di comandi impartiti tramite dispositivi di *input* (tastiera, bottoni, leve)[15].

Il progetto teorizzato da Bush, dunque, permetterebbe l'indicizzazione associativa dei documenti, aspetto che costituisce la caratteristica fondamentale dei moderni ipertesti. Purtroppo le idee del

[14] V. BUSH, *ivi*, p. 102.
[15] V. BUSH, *ivi*, p. 106.

grande scienziato statunitense sono state troppo in anticipo rispetto ai tempi, come è avvenuto negli anni sessanta a Douglas Engelbart, che in quel periodo inventa il *mouse* per facilitare l'utilizzo di un sistema informatico di elaborazione testuale (da lui sviluppato), nonostante non esistessero ancora interfacce grafiche che consentissero l'utilizzo degli elaboratori[16]. La bontà delle intuizioni di Bush è stata confermata solo dopo molti anni rispetto all'uscita del citato *"As we may think"*: infatti il *World Wide Web* non è altro che un enorme ipertesto, che oggi ha diffusione planetaria, ha cambiato il mondo ed in realtà rappresenta una realizzazione di quanto proposto negli ormai lontani anni quaranta dallo scienziato statunitense, il quale non ha tuttavia coniato il termine «ipertesto», comunemente utilizzato per definire un testo che consente una lettura non sequenziale delle informazioni in esso contenute. Il termine in questione è stato infatti coniato da Ted Nelson negli anni sessanta, nell'ambito del progetto «*Xanadu*», finalizzato alla realizzazione di un sistema ipertestuale globale assai avanzato, che dovrebbe essere dotato, fra l'altro, di una migliore gestione dei collegamenti rispetto a quanto avviene oggi nel *WWW*, nei cui confronti Nelson è assai critico; tuttora *Xanadu* è nella fase progettuale, nonostante il lavoro su di esso sia iniziato negli anni sessanta.

[16] W. K. ENGLISH – GLISH TNGELBART – GELBARTERMAN, *Display-Selection Techniques for Text Manipulation*, in *IEEE Transactions on Human Factors in Electronics*, 1967, 1, pp. 5-15. Nello studio sperimentale sintetizzato nell'articolo, gli aa. utilizzarono varie periferiche di *input* oltre ad un *mouse*, come una tastiera, un *joystick* ed una penna ottica. Il genio di Engelbart risulta con veemenza da tali intuizioni, non rimaste allo stadio di mero pensiero, ma addirittura realizzate realmente, in un periodo in cui l'informatica moderna si trovava nella sua fase primordiale.

3. CENNI SULL'ALGEBRA BOOLEANA

Nell'Ottocento, il pensiero di **George Boole** hanno è stato fondamentale per la "matematizzazione della logica, sia pure concepita come una *formulazione* secondo i canoni del linguaggio matematico"[17]: al riguardo, l'opera fondamentale di Boole, edita nel 1854, è intitolata proprio *An Investigation of the Laws of Thought on which are founded the Mathematical Theories of Logic and Probabilities*. Suo scopo è "d'indagare le leggi fondamentali di quelle operazioni della mente per mezzo delle quali si attua il ragionamento; di dar loro espressione nel linguaggio simbolico di un calcolo e d'istituire, su questo fondamento, la scienza della logica costruendone il metodo; di fare, di questo metodo, la base di un metodo generale per l'applicazione della dottrina matematica della probabilità e, in ultimo, di ricavare dai diversi elementi di verità portati alla luce nel corso di queste indagini alcune indicazioni probabili sulla natura e la costituzione della mente umana"[18].

Nell'opera appena citata sono stati messi a punto gli strumenti matematici necessari per combinare le proposizioni (i c.d. *operatori logici* o *booleani*) ed in grado di portare a conclusioni logicamente valide, tramite la trasformazione delle proposizioni in simboli astratti, validi per ogni caso, e derivando le regole per effettuare su di essi le varie

[17] A. AGAZZI, *Il significato concettuale della logica booleana*, in A. AGAZZI – AZZIASSALLO (a cura di), *George Boole. Filosofia, logica, matematica*, Milano, 1998, p. 38. Ciò è dovuto, in primo luogo, alla circostanza che "a partire dagli inizi dell'età moderna, matematizzare un ambito di conoscenza è stato considerato come il mezzo migliore per assicurarvi rigore, oggettività, fecondità e, in ultima analisi, per promuoverlo al rango di *scienza* (con tutti i connotati positivi che una simile qualifica veniva a comportare)" (*Ibidem*).

[18] G. BOOLE, *Indagine sulle leggi del pensiero su cui sono fondate le teorie matematiche della logica e della probabilità*, tr. it., Torino, 1976, p. 9.

trasformazioni[19].

Boole afferma che la matematica non deve necessariamente trattare grandezze o numeri, ma anche variabili che non siano né le une, né gli altri[20]: l'algebra booleana, dunque, mette in relazione delle proposizioni di cui si può stabilire il valore di verità. La logica simbolica è un linguaggio matematico che si serve, per rappresentare il comportamento di determinati sistemi, di simboli letterali in sé astratti (*variabili*), che assumono un significato diverso a seconda dello specifico sistema. Sino all'opera di Boole, l'algebra era sempre stata legata a valori numerici ed inoltre le variabili potevano assumere qualsiasi valore. Nell'algebra teorizzata dall'illustre matematico, invece, le variabili possono assumere solo due valori (ad esempio, vero o falso), per cui tale logica è detta binaria o diadica.

Non si deve ritenere che questi studi abbiano solo una incidenza teorica: in seguito, infatti, essa ha trovato una realizzazione pratica nella costruzione degli elaboratori elettronici, il cui funzionamento è basato proprio su una logica di tipo binario, a causa della semplicità di individuazione dei due stati caratteristici in molti componenti (ad esempio, interruttore chiuso od aperto)[21]. Del resto, l'algebra booleana si

---

[19] E. FERRI – G. GIACOBBE – G. TADDEI ELMI, *Informatica e ordinamento giuridico*, Milano, 1988, p. 21.

[20] M. G. LOSANO, *op. cit.*, p. 95.

[21] Dalla logica simbolica si differenzia la logica deontica (dal greco *domai*, dovere). Punto di partenza è la considerazione che se nel discorso naturale una proposizione può essere vera o falsa, altrettanto non può dirsi con riferimento alle norme giuridiche, perché il diritto si esprime mediante proposizioni di varia tipologia, per cui nella logica deontica si preferisce parlare delle categorie del permesso, del proibito e dell'obbligatorio. Pertanto, la logica deontica si differenzia nettamente dalla logica del discorso naturale detta aletica (dal greco *alétheia*). Inoltre, "la logica deontica si preoccupa, quando parla di modalità, della struttura della norma, problema che è però in funzione dell'inferenza di una norma dall'altra e che incontra la difficoltà nel

presenta come un sistema algebrico "suscettibile di molteplici interpretazioni. Si tratta cioè di una forma rigorosa che può essere fruttuosamente al servizio di molteplici contenuti"[22], e la realtà fattuale ha dimostrato la rispondenza a verità di tale affermazione, ove si consideri che la rivoluzione informatica è anche frutto, ovviamente in parte, dell'applicazione di tale logica.

4. I PRINCIPI DELLE RICERCHE DOCUMENTARIE E GLI OPERATORI LOGICI

L'utilizzo dell'informatica nell'ambito dell'attività di ricerca documentaria ha portato a nuove metodologie di ricerca, le quali permettono di sfruttare, almeno in parte, le potenzialità degli odierni strumenti informatici[23].

La ricerca sulle banche dati è caratterizzata, primariamente, dal

---

fatto che la teoria dell'inferenza vale per proposizioni descrittive, suscettibili di essere predicate di vero e falso e non per le prescrittive. Le risposte ai fini dell'utilizzo della logica anche per le proposizioni prescrittive sono state varie ma quella maggiormente utilizzata è quella che si riferisce ad una distinzione operata da Hare tra frastico e neustico per cui le operazioni logiche si compirebbero sulla prima parte (frastico). Il rappresentante più noto di questa linea è A. G. Conte che lavora da anni – come, del resto, fa Carcaterra – nel tentativo di realizzare una teoria delle regole costitutive. G. Carcaterra, in particolare, ha costruito una teoria "costitutiva" del diritto: pur riconoscendo che le norme hanno lo scopo indiretto di prescrivere sostiene che le norme giuridiche sono costitutive, vale a dire agiscono sul sistema giuridico costituendolo o modificandolo" (T. SERRA, *Appunti di filosofia del diritto*, Roma, 2003, p. 94).

[22] M. G. LOSANO, *op. cit.*, p. 96.

[23] Le ricerche nell'ambito della comprensione sostanziale del testo rappresentano l'obiettivo prossimo da raggiungere per l'informatica giuridica; in materia stanno assumendo sempre più importanza gli studi sul *Semantic Web*, nonostante le mille difficoltà sottese ad un simile progetto, in ragione dell'estrema complessità delle metodologie che permettano di passare dalla comprensione sintattica a quella semantica. Sul *Semantic Web* v. *infra*, cap. 5.

principio della libertà e causalità della ricerca: "ogni dato presente nei documenti costituisce una chiave di accesso autonoma e […] può essere liberamente scelta dall'utente"[24], il quale otterrà la selezione dei documenti presenti nella banca dati che contengono tali chiavi ed una disposizione delle relative informazioni non legata alla classificazione ed alla collocazione scelta dall'archivista, al contrario di quanto avviene con gli archivi cartacei.

Il secondo principio in materia è costituito dalla **libera combinabilità dei dati**, per cui "il ricercatore può ottenere una selezione unica ed istantanea dei documenti, anche sulla base di una pluralità di dati, ciascuno dei quali liberamente scelto, ottenendo così sempre una selezione dei documenti perfettamente adeguata alle proprie esigenze informative"[25]. Lo svolgimento di una ricerca obbliga dunque l'utente della banca dati ad un sforzo di riflessione, consistente nell'individuazione delle parole chiave in base alle quali svolgere la ricerca medesima. Bisogna dunque stabilire *a priori* quali termini siano indefettibili per lo svolgimento della ricerca e quali siano invece intercambiabili. Normalmente si procede a combinare più termini e ciò avviene mediante l'utilizzo degli **operatori logici o booleani**. Essi sono fondamentalmente tre:

a) AND (e): indica la compresenza di due o più elementi. In altri termini, "pone la condizione logica che i dati ricercati siano veri in modo congiunto o dipendente. La condizione è verificata se, e solo se, tutti i

[24] R. BORRUSO – L. MATTIOLI, *Computer e documentazione giuridica. Teoria e pratica della ricerca*, Milano, 1999, p. 107.
[25] R. BORRUSO – L. MATTIOLI, *ivi*, p. 126.

dati sono veri"[26], cioè se sono presenti tutte le parole ricercate. Ad esempio, se in una determinata banca dati si vogliono reperire tutti i documenti in cui si parla di «informatica giuridica», si digiterà «informatica AND giuridica»;

b) OR (o): indica l'alternativa fra più elementi. "Pone la condizione logica che i dati ricercati siano veri in modo congiunto o dipendente"[27], infatti può essere inclusivo, se nella selezione devono essere inclusi i documenti che contengono indifferentemente uno o più elementi legati dall'operatore, oppure esclusivo, se invece devono essere presenti alternativamente, per cui la presenza di uno deve escludere quella degli altri;

c) NOT (non): indica l'inesistenza di uno o più elementi. Il *computer* deve così escludere dalla selezione tutti quei documenti che contengono il termine preceduto dall'operatore in oggetto; inoltre, il *not* è monadico se si riferisce ad un solo operando, diadico se si richiede contemporaneamente la presenza di un dato e l'assenza di un altro[28].

Gli operatori logici booleani, in realtà, "*non* sono una «invenzione»: sono una *scoperta* e di una verità tanto evidente – a pensarci bene – da costituire il classico uovo di Colombo. Non sono, infatti, che il meccanismo attraverso il quale la nostra mente forma e verifica tutti i concetti. Cos'è un concetto, invero, se non un insieme di elementi, alcuni dei quali devono coesistere, altri possono indifferentemente esserci o non esserci e altri ancora non devono esserci? E poiché l'uomo è in grado di pensare e comunicare solo perché è in grado di organizzare *in*

[26] G. TADDEI ELMI, *Corso di informatica giuridica*, Napoli, 2003, p. 38.
[27] *Ibidem*.
[28] *Ibidem*.

concetti la realtà che percepisce, si può ben dire che gli operatori logici booleani costituiscono un tipo di logica niente affatto contraria e neppure diversa da quella che anche l'uomo applica, *ma una logica tipicamente umana*"[29].

Inoltre, la ricerca può essere agevolata dall'utilizzo degli operatori di prossimità, il cui impiego consente il reperimento di documenti che contengono i termini indicati solo la distanza fra essi non è superiore ad un certo numero di caratteri o di parole[30].

In tutti i casi citati sinora, le parole-chiave sono costituite da termini conosciuti nella completezza dei caratteri alfanumerici che li compongono; l'applicazione del principio del **mascheramento dei dati** consente l'effettuazione di ricerche inserendo nel sistema parole non complete, i cui caratteri non conosciuti sono sostituiti dai caratteri «*jolly*», in modo da reperire tutti quei documenti che contengono le parole formate dalle lettere precedenti o susseguenti al carattere *jolly* ma non, dunque, le parole esatte. È così possibile reperire documenti che contengono termini non conosciuti nella loro completezza oppure simili dal punto di vista alfanumerico, evitando di dover effettuare tante ricerche o a specificare tante voci quante sono le parole simili[31].

È poi possibile indicare soltanto il tipo (astratto) del dato di interesse, "(corrispondente ad un determinato campo o canale di ricerca che dir si voglia) per ricevere dal *computer* l'indicazione dei dati concreti, che corrispondono al tipo voluto, contenuti nei documenti esistenti in

[29] R. BORRUSO, *Computer e diritto*, I, *Analisi giuridica del computer*, Milano, 1988, p. 70.
[30] Gli operatori di prossimità sono i seguenti: NEAR (i termini ricercati devono essere compresenti nello stesso paragrafo); WITH (le parole-chiave devono essere adiacenti e disposte in modo sequenziale); ADJ (le *key-words* devono essere adiacenti).
[31] Tale tecnica di ricerca è detta anche ricerca concettuale a livello morfologico.

archivio ovvero in quelli già selezionati sulla base di altri dati (concreti)"[32]; nella terminologia del sistema Italgiure-Find[33], questo tipo di informazione è detto **analisi spettrale**. Ad esempio, è possibile ottenere una divisione di documenti in base al criterio temporale dell'anno di emanazione.

La ricerca, inoltre, può essere effettuata per **approssimazioni successive** (c.d. «scalettamento delle stringhe»)[34], in modo da restringerne gradualmente l'ambito e di reperire tutti i documenti d'interesse, che potrebbero invece venire esclusi all'esito di una ricerca svolta mediante l'inserimento di parole che ne restringerebbero subito l'ambito senza consentire una valutazione dell'entità delle informazioni potenzialmente utili.

Nei moderni archivi informatici la ricerca può essere svolta su ciascun dato immesso all'interno dell'archivio, per cui è possibile effettuare le c.d. ricerche *full text*, a differenza di quanto accade con gli archivi tradizionali, nei quali l'indicizzazione dei documenti è svolta a priori e ovviamente non può includere il loro contenuto integrale.

La prestazione dei sistemi informativi viene calcolata dalla scienza della documentazione mediante l'utilizzo dei quattro indici di prestazione[35]:

---

[32] R. BORRUSO – L. MATTIOLI, *ivi*, p. 156.
[33] È il sistema adottato dal Centro Elaborazione Dati (C.E.D) della Corte di Cassazione: su di esso v. *infra*, par. 6.
[34] R. BORRUSO – L. MATTIOLI, *ivi*, p. 163; "la ricerca mediante lo scalettamento delle stringhe determina un vero e proprio colloquio tra ricercatore ed elaboratore" (V. NOVELLI – VELLIANNANTONIO, *Manuale per la ricerca elettronica dei documenti giuridici*, Milano, 1991, p. 86).
[35] N. PALAZZOLO, *Strumenti per l'accesso all'informazione giuridica*, in ID. (a cura di), *Corso di informatica giuridica*, Catania, 1998, pp. 31-32.

a) *richiamo*, ossia la capacità del sistema di ottenere in risposta tutti i documenti pertinenti contenuti nell'intero archivio;
b) *precisione*, ossia la capacità del sistema di fornire in una certa risposta solo documenti pertinenti. Il "tasso di precisione o di pertinenza" è il rapporto fra il numero di documenti pertinenti la richiesta e il totale dei documenti recuperati attraverso una strategia di ricorso;
c) *silenzio*, ossia il rapporto fra i documenti pertinenti contenuti nell'archivio e i documenti che vengono perduti nella risposta;
d) *rumore*, ossia il rapporto fra tutti i documenti recuperati e quella parte, fra essi, non pertinente alla richiesta.

5. I THESAURI

Il *thesaurus*, o tesauro, è stato inizialmente definito da Peter Mark Roget[36] come uno strumento basilare per trasformare le idee in parole, mettendo pertanto il luce il problema della rappresentazione dei concetti attraverso codici linguistici. Il *thesaurus* da lui compilato nel 1852 era composto da una lista di termini a ciascuno dei quali erano affiancate

[36] Nel 1805 Roget, filologo, scienziato e fisico, creò il *Thesaurus of English Words and Phrases*, poi pubblicato nel 1852, ossia dopo circa cinquant'anni dal suo primo progetto di un sistema di classificazione verbale, progetto finalizzato a supplire alle proprie mancanze (come afferma l'a. nell'introduzione al Thesaurus del 1852). La prima edizione conteneva circa quindicimila parole, ma tale numero è progressivamente cresciuto con le edizioni successive, tanto che la decima edizione, edita nel 1992, contiene addirittura duecentocinquantamila parole. Il *thesaurus* creato da Roget è suddiviso in sei classi primarie, a loro volta suddivise in altre sottoclassi secondo una organizzazione ad albero.

tutte le altre parole che con esso avevano una relazione. Nel corso degli anni sono state proposte altre definizioni di thesaurus, fra le quali bisogna ricordare la definizione ISO (*International Organization for Standardization*) n. 2788 del 1974, ai sensi della quale, in termini di funzione, il thesaurus è uno strumento terminologico usato per tradurre il linguaggio naturale dei documenti, degli indicizzatori o degli utenti in un linguaggio di sistema, più strutturato, detto anche linguaggio documentario o linguaggio di informazione. In termini di struttura esso è un vocabolario controllato e dinamico di termini semanticamente correlati che coprono un determinato ambito disciplinare.

L'ISO ha poi aggiornato tale definizione nel 1986, nelle *Linee guida per la costruzione e lo sviluppo di thesauri monolingue*, affermando che un **thesaurus** è il vocabolario di un "linguaggio di indicizzazione" controllato, organizzato in maniera formale, in modo da rendere esplicite le relazioni "a priori" tra i concetti. Esso è dunque circoscritto solo alla parte lessicale (semantica) di un linguaggio d'indicizzazione e di ricerca, cui va abbinato il *corpus* di norme (sintassi) che regolano i rapporti sintagmatici tra gli elementi di un enunciato di soggetto, al fine di ottenere un codice documentario completo. I termini utilizzati nel vocabolario sono sì sottoposti a controllo, ma vengono disposti in ordine alfabetico ed appartengono al più vasto insieme della lingua naturale, mentre gli schemi di classificazione detti artificiali puri si differenziano perché i concetti, rappresentati da notazioni numeriche o alfanumeriche, hanno un significato solo all'interno del proprio sistema[37]. Il concetto di vocabolario controllato è finalizzato alla convergenza del

[37] S. SPINELLI, *Introduzione ai thesauri*, in http://mail.biocfarm.unibo.it/~spinelli/indicizzazione/thesauri.htm.

lessico dell'autore con il lessico del ricercatore, in modo da stabilire una relazione biunivoca tra termine e concetto che conduce all'ottenimento della univocità semantica, per cui ad un termine corrisponde un concetto e, all'inverso, ad un concetto corrisponde un termine. Ciò consente di superare il maggior pregio ed il maggior difetto del linguaggio naturale, nel quale, da un lato, ridondanze, ambiguità, polisemie, omonimie, ecc., garantiscono ricchezza ed espressività, dall'altro rendono difficile l'organizzazione funzionale dei motori di ricerca.

Il *thesaurus*, dunque, risponde all'esigenza di standardizzare il linguaggio scientifico, al fine di evitare nozioni divergenti cui necessariamente consegue una confusione sia semantica che, soprattutto, concettuale. La sistematizzazione delle nozioni e dei termini utilizzati nell'ambito dell'informatica giuridica si dimostra dunque necessaria, sia per la ricerca che la didattica, proprio perché chiarifica e definisce concetti altrimenti oscuri o dagli incerti confini. La fase costruttiva di un *thesaurus* comporta pertanto la raccolta e la collazione dei sinonimi, dei quasi sinonimi e degli antonimi che descrivono il medesimo concetto e la scelta di uno solo di questi termini, che viene detto *termine preferito* (PT, *Preferred Term*) o *descrittore* in quanto è il termine utilizzato per descrivere un determinato concetto; il contenuto semantico del termine preferito viene poi ridotto ad un solo significato, generalmente il più tipico nell'ambito disciplinare del tesauro. Tutti gli altri termini sono invece detti *termini non preferiti* (NPT, *Non Preferred Term*) e possono essere utilizzati per rinviare al termine preferito. I concetti rappresentati dai termini possono essere entità concrete (ad esempio oggetti), astratte (ad esempio una disciplina o un'azione), individuali o "classi di uno"

analoghe a nomi propri: sempre nella fase costruttiva è necessario controllare l'appartenenza dei termini utilizzati a queste categorie, in quanto possono influenzare le procedure utilizzate nel *thesaurus*.

Le relazioni fra i termini sono definite da una relazione esplicita e formalizzata, per cui ogni termine è inserito in una rete relazionale che ne chiarisce ulteriormente il contenuto semantico, e che mostra la distanza semantica tra i termini stessi. Inoltre, le relazioni sono "a priori", dunque ineriscono all'ambito semantico dei termini e sono sempre vere in qualsiasi ambito.

Si distingue fra relazioni di:

a) *preferenza* (o di *sinonimia* o di *equivalenza*): identifica un gruppo di equivalenza fra termini, tra i quali si sceglie il termine preferito, mentre gli altri vengono detti termini non preferiti o sinonimi[38]. Viene utilizzata per rapporti di quasi-sinonimia, *upward posting*[39], antinomia[40];

[38] L'operatore US (dall'inglese *USe*, usa) evidenzia la relazione fra termine non preferito (NPT, *Non Preferred Term*) e termine preferito (PT, *Preferred Term*), il suo reciproco UF *(Used For,* usato per) identifica invece la relazione inversa. In tale categoria rientrano rapporti di sinonimia vera, varianti ortografiche, sigle e acronimi, preferenza linguistica. Oltre alla sinonimia propria, essa consente di mettere in relazione anche termini non strettamente sinonimici (*sinonimia convenzionale*), in cui i termini sono considerati sinonimi solo all'interno del contesto dei documenti gestiti dal tesauro.

[39] Si parla di *upward posting*, o *rinvio al superiore gerarchico*, per termini in relazione gerarchica di cui non interessa gestire la specificità. Si usa il termine più generico.

[40] Ovviamente la collocazione dell'antinomia quale sottospecie della sinonimia risponde ad una esigenza empirica, poiché si ritiene che la trattazione di un aspetto di un problema probabilmente toccherà anche il suo opposto, per cui si assume la sinonimi di termini antinomici ai fini dell'indicizzazione e della ricerca.

b) *gerarchia*, collega verticalmente tra loro i termini appartenenti alla stessa famiglia semantica[41], esprimendo, dunque, un rapporto di subordinazione o di sovraordinazione mediante una organizzazione ad albero[42]. I thesauri possono essere monogerarchici e poligerarchici: nei primi i termini possono appartenere ad una sola categoria; nei secondi i termini possono appartenere a più categorie;

c) *associazione*, è residuale perché identifica una relazione non definibile né come sinonimica né come gerarchica e tuttavia innegabile[43].

Tali relazioni non sono esplicitate da tutti i thesauri, ma comunque la relazione di gerarchia è quella più utilizzata e viene espressa graficamente attraverso una gerarchia classificatoria ad albero, attraverso

[41] È indicata con l'operatore BT (*Broader Term*= termine più ampio) e col suo reciproco NT (*Narrower Term*= termine più ristretto).

[42] I termini subordinati sono anche detti *iponimi*, quelli sovraordinati vengono anche detti *iperonimi*. In tale categoria rientrano la relazione *generica* (genere/specie: detta anche relazione *is-a*, esprime il legame che esiste tra una categoria e i suoi elementi. Affinché sia corretta è necessario che tutte le istanze del termine subordinato siano istanze del termine sovraordinato. Viene identificata con le sigle BTG e NTG), *partitiva* (parte/tutto: detta anche relazione *has-a*,esprime il legame fra un concetto complesso e i suoi componenti. Le istanze del termine subordinato devono implicare il termine sovraordinato e vengono utilizzate le sigle BTP e NTP), *esemplificativa* (specie/esempio: rappresenta il legame che esiste tra una classe ed un suo individuo).

[43] Questa relazione è caratterizzata da reciprocità e viene indicata con l'operatore RT (*Related Term*, termine associato). I relativi termini possono appartenere alla stessa categoria: in tal caso, i termini possono avere uno stesso termine sovraordinato ed un significato parzialmente sovrapponibile; oppure i termini possono rappresentare concetti legati da una relazione di tipo "familiare" o di tipo "derivato". I termini possono anche appartenere a categorie diverse, ma l'uno deve comunque implicare l'altro: come esempi si ricordano una disciplina e il suo oggetto di studio, un processo od operazione e il suo agente o il suo strumento, una azione e il suo prodotto, una azione e chi o cosa la subisce, oggetti e fenomeni e loro proprietà, concetti e loro origini, concetti legati da rapporti causali, una cosa e il suo antidoto, un concetto e la sua unità di misura, locuzioni sincategorematiche (termini composti) e loro nomi sottocategoriali.

la quale dal termine più generale (*Top Term*), che esprime una intera classe di concetti, si scende via via ai termini più specifici.

La presentazione del *thesaurus* avviene in due modi: classificato o alfabetico. La parte classificata evidenzia l'intera gerarchia semantica dal termine più generale al più specifico; quella alfabetica ritrova i termini collegati a quello ricercato, mentre la struttura classificatoria rimane implicita[44].

In Italia si può ricordare *THES/BID*, del 1984, che "rappresenta il primo tentativo organico di standardizzazione della terminologia e sistematizzazione dei concetti afferenti a questo nuovo campo interdisciplinare, sviluppatosi dall'impatto delle moderne tecnologie d'elaborazione delle informazioni con la scienza e la prassi del diritto"[45], e *THES/ITLaw*, del 1988, che costituisce l'aggiornamento e lo sviluppo del primo[46].

---

[44] N. PALAZZOLO, *Strumenti per l'accesso all'informazione giuridica*, in ID. (a cura di), *op. cit.*, p. 33.

[45] C. CIAMPI – AMPIAMELI – MELIRIVISONNO, *THES/BID. Thesaurus d'informatica e diritto*, Milano, 1984, p. VII.

[46] C. CIAMPI – E. FAMELI – MELIRIVISONNO, *THES/ITLaw. A Multilingual Thesaurus of Terminology in "Information Technology and the Law"*, in *Inf. dir.*, 1998, 2 (numero monografico). Gli autori del thesaurus in oggetto rilevano che "il *THES/ITLaw*, essendo stato costruito – come già il precedente *THES/BID* – non *a priori*, cioè prima dell'organizzazione del sistema di documentazione nel settore applicativo tematicamente collegato, bensì *a posteriori*, sulla base dell'analisi lessicale svolta sui titoli e sugli *abstracts* delle unità bibliografiche selezionate per la realizzazione dell'archivio d'informatica e diritto, tendenzialmente registra quella complessa evoluzione che, nel lessico specialistico proprio di questo assai interdisciplinare settore della conoscenza, s'è verificata nell'arco di oltre tre lustri di fondamentali progressi nelle tecnologie dell'informazione e della comunicazione e di profondi sconvolgimenti nell'organizzazione giuridica della società e del lavoro" (p. 5).

6. LE BANCHE DATI GIURIDICHE

"Una banca dati è un qualsiasi insieme di dati registrati su un supporto leggibile da parte di un computer. Tuttavia, in senso più specifico si parla di banca dati solo per designare le raccolte di dati" che siano utilizzabili da più utenti o da più programmi informatici, che consistano di più *file* integrati tra di loro e che offrano all'utente una rappresentazione astratta (o logica) dei dati[47]. Bisogna poi distinguere fra basi di dati (*database*) e sistemi documentari (*information retrieval*); le prime privilegiano l'aspetto della gestione dei dati (elaborazione, aggiornamento e verifica), i secondi sono finalizzati alla consultazione a fini informativi (ricerca e selezione dei dati rilevanti).

In Italia il primo sistema di documentazione giuridica risale al 1971, con la creazione del sistema «**Italgiure-Find**» della Corte di Cassazione, che inizialmente richiedeva la conoscenza della sintassi del linguaggio di interrogazione utilizzato nell'ambito del sistema. Successivamente, il Centro Elettronico di Documentazione (C.E.D.) della Suprema Corte ha sviluppato *Easy Find*, una interfaccia grafica che facilita enormemente le operazioni di ricerca nella banca dati. Oggi il C.E.D. offre un servizio di consultazione telematica di testi di interesse giuridico raccolti e organizzati in apposite banche dati on-line (quarantadue archivi per oltre quattro milioni di documenti), nelle quali, ovviamente, gli archivi normativi e giurisprudenziali sono i principali. L'accesso alla consultazione degli archivi avviene mediante il

[47] P. GUIDOTTI – IDOTARTOR, *Banche dati e sistemi di documentazione giuridica*, in N. PALAZZOLO (a cura di), *op. cit.*, p. 111; sullo stesso argomento v. anche: M. RAGONA, *Banche dati e sistemi informativi giuridici*, in R. NANNUCCI (a cura di), *Lineamenti di informatica giuridica*, Napoli, 2002, pp. 247-292.

collegamento telematico con la banca dati del C.E.D. attraverso il sistema di ricerca Italgiure-Find o attraverso l'interfaccia Easy Find. Il collegamento è concesso gratuitamente agli organi costituzionali, giurisdizionali e delle amministrazioni dello Stato, ai magistrati e ai procuratori e avvocati dello Stato, mentre per tutti gli altri utenti l'accesso è possibile solo dietro il pagamento di un canone di abbonamento annuo. Il sistema di ricerca consente il reperimento di documenti sia tramite interrogazioni *full-text* che per estremi (numero, data, parti, ecc.). La consultazione dei documenti avviene in forma ipertestuale, consentendone pertanto una lettura non sequenziale e permettendo di saltare con pochi click da un documento all'altro, anche se appartenenti ad archivi diversi (ad esempio, da una massima è possibile saltare ad una legge o ad un'altra massima, eventualmente difforme o conforme).

Anche il sistema Guritel[48], dell'Istituto Poligrafico e Zecca dello Stato, è quasi interamente a pagamento, sia per gli utenti pubblici che privati. In esso trovano spazio vari archivi, e l'archivio detto proprio Guritel contiene il testo delle Gazzette Ufficiali della Repubblica Italiana pubblicate dal primo gennaio 1987 sino ad oggi, ma solo quelle uscite nei sessanta giorni precedenti la data di consultazione sono consultabili gratuitamente. Considerando che mediante la Gazzetta Ufficiale il cittadino viene (teoricamente) a conoscenza delle nuove leggi che dovranno, fra l'altro, regolamentare la sua condotta, non si capisce perché tale sistema non sia liberamente accessibile, tenendo oltretutto presente i bassi costi di gestione di un simile servizio, soprattutto se paragonati ai costi della pubblicazione cartacea.

[48] Raggiungibile all'indirizzo http://dbase.ipzs.it/indispol/homeipzs.

Nell'ambito dell'accesso alla documentazione giuridica, assume una importanza fondamentale il progetto «**Norme in Rete**»[49], cui collaborano i maggiori enti istituzionali italiani (Senato della Repubblica, Camera dei deputati, Ministero della Giustizia). Il progetto, intrapreso nel 1999, dovrebbe consentire l'accesso gratuito (via Internet) all'informazione normativa e, in un secondo tempo, anche alla produzione giurisprudenziale ed agli atti amministrativi, razionalizzando l'organizzazione degli strumenti informativi. Il progetto è improntato alla decentralizzazione, poiché le norme dovrebbero essere contenute nei siti delle istituzioni che le hanno poste in essere e che aderiscono al progetto, organizzando le informazioni secondo gli *standard* ivi previsti. Si dovrebbe dunque procedere alla marcatura degli atti in linguaggio XML (*eXtensible MarkUp Language*)[50]. Ogni atto viene identificato dai *metadati*, ossia da tutti gli elementi necessari a descriverlo[51]; nel progetto, la metainformazione è contenuto nel *DTD Meta (Document Type Definition*[52]),

[49] Raggiungibile all'indirizzo http://www.normeinrete.it.

[50] *"XML is a set of rules for defining semantic tags that break a document into parts and identify the different parts of the document. It is a meta-markup language that defines a syntax in which other field-specific markup languages can be written"* (E. R. HAROLD, *XML Bible*, New York-Indianapolis-Cleveland, 2001, p. 3).

[51] In argomento bisogna ricordare che "l'impiego della dogmatica giuridica nell'annotazione dei testi (elettronici) costituirà […] una pratica delicata, che dovrà ovviamente essere condotta nei modi appropriati. La sua conversione in «metainformazione» per l'estrazione dai testi di informazioni specifiche gioverà a mio parere un ruolo notevole, specie considerando la necessità di divulgazione derivante non solo dalla natura dei dati, le leggi, ma anche dal mezzo informativo, Internet, i cui utenti non saranno solo giuristi e specialisti, ma davvero tutti" (C. BIAGIOLI, *L'impiego della dogmatica giuridica in Internet*, in *Inf. dir.*, 1999, 1, p. 113).

[52] *"DTD is an acronym for document type definition. A document type definition lists the elements, attributes, entities, and notations that can be used in a document, as well as their possible relationships to one another. A DTD specifies a set of rules for the structure of a document"* (E. R. HAROLD, *op. cit.*, p. 211).

collegato dalle *URN (Uniform References Notation)*[53] al *DTD Norma* che provvede alla strutturazione del testo.

Accanto a tali banche dati, accessibili per via telematica, sono state create banche dati poste su supporto ottico, aventi ad oggetto per lo più la legislazione vigente (a tutti i livelli) e la giurisprudenza. L'avvento dei DVD-ROM ha permesso di superare il problema del limitato spazio di archiviazione dei CD-ROM, per cui le nuove banche dati su DVD assommano oggi il contenuto di più CD, con evidenti vantaggi in termini di praticità ed economicità.

7. INFORMAZIONI *ON LINE* ED *OFF LINE*

L'accesso alle informazioni memorizzate in forma elettronica può essere effettuato sia in locale sul computer che si sta utilizzando in un determinato momento, che contiene i dati richiesti, (*off line*) sia in remoto mediante la connessione telematica ad un sistema remoto che contiene tali dati (*on line*).

Nel primo caso, le informazioni devono essere memorizzate su un supporto, che può essere removibile, come un CD-ROM o un DVD-

[53] "L'adozione dei nomi uniformi consente la realizzazione di sistemi automatici per costruire la rete dei collegamenti tra i documenti e contribuisce ad elevare la qualità dei servizi offerti dal progetto, a beneficio sia degli utenti finali che potranno usufruire di funzionalità di navigazione più estese, sia delle amministrazioni pubbliche che potranno migliorare la qualità delle funzioni offerte sui propri siti riducendo l'impegno redazionale manuale. La creazione di funzionalità di navigazione ipertestuale tra riferimenti normativi richiede interventi redazionali che avvengono generalmente attraverso due fasi: il *riconoscimento* di un riferimento all'interno di un testo in linguaggio naturale e l'*associazione* a tale riferimento dell'indirizzo fisico della pagina web su cui è pubblicato il testo del provvedimento che è citato" (C. LUPO, *Definizione delle regole per l'assegnazione dei nomi uniformi ai documenti giuridici*, in http://www.normeinrete.it/stdoc/definizione_regole_nomi_uniformi051101.doc).

ROM, o fisso, come un *hard disk* (a meno di utilizzare *hard disk* posti all'interno di cassettini estraibili). In tali casi, l'unica spesa da sostenere è costituita dall'acquisto della banca dati, cui generalmente si accompagna un aggiornamento periodico per un tempo stabilito, anche se nella fascia di tempo intercorrente fra un aggiornamento e l'altro la banca dati è ovviamente limitata al contenuto memorizzato nel supporto. Le informazioni contenute in locale sul proprio elaboratore risultano così sempre accessibili, con una velocità maggiore rispetto a quanto è possibile con le banche dati *on line*, che oltretutto potrebbero non essere sempre consultabili nell'eventualità di problemi di connessione oppure di guasti al *server* che contiene i dati. Inoltre, se già l'avvento del *compact disc* ha consentito il superamento del problema del trasferimento di grosse quantità di dati da un sistema all'altro e la creazione di banche dati giuridiche assai vaste, la successiva diffusione dei DVD (*Digital Versatile Disc*), ben più capienti[54], ha portato all'unione di banche dati contenute su più CD su un solo DVD, col vantaggio di poter passare da un archivio all'altro con pochi *click* del *mouse*, senza il bisogno di dover sostituire il supporto e di dover passare da un programma di consultazione all'altro.

Nel caso in cui l'accesso avvenga per via telematica, ci si connette ad un altro elaboratore, nel quale sono contenute le informazioni che si stanno cercando. L'espansione della rete Internet ha permesso di abbandonare altre tecnologie proprietarie, per cui nelle banche dati *on line*

[54] Un normale CD può infatti contenere sino a 700 Mb di dati (eccezion fatta per alcuni nuovi supporti più capienti che presentano tuttavia problemi di compatibilità con alcuni lettori CD-ROM); un DVD singolo strato e singola faccia contiene 4,7 Gb di dati, doppio strato e singola faccia 8,54 Gb, doppia faccia e singolo strato 9,4 Gb, doppia faccia e doppio strato 17,4 Gb.

la connessione al computer che le ospita avviene generalmente via Internet. Dal momento che il controllo della banca dati spetta a chi la produce, il suo aggiornamento può essere continuo e ciò assume grande importanza in un ordinamento caratterizzato da una amplissima produzione normativa e giurisprudenziale. Ovviamente un aggiornamento continuo comporta costi notevoli per il produttore della banca dati, che dovranno pertanto essere sopportati dagli utenti, i quali devono inoltre provvedere in proprio alla connessione per via telematica, dunque con costi aggiuntivi, anche se il problema è minimizzato dalla progressiva diminuzione dei costi di connessione e dalla diffusione dei collegamenti c.d. *flat*, il cui costo è stabilito a *forfait*, indipendentemente dalla durata della connessione. Un ulteriore problema, meramente eventuale, è dovuto alla possibilità di malfunzionamenti del *server* che ospita la banca dati, che potrebbero concretizzarsi nell'impossibilità di accedervi, seppur per un periodo limitato di tempo. Non sussiste, invece, il problema della consultazione successiva alla connessione delle informazioni così ottenute, in quanto è in via generale possibile procedere alla loro stampa su carta oppure alla memorizzazione in forma elettronica sul proprio computer per potervi poi accedere in locale, mentre l'accesso ai dati può avvenire da qualsiasi parte si trovi l'utente, purché possa utilizzare una connessione ad Internet, che oggi le moderne tecnologie consentono anche con i comuni telefoni cellulari in standard GPRS.

Oggi le banche dati giuridiche vengono comunemente fornite su supporto ottico, con la possibilità di aggiornarle *on line* dietro pagamento di una somma ulteriore. Ciò consente di unire, al contempo, i vantaggi

delle banche dati *off line* con quelli delle banche dati *on-line*, per quanto i relativi costi siano abbastanza elevati e dovuti, probabilmente, alla settorialità del mercato nonché al comunque notevole lavoro che comportano la creazione e l'aggiornamento di una banca dati giuridica.

CAPITOLO 4

IL WEB SEMANTICO

1. DAL *WORLD WIDE WEB* AL *WEB* SEMANTICO

Il *World Wide Web*[1] ha avuto un successo enorme in un arco di tempo realmente ristretto, divenendo progressivamente una fonte inesauribile di informazioni per ciascun navigatore, anche se si è sinora dato per scontato che l'accesso ai dati contenuti nelle pagine *web* venisse effettuato da una persona umana, senza badare alla possibilità di un trattamento automatizzato dei dati presenti *on line*. La verifica dell'attendibilità della maggior parte delle informazioni così reperibili è dunque, lasciata al singolo utente, che, con le proprie capacità cognitive, valuta il contenuto delle pagine *web*[2]. Gli elaboratori elettronici non possiedono simili capacità, indipendentemente dai progressi compiuti nell'ambito degli studi sull'intelligenza artificiale: la flessibilità del pensiero umano non ha di certo eguali nel «mondo artificiale».

Oggi le pagine *web* sono generalmente scritte in linguaggio HTML (*HyperText Markup Language*) e sono interpretate dal computer da un punto di vista formale, eseguendo le operazioni relative al modo in cui è scritta ogni singola pagina. È così possibile utilizzare i c.d. *hyperlink*, ossia

[1] Su Internet ed il WWW v. *infra*, cap. 6.
[2] R. GUHA – R. MCCOOL, *TAP: a Semantic Web platform*, in *Computer Networks*, 2003, 42, p. 558. Del resto, "la differenza tra un programma di calcolatore ed il cervello è che il primo manipola simboli, il secondo annette ad essi un significato. La semantica non trova nella sintassi la condizione necessaria e sufficiente per la sua determinazione" (F. ROMEO, *Il diritto artificiale*, Torino, 2002, p. 53).

i collegamenti ipertestuali, che consentono di passare da un punto all'altro della medesima pagina o di passare ad un altro documento; tramite questo linguaggio l'elaboratore provvede inoltre alla impostazione grafica di ogni pagina, disponendo il testo e le immagini in base a quanto disposto in codice HTML.

La comprensione del significato della pagina *web* si arresta, dunque, all'interpretazione e all'esecuzione dei comandi preventivamente imposti, per cui l'elaboratore elettronico non comprende il reale significato contenutistico delle varie pagine *web*. Il c.d. *Semantic Web* dovrebbe consentire ai computer il passaggio dalla comprensione meramente formale dei documenti posti su Internet alla comprensione sostanziale. Ciò consentirebbe agli agenti *software* di operare in piena autonomia, automatizzando virtualmente ogni operazione che potrebbe essere svolta sul *web*. Ovviamente è necessario sviluppare le tecniche che consentiranno un rapido trasferimento delle informazioni e l'esecuzione di applicazioni remote[3] e le ricerche in tal senso sono oggi svolte sotto l'egida del *World Wide Web Consortium* (W3C).

In tale ambito si colloca anche un importante articolo di Tim Berners-Lee (l'inventore del *World Wide Web*), James Hendler e Ora Lassila, comparso sul numero di maggio 2001 della rivista *Scientific American* ed intitolato proprio *The Semantic Web*[4]. Gli autori affermano che il *Semantic Web* rappresenta una estensione dell'attuale WWW, in grado di attribuire un significato preciso a ciascuna informazione, consentendo di migliorare l'interazione fra l'uomo e la macchina.

---

[3] C. FILLIES – G. WOOD-ALBRECHT – F. WEICHHARDT, *Pragmatic applications of the Semantic Web using SemTalk*, in *Computer Networks*, 2003, 42, p. 600.
[4] T. BERNERS-LEE – J. HENDLER – O. LASSILA, *The Semantic Web*, in *Scientific American*, 2001, pp. 35-43.

Al fine di garantire lo sviluppo del *Web* Semantico, gli studi odierni sono concentrati su tre settori principali[5]:

a) specificazione dei linguaggi che formeranno la struttura del *Semantic Web*;
b) specificazione e sviluppo dei componenti strutturali che formeranno l'infrastruttura del *Web* Semantico e dei relativi strumenti;
c) prototipizzazione delle applicazioni che utilizzano i linguaggi e i componenti e definendo il contenuto necessario.

2. LA RAPPRESENTAZIONE DELLA CONOSCENZA E IL LINGUAGGIO

La base teorica che costituisce il punto di partenza per l'implementazione pratica del Web Semantico è da individuarsi nei numerosi studi sull'intelligenza artificiale, compiuti molto prima della nascita e dello sviluppo del *World Wide Web*, e in special modo sulle ricerche nell'ambito della «rappresentazione della conoscenza» (*knowledge representation*). I sistemi teorizzati in tale ambito sono centralizzati, per cui ciascuno deve condividere la medesima definizione dei concetti utilizzati, a scapito delle esigenze di versatilità che necessariamente si impongono. Sul punto si riscontra la prima differenza con il *Web* Semantico, che è invece caratterizzato dalla decentralizzazione, analogamente a quanto accaduto con il WWW, nei primi anni novanta criticato, fra l'altro,

[5] C. GOBLE, *The Semantic Web: an evolution for a revolution*, in *Computer Networks*, 2003, 42, p. 551.

proprio per la mancanza di una struttura centrale, che non avrebbe dunque consentito l'organizzazione dei dati, il cui reperimento sarebbe stato praticamente impossibile. In realtà, alla grande mole di informazioni disponibili *on line* si è accompagnata l'evoluzione dei motori di ricerca, i quali, usando una metafora, come fari hanno orientato il percorso dei naviganti. La decentralizzazione, dunque, rappresenta una scelta obbligata per poter garantire la versatilità del sistema. Per la sua realizzazione è necessario predisporre una logica che, al contempo, descriva le proprietà complesse degli oggetti e sia abbastanza semplice per essere sempre comprensibile dagli agenti *software*[6].

Bisogna infatti tenere presente che il *Web* Semantico conterrà una molteplicità di tipologie relazionali fra le varie risorse, che, a loro volta, potranno consistere non solo in oggetti *software*, (come pagine *web*, filmati, brani musicali) ma anche in persone, luoghi, eventi, ovviamente nella loro rappresentazione virtuale[7].

Il Web Semantico richiede la presenza di «metadata relazionali», ossia metadata *"that descrive how resource descriptions instantiate class definitions and how they are semantically interlinked by properties"*[8]. Per la sua realizzazione è necessario utilizzare un linguaggio di marcatura (*markup language*) che abbia una semantica ben definita allo scopo di offrire al *computer* la possibilità di porre in essere una interpretazione univoca. I linguaggi semantici sono sviluppati sulla base di quelli già presenti sul *Web* e le risorse sono identificate da un *Universal Resource Identifier* (URI), che ne consente, appunto, l'identificazione, come avviene nelle pagine *web*. Gli

[6] T. BERNERS-LEE – J. HENDLER – O. LASSILA, *op. cit.*, p. 38.
[7] R. GUHA – R. MCCOOL, *op. cit.*, p. 558.
[8] S. HANDSCHUSH – S. STAAB, *CREAM: CREAting Metadata for the Semantic Web*, in *Computer Networks*, 2003, 42, p. 579.

URI assicurano che i concetti non siano mere parole contenute in un documento, ma che siano collegati ad una definizione univoca reperibile liberamente sul *web*.

Sono così stati sviluppati "metodi (e linguaggi) che intendono descrivere la semantica dei documenti, introducendo un impianto descrittivo definito su tre livelli: un linguaggio relazionale del tipo "soggetto – predicato – oggetto", per descrivere metadati e modelli dei dati, l'RDF (*Resource Description Framework*); un linguaggio e una sintassi che insieme definiscano e descrivano il vocabolario delle rappresentazioni desiderate, ossia un'estensione dell'RDF pensata per la rappresentazione di strutture più generali, di carattere classificatorio (classi e sottoclassi, per esempio). Queste strutture prendono il nome di schemi e il linguaggio è denominato *RDF Schema*. Infine, un livello nel quale viene definita formalmente la semantica e gli strumenti di supporto per l'interpretazione automatica. A questo livello, che riguarda la descrizione della realtà di riferimento, si collocano proposte di formalismi"[9] quali OIL[10] (*Ontology Interchange Language*), DAML (*DARPA Agent Markup Language*) + OIL[11] e OWL (*Web Ontology Language*)[12].

---

[9] M. PARODI – A. FERRARA, *XML, Semantic Web e rappresentazione della conoscenza*, in *Mondo digitale*, 2002, 3, p. 44.

[10] *"The Ontology Inference Layer OIL is a proposal for a web-based representation and inference layer for ontologies, which combines the widely used modelling primitives from frame-based languages with the formal semantics and reasoning services provided by description logics"* (http://www.ontoknowledge.org/oil/index.shtml).

[11] *"DAML+OIL is a semantic markup language for Web resources. It builds on earlier W3C standards such as RDF and RDF Schema, and extends these languages with richer modelling primitives. DAML+OIL provides modelling primitives commonly found in frame-based languages"* (http://www.daml.org/2001/03/reference). Per un'applicazione del DAML-S DAML + OIL ai *web services*, v. S. NARAYANAN – S. MCILRAITH, *Analysis and simulation of Web services*, in *Computer Networks*, 2003, 42, pp. 675-693.

[12] *"The OWL Web Ontology Language is designed for use by applications that need to process the content of information instead of just presenting information to humans. OWL facilitates greater machine interpretability of Web content than that supported by XML, RDF, and RDF Schema (RDF-S) by providing additional vocabulary along with a formal semantics. OWL has three*

In particolare, il linguaggio XML, in sé e per sé, permette la strutturazione dei documenti ma non la comprensione del significato della struttura medesima[13]. L'RDF[14], invece, esprime il significato codificandolo in una serie di triplette (analogamente ad una proposizione semplice composta da soggetto, verbo ed oggetto), che possono essere scritte utilizzando i *tag* XML. Più specificatamente, in un sistema scritto in RDF, un documento fa asserzioni che cose specifiche (qualsiasi cosa: una persona, un oggetto, una pagina *Web*, ecc.) hanno proprietà (come "è sorella di") con valori determinati (un'altra persona, un'altra pagina *Web*). I soggetti, i verbi e gli oggetti sono identificati dagli URI[15].

L'aggiunta della semantica, dunque, consente l'interpretazione univoca delle informazioni strutturate; in tal modo, inoltre, si concretizza una significativa mutazione del *World Wide Web*, che, da un lato, da semplice (ma praticamente illimitata) collezione di documenti diviene un'ampia base di conoscenza, dall'altro diviene una periferica computazionale distribuita grazie ai *Web Services*, ossia ai programmi accessibili via *web* che costituiscono l'ultima generazione dell'informatica

---

increasingly-expressive sublanguages: OWL Lite, OWL DL, and OWL Full" (http://www.w3.org/TR/owl-features/).

[13] La struttura di un documento redatto in XML viene descritta mediante un DTD (*Document Type Definition*): evidente l'analogia con l'albero di Porfirio, ossia con una struttura finalizzata all'interpretazione delle categorie aristoteliche, secondo la quale, all'interno di ogni tipo di predicato (categorie di sostanza, relazione, quantità, ecc.), si può immaginare un collegamento a cascata di modi di predicazione, adatti a soggetti sempre meno numerosi, a partire dal genere sommo (la categoria) per giungere gradualmente alla specie più determinata, al di sotto della quale non esistono più ulteriori specie, bensì solo individui.

[14] Sull'RDF v. http://www.w3.org.org/rdf/.

[15] T. BERNERS-LEE – J. HENDLER – O. LASSILA, *op. cit.*, pp. 39-40. *"More precisely, RDF provides (i) a Standard Representation Language for metadata based on directed labeled graphs in which nodes are called resources (or literals) and edges are called properties; (ii) a Schema Definition Language (RDFS), for creating vocabularies of labels for these graph nodes (called classes) and edges (called property types) and (iii) an XML syntax for expressing metadata and schemas in a form that is both humanly readable and machine understandable. The most distinctive feature of the RDF/S data model is its ability to superimpose several descriptions for the same Web resources in a variety of application contexts"* (G. KARVOUNARAKIS *et al.*, *Querying the Semantic Web with RQL*, in *Computer Networks*, 2003, 42, pp. 617-618).

distribuita[16].

3. LE ONTOLOGIE

"Il concetto di ontologia è stato introdotto nell'intelligenza artificiale con il duplice scopo di fondare metodologie di rappresentazione della conoscenza che abbiano validità universale e di risolvere i problemi di semantica sottostanti. […] L'ontologia può essere definita in relazione al suo *oggetto*, cioè 'l'essere in quanto esistente'; o in relazione alla *funzione*, che la colloca fra le discipline filosofiche (le scienze epistemologiche in primis), ma anche fra quelle non filosofiche, come la logica e la teoria della conoscenza: ontologia come disciplina dei rapporti fra i concetti e gli oggetti del reale, come conoscenza dell'essere in universale. L'ontologia come metodo di conoscenza (*ontologismo*) considera l'essenza come punto di partenza, per cui la conoscenza oggettiva è anteriore alla conoscenza soggettiva della psicologia o della ideologia"[17].

Nell'ambito delle ricerche sul *Semantic Web*, le «ontologie» vengono definite come raccolte di informazioni, finalizzate alla risoluzione della possibile molteplicità di identificatori di un medesimo concetto dovuto alla molteplicità dei database e sorge pertanto la necessità di sviluppare una metodologia che consenta al *software* la comprensione del concetto[18]. "Può sembrare sorprendente che una disciplina collocata da sempre nella sfera filosofica sia diventata elemento essenziale degli studi sulle

[16] C. GOBLE, *op. cit.*, p. 553.
[17] D. TISCORNIA, *Il diritto nei modelli dell'intelligenza artificiale*, Bologna, 1996, p. 73.
[18] T. BERNERS-LEE – J. HENDLER – O. LASSILA, *op. cit.*, pp. 40-41.

tecnologie dell'informazione, ma va considerato che più si affinano i risultati delle ricerche tecnologiche, più la necessità di una base teorica solida aumenta. In questo caso, è evidente che le funzioni informatiche fondate sulla rappresentazione della realtà e delle conoscenze sulla realtà necessitano in primo luogo di criteri per impostare una metodologia su 'cosa' e 'come' rappresentare e che questo deve essere il più possibile generalizzabile ed universalizzabile, vale a dire ontologicamente e formalmente fondato"[19].

L'ontologia assume carattere fondamentale nella struttura del *Semantic Web*, perché consente la combinazione e la comparazione di informazioni che provengono da database distinti: ciò avviene in maniera trasparente per il fruitore, perché le relative operazioni vengono svolte automaticamente da agenti *software* all'uopo progettati.

4. LE APPLICAZIONI GIURIDICHE

La comprensione sostanziale del testo da parte degli elaboratori elettronici assume grande rilevanza per il diritto per una molteplicità di implicazioni. Basti pensare all'ulteriore sviluppo dei sistemi esperti, che potrebbero svolgere funzioni di analisi ed elaborazione testuale, potendo teoricamente portare alla creazione di veri e propri sistemi informativi giudiziali, eventualmente anche a fini decisori e comunque ad ausilio dell'attività del giudice. Questa è solo una delle tante possibilità offerte dalla realizzazione del *Web* Semantico e dalla sua estensione anche all'ambito giuridico, potenzialmente attuabile, come è del resto successo

[19] D. TISCORNIA, *Strumenti intelligenti per l'accesso all'informazione giuridica su Internet*, in http://www.ittig.cnr.it/ organizzazione/personale/pubblicazioni-tiscornia/IEIarticolo.rtf.

con la diffusione della Rete, che ha offerto nuove possibilità per la conoscenza giuridica.

Anche le attività di informatica giuridica documentaria, in particolar modo quelle di *information retrieval*, potrebbe trovare nuova linfa in una organizzazione delle informazioni effettuata in maniera automatizzata da parte degli elaboratori, con relativo abbattimento dei costi, a tutto beneficio degli utenti finali. Soprattutto le ricerche effettuate in un ambiente organizzato secondo le metodologie del *Web* Semantico sarebbero assai più semplici ed efficaci, poiché oggi esse vengono svolte sui testi isolando le parole dal loro contesto, per cui è necessaria una certa abilità anche nell'impostazione dei parametri di ricerca al fine di reperire i documenti effettivamente rilevanti, proprio perché l'intrinseca ricchezza del linguaggio naturale porta ad attribuire ad un medesimo termine più significati, variabili in base al contesto; senza considerare, fra l'altro i sinonimi, per cui una ricerca realmente completa dovrebbe essere effettuata tenendo presente quali parole potrebbero essere usate in sostituzione di altre.

Ovviamente il primo obiettivo da perseguire rimane sempre l'immediata conoscibilità dell'informazione da parte dell'uomo e solo in un secondo momento da parte dell'elaboratore; in ambito giuridico, inoltre, la conoscenza "è normalmente espressa nel linguaggio naturale e deve continuare ad esserlo, se il diritto vuol conservare la capacità di indirizzare adeguatamente l'operare dei cittadini e degli operatori giuridici"[20].

[20] G. SARTOR, *Linguaggi (e sistemi) informatici e linguaggio giuridico*, in A. ARTOSI – G. BONGIOVANNI – NGIOIDA (a cura di), *Problemi della produzione e dell'attuazione normativa*, III, *Analisi del linguaggio giuridico, legistica e legimatica*, Bologna, 2001, p. 291.

Ciò premesso, può dunque affermarsi che il «prossimo passo avanti» nel settore dell'informatica giuridica potrebbe essere costituito proprio dal *Web* Semantico, non tanto con riferimento alla possibilità di sostituzione a fini decisori del giudice, ma piuttosto nell'ambito dell'automazione di alcuni compiti facilmente delegabili agli agenti *software* e soprattutto grazie alle nuove possibilità offerte nel settore dell'informatica giuridica documentaria.

Inoltre, il Web Semantico può rendere assai più efficaci gli agenti *software* se essi saranno programmati in modo da sfruttarne il potenziale. La loro efficacia crescerà in maniera esponenziale con la scrittura di pagine secondo gli standard del Web Semantico e con la diffusione dei servizi automatizzati, compresi altri agenti *software*, in modo da garantirne l'interoperabilità. L'attendibilità delle informazioni può essere verificata mediante un sistema di firma digitale, dunque utilizzando tecnologie preesistenti[21]. Fra le possibili applicazioni è doveroso fare riferimento al commercio elettronico: già oggi alcune fasi nelle quali si realizza una transazione *on line* sono automatizzate, ma lo sviluppo del *Web* Semantico potrebbe favorire sia gli acquirenti che i venditori[22].

Ovviamente bisogna anche sviluppare tecnologie che evitino la perpetrazione di illeciti dovuti a tentativi di «ingannare» gli agenti *software*, come oggi accade con l'utilizzo abusivo dei *meta tag*, ossia con l'inserzione di parole non visibili da parte di chi consulta una pagina *web*, ma leggibili dai motori di ricerca automatici, che in questi casi valutano i siti non solo in base al loro contenuto, ma anche in seguito alla lettura di

[21] T. BERNERS-LEE – J. HENDLER – O. LASSILA, *op. ult. cit.*, p. 42.
[22] Per una esposizione delle possibilità offerte dal Web Semantico nell'ambito del *Business 2 Business* v. D. TRASTOUR – C. BARTOLINI – C. PREIST, *Semantic Web support for the business-to-business e-commerce pre-contractual lifecycle*, in *Computer Networks*, 2003, 42, pp. 661-673.

tali parole. In ogni caso, se verranno superati i problemi tecnici legati alla stessa struttura del *Semantic Web*, potrà realizzarsi la più grande evoluzione nell'ambito di Internet dopo il *World Wide Web*.

CAPITOLO 5

LA CRITTOGRAFIA

1. ORIGINI ED EVOLUZIONE

La **crittografia** è la scienza che studia i sistemi per rendere le informazioni segrete e leggibili solo a chi possiede la chiave per decifrarle[1]. Essa ha origini assai antiche ed è stata utilizzata al fine di garantire la segretezza delle comunicazioni, che assume importanza fondamentale soprattutto nel corso di eventi bellici. Il termine deriva dal greco *crypto* (nascondo, celo) e proprio in Grecia si sono avute le prime esperienze in questo ambito, nel 400 a.C., seguite qualche anno dopo dal trattato di Enea il Tattico su cifre e messaggi segreti. Anche Giulio Cesare, durante le campagne in Gallia, usava una primitiva tecnica per rendere incomprensibile il contenuto della propria corrispondenza privata: sostituiva ogni lettera con quella successiva nell'ordine alfabetico. Molti anni dopo, in epoca medievale la crittografia si è dimostrata utile anche nel settore economico, a causa dei rilevanti interessi in gioco, per cui si è progressivamente evoluta, diventando sempre più complessa, in ragione dell'utilizzo di algoritmi studiati nell'ambito della matematica.

Accanto alla crittografia, finalizzata all'occultamento del contenuto

[1] È stata anche definita come "the study of mathematical techniques related to aspects of information security such as confidentiality, data integrity, entity authentication, and data origin authentication" (A. MENEZES – NEZVAN OORSCHOT – RSCHANSTONE, *Handbook of Applied Cryptography*, Boca Raton, 1996, p. 4).

di un messaggio, si è posta la **steganografia**, il cui scopo è garantire la segretezza delle comunicazioni nascondendo la comunicazione stessa[2]. Il termine deriva dalle parole greche *steganòs* (coperto, nascosto) e graphein (scrittura), per cui la steganografia è *la scrittura nascosta*, o, *rectius*, l'insieme delle tecniche che consente a due o più persone di comunicare in modo tale da nascondere la stessa esistenza della comunicazione agli occhi di

[2] L'origine della steganografia è molto antica: si narra, infatti, che già Erodoto avesse utilizzato una ingegnosa ed efficace tecnica di steganografia. Egli aveva infatti fatto rasare il cranio di uno schiavo, per potervi tatuare un messaggio segreto, poi occultato dalla ricrescita dei capelli. Giunto a destinazione, lo schiavo doveva nuovamente radersi il capo, al fine di consentire la lettura del messaggio. Il termine «steganografia» è stato invece coniato all'incirca nel 1500 dall'Abate Tritemio (Johann Heidenberg), uomo dalla vita molto travagliata. A soli ventidue anni diventava l'Abate del monastero di Spanheim, risollevandolo da un lungo declino e facendolo diventare famoso in tutta Europa anche per la sua biblioteca, composta da circa duemila volumi. Nel frattempo cresceva anche sua la fama di santo e di mago, ma nel 1506, mentre si trovava a Würzburg per una missione, veniva tuttavia sollevato dalla sua carica a causa della rivolta dei monaci del monastero, stanchi dell'indefesso lavoro che erano costretti a svolgere sotto la sua guida. Tritemio decideva di rimanere nell'abbazia di San Giacomo, a Würzburg, a meditare e a scrivere sino alla sua morte, avvenuta nel 1516. Il volume «Steganographia» veniva tuttavia stampato solo nel 1606, dopo circa un secolo dalla sua stesura, e veniva tramandato mediante copie scritte a mano, cui probabilmente si devono gli errori presenti nell'opera di Tritemio, il quale aveva elaborato addirittura quaranta sistemi principali e dieci sotto-sistemi secondari, tutti finalizzati all'occultamento delle informazioni. Oggi si distingue fra tre tipologie di steganografia: sostitutiva, selettiva e costruttiva; le tecniche basate sulla prima tipologia sfruttano il rumore generato dalla maggior parte dei canali di comunicazione (linee telefoniche, trasmissioni radio, ecc.) nella trasmissione dei segnali, sostituendolo con un altro segnale che in realtà costituisce il messaggio segreto, non distinguibile senza la conoscenza della chiave segreta. La steganografia selettiva, a quanto è dato sapere, non ha sinora avuto realizzazioni pratiche, perché basata sul susseguirsi di più tentativi finalizzati a soddisfare una determinata condizione, per cui la quantità di informazioni che si riesce ad ottenere non è proporzionata allo sforzo da effettuare per il suo ottenimento. Infine, le tecniche di steganografia costruttiva permettono di sostituire il rumore generato dal sistema di comunicazione con l'informazione segreta, modificata imitando le caratteristiche statistiche del rumore originale, anche se costruire il modello del rumore è un'operazione molto complicata ed, eventualmente, un modello più accurato potrebbe distinguere le differenze fra il rumore sostituito ed il sostituto, vanificando le esigenze di segretezza.

un eventuale osservatore, «mimetizzandola», ad esempio, in un'altra comunicazione. Alla steganografia si ricorre non solo per superare eventuali inadeguatezze dei sistemi crittografici, ma anche per superare le restrizioni poste dai vari Paesi ai sistemi da ultimo citati.

Dall'analisi dell'evoluzione della crittografia è possibile evincere alcuni requisiti di base che i sistemi crittografici devono soddisfare per poter essere considerati sufficientemente *robusti*, ossia difficilmente attaccabili da qualsiasi tentativo di *crittoanalisi*. Viene così in rilievo il «principio di Kerckhoff», in base al quale la conoscenza del sistema di crittografia non consente di decifrare il testo, in modo che la robustezza del sistema non sia legata alla segretezza dell'algoritmo, ma piuttosto alla segretezza della chiave.

L'interesse per la crittografia ha avuto uno sviluppo graduale, che oggi risulta tuttavia accelerato dalla sempre crescente diffusione dei *computers*, in ragione della molteplicità di potenziali utilizzi delle tecniche crittografiche, che spaziano dalla firma digitale alla sicurezza delle transazioni, in ambiti nei quali non si può prescindere dalla sicurezza e dalla segretezza delle comunicazioni.

La crittografia è basata sull'inesistenza di un celere sistema di calcolo dei fattori primi che, moltiplicati fra loro, formano un certo numero. Bisogna dunque eseguire una per una tutte le divisioni per scoprire se il numero dato è divisibile per un altro senza che ci sia resto. Tanto più il numero da analizzare è grande, cioè composto da molte cifre, tanto maggiore sarà il tempo necessario per sapere da quali fattori primi è composto. Se tutte le lettere che compongono un testo vengono trasformate in numeri e se su questi viene effettuata una serie di

moltiplicazioni si ottiene un numero enorme, che può essere decifrato solo se si dispone del cifrario e della chiave. In mancanza, l'unica via per conoscerne il contenuto è cercare di decrittare il numero, lasciando il *computer* a tentare tutte le combinazioni possibili, ma i moderni algoritmi di crittografia sono tanto avanzati che il tempo richiesto per la decrittazione di un testo cifrato con una chiave di grosse dimensioni è addirittura nell'ordine di mesi od anni, anche con elaboratori molto potenti.

I primi sistemi di crittografia non erano tuttavia strutturati in maniera tale da poterne prevedere un largo utilizzo, perché erano basati su una *cifratura simmetrica*: il testo veniva infatti cifrato con la stessa chiave che bisognava necessariamente utilizzare per decifrarlo in seguito, con la conseguenza che se si voleva inviare un testo cifrato con tale sistema era necessario fornire la chiave al destinatario del testo. Ovviamente, più testi venivano spediti a più persone diverse, più si diffondeva la chiave, a tutto discapito della sicurezza.

Il superamento di questo problema è avvenuto nel 1976, anno in cui è stato pubblicato un articolo di Whitfield Diffie e Martin E. Hellman, entrambi dell'Università di Stanford, intitolato *New Directions in Cryptography*[3]. I due studiosi hanno infatti dimostrato la possibilità di utilizzare un sistema di *cifratura a chiavi asimmetriche*, nel quale il testo viene cifrato con una chiave privata e decifrato con una chiave pubblica, in possesso del destinatario. Le due chiavi devono essere indipendenti, per cui dalla conoscenza di una non si possa giungere alla conoscenza dell'altra.

[3] W. DIFFIE – FFIE E ELLMAN, *New Directions in Cryptography*, in *IEEE Transactions on Information Theory*, 1976, 22, pp. 644-654.

Nel 1977 Ronald Rivest, Adi Shamir e Leonard Adleman, tutti del MIT, hanno inventato un algoritmo (detto RSA, dalle loro iniziali) finalizzato alla costruzione di cifrari a chiave asimmetrica utilizzando particolari proprietà formali dei numeri primi con qualche centinaio di cifre. Anche se esiste la possibilità teorica che nuove scoperte matematiche possano metterne in dubbio l'affidabilità, il sistema si è sinora dimostrato molto sicuro e la sua qualità è unanimemente riconosciuta. L'algoritmo è stato brevettato dai tre studiosi, i quali hanno poi fondato un'azienda, la *RSA Data Security*, per poterlo sfruttare a fine di lucro, cedendo i diritti di utilizzazione ad altre società, come Microsoft e Netscape, senza considerare che il ben noto *Pretty Good Privacy* (PGP) è basato proprio su una sua variante.

Le applicazioni della crittografia sono dunque ben più presenti nella vita quotidiana di quanto si pensi e lo sviluppo tecnologico potrà proseguire anche grazie al progresso delle conoscenze *in subiecta materia*, perché l'esigenza di tutela della riservatezza delle informazioni si fa via via più forte per una molteplicità di fattori in più ambiti, tutti accomunati dall'interscambio dei dati in forma elettronica, come è del resto ovvio nella moderna «società dell'informazione». Oggi, del resto, l'informazione si caratterizza per essere immateriale, digitalizzata, trasferibile da un capo all'altro del globo in poche frazioni di secondo; rappresenta inoltre la nuova forma di circolazione del denaro, per cui patrimoni anche assai ingenti viaggiano con pochi *click* del *mouse*. In realtà, dietro quei pochi *click*, in pochi secondi si svolgono complesse operazioni tese a garantire la sicurezza di quanto avviene mediante i *computers*, nascoste dietro interfacce sempre più facili da gestire, che

semplificano notevolmente l'interazione fra l'uomo e la macchina. I risvolti sono dunque molteplici: la tutela della posta elettronica, nel rispetto del fondamentale diritto alla *privacy*; la sicurezza delle transazioni, al fine di consentire lo sviluppo del commercio elettronico; più in generale, la protezione di qualsiasi comunicazione che avvenga in forma elettronica, nel rispetto dell'autodeterminazione della persona. Del resto, quale tutela può avere un individuo sempre più solo dinanzi un'invadenza statuale che si concretizza in un controllo sempre più globale sulla vita di chi è sempre più «suddito» e sempre meno «cittadino»? Già il ben noto «Echelon» è un sistema di sorveglianza globale che surrettiziamente controlla le comunicazioni, analogiche e digitali, e i flussi di dati che attraversano il mondo; addirittura il progetto dell'*Information Awareness Office*, portato avanti dagli Stati Uniti, è finalizzato ad un controllo senza precedenti di tutto quanto avviene nel mondo, cagionando una lesione della *privacy* senza precedenti[4]. Una corretta applicazione delle tecniche di crittografia può dunque porre un freno ad una invadenza statuale che, nonostante la sua illegittimità, non solo continua a persistere, ma è addirittura in espansione.

2. CENNI SULLA REGOLAMENTAZIONE DELLE TECNICHE DI CRITTOGRAFIA

Le comunicazioni interpersonali non dovrebbero essere dunque

[4] Sull'Information Awareness Office sia consentito rinviare, per maggiori approfondimenti, a: G. FIORIGLIO, *La privacy e i sistemi di controllo di intercettazione globale: il caso dell'Information Awareness Office*, in *L'ircocervo*, http://www.lircocervo.it/NotiziaStandard.asp?IDNotizia=17122&IDCategoria=5737.

sottoposte a controlli, nel rispetto della *privacy* di tutti; ciononostante, non tutte le tecniche di crittografia sono utilizzabili nei vari stati, proprio perché esse sono così efficaci da vanificare eventuali attività di intercettazione, tanto che gli strumenti di crittografia sono considerati *dual-use good*, al contempo mezzi di protezione della riservatezza e strumenti militari. L'attività in tal senso è caratterizzata da una spiccata internazionalizzazione, come nel caso del *Coordinating Committee for Multilateral Export Control* (COCOM), organizzazione creata nel 1950 al fine di assicurare un mutuo controllo dell'esportazione di prodotti strategici e tecnologie. Essa comprendeva diciassette stati: Australia, Belgio, Canada, Danimarca, Francia, Germania, Giappone, Grecia, Italia, Lussemburgo, Norvegia, Olanda, Portogallo, Regno Unito, Spagna, Stati Uniti d'America, Turchia, mentre i membri cooperativi erano Austria, Finlandia, Hong Kong, Irlanda, Nuova Zelanda, Svezia e Svizzera. Nel 1991 il COCOM consentiva l'esportazione del *software* di crittografia nel mercato di massa, fatta eccezione per alcuni Paesi ritenuti sostenitori di organizzazioni terroristiche (come Iraq, Libia e Corea del Nord). Tale regolamentazione era tuttavia ritenuta troppo permissiva dagli U.S.A., ove gli strumenti di crittografia forte (cioè con codifica superiore ai 40 *bit*) venivano considerati pericolosi tanto quanto i dispositivi bellici. Successivamente, la fine della Guerra Fredda ed il bisogno di porre in essere nuovi accordi per affrontare i problemi per la sicurezza nazionale ed internazionale dovuti alla diffusione di armi convenzionali e di tecnologie ed oggetti a duplice uso, spingevano il 16 novembre 1993 i paesi membri del COCOM a sciogliere l'organizzazione al fine di costituire un nuovo accordo multilaterale, inizialmente denominato

«New Forum», cui si aggiungevano, in seguito, anche Austria, Finlandia, Irlanda, Nuova Zelanda, Svezia e Svizzera. Il 29 e il 30 marzo 1994 a Wassenaar, in Olanda, si confermava questa scelta, provocando lo scioglimento del COCOM avvenuto il 31 marzo 1994.

Nel 1996 veniva finalmente adottato il *Wassenaar Arrangement On Export Controls for Conventional Arms and Dual-Use Goods and Technologies*, sottoscritto da Argentina, Australia, Austria, Belgio, Bulgaria, Canada, Danimarca, Federazione Russa, Finlandia, Francia, Germania, Giappone, Grecia, Irlanda, Italia, Lussemburgo, Norvegia, Nuova Zelanda, Olanda, Polonia, Portogallo, Regno Unito, Repubblica Ceca, Repubblica di Corea, Romania, Slovacchia, Spagna, Svezia, Svizzera, Turchia, Ucraina, Ungheria, U.S.A. L'Accordo è finalizzato alla promozione della sicurezza e della stabilità nazionali ed internazionali, incentivando la trasparenza e responsabilizzando le attività di esportazione di armi convenzionali e di beni e tecnologie a duplice uso, così da prevenire squilibri potenzialmente destabilizzanti.

Nell'Unione Europea, fra gli altri, bisogna menzionare la *Council Regulation 22 June 2000, n. 1334 setting up a Community regime for the control of exports of dual-use items and technology*, la quale consente la libera circolazione dei sistemi di crittografia fra i vari Stati membri, fatta eccezione per sistemi di crittoanalisi più sofisticati, per i quali è necessaria una particolare autorizzazione. Una *Community general export authorisation* è invece necessaria per l'esportazione di tali sistemi verso Australia, Canada, Giappone, Norvegia, Nuova Zelanda, Polonia, Repubblica Ceca, Svizzera, Ungheria e U.S.A. In termini generali, l'UE persegue una politica improntata alla creazione di linee guida che lascino liberi gli Stati

membri di regolamentare autonomamente la crittografia e le sue applicazioni pratiche; quasi tutti i singoli stati, tuttavia, si sono più o meno pedissequamente adeguati alle indicazioni comunitarie ed internazionali[5].

3. IL PGP (PRETTY GOOD PRIVACY) E IL CASO ZIMMERMANN

Fino a pochi anni fa i sistemi di crittografia erano prerogativa di organizzazioni statuali e venivano creati per lo più a fini militari, per cui gli studi in tal senso erano protetti dal massimo riservo ed anche oggi i sistemi utilizzati dagli enti governativi sono basati su algoritmi che non vengono resi pubblici. Nel 1991, tuttavia, venne diffuso liberamente su Internet un *software* rivoluzionario: *Pretty Good Privacy* (PGP), un programma che tuttora utilizza algoritmi pubblici, ampiamente conosciuti e studiati, e ciononostante riesce a garantisce un ottimo livello di sicurezza. PGP non presenta difetti evidenti, perché essi sarebbero dovuti venire alla luce dopo anni di studio di un *software* che è stato distribuito liberamente, senza i vincoli imposti dalle aziende del settore, che vogliono generalmente impedire l'analisi del codice dei propri prodotti. Al contrario, questo programma è stato sin da subito distribuito congiuntamente ai propri sorgenti ed il suo sviluppo avviene in un continuo dialogo con la comunità degli utenti. Esso consente altissimi

[5] G. ZICCARDI, *Crittografia e diritto. Crittografia, utilizzo e disciplina giuridica documento informatico e firma digitale segretezza delle informazioni e sorveglianza globale*, Torino, 2003, cui si rinvia anche per maggiori approfondimenti sulle tematiche in oggetto. Cfr., inoltre, C. SARZANA DI S. IPPOLITO, *Le iniziative internazionali in tema di sistemi crittografici con riferimento alla tutela dei dati personali*, in *Dir. inf.*, 1998, 1, pp. 1-13.

livelli di protezione delle informazioni, tanto da aver suscitato notevoli preoccupazioni all'interno del governo statunitense dell'epoca, sfociate in duri attacchi legali nei confronti di Zimmermann[6].

Le indagini nei suoi confronti iniziarono nel 1993 e terminarono nel 1996. In quegli anni c'era stata una forte mobilitazione generale a favore di Zimmermann, al quale fu assicurata una difesa legale soprattutto grazie all'interesse di varie organizzazioni umanitarie. Egli era stato accusato di aver violato le norme in tema di esportazione di prodotti *dual-use*, in quanto il sistema PGP è un sistema di crittografia forte, dunque sottoposto a stringenti vincoli di distribuzione. Il punto principale è che questo *software* era stato posto su *USENET* da un utente anonimo, la cui identità non è mai stata scoperta. Una volta che il programma ha iniziato a circolare nulla ne ha più potuto fermare la diffusione, in ragione delle caratteristiche intrinseche della trasmissione di dati informatici, i quali sono (di base) duplicabili all'infinito, e bloccare la diffusione di un determinato *file*, una volta che questo è stato immesso su Internet, è praticamente impossibile, sia per l'elevatissimo numero di persone che possono accedervi, sia per la de-territorializzazione che costituisce una caratteristica fondamentale della Rete, per cui gli Stati Uniti non potrebbero (in punto di diritto) imporre le proprie leggi al cittadino di un altro stato (sempre rimanendo fermo il principio che impedire la diffusione di un *file* già immesso *on line* è *di fatto* impossibile). Ad ogni modo, non si può ritenere che l'immissione del *software* in

[6] Zimmermann si è laureato nel 1978 in *computer science* presso la *Florida Atlantic University*. Nel 1996, al termine delle sua vicende legali, ha fondato la PGP Inc, poi acquistata nel dicembre 1997 dalla Network Associates Inc e nel 2002 dalla PGP Corporation, per la quale oggi svolge le attività di consigliere straordinario e di consulente, oltre ad essere membro dello Stanford Law School's for Internet and Society ed a lavorare come consulente per altre società esterne.

questione su un computer posto in Rete integri gli estremi della esportazione, a meno di fornire una lettura estensiva delle norme in questione, che non sembra tuttavia accettabile in disposizioni tese comunque a limitare attività espressive dell'ingegno umano e finalizzate, oltretutto, alla tutela di diritti fondamentali. Inoltre, Zimmermann aveva sempre negato di aver reso disponibile il proprio *software* sul *USENET*, né erano state fornite prove in senso contrario.

La posizione del governo statunitense era comunque debole, tanto che in realtà non venne mai formalmente intrapresa un'azione legale nei confronti di Zimmermann. Nel 1996, infatti, i procuratori Michael J. Yamaguchi and William P. Keane dichiaravano che l'*U.S. Attorney's Office in the Northern District of California* non avrebbero proceduto legalmente nei confronti di Zimmermann per l'immissione del programma PGP su USENET, senza tuttavia spiegare le motivazioni alla base di questa decisione. Bisogna comunque considerare che un'eventuale sconfitta in giudizio avrebbero comportato gravissime conseguenze per gli Stati Uniti, che, come noto, sono un ordinamento di *common law*, per cui un eventuale precedente in tal senso avrebbe avuto una forza dirompente anche per casi simili; inoltre, Zimmermann era sostenuto da numerosissime persone, dunque la scelta di non proporre un'azione nei suoi confronti forse rispondeva a motivi politici in senso stretto ed alla paura di rischiare una sconfitta nelle aule di giustizia.

CAPITOLO 6

INTERNET E PROBLEMATICHE GIURIDICHE

1. ASPETTI GENERALI

La rete Internet ha avuto uno sviluppo repentino e forse inimmaginabile: nata quale strumento militare, in pochi anni è diventata risorsa di uso comune e fonte di inesauribile conoscenza, in quanto permette la diffusione in tutto il mondo di idee, proprie ed altrui, e dunque consente una libertà praticamente infinita di informare ed informarsi.

Fino a pochi anni fa, infatti, la diffusione delle informazioni era deputata ai *mass media* tradizionali, ossia ai sistemi radio-televisivi ed alle riviste e ai quotidiani, con la conseguenza di dover effettuare un vaglio di ciò che si poteva o doveva far conoscere; tali mezzi sono inoltre caratterizzati da univocità, relegando l'ascoltatore, lo spettatore od il lettore a meri recettori passivi di informazioni, mentre la Rete consente l'interazione dell'utente con la realtà virtuale che gli si pone davanti, offrendo una prima impensabile possibilità di dialogo e di confronto fra soggetti lontani sia dal punto di vista meramente fisico che culturale.

L'espansione di Internet e la facilità, oltre che l'economicità, di poter usufruire di servizi e di offrirne di ulteriori consentono di superare quelle difficoltà di ordine pratico connesse ai tradizionali sistemi di trasmissione delle informazioni, ma pongono tuttavia problematiche

nuove, le quali si presentano stimolanti per lo studioso, difficoltose per gli operatori del diritto (giudici ed avvocati), rischiose per l'uomo comune.

Bisogna infatti considerare che alla grande libertà di cui tutti possiamo godere, purché dotati di un *computer* (anche di modesta potenza elaborativa) e di una connessione alla Rete, fa tuttavia da contraltare il rischio di lesione di diritti, nostri ed altrui, fra cui spicca certamente il diritto alla *privacy*. Una condotta delittuosa, infatti, se si concretizza nell'illecita diffusione di informazioni di qualsiasi tipo, che sarebbero dovute rimanere riservate, quando viene posta in essere su Internet esce dalla sfera di controllo del soggetto agente e la diffusione di tali dati è potenzialmente illimitata, senza che, di fatto, nessuno possa eliminare le conseguenze lesive del fatto o limitarne l'incidenza. A ben vedere, comunque, proprio gli Stati nazionali, ossia quei soggetti che dovrebbero garantire il rispetto dei diritti dei propri cittadini, sono i primi a calpestarli, tra l'altro non in nome di pretese ideologie, ma addirittura per trarne (illecito) profitto, come già è successo con vari sistemi di controllo e di intercettazione, dei quali il più noto è certamente Echelon.

La crisi delle odierne democrazie rappresentative e la conseguente sfiducia dei governati nei confronti dei governanti fanno agevolmente comprendere che si diffonde un bisogno di legalità e difficilmente si vuole continuare a sottostare a pretese illegittime e finalizzate al tornaconto personale di pochi soggetti, come probabilmente avverrà con la realizzazione del progetto «Palladium»[1] e dell'Information Awareness

[1] Il *Palladium* è un sistema che in futuro potrebbe essere implementato su qualsiasi sistema informatico, allo scopo di controllarne l'utilizzo, consentendo l'utilizzo delle sole risorse autorizzate (*trusted*) ed impedendo l'accesso a tutto quanto non sia

Office[2] e come è reso evidente dal *modus operandi* della RIIA nella lotta alle violazioni del diritto d'autore: essa, infatti, intercetta le comunicazioni *on line* ritenute sospette al fine di risalire ai navigatori che potrebbero porre in essere condotte lesive del diritto d'autore, realizzando tuttavia un illecito ben più grave di quelli che vorrebbe punire, perché un'attività di intercettazione di flussi di dati viola la sfera privata del soggetto intercettato e non può, in linea di principio, essere svolta neanche dalle forze dell'ordine senza una preventiva autorizzazione dell'autorità giudiziaria, proprio perché incide su un diritto inviolabile dell'uomo. Del resto, risalire agli autori degli illeciti implica necessariamente un controllo su tutti i navigatori, compresi coloro che mai hanno posto in essere condotte lesive del diritto d'autore, poiché altrimenti non sarebbe possibile giungere all'individuazione dei sospetti.

Del resto, le frequenti istanze di «criminalizzazione» di Internet mirano a cercare di porre un freno a quella libertà senza precedenti di cui oggi gode l'uomo e a ristabilire un controllo statuale sulla diffusione delle proprie idee e sulle attività svolte *on line* da cittadini di qualsiasi stato, anche diverso da quello di appartenenza del navigatore. L'annullamento delle distanze ha difatti messo in crisi i tradizionali ambiti di giurisdizione

---

preventivamente vagliato dal consorzio TCPA (*Trusted Computing Platform Alliance*, composto dalle maggiori aziende del settore dell'*information techonology*). Non sarebbe addirittura consentito l'accesso ai siti *web* che non siano *trusted*, con una ovvia limitazione del diritto alla libertà informatica di tutti.

[2] L'*Information Awareness Office* è un progetto portato avanti negli Stati Uniti, finalizzato alla realizzazione del più completo ed avanzato sistema di intercettazione mai creato, rendendo possibile la videosorveglianza globale e l'acquisizione di qualsiasi tipologia di dati, ivi comprese le informazioni biometriche. Sul punto sia consentito rinviare a G. FIORIGLIO, *La privacy e i sistemi di controllo di intercettazione globale: il caso dell'Information Awareness Office*, in *L'ircocervo*, 2003, 2, sez. leg.

statuale, provocando, quale reazione, l'anzidetta pretesa di controllo ben al di fuori dei normali limiti di competenza nazionale, la quale provoca poi, in alcuni casi, fenomeni di disobbedienza civile elettronica[3], riconducibili, talvolta, ai c.d. *hackers*, che non sono certo dei criminali, al contrario dei c.d. *crackers*, ossia coloro che commettono crimini informatici.

Non si può e non si deve, comunque, né criminalizzare né censurare Internet: il Web deve rimanere libero, pur considerando che le condotte che si realizzano nel *cyberspace* si riverberano nel mondo materiale e che dunque una regolamentazione, per quanto minima, debba esserci. Non si può tuttavia centralizzare questa immensa risorsa, il cui punto di forza è proprio la decentralizzazione, che impedisce, in linea generale, la possibilità di instaurare un monopolio teso al controllo globale dei flussi dati che viaggiano sulla Rete. In particolare, il carattere di universalità del *World Wide Web*, che non si identica con l'intera Rete, ma che ne costituisce una componente oggi primaria, è stato acquisito proprio grazie all'assenza di un controllo centrale, che avrebbe potuto limitarne la crescita e con essa le potenzialità di mezzo di espressione del pensiero umano.

È di tutta evidenza, pertanto, che l'importanza di Internet va ben oltre quella di una qualsiasi altra invenzione: a memoria d'uomo, nulla ha permesso di creare quella sorta di universo parallelo in cui essa si concretizza[4]. Difatti, la crescita del cyberspazio corrisponde "a un

[3] Sulla disobbedienza civile (compresa quella elettronica) v. T. SERRA, *La disobbedienza civile. Una risposta alla crisi della democrazia?*, Torino, 2002.

[4] "La rivoluzione in atto non trova le sue radici in movimenti culturali, filosofici o politici (sebbene, come era facile prevedere, abbia dato luogo a movimenti di tal fatta), in quanto essa è determinata, più semplicemente, dall'utilizzazione diffusa del

desiderio di comunicazione reciproca e d'intelligenza collettiva"; esso "non è una particolare infrastruttura tecnica di telecomunicazione, ma una certa maniera di servirsi delle infrastrutture esistenti, per quanto imperfette siano. […Esso...] mira, attraverso collegamenti fisici di qualsiasi genere, *a un tipo particolare di rapporto tra le persone*"[5]. Questo rapporto è nuovo, può costituire un nuovo terreno di dibattito e di confronto fra persone e culture diverse, grazie all'abbattimento delle distanze, e può contribuire alla nascita di vere e proprie comunità, formate dagli individui più diversi, resi simili dal perseguimento di un obiettivo comune.

2. NASCITA ED EVOLUZIONE DI INTERNET

Ricostruire la storia di Internet, partendo dai primordi per arrivare

---

nuovo strumento di comunicazione (il *medium* […]). È forse la prima volta nella storia recente dell'umanità che un'innovazione di processo influenza in modo tanto diretto i comportamenti umani al punto di determinare così importanti trasformazioni culturali e sociali" (F. DI CIOMMO, *Internet e crisi del diritto privato: tra globalizzazione, dematerializzazione e anonimato virtuale*, in *Riv. crit. dir. priv.*, 2003, 1, p. 122).

[5] P. LÉVY, *Cybercultura. Gli usi sociali della nuova tecnologia*, tr. it, Milano, 2001, p. 120. Paul Virilio si pone in senso contrario ed afferma, fra l'altro, che "i più giovani, […] incollati allo schermo fin dalla scuola materna, sono già colpiti da disturbi ipercinetici dovuti a una disfunzione del cervello che genera un'attività sconnessa, gravi disturbi dell'attenzione, brusche scariche motorie incontrollabili. Aspettando, con la banalizzazione dell'accesso alle autostrade dell'informazione, la moltiplicazione dei viaggiatori a domicilio, questi lontani rampolli del lettore silenzioso, che soffriranno da soli dell'insieme dei disturbi della comunicazione, acquisiti nel corso degli ultimi secoli dalla tecnica" (*La bomba informatica*, tr. it., Milano, 2000, p. 37). Tuttavia, l'osservazione empirica della realtà, per quanto non ci offra un quadro idilliaco dell'umanità odierna, consente, per fortuna, di ritenere eccessive e generalizzanti queste affermazioni, che probabilmente costituiscono più che altro una forte provocazione ed una denuncia verso uno sviluppo tecnologico a volte più involutivo che evolutivo, perché non finalisticamente orientato ma fine a sé stesso, nel cui ambito spesso ciò che è realizzabile è lecito proprio perché è realizzabile.

sino agli ultimi sviluppi, è compito improbo e dalle molteplici impostazioni: bisognerebbe infatti analizzare non solo i motivi politici, ma anche la passione e gli ideali che hanno spinto gli scienziati statunitensi a creare quel sistema che avrebbe poi rivoluzionato il mondo. Un'analisi completa richiederebbe, dunque, di analizzare le vicende relative ad Internet da più punti di vista: politico, sociologico, tecnico, giuridico, ma in questa sede si ritiene più utile fornire delle nozioni di base e accennare a quei testi il cui esame appare imprescindibile per l'approfondimento di tematiche assai interessanti[6].

Le basi per lo sviluppo tecnologico che avrebbe poi portato alla realizzazione della Rete sono state poste nel 1958, nel periodo della «guerra fredda», con la costituzione dell'*Advanced Research Projects Agency* (ARPA[7]) da parte degli Stati Uniti, allo scopo di stimolare la ricerca scientifica anche in ambito militare nonché di ristabilire la supremazia tecnologica nei confronti dell'Unione Sovietica, che un anno prima aveva messo in orbita il satellite spaziale *Sputnik*.

Nel 1962 Jack Ruina, all'epoca direttore dell'ARPA, chiamava Joseph Carl Robnett Licklider (detto «Lick») alla guida dell'*Information Processing Techniques Office* (IPTO), che avrebbe fornito un apporto determinante per la progettazione e lo sviluppo della rete che oggi è Internet. Già nel medesimo anno, infatti, l'illustre studioso parlava di un «*galactic network*», ossia di un insieme di computer interconnessi cui sarebbe stato possibile accedere da qualsiasi luogo.

Nello stesso anno si verificava anche la crisi cubana e si riteneva

[6] Sulla storia di Internet v.: C. GUBITOSA, *La storia di Internet*, Milano, 1999; sulla storia del *World Wide Web* v. T. BERNERS-LEE, *L'architettura del nuovo Web*, tr. it, Milano, 2001.
[7] Oggi *Defense Advanced Research Projects Agency* (DARPA).

assai probabile lo scoppio di una guerra nucleare, per cui l'*U.S. Air Force* incaricava Paul Baran[8], del RAND, di progettare un sistema di comunicazioni che potesse funzionare anche in caso di guerra e che dunque potesse sopportare eventuali danneggiamenti. Un risultato fondamentale di tali studi è da individuarsi nella progettazione della c.d. «commutazione di pacchetto» (*packet switching*), ossia la possibilità di suddividere un messaggio in più parti («pacchetti»), inviabili separatamente, con la conseguenza di non dover occupare una intera linea di collegamento per la trasmissione di dati, i quali così viaggiano in parallelo. Nello stesso periodo il *packet switching* veniva teorizzato anche da Leonard Kleinrock[9], del MIT (*Massachusetts Institute of Technology*), e da Donald Davies, del *National Physical Laboratory* (NPL) inglese. È alquanto singolare che le ricerche sul punto vennero portate avanti parallelamente (e su presupposti diversi) senza che i ricercatori del RAND, del MIT e del NPL avessero notizia dei reciproci progetti.

Al progresso degli studi sinora menzionati si accompagnava l'evoluzione del progetto del *galactic network* di Licklider, portato avanti dal suo successore Lawrence G. Roberts, ricercatore al MIT. Nel 1967 Roberts presentava pubblicamente il progetto «ARPAnet», suscitando reazioni contrastanti ed ottenendo altresì alcune importanti adesioni al progetto, come quella di Douglas Engelbart (poi noto anche per la creazione del *mouse*) dello Stanford Research Institute.

Nel 1969 lo Stanford Research Institute e le Università dello Utah

---

[8] P. BARAN, *On distributed communications*, 1964, oggi in http://www.rand.org/publications/RM/baran.list.html.

[9] L. KLEINROCK, *Information Flow in Large Communications Nets*, Proposal for a Ph.D Thesis, Cambridge, 1961, reperibile in http://www.lk.cs.ucla.edu/LK/Bib/REPORT/PhD/.

e della California (a Los Angeles e a Santa Barbara) aprivano quattro nodi stabilendo una connessione e denominando ARPAnet la rete così ottenuta. In particolare, la prima connessione veniva effettuata fra l'Università della California a Los Angeles, sotto la guida di Kleinrock, e lo Stanford Research Institute, sotto la guida di Engelbart.

Negli anni settanta il DARPA continuava a sostenere ARPAnet, finanziando le ricerche necessarie per perfezionarne il funzionamento. Tali sforzi venivano progressivamente premiati, e in tal senso è di fondamentale importanza la creazione del protocollo TCP/IP (sviluppato, fra gli altri, da Bob Kahn e da Vinton Cerf), che sostituiva il protocollo di rete utilizzato dal 1970 sino a quel momento, denominato *Network Control Program* (NCP). Nel 1983 il TCP/IP veniva adottato come *Military Standard* (MIL STD) e veniva prescritto il suo utilizzo su tutti i *server* della rete. Per agevolarne la diffusione, il DARPA sosteneva economicamente la creazione della ditta «Bolt Boranek and Newman Inc.» (BBN) affinché il TCP/IP venisse implementato nel sistema operativo BSD Unix. Nello stesso anno ARPAnet veniva divisa in MILNET e in una ARPAnet di minori dimensioni e veniva utilizzato il termine Internet per designare l'intere rete (ossia MILNET e ARPAnet), cui nel 1985 si univa NSFnet, creata dalla *National Science Foundation* (NSF).

La NSF voleva rivoluzionare il modo di intendere la Rete, consentendo l'interconnessione fra gli elaboratori di tutti gli scienziati statunitensi. Per questo motivo nel 1987 creava una nuova e più veloce struttura centrale di collegamento (*backbone*), creando inoltre reti regionali e locali. La velocità del *backbone* della NSF aumentava vertiginosamente

in pochissimi anni: 56 Kbps nel 1986, 1.5 Mbps (T1) nel 1988, 45 Mbps (T3) nel 1990.

Nel 1986, intanto, era stato attivato il primo nodo Internet in Italia presso il CNUCE (Centro Nazionale Universitario per il Calcolo Elettronico): per il collegamento internazionale veniva utilizzato un canale satellitare da 64 Kb/s, condiviso fra cinque stazioni terrestri. L'anno successivo iniziava la cooperazione fra CNR, INFN, ENEA, CILEA, CINECA, CSATA, che avrebbe poi portato alla formazione del "Gruppo Armonizzazione Reti per la Ricerca" (GARR). Al fine di potenziare la rete scientifica italiana, nel 1989 veniva finanziato il progetto di creazione di una dorsale italiana da 2 Mb/s, attivata l'anno successivo.

Proprio in quegli anni avveniva la vera svolta nell'evoluzione della Rete, con una crescita esponenziale del numero degli elaboratori collegati ad Internet; un primo cambiamento epocale si verificava nel 1990, da un lato con la chiusura di ARPAnet, dall'altro con la creazione di *World comes on-line*, il primo fornitore (*provider*) privato di accesso ad Internet per mezzo della normale connessione telefonica.

Fra il 1990 e il 1991 Tim Berners-Lee, del CERN (*Conseil Européen pour la Recherche Nuclèaire*), creava il *World Wide Web*, rendendo semplice e veloce la consultazione dei documenti posti su Internet. L'illustre studioso partiva dal presupposto che tutti i computer fossero interconnessi e programmati in modo tale da consentire la condivisione e il reperimento delle informazioni contenute in essi, creando così una rete di informazioni. Per definire il suo progetto avrebbe utilizzato "un termine usato in matematica per denotare un complesso di nodi e maglie

in cui ogni nodo può essere collegato a un altro, […che] rifletteva la natura distribuita delle persone e dei computer che il sistema poteva mettere in collegamento, offrendo la promessa di un sistema potenzialmente globale": WWW, *World Wide Web*[10]. Berners-Lee realizzava così un linguaggio ipertestuale (l'HTML, *HyperText Markup Language*), in modo da permettere una lettura non sequenziale delle informazioni contenute in ciascun computer connesso alla Rete e da consentire il passaggio da un computer all'altro mediante i *link* (collegamenti) esterni, mentre i documenti sono identificati da un *Uniform Resource Locator* (URI)[11], grazie al quale essi sono reperibili da chiunque sia *on line*: l'URL svolge nel *web* la stessa funzione svolta da un indirizzo nel mondo fisico e consente di specificare quale protocollo debba essere utilizzato e dove trovare la risorsa utilizzata[12]. Veniva inoltre sviluppato un *software* (il c.d. *browser*[13]) che consentiva di leggere e scrivere le pagine in formato HTML nonché di navigare nel *web* grazie al protocollo HTTP (*HyperText Transfer Protocol*), ossia il protocollo grazie al quale i diversi sistemi possono dialogare e mediante il quale avviene il trasferimento dei dati da un computer all'altro.

---

[10] T. BERNERS-LEE, *op. ult. cit.*, p. 34.

[11] In realtà Tim Berners-Lee aveva proposto l'utilizzo dell'espressione *«Universal Resource Identifier»*, ma si erano levate proteste da parte di alcuni componenti della IETF (*Internet Engineering Task Force*) a causa del termine «Universal», per cui si decise di utilizzare l'espressione citata nel testo.

[12] Un esempio di URI: "http://www.parlamento.it/senato.htm". Le prime lettere dicono al *browser* quale protocollo di comunicazione è utilizzato, la parte "www.parlamento.it" identifica il *server* ove reperire il documento, mentre "senato.htm" è il documento specifico contenuto nel *server*. La prima parte è separata dai due punti e dal doppio *slash* (/), mentre gli *slash* singoli che seguono separano le singole parti; all'interno del *server* i *file* e le *directory* sono dunque disposti ad albero.

[13] Il primo *browser web* è stato creato da Berners-Lee su un elaboratore NeXT e denominato "WorldWideWeb".

Alla decentralizzazione del *Web* si contrapponeva e si contrappone tuttora la centralizzazione dell'attività di assegnazione dei «nomi di dominio», ossia dei nomi di un servizio, di un sito *web* o di un computer, inserito in un sistema gerarchico di autorità delegata detto *Domain Name System* (DNS). Tali nomi sono assegnati dalla IANA (*Internet Assigned Numbers Authority*, http://www.iana.org), privatizzata nel 1998 per scelta del governo statunitense (v. *infra*).

Ai primi *browser* inizialmente sviluppati (nel 1993 erano già più di cinquanta) faceva seguito (nel febbraio del 1993) il «Mosaic», sviluppato da Marc Andreessen, studente nel National Center for Supercomputing Applications (NCSA). Andreessen si era dimostrato molto attento alle esigenze degli utenti, riuscendo così a creare un *software* assai semplice da utilizzare; gli sforzi profusi nella sua creazione non sarebbero stati vani, perché nel 1994 il gruppo di ricerca confluiva in una nuova azienda denominata «Netscape», che nello stesso anno (il 15 dicembre) presentava un nuovo *browser* denominato «Navigator», distribuito gratuitamente su Internet[14].

Nell'ottobre del 1994, in seno al CSL (*Computer Science Laboratory*) del MIT, Berners-Lee fondava il World Wide Web Consortium (W3C, http://www.w3.org), allo scopo di "spingere il Web al suo pieno potenziale", sviluppando protocolli comuni che ne assicurino l'evoluzione e l'interoperabilità. Il W3C poteva inoltre godere dell'appoggio del DARPA, del CERN, della Commissione Europea e

[14] La scelta di distribuire gratuitamente il *software* evidenzia l'intento della Netscape di trarre profitto non dal «Navigator», ma piuttosto dalla pubblicità posta sul suo sito (che ovviamente costituiva la prima pagine cui il *browser* si connetteva, per quanto si potesse modificare tale opzione), compresa quella agli ulteriori servizi offerti (a pagamento) dalla Netscape.

dell'INRIA (*Institut National de Recherche en Informatique et en Automatique*).

Nello stesso periodo l'Università del Minnesota esprimeva l'intenzione di pretendere il pagamento di un canone da parte delle aziende private che utilizzavano «Gopher», con la conseguenza di decretarne l'abbandono da parte di questa fascia di utenza. Per evitare che anche la tecnologia alla base del Web potesse subire il medesimo destino, il CERN, accettando la proposta di Berners-Lee, permetteva a tutti di usare gratuitamente il protocollo e il codice del Web.

Dal 1995 la NSF non costituisce più la struttura centrale (*backbone*) primaria di Internet, che è oggi gestita da *provider* commerciali a livello nazionale (*tier-one*) e regionale, i quali gestiscono le infrastrutture. Gli *Internet service providers* (ISP) forniscono invece l'accesso locale e i servizi agli utenti. Le varie reti confluiscono poi nei *Network Access Point* (NAPs), ossia nei punti di interconnessione.

Nel 1998 la ICANN (*Internet Corporation for Assigned Names and Numbers*) ha preso il posto della IANA: è una organizzazione *no-profit*, che dunque gestisce l'attività relativa all'assegnazione degli indirizzi IP, sia con riferimento alla loro componente numerica che ai nomi a dominio[15] (ossia l'indirizzo espresso in lettere di una risorsa su Internet). In Italia tale attività è svolta dalla *Naming Authority*, che stabilisce le procedure operative, e dalla *Registration Authority*, detta anche *Italian Network*

[15] I domini sono suddivisi in più livelli: all'apice si trovano i domini di primo livello (*Top Level Domain*, TLD), a loro volta suddivisibili in domini di secondo livello, anch'essi ulteriormente suddivisibili secondo lo stesso criterio. Ad esempio, nell'indirizzo *web* «www.parlamento.it», «.it» rappresenta il TLD, «parlamento.it» il dominio di secondo livello. All'epoca di ARPAnet i TLD erano solo sette: «.com», «.edu», «.gov», «.mil», «.net», «.org», «.int». Successivamente sono stati creati i domini di primo livello nazionale (*Country Code Top Level Domain*, ccTLD), come «.it», «.de», cui se ne sono aggiunti altri, come «.biz», «.info», ecc.

Information Center (it-nic). Nel rispetto delle regole previste dalla *Naming Authority*, la *Registration Authority* assegna, gestisce e mantiene il database dei nomi a dominio.

Anche oggi Internet non è gestita a livello centrale, ma accanto ai soggetti sinora citati se ne pongono altri, che ne definiscono e gestiscono il funzionamento. Bisogna dunque ricordare l'*Internet Society* (ISOC, http://www.isoc.org) il cui scopo è facilitare lo sviluppo degli standard, dei protocolli e delle infrastrutture tecniche di Internet, grazie ad un dibattito aperto sulla sua evoluzione, in un ambiente caratterizzato da una cooperazione internazionale e nel rispetto del principio di un uso aperto e libero della Rete, respingendo dunque interventi regolamentativi censori che possano violare il diritto alla libera manifestazione del pensiero. Essa è stata fondata nel 1992, per fornire il supporto economico necessario allo sviluppo degli standard nel caso in cui i finanziatori avessero diminuito l'entità dei propri contributi. Nel suo ambito operano altre organizzazioni: l'*Internet Architecture Board* (IAB, http://www.iab.org), che monitorizza lo sviluppo di Internet ed effettua pianificazioni a lungo termine con riferimento all'evoluzione della sua struttura, oltre a coordinare i vari settori della IETF (v. *infra*); l'*Internet Engineering Steering Group* (IESG, http://www.ietf.org/iesg.html), che gestisce proceduralmente le attività tecniche dei gruppi, approva le specifiche e ne cura la pubblicazione; l'*Internet Research Task Force* (IRTF, http://www.irtf.org), che istituisce piccoli gruppi di ricerca che si occupano dell'evoluzione di vari aspetti tecnici della Rete, come i protocolli e la sua architettura; infine, l'*Internet Engineering Task Force* (IETF, http://www.ietf.org), creata nel 1986. La IETF organizza gli

incontri finalizzati alla realizzazione e alla discussione degli standard; essa è una comunità che si prefigge l'obiettivo di contribuire all'evoluzione di Internet. È suddivisa in otto aree tecniche, al cui vertice è posto un direttore di area (AD); gli AD sono membri dello IESG. Non ci si può iscrivere allo IETF, ma si può partecipare alle *mailing lists* e agli incontri, tenuti tre volte l'anno in posti diversi del mondo: infatti tutte le sue attività sono pubbliche ed aperte a tutti. I singoli lavori sono invece svolti da vari *working groups*, creati *ad hoc* per ciascun obiettivo specifico. Chi eccelle nelle attività e nei gruppi di lavoro dello IETF può essere eletto nello IAB e nello IESG. Le specifiche approvate nello IETF vengono pubblicate come *Requests for Comment* (RFC), e nel corso del loro sviluppo le versioni di lavoro divengono di pubblico dominio e prendono il nome di *Internet Drafts*, i quali durano sei mesi, dopo i quali possono essere rimossi, approvati come RFC o riproposti (anche se modificati). Le specifiche evolvono attraverso una serie di livelli conosciuti come *standard tracks*[16], e se una di esse viene diffusamente valutata in maniera

[16] Lo *standard track* si può così suddividere: *proposed standard* (specifica stabile, valutata positivamente dalla comunità di riferimento); *draft standard* (specifica di cui esistono almeno due implementazioni indipendenti ed interoperabili oltre ad un'esperienza positiva di usabilità ed utilità); *Internet standard* (specifica ampiamente e positivamente utilizzata, anche in virtù di un ampio raggio di implementazioni interoperabili). Le specifiche nello *standard track* possono essere *technical specifications* (inerenti protocolli, procedure, servizi, ecc.) o *applicability statement* (definisce come e quando bisogna utilizzare uno *standard* per fornire una certa caratteristica su Internet). L'applicabilità di uno *standard* viene classificata in tre livelli: *required* (lo *standard* è un elemento necessario per qualsiasi implementazione del TCP/IP); *recommended* (se ne consiglia l'implementazione che non è comunque obbligatoria); *elective* (la scelta sull'implementazione è opzionale). Inoltre, esistono tre *non-standard tracks*: *experimental* (il protocollo è utilizzato solo a fini di ricerca); *historic* (il protocollo è ormai obsoleto e se ne sconsiglia l'utilizzo); *informational* (fornisce informazioni di interesse generale per la comunità degli utenti di Internet, ma non ne definisce un protocollo *standard*).
Il processo di standardizzazione si articola nelle seguenti fasi: un AD raccomanda un gruppo di lavoro affinché la specifica entri nello standard track; il *working group*

positiva in base all'uso ed alle implementazioni che ne vengono fatte, diviene un *Internet Standard*.

3. INTERNET: ASPETTI TECNICI

L'analisi dell'effettivo funzionamento della rete Internet richiede conoscenze specifiche frutto di una preparazione, anche interdisciplinare, che normalmente il giurista non possiede, anche a causa dell'estrema rapidità con cui è avvenuta la rivoluzione tecnologica, che in pochi anni ha mutato la società. All'enorme diffusione dei *computers*, molti dei quali connessi alla Rete, si accompagna una molteplicità di fatti «avvenuti» nel *cyberspace* che producono conseguenze giuridicamente rilevanti. Non si può tuttavia guardare unicamente alla conseguenza della condotta, ma bisogna pure prendere in considerazione le modalità con cui essa si realizza, al fine di una corretta sussunzione del fatto entro le eventuali norme giuridiche applicabili.

Pertanto, affinché anche l'operatore del diritto possa interessarsi con cognizione di causa alla disciplina delle norme relative all'informatica, è assolutamente necessaria una conoscenza di base di alcuni elementi teorico-pratici di questa materia, e ciò sia in prospettiva *de jure condito* che *de jure condendo*, al fine di poter offrire una valutazione

---

elabora e pubblica la specifica come *Internet draft*, a disposizione di tutti per almeno due settimane; lo IESG stabilisce se la specifica è matura per un processo di raccomandazione; lo IETF effettua una revisione finale (*last call*); la specifica viene pubblicata come RFC e l'*Internet draft* viene rimosso; la specifica rimane *proposed standard* per almeno sei mesi e *draft standard* per almeno quattro, prima di poter diventare *Internet standard*; si associa un documento di applicabilità ad uno o più standard per determinarne *status* ed applicabilità (tali documenti vengono utilizzati anche per modificare od eliminare uno standard già approvato).

delle varie fattispecie basata non su preconcetti o convinzioni personali ma piuttosto sulla realtà, senza dover comunque prendere in considerazione quegli aspetti squisitamente tecnici che ovviamente costituiscono l'oggetto di studio di altre discipline.

Un'analisi, seppur sommaria, degli aspetti tecnici di Internet deve necessariamente partire dal concetto di rete, certamente non esclusivo del campo informatico: basti pensare alle reti elettriche o telefoniche. Una rete è composta da «nodi» e «connessioni» che legano due nodi, ognuno dei quali può avere più connessioni, che, a loro volta, possono essere fisiche o *wireless*. Proprio le reti elettriche e telefoniche sono esempi di reti del primo tipo, mentre quelle televisive e di telefonia mobile sono di tipo *wireless*.

Con precipuo riferimento alle reti che collegano i computer, bisogna primariamente distinguere fra reti «locali» (*Local Area Network*, LAN) e «geografiche» (*Wide Area Network*, WAN). Le LAN collegano elaboratori posti a distanza ridotta, ad esempio in un medesimo edificio, mentre le WAN collegano siti o reti geograficamente distanti: **Internet** è, dunque, una WAN che collega più LAN.

Gli elaboratori possono essere interconnessi mediante dispositivi che consentono la trasmissione e la ricezione di informazioni: ciò può avvenire sia mediante cavi di varia tipologia che tramite periferiche *wireless*. Nel primo caso la velocità sarà assai maggiore, ma ovviamente è necessario collegare materialmente le periferiche, mentre nel secondo basterà porre i dispositivi alla distanza corretta, tenendo presente che la qualità del segnale (e di conseguenza la velocità) diminuirà con l'aumentare della distanza.

Una volta realizzato il collegamento fra gli elaboratori è necessario che questi possano dialogare fra loro, sia per potersi reciprocamente «vedere» che scambiare dati; come l'uomo comunica con il linguaggio, cioè con un protocollo conosciuto fra chi dialoga, così i computer dialogano fra loro utilizzando un protocollo comune: nel caso di Internet, il TCP/IP (*Transmission Control Protocol/Internet Protocol*). Tale *standard* ha consentito una diffusione della Rete tanto capillare, perché è assolutamente indipendente dal modo in cui la rete è realizzata, sia a livello *hardware* che *software*, ed è inoltre uno standard aperto, utilizzabile senza limitazioni da chiunque su qualsiasi *computer* e su tutti i sistemi operativi, che oramai lo supportano in maniera nativa.

In Internet gli elaboratori devono poter essere identificati univocamente e ciò avviene mediante l'assegnazione di un indirizzo IP[17], composto da quattro triplette di numeri che arrivano, ciascuna, sino a 255. Il protocollo IP[18] consente la trasmissione di dati tra due computer

[17] Riguardo l'indirizzamento, bisogna sottolineare che "*a distinction is made between names, addresses, and routes. A name indicates what we seek. An address indicates where it is. A route indicates how to get there. The internet protocol deals primarily with addresses*" (RFC 791, september 1981, p. 6).

[18] Oggi questo protocollo è implementato nella sua versione 4, ormai in uso da più di vent'anni. Il suo problema principale è costituito dal limitato numero di indirizzi IP teoricamente disponibili, per cui nelle ricerche relative al suo sviluppo ci si è concentrati sul superamento di tale limite e si è giunti al c.d. IPv6, sviluppato nell'ambito della IETF. Prima della sua diffusione globale è prevista una fase transitoria in cui coesisteranno entrambe le versioni del protocollo, per giungere poi ad una graduale sostituzione della versione precedente. Nell'IPv4, il sistema di indirizzamento è definito da un numero di 32 bit che permette fino a 4.294.967.295 indirizzi e, come detto, l'indirizzo IP è rappresentato da quattro gruppi di numeri decimali di otto bit (*bytes*) divisi da punti; nell'IPv6 il numero di cui sopra passa da 32 bit a 128 bit (16 ottetti), rendendo così disponibile un numero enorme di possibili combinazioni (addirittura 340.282.366.920.938.463.463.374.607.431.768.211.456 indirizzi, ossia trecentoquaranta miliardi di miliardi di miliardi). Per quanto i circa quattro miliardi di indirizzi consentiti dall'IPv4 possano sembrare più che sufficienti per le esigenze attuali della società, bisogna considerare che il numero di quelli

identificati univocamente tramite l'indirizzo IP: tali dati sono suddivisi in pacchetti di una certa dimensione ai quali vengono assegnati gli indirizzi del mittente e del destinatario. Il protocollo TCP assicura l'arrivo a destinazione dei pacchetti inviati e verifica che i pacchetti ricevuti siano sistemati secondo l'ordine di trasmissione, provvedendo a riordinare quelli che non hanno seguito l'ordine corretto. Lo stesso protocollo garantisce, dunque, che la trasmissione sia andata a buon fine ed eventualmente chiede di nuovo quei dati che non sono giunti all'altro calcolatore, provvedendo, in ogni caso, a ricostruire l'esatta sequenza dei dati inviati dal mittente.

L'enorme espansione di Internet si è riverberata anche sulle reti locali, dal momento che nella maggior parte delle LAN viene utilizzato proprio il protocollo TCP/IP per permettere la comunicazione fra i

---

effettivamente utilizzabili è assai inferiore. L'indirizzo IP è suddiviso in due campi, dei quali l'uno identifica la rete, l'altro l'*host*. Gli indirizzi sono così divisi in tre classi principali (A, B, C), che si differenziano in base al numero dei *byte* utilizzati per identificare la rete e l'*host*. In particolare, nella classe A (rappresentata dagli indirizzi IP compresi tra 1.0.0.0 e 127.255.255.255) il primo *byte* identifica la rete, mentre i tre *byte* successivi identificano l'*host*. Si possono pertanto ottenere 127 reti, ciascuna costituita da 16.777.216 *host*. Nella classe B (costituita dagli indirizzi IP compresi tra 128.0.0.0 e 191.255.255.255) la rete è identificata nei primi due *byte*, mentre i due successivi fanno riferimento agli *host* per un totale di 16.384 reti composte da 65.536 *host*. Nella classe C (composta dagli indirizzi compresi tra 192.0.0.0 e 223.255.255.255) l'*host* è identificato solo dall'ultimo *byte* mentre i primi tre rappresentano la rete, per cui è possibile gestire 2.097.152 reti composte da 256 *host*. Le reti appartenenti alle suddette classi possono essere suddivise in sottoreti (*subnets*), al fine di agevolare le operazioni di *routing* e di gestione degli indirizzi, nonché per ottimizzare l'utilizzo degli indirizzi IP in ragione della loro intrinseca finitezza. La suddivisione di una rete in due o più sottoreti si esegue attraverso la *netmask*, che stabilisce quali indirizzi IP possono essere usati nelle sottoreti. Inoltre, sono stati predisposti alcuni indirizzi IP privati che non possono essere utilizzati dai vari *provider* (ossia 10.254.254.254, dal 172.16.0.0 al 172.31.254.254 e dal 192.168.0.0 al 192.168.254.254). Infine, alle tre classi citate se ne affiancano altre due (D, E): gli indirizzi di classe D identificano infatti un indirizzo *multicast* (nelle trasmissioni in *multicast* un solo *host* trasmette e tutti gli altri ricevono), mentre gli indirizzi di classe E sono utilizzati a fini sperimentali.

computer collegati, consentendo di superare i problemi di una eccessiva proliferazione di standard diversi, che consistono nella difficoltà di far dialogare sistemi differenti cui necessariamente consegue un aumento dei costi di configurazione e di gestione[19].

Attualmente, il protocollo TCP/IP è supportato da tutti i sistemi operativi (Windows, Linux, Unix, Macintosh), per cui il suo utilizzo rende possibile la comunicazione fra più computer aventi caratteristiche ben differenti. Anche il linguaggio con cui sono scritte le pagine *web* è comprensibile da elaboratori differenti, essendo oramai uno standard, seppur in lenta evoluzione: alcuni siti sono scritti in «Flash», che consente la creazione di effetti grafici molto avanzati, rendendo dunque la navigazione in Internet molto gradevole, ma la maggioranza dei siti è scritta in HTML (*Hypertext Markup Language*), un linguaggio ipertestuale. L'ipertesto presenta numerosi vantaggi rispetto al tradizionale metodo di predisposizione delle informazioni, come avviene, ad esempio, in un libro: utilizzando un ipertesto, infatti, il lettore può saltare da una parte all'altra del testo con un semplice *click* del mouse, saltando automaticamente quella mole di informazioni ritenute non rilevanti, mentre leggendo un libro si è vincolati ad una lettura sequenziale. È inoltre possibile spostarsi da un documento all'altro sempre con le stesse modalità: ad esempio, in un ipertesto dedicato al diritto civile, l'art. 2050 c.c. potrebbe essere collegato alle leggi che utilizzano il regime di responsabilità ivi delineato, come la legge sulla *privacy*, e da qui, eventualmente, essere collegati alla relativa giurisprudenza. Questo breve esempio permette di comprendere come un ipertesto possa rendere assai

[19] Fra i vari standard si possono qui ricordare: NetBEUI (IBM e Microsoft); IPX/SPX (Novell); AppleTalk (Apple).

più proficua un'attività di studio e di ricerca, automatizzando quelle attività collaterali che distraggono dall'obiettivo concreto e dunque consentendo di concentrarsi solo sull'aspetto centrale.

Quando tali informazioni sono accessibili *on line*, la loro consultazione è resa possibile mediante la connessione ad un sito *web*, che si verifica quando il proprio computer (detto *client*) si collega ad un altro elaboratore (detto *server*), nel quale sono memorizzate le pagine che si intende visitare. Il *World Wide Web* (WWW) non si identifica tuttavia con Internet, per quanto venga sovente utilizzato come sinonimo: rappresenta invece quella componente di facile accesso che ha grandemente contribuito alla diffusione della Rete e che la ha fatta diventare un ipertesto di infinite dimensioni.

Accanto al protocollo HTTP si pongono anche altre tipologie di interscambio dei dati (non sostitutivi del TCP/IP, cui si affiancano) come il *File Transfer Protocol* (FTP), il *Telnet*, il *Simple Mail Transfer Protocol* (SMTP). L'FTP rappresenta lo standard su Internet per il trasferimento di *file*, ossia la trasmissione di file completi da un sistema all'altro. Per poter accedere al sistema che ospita il *file* è necessaria un'autorizzazione preventiva, a meno che il server non sia impostato per consentire anche l'accesso anonimo come *guest*. Questo protocollo è supportato da pressoché tutti i sistemi operativi, per cui il trasferimento di *file* è possibile fra computer totalmente diversi, sia dal punto di vista *hardware* che *software*. Il *Telnet* consente ad un computer connesso ad un altro elaboratore di operare come un suo terminale ad esso direttamente collegato, permettendo di controllarlo in remoto[20]. Infine, l'SMTP è il

[20] Nei *software telnet* viene implementata l'emulazione di varie tipologie di terminali.

protocollo più utilizzato nell'ambito della posta elettronica e consente il trasferimento delle *e-mail* da un *server* di posta all'altro[21]. La posta elettronica, insieme al WWW, costituisce certamente una delle componenti fondamentali che ha contribuito all'odierna diffusione di Internet, perché ha consentito una celerità di comunicazione ed una flessibilità senza pari[22].

Alla riservatezza dei messaggi di posta elettronica si contrappone il carattere di pubblicità dei *«newsgroups»*, o «gruppi di discussione» o «*forum*», i quali consistono in una sorta di bacheca elettronica, in cui chiunque può, tramite elaboratore elettronico, leggere i messaggi apposti da altri utenti e aggiungere i propri contributi[23]; il loro numero è elevatissimo (svariate migliaia) e coprono argomenti di varia natura; si distinguono in moderati e non, a seconda della presenza o meno del c.d. moderatore, che analizza i messaggi in arrivo ed elimina gli interventi non in linea, per forma o contenuto, con le tematiche e i requisiti del

[21] Il funzionamento del protocollo SMTP è alquanto semplice: dopo la creazione di un messaggio di posta elettronica, ad esso viene apposto l'indirizzo di destinazione e subito inviato dall'applicazione locale (*Mail User Agent*) a quella SMTP, che memorizza il messaggio. Ad intervalli periodici il *server* controlla se ci sono nuovi messaggi da inviare e, in caso positivo, procede in tal senso. Se ciò non risulta possibile riprova per un certo numero di volte e se la situazione di impossibilità della consegna persiste, provvede alla cancellazione del messaggio oppure alla sua restituzione al mittente.

[22] Basti pensare alla possibilità di allegare *file* di qualsiasi tipo a ciascun messaggio, che giungono a destinazione in pochi secondi (il tempo varia, ovviamente, in relazione alla dimensione complessiva del messaggio nonché alla velocità del *server* e del *client*). Per inviare una *e-mail*, oltre, ovviamente, la connessione ad Internet, è necessario conoscere solamente l'indirizzo del destinatario (del tipo nome@host.it), similmente a quanto avviene con le spedizioni effettuate a mezzo del servizio postale.

[23] Si distinguono dalle *mailing lists* perché esse sono costituite da comunicazioni effettuate mediante posta elettronica, pertanto leggibili solo dagli iscritti (*subscribers*), mentre i messaggi inviati nei *newsgroups* sono leggibili da chiunque vi abbia accesso.

gruppo[24].

Fra le nuove frontiere bisogna citare i programmi di *file sharing* (condivisone di *file*), detti anche *software* di *peer to peer*. Essi consentono uno scambio diretto fra i *file* ospitati sulle macchine di ciascun utente e stanno diventando sempre più evoluti, grazie all'apporto di vere e proprie comunità di utenti che portano avanti l'idea della condivisione delle risorse. Il primo *software* di *file sharing* di massa è l'ormai celebre *Napster*, del 1999, assai primitivo se paragonato ai sistemi attuali: consentiva la sola condivisione di *file* musicali, divenuta possibile grazie alla nascita del formato *mp3*, che ne consente un'ottima compressione garantendo al tempo stesso un'eccellente qualità del *file* compresso, paragonabile alla qualità garantita dalla registrazione su supporti di tipo CD audio. Nei confronti di Napster è stata posta in essere una forte battaglia legale da parte delle *major* discografiche[25], ma dopo la sua

[24] Il protocollo utilizzato per la distribuzione dei messaggi nei *newsgroup* è detto *Network News Transfer Protocol* (NTTP). In linea di principio, i *newsgroup* sono ospitati su un unico elaboratore (*server*), al fine di limitare sia la circolazione di messaggi duplicati sia l'occupazione dello spazio su disco in tutti gli *host client*. Il computer centrale serve, generalmente, una cospicua fascia di utenza (ad esempio, tutti i clienti di un *provider*), consentendo l'accesso all'archivio dei messaggi e memorizzando quelli messaggi che gli vengono inviati via NTTP. Il medesimo protocollo è utilizzato dai vari *newsfeed* per realizzare l'interscambio dei messaggi ospitati da ciascuno di essi.

[25] Le varie *majors* stanno conducendo svariate battaglie legali non solo contro i produttori dei *software* in oggetto, ma hanno anche proceduto all'identificazione degli utenti sospettati di aver scambiato opere protette da *copyright*. Tale attività si è realizzata, per forza di cose, mediante un monitoraggio dell'attività degli utenti, ivi compresi coloro che mai hanno commesso illeciti; poiché l'intercettazione di flussi di dati è generalmente considerata un reato, in quanto lede la *privacy* individuale, risulta palese la ben più grave illiceità cui portano simili condotte, considerando che, sempre in linea di principio, la riservatezza è un diritto fondamentale dell'individuo, che non può sopportate lesioni generalizzate da parte di soggetti privati al di fuori del controllo dell'autorità giudiziaria, perché la sua violazione può essere disposta solo per gravi motivi, eventualmente qualora confligga con un diritto di rango pari o superiore.

chiusura sono stati creati altri programmi, ben più flessibili e non più basati su *server* centrali. Difatti, nonostante i *file* ospitati dagli utenti di Napster si trovassero sui propri computer, era stata creata una rete di *server* centrali che facevano da tramite fra gli utenti stessi. Con i moderni sistemi è possibile fare a meno dei *server* centrali, costituendo reti *server-less* o creando una galassia di *mini-server*, facendo sì, ad esempio, che ogni utente sia allo stesso tempo *server* e *client* oppure che un grosso numero di utenti faccia da *server*, in modo da essere difficilmente rintracciabili e dunque sottoposti a controlli, di per sé inefficaci, a meno di non controllare tutte le comunicazioni effettuate *on line* al fine di individuare quelle illecite, ledendo tuttavia la *privacy* di tutti coloro che vengono sottoposti ad indebiti controlli e dunque ponendo in essere un illecito ben più grave perché lesivo dei diritti fondamentali della persona.

4. I MOTORI DI RICERCA SU INTERNET

I motori di ricerca (o *search engines*) consentono di individuare pagine e/o siti *web* di interesse, mediante ricerche testuali o navigazione in categorie predefinite. Costituiscono uno strumento insostituibile per qualunque navigatore, posta l'immensità del *World Wide Web*, la cui fortissima espansione è dovuta in parte anche alla loro efficienza ed alla loro semplicità di utilizzo. Un sistema di ricerca è formato da tre componenti principali:

a) un sistema finalizzato alla ricerca ed all'analisi delle pagine *web*;

b) un archivio nel quale sono contenute le informazioni sulle pagine catalogate;
c) una interfaccia che consente la consultazione delle informazioni reperite.

Esistono tre tipologie di motori di ricerca: automatici (o *crawlers*), *directory engines* (o indici), *metacrawlers*. I primi sono basati su dei *software* (detti *spiders*, o *robots*, o *bots*) che automaticamente reperiscono pagine *web*, le analizzano e le classificano. In linea generale, l'utente può effettuare ricerche sui siti *web* mediante la digitazione dei termini di ricerca all'interno di un'apposita mascherina. L'utilizzo degli *spider* consente un aggiornamento costante del *database* che contiene l'elenco dei siti, ma sussiste il problema della precisione e dell'attinenza dei risultati dell'operato di tali *software*, che non sempre riescono a fornire una corretta classificazione dei siti. I *crawlers* si differenziano l'uno dall'altro per i criteri seguiti dai propri *spider*, criteri basati su algoritmi che non vengono resi pubblici e sovente modificati.

Fra i motori di ricerca automatici un posto di assoluto rilievo è occupato da «Google» (http://www.google.com), il cui indice contiene più di tre miliardi di URL. Il nucleo principale di *Google* è costituito da un particolare sistema di classificazione, detto «PageRank», sviluppato presso l'Università di Stanford da Larry Page e Sergey Brin. Tale sistema fa in realtà parte di una struttura più complessa, che oggi consente una classificazione di ottimo livello dei vari siti grazie all'utilizzo di una molteplicità di variabili che prendono in considerazione il contenuto delle singole pagine, i collegamenti ad un sito effettuati da altri siti

nonché il contesto in cui sono posti gli stessi *link*[26].

La seconda tipologia di motori di ricerca è costituita dai *directory engines*, nei quali la ricerca delle pagine da indicizzare non viene svolta in maniera automatizzata, ma viene effettuata manualmente da personale umano, che provvede a classificare i siti secondo le linee tematiche, offrendo all'utente finale la possibilità di fare ricerche mediante l'inserimento delle parole chiave nella mascherina di ricerca oppure di sfogliare le singole categorie, organizzate in classi tematiche e ripartite in altre sottoclassi secondo una classica suddivisione ad albero. Ovviamente, essendo basati su una valutazione umana, tali sistemi sono più precisi rispetto ai *crawlers*, ma questa maggiore accuratezza non consente né l'aggiornamento tanto rapido di cui possono invece fruire i secondi né una simile ampiezza di *database*[27].

Il più importante motore di ricerca in questa categoria è senza dubbio «*Yahoo*» (http://www.yahoo.com), creato nel 1994 da David Filo

[26] Più specificatamente, Google interpreta un collegamento dalla pagina A alla pagina B come un «voto» espresso dalla prima in merito alla seconda. Oltre al calcolo del numero dei voti così assegnati a una pagina, il sistema prende in esame la pagina che ha assegnato il voto, dando maggiore perso ai voti espressi da pagine c.d. «importanti». A tali siti, infatti, PageRank assegna un «voto» più elevato di cui Google tiene conto ogni volta che esegue una ricerca. A questo criterio «soggettivo» è affiancato da sofisticate procedure di ricerca testuale per il reperimento delle pagine rispondenti ai criteri di ricerca indicati, effettuando un'analisi contenutistica della pagina cercata nonché delle pagine ad essa collegate.
Oltre *Google* è doveroso menzionare anche *Altavista* (http://www.altavista.com), creato nel 1995 e subito divenuto famosissimo, fra l'altro, sia perché per la prima volta consentiva di formulare le interrogazioni secondo il linguaggio naturale e sia per la sua velocità nel fornire i risultati delle ricerche, dovuta alla potenza degli elaboratori utilizzati.

[27] Per quanto l'osservazione possa sembrare di scuola, è doveroso puntualizzare che, in astratto, i sistemi basati sulla valutazione umana potrebbero eguagliare o superare i *crawler*, a patto di utilizzare un numero enorme di persone deputate alla ricerca ed alla indicizzazione dei siti; ovviamente tale numero sarebbe così elevato da rendere praticamente irrealizzabile tale ipotesi.

e Jerry Yang dell'Università di Stanford. La disposizione dei siti all'interno delle *directory* di *Yahoo* è sempre stata svolta manualmente, mentre la possibilità di ricerca consisteva inizialmente in una ricerca semplice all'interno del *database*. Successivamente è stata automatizzata una parte del processo di raccolta e classificazione delle informazioni, rendendo più labile la distinzione fra le prime due categorie. Oggi *Yahoo*, ferma restando la suddivisione in *directory*, si affida a *Google* per l'effettuazione delle ricerche, mentre anche il secondo presenta una suddivisione per categorie, finalizzata alla realizzazione dell'*Open Directory Project*, ossia alla creazione della più completa *directory* del Web.

La terza categoria è quella dei *metacrawlers*, costituita da quei motori di ricerca che non hanno un proprio *database* da interrogare, ma che invece svolgono la propria attività sui motori di ricerca veri e propri. Pertanto, una volta inviata la *query*, il sistema provvede ad effettuare la ricerca simultaneamente su più motori di ricerca, comparando automaticamente i risultati di ciascuno e dunque consentendo, in linea teorica, di giungere ai migliori esiti. Il primo esempio di questa tipologia è proprio «Metacrawler» (http://www.metacrawler.com), creato nel 1994 da Erik Selberg e Oran Etzioni dell'Università di Washington e tuttora funzionante.

Emerge pertanto con chiarezza che la suddivisione tradizionale non consente di cogliere tutti gli aspetti dei moderni motori di ricerca, che oggi, per lo più, si caratterizzano per essere ibridi. Essi rappresentano il miglior mezzo per assicurare visibilità ad un sito, per cui essere elencati ai primi posti di una *directory* o comunque risultare sempre fra i risultati più rilevanti all'interno di un'ampia fascia di ricerche,

assume un rilievo economico non indifferente, tanto che per assicurarsi i primi posti in alcuni motori di ricerca bisogna retribuire chi li gestisce[28]. Ciò ovviamente comporta una elencazione non obiettiva e *Google* è da lodare anche in questo senso, perché, a quanto è dato sapere, la pubblicità si limita solo a dei piccoli spazi che non appesantiscono la navigazione né interferiscono coi risultati delle ricerche.

5. L'IMMATERIALITÀ E L'A-TERRITORIALITÀ DEL CYBERSPACE

Internet rappresenta un mondo parallelo, un mondo virtuale governato da «leggi» particolari: rappresenta dunque una rivoluzione, che ci impone di considerarla con un metro di giudizio diverso da quello comunemente utilizzato, che tenga conto delle sue caratteristiche peculiari, prime fra tutte l'**immaterialità** e l'**a-territorialità**. La prima è connaturata agli strumenti informatici, che permettono la digitalizzazione delle informazioni, e pertanto non è una caratteristica esclusiva della Rete, mentre la seconda rappresenta un cambiamento epocale.

L'evoluzione storica ha infatti evidenziato la forte relazionalità fra l'uomo e il territorio su cui vive, che ha comportato lo sviluppo di differenti ceppi; così le tradizioni, anche attuali, sono in realtà legate ad alcuni territori. Un primo cambiamento è dovuto all'emigrazione, con lo spostamento di soggetti da un ambiente all'altro; sempre più spesso, tuttavia, il mutamento territoriale si accompagna ad una rivendicazione

[28] Secondo i modelli del *pay per inclusion* oppure del *pay per click*. Nel primo caso la retribuzione è dovuta per il solo fatto dell'inclusione all'interno delle categorie; nel secondo l'entità del dovuto è commisurata al numero dei *click* che dal sito del motore di ricerca conducono al sito pagante. Il più celebre *search engine* rientrante in tale categoria è *Overture* (http://www.overture.com).

delle usanze della propria terra di origine, che si vogliono perpetuare anche nel luogo di destinazione. Gli stessi Stati moderni riconoscono e tutelano queste situazioni e il riconoscimento di tradizioni diverse dalle proprie: pertanto, alcune usanze, legate alla territorialità, la superano. Tuttavia, proprio il concetto di Stato, assieme a quello di diritto, risulta indissolubilmente legato ad un concetto di spazialità inteso nella sua accezione tradizionale, poiché "l'occupazione del territorio è l'atto primordiale che istituisce il diritto, e senza il suo territorio lo Stato moderno sarebbe un nonsenso"[29]. Il concetto di territorio è infatti ricondotto all'ambito fisico-spaziale o geografico sul quale ciascun Stato esercita il proprio dominio e ciò vale anche per quei concetti apparentemente più complessi dal punto di visto giuridico, come lo spazio aereo, le acque territoriali e il sottosuolo, tutti comunque indissolubilmente legati proprio al territorio.

Internet rappresenta l'estremizzazione del superamento della territorialità, perché offre un nuovo mondo senza confini, allo stesso tempo legato alla realtà così come viene comunemente intesa e tuttavia slegato da essa. "Il computer non è un mezzo per stare nel mondo. Il mezzo ha creato il proprio mondo, nel quale si può entrare o non entrare. Quegli, che valica il confine e ne percorre le rotte, è perciò *diviso* tra mondo e sopra-mondo, fra terra e spazio telematico, tra luoghi e non-luogo. Si delineano problemi giuridici, gravi e inattesi. […] La perdita dei luoghi non consente l'immediata individuazione del diritto applicabile. *Il dove giuridico attende nuovi criteri*"[30].

---

[29] A. C. AMATO MANGIAMELI, *Diritto e cyberspace. Appunti di informatica giuridica e filosofia del diritto*, Torino, 2000, p. 8.
[30] N. IRTI, *Norma e luoghi. Problemi di geo-diritto*, Roma-Bari, 2001, p. 66.

Il cyberspazio, dunque, mette in crisi lo Stato, e ciò è "un grandissimo male per chi […] è caparbiamente attestato in difesa d'una realtà che affonda le sue radici (materiali) nel "corpo" e nel "territorio""[31]. Non si può inoltre "trascurare il fatto che l'annullamento delle distanze spazio-temporali, cioè la *de-territorializzazione* della presenza e dell'azione umana, emancipa alcuni dai vincoli territoriali e li libera dagli ostacoli di carattere fisico, mentre altri – incapaci di liberarsi nei *nonluoghi* – restano relegati in un territorio che ha ormai perso di significato e che quindi non è in grado di attribuire alcuna identità"[32].

Non si può del resto negare che l'immaterialità diventa oggetto del diritto, operando in tal modo una vera e propria rivoluzione perché la tradizione giuridica è generalmente legata alla corporeità[33]. L'informatica, dunque, accelera questo cambiamento, avvertito soprattutto nell'ambito della circolazione di una ricchezza anch'essa dematerializzata, e in tale quadro l'interconnessione globale dei sistemi assume carattere centrale, perché stravolge i tradizionali concetti di spazio e di tempo e crea un nuova realtà spaziale complessa.

Nel *cyberspace* lo spazio in cui ci si muove virtualmente, infatti, non è mai strutturato a priori, è dinamico, è spazio-movimento[34]. Costituisce uno spazio in cui esplicare la propria personalità senza il timore di discriminazioni e senza grossi rischi, per ora, di incorrere in meccanismi censori che ingiustamente possano limitare il teoricamente inviolabile diritto alla libera manifestazione del pensiero. Come è stato notato in

[31] A. C. AMATO MANGIAMELI, *op. cit.*, p. 10.
[32] A. C. AMATO MANGIAMELI, *ivi*, p. 12.
[33] V. ZENO-ZENCOVICH, *Informatica ed evoluzione del diritto*, in *Dir. inf.*, 2003, 1, p. 92.
[34] M. BIFULCO, *Virtuale e cyberspazio*, in G. CASSANO (a cura di), *Il commercio via Internet. Profili giuridici, fiscali, tributari, comunitari, sociali, filosofici, normativi*, Piacenza, 2002, p. 21.

dottrina, è paradossale che una tecnologia sviluppata per potenziare la più grande potenza militare del globo 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[35].

Il superamento dei limiti posti dalla territorialità del mondo «reale» assume rilevanza in vari settori, anche di importanza fondamentale, come nel mondo del lavoro: si pensi al telelavoro[36], che è realtà già da tempo e che rappresenta una vera propria rivoluzione nell'ambito di determinate tipologie di rapporti di lavoro, sinora quasi indissolubilmente legate alla presenza fisica nel posto di lavoro, che ora invece viene a coincidere con la propria abitazione, con una lunga serie di benefici. Si verifica, infatti, una diminuzione dei costi, sia per le aziende, che non devono preoccuparsi di creare gli spazi necessari ai propri dipendenti nell'ambito della propria sede, sia per i lavoratori stessi, che non sono obbligati a dover provvedere allo spostamento fisico nel posto di lavoro, che diviene virtuale. Tale prospettiva può portare miglioramenti anche alla collettività, perché evita lo spostamento quotidiano di una massa di persone in ambiti metropolitani sempre più caotici e vessati da problemi

[35] A. VITERBO – TERBODIGNOLA, *La rete: tecnologia di libertà?*, in *Dir. inf.*, 2003, 2, pp. 225-226.

[36] Sul telelavoro cfr., fra gli altri: A. BOTTINI, *Il telelavoro*, in S. NESPOR, *Internet e la legge. Come orientarsi negli aspetti giuridici della rete*, Milano, 1999, pp. 205-216; G. CASSANO – SSANOPATRIELLO, *Il* telelavoro*: prime esperienze, inquadramento giuridico e contrattazione collettiva*, in *Dir. inf.*, 2000, 2, pp. 135-198; G. CASSANO – S. LOPATRIELLO, *Il telelavoro: profili giuridici e sociologici*, in *Dir. inf.*, 1998, 2, pp. 379-452; M. SELAM, *Le novità del telelavoro*, in A. LISI (a cura di)*, Internet: profili giuridici e opportunità di mercato – dall'e-commerce alle aste on line*, Rimini, 2002, pp. 85-102.

di traffico ed inquinamento[37]. L'evoluzione delle tecnologie informatiche può inoltre offrire nuove possibilità di lavoro anche a soggetti con difficoltà motorie, che, come tutti, grazie all'utilizzo dei computer possono svolgere attività lavorative nella propria abitazione. Il telelavoro presenta tuttavia un aspetto negativo da non sottovalutare: costituisce uno stimolo all'isolamento, al rifugio in un nonluogo, alla concreta possibilità di essere fisicamente soli pur fra tanti compagni virtuali.

Il rischio dell'individuo che «vive» nel *cyberspace* è proprio questo, insito nello stesso termine che lo definisce: rimanere un *individuo*, staccato dalla *collettività*, incapace di relazionare direttamente e capace di dialogare solo mediante uno schermo che può costituire uno scudo verso il mondo esterno. Forse, quando sarà compiutamente realizzato lo scambio generazionale e i futuri adulti saranno tutti cresciuti a stretto contatto con l'informatica, navigare su Internet sarà per loro un'attività di mera *routine* e tale problema potrebbe non sussistere (o acuirsi), perché le nuove tecnologie saranno state oramai compiutamente «metabolizzate».

In questo senso, tuttavia, anche ribadire la propria individualità potrebbe risultare quanto mai arduo, in un mondo virtuale che non è a misura d'uomo, nel quale la spersonalizzazione può concretizzarsi in una moltiplicazione della propria identità, col risultato di avere tante identità quanti sono i contesti in cui ci si pone, grazie alla rassicurante presenza del computer, che può filtrare le informazioni e «proteggere» chi naviga dagli altri.

---

[37] Inoltre, "è possibile garantire cicli di lavorazione e servizi continui (24 ore su 24) a costi minori, utilizzando anche personale residente in paesi appartenenti a fusi diversi: si parla addirittura di *transborder teleworker*" (R. NANNUCCI, *La società dell'informazione nel terzo millennio*, in ID. (a cura di), *Lineamenti di informatica giuridica*, Napoli, 2002, p. 538).

Il *cyberspace* è però anche un punto di incontro, può essere una nuova *agorà* virtuale, nella quale scambiare liberamente le proprie opinioni e riscoprire la propria individualità mediante il dialogo con gli altri, in un territorio che, rivoluzionando le leggi della fisica, è in tutti i luoghi ed in nessuno di essi. Esso "travalica i confini degli Stati nazionali, supera le barriere doganali, elimina le differenze culturali fra i popoli, svolge un compito importantissimo per il destino dell'umanità. Giacché essa realizza un rapporto sul piano mondiale fra gli uomini d'ogni specie, crea o certifica l'esistenza di un senso comune dell'umanità, per cui ogni uomo può riconoscersi in un altro uomo"[38]. L'uomo può dunque sfruttare questa nuova possibilità: sta alla responsabilità di ciascuno scegliere se isolarsi o se condividere queste esperienze, se essere staccato dalla collettività o se farne parte ma nel rispetto della propria individualità. Ad ogni modo, "si può auspicare che tra le relazioni sociali reali e la comunità virtuale si realizzi integrazione perché solo in questa ipotesi le comunità virtuali possono avere una potenzialità positiva in quanto suscettibili di rappresentare nuove modalità di agire comunicativo"[39].

L'utilizzo della Rete può inoltre giovare non solo al singolo, ma può contribuire all'attenuazione della crisi delle moderne democrazie rappresentative, nelle quali c'è troppa distanza fra i rappresentanti e i rappresentati, con una conseguente sfiducia nei confronti dello Stato

[38] V. FROSINI, *L'orizzonte giuridico dell'Internet*, in *Dir. inf.*, 2000, 2, p. 275. Inoltre, il *cyberspace* può costituire uno spazio per la crescita dell'identità individuale: "se l'io del virtuale è flessibile e molteplice, se dietro lo schermo del computer si scoprono *molti sé*, una comprensione profonda dell'identità nella vita reale passa anche attraverso il *sé* (i *molti sé*) *on line*" (A. C. AMATO MANGIAMELI, *op. cit.*, p. 209).
[39] T. SERRA, *L'uomo programmato*, Torino, 2003, p. 33.

moderno, come dimostrano i numerosi episodi di disobbedienza civile, in realtà espressione di una diffusa esigenza di legalità e di partecipazione alle dinamiche istituzionali. Sembra paradossale affermare che proprio Internet, che mette in crisi lo Stato e il diritto, entrambi, come detto, legati alla territorialità ed alla materialità, a tale crisi possa contribuire a porre rimedio. Bisogna dunque sottolineare quella caratteristica fondamentale della Rete consistente nell'annullamento delle distanze, che si accompagna alla celerità ed alla facilità d'accesso alle informazioni, che sempre meno sono cartacee e sempre più sono digitalizzate, immateriali, facilmente trasmissibili e condivisibili. I tentativi di governo elettronico sono allo studio, e per quanto possa sembrare strano, un esempio efficace di dialogo fra lo Stato e i cittadini viene proprio dall'Italia, che generalmente è in cronico ritardo nel comprensione, prima, e nella regolamentazione, poi, di tutto ciò che riguarda l'informatica e il diritto. Nel 1996, infatti, la commissione *ad hoc*, diretta da Donato A. Limone ed istituita dall'AIPA (Autorità per l'Informatica nella Pubblica Amministrazione) al fine di creare un disegno di legge sul documento elettronico e la firma digitale, ha reso disponibile sul sito *web* dell'Autorità la bozza del disegno di legge, invitando tutti a fornire impressioni sul lavoro svolto dalla commissione e a formulare pareri per eventuali modifiche da apportare al testo così reso pubblico. Dopo un anno la materia è stata regolamentata, anche grazie al pubblico dibattito telematico, con un intervento legislativo che ha posto l'Italia all'avanguardia in quel settore[40].

[40] Sul documento informatico e la firma digitale v. *infra*, cap. 9. Si può comunque anticipare che, purtroppo, i successivi interventi legislativi, sia a livello nazionale che

Purtroppo questo esempio non è stato seguito per la formazione di altri testi legislativi, ma indica una delle strade percorribili per attenuare quel divario che sembra ormai insanabile fra il legislatore e il corpo sociale. Ovviamente, per non porre in essere discriminazioni e dunque per consentire a tutti la possibilità di essere *on line*, sarebbero necessarie sia una seria opera di alfabetizzazione informatica che la predisposizione di postazioni informatiche collegate ad Internet e liberamente utilizzabili. Il *cyberspace*, così, da *nonluogo*, potrebbe diventare un territorio virtuale nel quale lo Stato, ben lungi dall'esercitarvi qualsiasi pretesa di sovranità, potrebbe porre nuove fondamenta a base della sua ricostruzione, fondamenta che paradossalmente potrebbero essere ben più solide di quelle che attualmente reggono ordinamenti assai vacillanti, perché esse sarebbero basate su un dialogo continuo fra Stato e cittadini, fra rappresentanti e rappresentati. Questo dialogo, infatti, è più difficile da realizzare nella gravosa fisicità del mondo «reale», perché sottoposto ad insuperabili ostacoli di carattere materiale, e dunque potrebbe realizzarsi solo se la classe politica si occupasse del bene comune, riuscendo inoltre a capire quali sono le esigenze dei cittadini. Il mondo virtuale, annullando tutte le distanze, consente davvero quella partecipazione globale a questioni di carattere generale che riguardano tutti, alle quali tutti dovrebbero poter partecipare, se così vogliono, grazie ad una Rete che forse, più che caratterizzata dalla a-territorialità è caratterizzata dalla *omni-territorialità*, ossia da una estensione che si identifica non con un singolo territorio bensì con tutti i territori

---

comunitario, hanno portato il caos in una materia che sino a quel momento era stata sapientemente regolata, con una grande modernità di vedute.

raggiungibili dall'uomo[41].

Nel quadro sin qui delineato, il *cyberspazio* consente, inoltre, la nascita di un'*intelligenza collettiva*, perché spazio dall'immane estensione eppur percorribile in pochi istanti, grazie alla tecnologia che, come detto, annulla le distanze. Risulta così possibile effettuare una sinergia fra i saperi, le immaginazioni e le energie spirituali di chi si connette[42], purché sia sempre garantita a tutti la possibilità di manifestare liberamente il proprio pensiero.

6. IL RUOLO DEL DIRITTO NELLA REGOLAMENTAZIONE DEL CYBERSPAZIO

L'evoluzione tecnologica obbliga il diritto ad adeguarsi continuamente ad una realtà in incessante evoluzione. In alcuni casi bisogna dunque adeguare ed ampliare la disciplina positiva esistente, nonostante la particolarità e le molteplici conseguenze della diffusione di talune novità tecnologiche, che spesso si susseguono con impressionante rapidità; "ma si tratta pur sempre di operazioni assolutamente tradizionali per i giuristi, e basterà pensare - per convincersene - alla notevole quantità di elaborazioni creative che nel corso della storia europea ha subito il diritto romano. D'altra parte, il diritto, la disciplina positiva in genere viene ad esistenza quando la realtà dei rapporti umani la ha resa indispensabile; ed anche questa è una costante della storia culturale della

[41] Del resto, come si è accennato in precedenza, oggi la connessione ad Internet prescinde dalla posa in opera dei cavi che trasmettono i dati, potendo essere effettuata anche mediante dispositivi di tipo *wireless*.
[42] P. LÉVY, *op. ult. cit.*, p. 127.

civiltà occidentale"[43].

Internet, pertanto, può e deve essere regolamentata, perché essa non costituisce una realtà staccata dal mondo «fisico», non solo perché le strutture che in senso lato ne consentono il funzionamento e l'utilizzo sono necessariamente materiali, ma anche perché ciò che avviene *on line* non è senza conseguenze sul mondo *off line*. Il carattere di a-territorialità (o forse di omni-territorialità) del cyberspazio è alla base dell'esigenza di una sua regolamentazione svolta mediante un'attività legislativa internazionale uniforme[44]. Del resto, oggi l'organizzazione del mondo si sta rapidamente evolvendo e, per rappresentarne un carattere fondamentale, si può utilizzare "la formula, suggerita dai fisici, della pari dimensione dell'infinitamente grande e dell'infinitamente piccolo. L'infinitamente grande, nel nostro discorso, è la società globale, che supera i confini nazionali e riduce il pianeta ad unità; l'infinitamente piccolo, a volte inconsapevolmente, si sta trasformando per adeguarsi

[43] C. DE MARTINI, *Telematica e diritti della persona*, in *Dir inf.*, 1996, 6, p. 861. In merito si può ricordare quanto affermato da Sergio Cotta più di trent'anni fa: "rispetto alla situazione dei secoli XVIII e XIX, le parti oggi si sono rovesciate. Se allora era il *costruito* (la norma legislativa) che precedeva, come forza propulsiva e innovatrice, il *dato* (la mentalità e la prassi giuridiche comuni) arretrato e ritardante, oggi invece è il contrario che si verifica. Rispetto all'impetuoso sviluppo tecnologico della società, l'ordinamento vigente, e come istituzioni e come norme, è vecchio e inadeguato, e quindi frenante, per cui leggi e provvedimenti normativi giungono per lo più in ritardo. […] Tra l'apparato giuridico vigente – ideato per una situazione politica, economica e sociale profondamente diversa e per tanti aspetti superata – e la realtà della trasformazione nonché le esigenze dello sviluppo, si è ormai creato un divario troppo profondo perché a colmarlo basti, da parte del giurista, una pura e semplice opera di coordinamento e di unificazione del materiale giuridico esistente" (*La sfida tecnologica*, Bologna, 1968, pp. 172-173).

[44] In questo senso: T. BALLARINO, *Internet nel mondo della legge*, Padova, 1998, p. 222; C. DE MARTINI, *op. cit.*, p. 865; S. SEMINARA, *La responsabilità penale degli operatori su Internet*, in *Dir. inf*, 1998, 4-5, p. 774, il quale, con un pessimistico realismo, sottolinea che "solo nel regno dell'utopia la globalità di Internet oggi può trovare corrispondenza nella globalità di un diritto «comune»".

all'infinitamente grande"[45].

La citata attività legislativa internazionale uniforme per una volta dovrebbe unire i vari stati perseguendo il fine della tutela e dello sviluppo della persona umana, poiché Internet rappresenta oramai un bene comune dell'umanità, sul quale non si possono e non si debbono accampare pretese di singole nazioni tese ad accumulare ingiusti vantaggi su una realtà che, per quanto nata in un singolo paese, ha oggi carattere globale e la cui sempre crescente ricchezza contenutistica è dovuta ad un apporto comune di un numero indefinito di soggetti. Inoltre, coloro che hanno contribuito alla nascita della Rete e che ne hanno consentito lo sviluppo, hanno sempre perseguito il fine ultimo dell'accrescimento della conoscenza umana, improntando i propri contributi alla collaborazione reciproca e al confronto continuo, non per bramosia di denaro, ma per amore della scienza.

Anche non condividendo questa visione valoriale, si deve comunque convenire che l'inscindibilità dei singoli apporti ed i caratteri di globalità, decentralizzazione ed immaterialità del cyberspazio non possono consentirne una regolamentazione da parte di un singolo stato perché essa avrebbe conseguenze di vario tipo. Innanzi tutto, andrebbe in conflitto con le concorrenti giurisdizioni degli altri paesi, a meno di non isolarsi dalla Rete; inoltre, cagionerebbe la lesione del diritto di

[45] F. GALGANO, *Diritto ed economia alle soglie del nuovo millennio*, in *Contr. impr.*, 2000, 1, p. 201. Del resto, oggi l'*information technology* ed i trasporti "hanno creato una necessaria interdipendenza delle comunità statali. I c.d. affari interni di uno Stato sui quali non era ammessa alcuna interferenza da parte degli altri Stati e della Comunità internazionale non sono neppure più chiaramente identificabili. Gli «affari interni» e gli «affari esterni» si confondono. Non solo. Spesso anche i residui spazi di decisioni interne risentono di vincoli esterni" (S. M. CARBONE, *Il ruolo dell'avvocato nella* new economy *(con particolare riguardo all'utilizzo delle tecniche di d.i.p.)*, in *Contr. impr.*, 2000, 3, p. 1204).

libertà informatica, che si può sostenere costituisca un diritto fondamentale dell'uomo, dunque inviolabile, perché rappresenta un modo di svolgimento della propria personalità ed un'opportunità senza precedenti di manifestare liberamente il proprio pensiero, di informare e di essere informato, sia pubblicamente sia mediante l'uso della posta elettronica[46]. Tuttavia, quanto più una libertà è regolamentata, tanto meno essa è «libera», per cui, se si vuole conservare questa libertà, bisogna ridurre al minimo indispensabile qualsiasi intervento normativo, valutando ogni proposta di regolamentazione in base alla sua incidenza sulla libertà di comunicazione, alla valutazione dell'importanza degli interessi che si intendono tutelare attraverso la regolamentazione e alla possibilità di utilizzare forme meno pervasive di regolamentazione al fine di tutelare quegli interessi[47]. Inoltre, il diritto di libertà informatica non ha

[46] Sul punto cfr. S. FOIS, *Informazione e diritti costituzionali*, in *Dir. inf.*, 2000, 2, p. 264, il quale afferma che "le nuove tecnologie, dunque, sembrano permettere ai singoli, e per di più in maniera che può essere interattiva, di modulare l'uso del mezzo di comunicazione in maniera in modo che lo stesso «messaggio» può essere insieme od alternativamente informazione al pubblico e/o informazione «privata»; tutto ciò entro certi limiti giustifica che si possa parlare di un unica libertà di comunicazione, comprensiva della libertà di manifestazione e di quella di comunicazione interpersonale. Ma, se la tendenza è a fondere in un unico diritto i diritti finora distintamente garantiti dall'art. 21 e dall'art. 15 della Costituzione Italiana, ne deriva da un lato la conferma che il diritto ad informare ha natura assolutamente inviolabile, e dall'altro lato definitivamente esclude la possibilità di considerare e trattare come un «potere» la libertà di informare che può atteggiarsi anche come quella di privata corrispondenza. Ciò contribuisce a far cadere anche l'ultimo «totem» al quale si aggrappano tutti coloro che svalutano la valenza della libertà d'informazione come diritto squisitamente individuale, non funzionale né funzionalizzabile, e che tendono ad assoggettarlo a clausole generali basate sul riferimento ad interessi che trascendono quelli dei singoli individui."

[47] Così V. ZENO-ZENCOVICH, *I rapporti fra responsabilità civile e responsabilità penale nelle comunicazioni su Internet*, in *Dir. inf.*, 1999, 1, p. 1050. Inoltre, "il sistema giuridico adatto alla società tecnologica esige senza dubbio una solida struttura portante, consistente *in primis* di principi regolativi generali e di norme di organizzazione, di produzione, di competenza, che istituiscano autorità legittime, conferiscano poteri e

più solo un carattere negativo, consistente nella pretesa di tutela passiva rispetto al trattamento informatizzato dei dati personali, ossia di rispetto della *privacy*, anch'essa intesa in senso passivo; il diritto di libertà informatica "è diventato una pretesa di libertà in senso attivo, non libertà *da* ma libertà *di*, che è quella di valersi degli strumenti informatici per fornire e per ottenere informazioni di ogni genere. É il diritto di partecipazione alla società virtuale, che è stata generata dall'avvento degli elaboratori elettronici nella società tecnologica: è una società dai componenti mobili e dalle relazioni dinamiche, in cui ogni individuo partecipante è sovrano nelle sue decisioni"[48].

In questa ultima prospettiva, inoltre, sorge un'esigenza ulteriore: assicurare che nel settore informatico la creatività e l'ingegno umano siano liberi e non mortificati da un mercato che si caratterizza per la creazione di *standard* che, lungi dal garantire la possibilità di sviluppo tecnologico, sono finalisticamente orientati al consolidamento delle attuali posizioni monopolistiche e alla sistematica estromissione dei concorrenti dal mercato. Il diritto deve regolamentare il settore informatico in generale ed il *cyberspace* in particolare affinché il progresso scientifico *in subiecta materia* sia rispettoso dei diritti fondamentali, fra i quali il più volte citato diritto di libera manifestazione del pensiero, che si estrinseca, tra l'altro, sia nella creazione di siti *web*, che costituiscono un contenitore nel quale poter inserire, in senso lato e metaforico, il proprio

---

stabiliscano procedure fisse e controllabili (è questo il livello giuridico-costituzionale). Seguiranno poi norme di particolare rigidità, come quelle penali o quelle tributarie, dalle quali dipende la libertà del cittadino. Ma al di là di questi livelli è opportuno che la struttura giuridica rimanga *aperta*, per cui sia possibile completarla mobilmente a seconda delle esigenze dello sviluppo" (S. COTTA, *op. cit.*, p. 181).

[48] V. FROSINI, *L'orizzonte giuridico dell'Internet*, in *Dir. inf.*, 2000, 2, p. 275.

pensiero, sia nella possibilità di sviluppare *software*, che potrebbe essere cancellata o limitata da iniziative private come il citato sistema «Palladium»: il diritto non deve solo essere repressivo nei confronti dei singoli, ma deve tutelarli in tutte quelle fattispecie che costituiscono una evidente violazione dei loro diritti[49].

Pertanto, il **diritto di Internet** dovrebbe essere minimo, flessibile e di carattere internazionale, e soprattutto dovrebbe essere repressivo solo in casi estremi e solo verso chiunque effettivamente leda altrui posizioni degne di tutela giuridica. È fondamentale abbandonare la prospettiva di una regolamentazione limitativa delle libertà, frutto di una concezione che pone Internet quale luogo, o nonluogo, di commissione di continui illeciti, per giungere, invece, ad una regolamentazione che tuteli i diritti e le libertà fondamentali contro qualsiasi lesione, anche se proveniente da potenze statuali od economiche.

7. IL PROVIDER

L'accesso ad Internet è reso possibile dalla predisposizione di un servizio da parte di un soggetto denominato *Internet access provider*, anche se, accanto a tale fondamentale prestazione, sempre più spesso si accompagnano servizi accessori, come la concessione di uno spazio *web* o di una o più caselle di posta elettronica: in tal caso si parla, più propriamente, di *Internet Service Provider* (ISP). Pertanto, qualsiasi attività

[49] "L'istanza oggi più avvertita è che la globalizzazione e Internet, in altri termini, le epifanie della società dell'informazione e della new economy non divengano strumenti di oppressione dei diritti della persona" (G. ALPA, *New economy e libere professioni: il diritto privato e l'attività forense nell'era della rivoluzione digitale*, in *Contr. impr.*, 2000, 3, p. 1202).

posta in essere su Internet, come la semplice visione di un sito *web* o l'invio di un messaggio di posta elettronica, è sempre posta in essere per mezzo del *provider*, dal momento che tutti i dati da e verso i *computers* dei suoi clienti passano tramite i suoi elaboratori. Quando l'ISP fornisce uno spazio *web* alla propria clientela può semplicemente mettere a disposizione un determinato spazio o creare e gestire il sito secondo i desideri della clientela stessa, ma comunque con un'attività propria. Nel primo caso si parla di *host provider*, nel secondo di *content provider*.

Queste distinzioni sono di importanza fondamentale per la ricostruzione del regime di responsabilità applicabile all'ipotesi di comportamenti illeciti effettuati via Internet attraverso gli elaboratori del *provider*. Difatti, nel caso in cui l'autore dell'illecito risulti anonimo[50], per consentire il risarcimento al danneggiato è necessario configurare la responsabilità del *provider*. Nella maggior parte dei casi è possibile risalire al nome dell'utente che ha commesso la violazione: ciò è realizzabile tramite l'utilizzo dei *file* di *log*[51], anche se al riguardo si pone l'ulteriore

[50] "L'anonimato, infatti, può essere usato per violare la *privacy* altrui"; così S. RODOTÀ, *Tecnopolitica*, Roma-Bari, 1997, p. 145; tuttavia "la possibilità di rimanere anonimi è indispensabile per garantire nel cyberspazio il rispetto dei diritti fondamentali alla riservatezza e alla libertà di espressione" (G. SANTANIELLO, *Privacy telematica e utilizzo di Internet, reti e servizi di telecomunicazioni*, in http://www.privacy.it/convirisant.html); B. DONATO, *La responsabilità dell'operatore di sistemi telematici*, in *Dir. inf.*, 1996, 1, p. 146, da un lato considera che "l'anonimato della connessione costituisce un incentivo al reato informatico", dall'altro esprime la preoccupazione che estendendo il regime della responsabilità oggettiva nei confronti del *provider*, venga giustificata l'intrusione di questi finanche nelle caselle di posta elettronica.

[51] Il *log file* memorizza lo *user ID* (o *login*, o nome di accesso), la *password* e tutte le azioni compiute da un determinato soggetto per mezzo dell'elaboratore elettronico con cui questi si collega alla Rete.

problema dell'utilizzo abusivo di *user ID* e *password* altrui[52].

Il primo caso europeo rilevante *in subiecta materia* si è verificato in Francia ed è stato deciso dalla Corte d'appello di Parigi il 10 febbraio 1999[53]: i giudici d'oltralpe hanno stabilito che il *provider* che offre ospitalità anonima e senza restrizioni di accesso, consentendo la diffusione di segni, scritti, immagini, suoni e messaggi, estranei alla corrispondenza privata, eccede il ruolo tecnico di semplice trasmettitore di informazioni ed è direttamente responsabile nei confronti dei terzi del compimento di atti illeciti all'interno dei siti che gestisce. Un altro caso straniero molto celebre (Godfrey v. Demon) è stato originato dalla diffamazione nei confronti del dott. Laurence Godfrey, avvenuta in un *newsgroup*: in questa occasione, è stata riconosciuta la responsabilità in capo al *provider* per l'immissione di dichiarazioni diffamatorie da parte di un soggetto rimasto anonimo[54].

---

[52] Si pensi al caso, tutt'altro di scuola, del tecnico che apprende le suddette informazioni durante la sua opera di configurazione o di riparazione di un determinato *computer* (anche se in tal caso sussiste la colpa del cliente, il quale dovrebbe subito cambiare la *password* o in ogni modo non comunicarla); in tal caso, comunque, troverebbe applicazione l'art. 615 *ter* cod. pen.

[53] In *Danno e resp.*, 1999, 7, p. 754, con nota di F. DI CIOMMO, *Internet, diritti della personalità e responsabilità aquiliana del provider*, pp. 756-765, e in *Dir Inf.*, 1999, 4-5, p. 926, con nota di G. M. RICCIO, *La responsabilità del provider nell'esperienza francese: il caso Hallyday*, pp. 929-941. Il caso riguardava la pubblicazione, sul sito http://altern.org/silversurfer, di fotografie di nudo ritraenti la sig.ra Estelle Hallyday, senza il suo consenso.

[54] Per una analisi più dettagliata del caso v. Y. AKDENIZ, *Case Analysis: Laurence Godfrey v. Demon Internet Limited*, in *Journal of Civil liberties*, 1999, 4 (2), e in http://www.cyber-rights.org/reports/demon.htm. Con riferimento alla responsabilità del *provider* in casi simili, si segnala la sentenza del Tribunale di Roma 4 luglio 1998 (in *Dir inf.*, 1998, 4-5, p. 807, con nota di P. COSTANZO, *I newsgoups al vaglio dell'autorità giudiziaria (ancora a proposito della responsabilità degli attori d'Internet)*, pp. 811-816), nella quale correttamente si afferma che "nel caso di un *newsgroup*, ed in particolare di un *newsgroup* non moderato, il *news server* si limita a mettere a disposizione degli utenti lo spazio virtuale dell'area di discussione e non ha alcun

In Italia, la responsabilità del *provider* ha trovato una prima disciplina solo con il d.lgs. 9 aprile 2003, n. 70 e la mancanza di una normativa di settore ha in alcuni casi portato la giurisprudenza ad applicare analogicamente la legge sulla stampa nei confronti del *provider*[55], anche se non sono mancate le pronunce in senso opposto[56]. In realtà, i tentativi di estendere alle comunicazioni telematiche la normativa sulla stampa hanno costituito "maldestre operazioni di disciplina giuridica di realtà assai diverse e ben più complesse. Un sistema può ben vivere con delle lacune e l'*horror vacui* nasconde spesso solo una radicata vocazione dirigistica degli apparati statali cui nulla deve e può sfuggire"[57].

---

potere di controllo e vigilanza sugli interventi che vi vengono inseriti e deve pertanto escludersi la legittimazione passiva del suo gestore".

[55] Trib. Napoli 8 agosto 1997, in *Giust. civ.*, 1998, 1, I, p. 259, con nota di L. ALBERTINI, *Le comunicazioni via Internet di fronte ai giudici: concorrenza sleale ed equiparabilità alle pubblicazioni a stampa*, pp. 261-267; inoltre, va segnalata l'ord. 23 giugno 1998 (reperibile in http://www.interlex.com/regole/sequestr.htm), con la quale la Procura della Repubblica presso la Pretura di Vicenza ha disposto il sequestro preventivo del *server* di «Isole nella rete».

[56] Trib. Teramo 11 dicembre 1997, in *Dir. inf.*, 1998, 2, p. 370, con nota di P. COSTANZO, *Libertà di manifestazione del pensiero e «pubblicazione» in Internet*, pp. 372-378; Trib. Roma 4 luglio 1998, cit.; G.U.P. Trib. Oristano 25 maggio 2000, in *Dir. inf.*, 2000, 4-5, p. 653, con nota di P. COSTANZO, *Ancora a proposito dei rapporti tra diffusione in Internet e pubblicazione a mezzo stampa*, pp. 657-664.

[57] V. ZENO-ZENCOVICH, *La pretesa estensione della telematica al regime della stampa: note critiche*, in *Dir. inf.*, 1998, p. 28. L'estensione della disciplina dettata in tema di stampa anche nei confronti del *provider* non sembra comunque sostenibile per più motivi: innanzi tutto, "le cause di responsabilità oggettiva sono un *numerus clausus* e le stesse non possono essere oggetto di interpretazione analogica" (R. RISTUCCIA – L. TUFARELLI, *La natura giuridica di Internet e le responsabilità del provider*, in http://www.interlex.it/regole/ristufa.htm); inoltre, se il legislatore è dovuto intervenire esplicitamente con la legge 6 agosto 1990, n. 223 per attribuire gli stessi obblighi dell'editore di una testata giornalistica al gestore di una stazione radiofonica o di una emittente televisiva, non si vede perché dovrebbe ritenersi applicabile tale normativa al *provider* senza un esplicito atto legislativo (in questo senso V. ZENO-ZENCOVICH, *op. ult. cit.*, p. 17 e D. MINOTTI, *Diffamazione, Internet e stampa: quando la legge non lascia comunque impuniti*, in http://www.penale.it/giuris/meri_051.htm); ancora, sussistono pesanti diversità contenutistiche e strutturali fra la fornitura del servizio di accesso alla rete e l'editoria; si pensi poi al preciso disposto dell'art. 1 legge

L'estensione della suddetta normativa anche ai *provider* li graverebbe di una responsabilità eccessiva ed essi potrebbero o dovrebbero diventare una sorta di «censori istituzionali»[58], il cui operato censorio potrebbe tuttavia essere sindacato, cadendo in un'*impasse* difficilmente superabile. Inoltre, anche se si volesse far rispondere il *provider* per *culpa in vigilando*, non si terrebbe conto dell'impossibilità tecnica di controllare tutto ciò che transita fra questi e l'utente che accede ad Internet[59].

47/48 (che reca la rubrica "Definizioni di stampa o stampato"): "sono considerate stampe o stampati, ai fini di questa legge, tutte le riproduzioni tipografiche o comunque ottenute con mezzi meccanici o fisico-chimici, in qualsiasi modo destinate alla pubblicazione"; risulta dunque palese l'assoluta incompatibilità della descrizione di cui all'art. 1 con la modalità di diffusione delle pubblicazioni a mezzo Internet (G.u.p. Trib. Oristano 25 maggio – 6 giugno 2000, cit) e poiché le norme della stessa legge che sanciscono la responsabilità civile dell'editore (art. 11) e l'obbligo della riparazione pecuniaria da parte dei diffamatori (art. 12) hanno come presupposto l'accertamento di un reato commesso col mezzo della stampa, necessariamente deve ritenersi che l'illecito commesso tramite una comunicazione telematica non integra in alcun modo la fattispecie (V. ZENO-ZENCOVICH, *op. ult. cit.*, p. 25).

[58] S. RODOTÀ, *Libertà, opportunità, democrazia, informazione*, relazione presentata al Convegno *Internet e privacy, quali regole?*, 8/9 maggio 1998, in http://www.garanteprivacy.it; nello stesso senso G. M. RICCIO, *op. cit.*, in *Dir. inf.*, 1999, p. 941. In questo senso anche P. COSTANZO, *Le nuove forme di comunicazione in rete: Internet*, in F. BRUGALETTA – UGALETTANDOLFI (a cura di), *Il Diritto nel Cyberspazio*, Napoli, 1999, p. 91-131; M. L. DE GRAZIA, *Il giurista ed Internet: ovvero come è possibile passare dalle interconnessioni tra informatica, telematica e diritto al ruolo del giurista nella regolamentazione di Internet*, in F. BRUGALETTA – UGALETTANDOLFI (a cura di), *Il Diritto nel Cyberspazio*, cit., pp. 187-188; M. DE MARI, *op. cit.*, p. 643. Inoltre in Trib. Roma 1 marzo 1999, segnalata in *Danno e resp.*, 1999, 10, p. 1048, incidentalmente si afferma che "il *provider* non può e non deve verificare il sito che gli si chieda di attivare".

[59] S. BARIATTI, *Internet e il diritto internazionale privato: aspetti relativi alla disciplina del diritto d'autore*, in *AIDA*, 1996, p. 61; F. LOLLI, *Il contenuti in rete tra comunicazione e informazione"*, in *Resp. com. impr.*, 1999, 3, p. 447; R. RISTUCCIA – STUCUFARELLI, *op. cit.*. Proprio questa è la ragione che non permette di accogliere l'idea dell'obbligatorietà di un controllo "da parte del distributore, del contenuto dei messaggi, prima che questi possano essere immessi in Rete" (C. DE MARTINI, *op. cit.*, p. 864). Sul punto, nell'intervento tenuto al Convegno *Internet e privacy, quali regole?*, 8/9 maggio 1998 (in http://www.garanteprivacy.it), Marco Barbuti, presidente dell'Associazione Italiana *Providers*, afferma che il *provider* non può conoscere "tutto ciò che passa attraverso la propria rete" e non ha i mezzi per effettuare un tale

In linea di principio, il *provider* dovrebbe invece rispondere qualora rimanga inerte o rifiuti di rimuovere dal proprio *server* messaggi, immagini, filmati o quant'altro denunciati quali lesivi di diritti altrui, qualora essi si appalesino tali, in base ad un giudizio sereno ed obiettivo: sul *provider* deve dunque gravare l'obbligo di attivarsi al più presto in caso di illecito conosciuto o conoscibile commesso tramite il proprio *server*[60]. Un obbligo siffatto dovrebbe ritenersi inoltre previsto dall'art. 1176 cod. civ., ai sensi del quale "nell'adempimento delle obbligazioni inerenti all'esercizio di un'attività professionale la diligenza deve valutarsi con riguardo alla natura dell'attività esercitata": dunque, il *provider* dovrebbe seguire delle regole di buona condotta tecnica che possono qualificare il suo comportamento quale "professionalmente diligente", con ovvie ripercussioni sul piano della responsabilità civile.

L'emanazione del d.lgs. 70/03, di recepimento della direttiva 2000/31/CE[61], avrebbe dovuto sopire il dibattito in materia[62], perché esso, come si è accennato, ha disciplinato anche la **responsabilità del**

---

controllo.

[60] F. DI CIOMMO, *op. cit.*, p. 761, *op. ult. cit.*, p. 761; P. SAMMARCO, *Atti di concorrenza sleale attraverso Internet e responsabilità del provider*, in *Dir. inf.*, 2002, 1, p. 107. In questo senso anche Trib. Napoli 4 settembre 2002: "Affinché il "provider", che si limiti ad ospitare sui propri "server" i contenuti di un sito Internet predisposto dal cliente, possa rispondere per le attività illecite poste in essere da quest'ultimo, non è possibile ravvisare un'ipotesi di colpa presunta, ma è necessario che sussista la colpa in concreto, ravvisabile, ad esempio, laddove venuto a conoscenza del contenuto diffamatorio di alcune pagine "web", non si attivi immediatamente per farne cessare la diffusione in rete."

[61] "Relativa a taluni aspetti giuridici dei servizi della società dell'informazione, in particolare il commercio elettronico, nel mercato interno".

[62] Il testo del d.lgs. 70/03 è stato definito "criptico, confuso, ridondante, con diversi passaggi che fanno rabbrividire i giuristi più attenti. […] Da una parte ci sono previsioni criptiche, incomprensibili anche nel testo originale in inglese, che il nostro legislatore ha ottusamente tradotto senza curarsi del loro significato, e che quindi possono significare tutto e nulla stesso tempo" (M. CAMMARATA, *Le trappole nei contratti di hosting*, in http://www.interlex.it/regole/trappole.htm).

provider. Il sistema previsto dalla direttiva, e recepito mediante il d.lgs. 70/03, 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"[63].

Il recepimento della direttiva è avvenuto mediante l'emanazione di un testo normativo che costituisce la mera trasposizione di quello comunitario: il legislatore italiano, infatti, non si è curato di apportare quelle modifiche che si palesano necessarie per il corretto inserimento delle disposizioni comunitarie nell'ambito dell'ordinamento giuridico italiano[64].

Nel sistema delineato dal d.lgs. 70/03 si distinguono tre tipologie principali:

a) *responsabilità nell'attività di semplice trasporto (mere conduit*, art. 14): si prevede l'esonero da responsabilità sia per il prestatore di un servizio consistente nella trasmissione, su una rete di comunicazione, di informazioni per conto degli

[63] G. COMANDÈ, *Al via l'attuazione della direttiva sul commercio elettronico, ma… serve un maggiore coordinamento*, in *Danno resp.*, 2003, 7-8, p. 811.

[64] In questo senso anche G. M. RICCIO, *La responsabilità degli* internet providers *nel d.lgs. n. 70/03*, in *Danno resp.*, 2003, 12, p. 1157. Un ulteriore carattere che denota la scarsa qualità del testo normativo in oggetto è messa in luce dall'a., il quale osserva che "è quantomeno singolare che, nel rubricare le norme, il legislatore adotti una doppia dizione, in italiano ed in inglese, accostando ai termini [semplice trasporto, memorizzazione temporanea, memorizzazione …] rispettivamente quelli di *mere conduit*, *caching* e *hosting*: una aggiunta che, francamente, non si comprende, attesa la sua inutilità e la sua irrilevanza sul piano giuridico" (p. 1159).

utenti (*mere conduit*) che per un *access provider*, purché essi non diano origine alla trasmissione, non ne selezionino il destinatario e non selezionino né modifichino le informazioni trasmesse[65];

b) *responsabilità nell'attività di memorizzazione temporanea (caching,* art. 15): si 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

[65] "Tale previsione pare, invero, tradire una disapplicazione del principio di neutralità tecnologica della norma, giacché nella prestazione di servizi internet, a differenza di quanto avviene nei servizi telefonici, il prestatore/provider assume un ruolo «tecnicamente» attivo nella gestione e nell'instradamento delle comunicazioni in transito, adottando politiche di gerarchizzazione dei contenuti anche attraverso indici automatici, ma senza avere la possibilità di incidere specificamente sui contenuti stessi" (A. PUTIGNANI, *Sul provider responsabilità differenziate*, in *Guida dir.*, 2003, 20, p. 48).

organo giurisdizionale od un'autorità amministrativa ne ha disposto la rimozione o la disabilitazione;

c) *responsabilità nell'attività di memorizzazione delle informazioni (hosting,* art. 16): si esonera da responsabilità l'*host provider* (ossia chi effettua la "memorizzazione di informazioni fornite da un destinatario del servizio") 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.

L'art. 17, infine, dispone che il *provider* non è assoggettato ad un obbligo generale di sorveglianza sulle informazioni che trasmette o memorizza, né ad un obbligo generale di ricercare attivamente fatti o circostanze che indichino la presenza di attività illecite. Il prestatore deve comunque "informare senza indugio l'autorità giudiziaria o quella amministrativa avente funzioni di vigilanza, qualora sia a conoscenza di presunte attività o informazioni illecite riguardanti un suo destinatario del servizio della società dell'informazione"; "fornire senza indugio, a richiesta delle autorità competenti, le informazioni in suo 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. 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"[66].

Questa norma ha dunque una notevole importanza, perché sancisce l'assenza di un obbligo di controllo da parte del *provider* sul contenuto dei dati immessi in rete dai propri clienti[67]; al disposto dell'art. 17, comunque, si poteva tranquillamente giungere per via interpretativa, per quanto in dottrina sia stato giustamente osservato che tale norma assume fondamentale importanza perché consente di porre fine al dibattito in materia[68].

Bisogna comunque considerare che un eventuale controllo, da parte del *provider*, del materiale immesso *on line* dai propri clienti, sarebbe

---

[66] Il combinato disposto degli artt. 16 e 17 rischia di creare non pochi problemi ai *provider* che non aggiornino le clausole inserite all'interno dei contratti di *hosting*, i quali generalmente prevedono "la facoltà del provider di verificare i dati immessi dall'utente e rimuovere quelli che appaiono illeciti o comunque non aderenti alla *netiquette* o alla *policy* dell'azienda. Clausole di questo tipo sono spesso usate proprio per mettere il fornitore al sicuro da eventuali responsabilità civili o penali. Orbene, dal momento in cui il provider dichiara di sorvegliare i contenuti immessi dai clienti si può presumere che egli possa essere effettivamente a conoscenza dell'eventuale illiceità di tali contenuti. E quindi si addossa le relative responsabilità! Dunque è necessario riformulare i contratti di hosting (e non solo di hosting) in modo di evitare questa trappola, e in qualche caso potrebbe non essere facile destreggiarsi tra le esigenze tecnico-organizzative e la necessità di tradurre il non-obbligo di sorveglianza previsto dalla legge nell'esclusione contrattuale di qualsiasi forma di sorveglianza o di "attivazione" del provider sui contenuti" (M. CAMMARATA, *op. cit.*).

[67] L. GIACOPUZZI, *La responsabilità del provider*, in http://www.diritto.it/articoli/dir_tecnologie/giacopuzzi9.html.

[68] G. M. RICCIO, *op. ult. cit.*, p. 1164.

da ritenersi assolutamente illecito, perché contrastante, *in primis*, 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". Pertanto, un eventuale intervento censorio del *provider* concreterebbe una violazione della norma da ultimo citata.

Con riferimento all'eventuale responsabilità penale del *provider* per illeciti commessi mediante i suoi elaboratori, bisogna considerare che l'art. 17 sancisce l'insussistenza di un obbligo giuridico di impedire l'evento nel caso di specie, per cui non può trovare applicazione l'art. 40 comma 2 cod. pen., il quale, letto congiuntamente all'art. 110 cod. pen., fonda la punibilità del concorso per omissione nel reato commissivo posto in essere da altri[69], per quanto sul *provider* gravi, comunque, l'obbligo di attivarsi nelle ipotesi di cui sopra.

La colpa assume, pertanto, un ruolo essenziale nell'ambito della responsabilità del *provider*, "nell'ottica di una delicata operazione di bilanciamento tra l'esigenza di individuare sicure figure cui imputare il danno onde 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 essere portatori di una particolare qualifica. Seppur nella consapevolezza dei rischi che possono derivare da facili schematismi in cui far forzatamente rientrare le evoluzioni della responsabilità civile sembra cioè che nel dibattito di questi ultimi anni la rivalutazione della colpa possa assurgere a simbolo della rinuncia sia ad un'aprioristica attribuzione di responsabilità che ad una preconcetta negazione di risarcimento nei

[69] D. MINOTTI, *Responsabilità penale: il provider è tenuto ad "attivarsi"?*, in http://www.interlex.it/regole/minotti8.htm; A. PUTIGNANI, *op. cit.*, p. 52.

confronti di chi abbia subito un danno perpetrato per via telematica"[70].

La scelta della colpa quale regime di imputazione della responsabilità, operata dalla direttiva 2000/31/CE e recepita dal d. lgs. 70/03, consente di superare i problemi legati alle opposte estremizzazioni teorizzabili in riferimento alla posizione civilistica del *provider*, quale soggetto *sempre* responsabile oppure quale soggetto *mai* responsabile. In tal modo, il danneggiato può ottenere il risarcimento del danno, cui è tenuto un soggetto la cui condotta deve tuttavia essere stata caratterizzata da diligenza, imprudenza, imperizia[71].

8. HACKERS E CRACKERS

Il fenomeno degli *hackers*[72] è spesso inteso in maniera scorretta, sia dai *mass media* che dall'opinione pubblica, probabilmente a causa di una cattiva informazione in materia. Forse la più celebre definizione in merito è fornita dal c.d. «Jargon file»[73]: al contrario della maggior parte degli utenti, che preferisce imparare solo il minimo necessario per poter utilizzare un computer, l'*hacker* è una persona che si diverte ad esplorare i dettagli dei sistemi informatici, migliorando sempre le proprie capacità

[70] A. PIERUCCI, *La responsabilità del provider per i contenuti illeciti della Rete*, in *Riv. crit. dir. priv.*, 2003, 1, pp. 164-165.

[71] In questo senso anche G. M. RICCIO, *op. ult. cit.*, p. 1169, cui si rinvia per un approfondimento della tematica in questione.

[72] La problematica in oggetto è assai complessa e non può essere esaurita in queste poche pagine, ma risulta anche molto attuale e soprattutto ricca di spunti di riflessione per il diritto, sia in una prospettiva puramente teorica che meramente pratica. Si rinvia, pertanto, ad uno scritto, attualmente in preparazione, nel quale sarà effettuata una più dettagliata analisi dei fenomeni costituiti da *hackers* e *crackers*.

[73] Reperibile sia in forma elettronica (all'indirizzo Internet "http://catb.org/esr/jargon/html/index.html") che in forma cartacea (E. S. RAYMOND (edited by), *The New Hacker's Dictionary*, Cambridge, 1996).

pensando più all'aspetto pratico che a quello teorico, perché guidata da una sfrenata passione per la programmazione[74]. Tale termine è nato all'incirca negli anni sessanta, fra l'altro nell'ambito del MIT, e non si riferisce solamente agli esperti di informatica, ma anche ai «fanatici» di qualsiasi disciplina scientifica. Un elemento deve unificare gli *hackers*: il gusto della sfida intellettuale di superare od aggirare i limiti della conoscenza attuale nella disciplina di cui ci si occupa. Nonostante essi si considerino una *élite* (una meritocrazia basata sull'abilità), accolgono volentieri i nuovi *hackers* che si siano messi in luce per le proprie capacità; difatti è preferibile essere considerati tali dagli altri piuttosto che auto-definirsi così.

Gli *hackers* veri e propri, dunque, non agiscono con l'intenzione di compiere reati informatici, né normalmente li compiono; vanno perciò distinti dai *crackers*, ossia coloro che agiscono allo scopo di violare sistemi informatici, per acquisire informazioni riservate o per puro vandalismo. Essi sono pertanto ben lontani dalla c.d. *etica hacker*, i cui caratteri fondamentali risiedono in primo luogo nella convinzione che la condivisione della conoscenza sia una bene essenziale e che la condivisione della propria esperienza, programmando codice liberamente modificabile e facilitando l'accesso alle relative informazioni, costituisca un vero e proprio obbligo morale. In secondo luogo, alcuni affermano la rispondenza a tale etica, dunque la liceità, del *system-cracking*, purché non vengano commessi furti, atti di vandalismo o di lesione della *privacy*. Se il principio della condivisione delle esperienze e delle informazioni è

[74] "Gli hacker programmano perché per loro le sfide della programmazione rivestono un *interesse* intrinseco. I problemi relativi alla programmazione suscitano nell'hacker una genuina curiosità che lo spinge a imparare ancora di più" (P. HIMANEN, *L'etica hacker e lo spirito dell'età dell'informazione*, tr. it., Milano, 2003, p. 15).

generalmente accettato dagli *hackers*, altrettanto non può tuttavia dirsi del secondo, ritenuto totalmente illecito da alcuni, mentre altri non solo lo ritengono perfettamente lecito, ma addirittura utile al gestore del sistema informatico violato qualora gli venga spiegato come è stato possibile effettuare il *cracking* e suggerendo come rimediare al problema: in tali casi, oltretutto, non viene richiesta la remunerazione per il «servizio» svolto, che può tutelare dai *crackers* veri e propri. Ne consegue che la generalizzata criminalizzazione degli *hackers* esprime una mancata conoscenza del fenomeno, perché essi sono ben distinti dai *crackers*.

Internet ha indubbiamente contribuito alla diffusione di tali fenomeni e provocatoriamente si potrebbe affermare che, addirittura in taluni casi di *cracking*, ciò non costituisca necessariamente un male, o quanto meno potrebbe costituire un male minore rispetto a violazioni ben più gravi. Com'è noto, le odierne democrazie sono in crisi, soprattutto con riferimento all'aspetto della rappresentatività, posta la sempre più ampia sfiducia nei confronti dei rappresentanti politici. Spesso lo Stato, del resto, anziché tutelare la popolazione, viene asservito alla tutela di discutibili interessi di parte di carattere economico, per cui si verifica la prevalenza dell'economia sul diritto.

A tale crisi della rappresentanza si accompagna una sempre più diffusa sfiducia anche nei confronti dell'autorità giudiziaria, che dovrebbe rappresentare un baluardo a difesa dei diritti di tutti, diritti che possono essere calpestati anche grazie alle storture dello stesso sistema giudiziario, caratterizzato da lentezza e farraginosità, il cui funzionamento non assicura la giustizia. Inoltre, i costi e il tempo necessario per far valere una pretesa dinanzi ai giudici spesso non

giustificano il ricorso all'autorità giudiziaria, con la conseguenza che soprattutto le grandi aziende possono impunemente cagionare micro-lesioni diffuse ai diritti dei propri clienti, i quali molto spesso sono costretti a dover far ricorso alle prestazioni di tali aziende: si pensi alla fornitura dell'energia elettrica o alla telefonia fissa, nel cui ambito la c.d. liberalizzazione dell'ultimo miglio stenta ancora a realizzarsi di fatto; oltretutto è sempre incombente il rischio di cartelli finalizzati a falsare il gioco della concorrenza.

Se gli atti di *hacking* in senso stretto, potendo consistere, ad esempio, nello studio del codice sorgente di un determinato *software*, talvolta illecito o considerato tale quando in realtà non lo è[75], o nell'aggiramento di determinati sistemi di protezione del *software* per effettuarne una copia di riserva (ossia a fini di *backup*)[76], non danno

[75] Si prenda in considerazione il caso DeCCS, realmente emblematico. Il DeCCS è un *software*, creato nel 1999, che permette la decrittazione di un film posto su DVD e crittato con il CCS (*Content Scrambling System*), consentendone la copia su *hard disk*. La spinta alla realizzazione del DeCCS consisteva nella necessità di creare un *software* che permettesse di visionare i film registrati su DVD (legittimamente acquistati) anche su sistemi «Linux», per i quali non esistevano appositi DVD *player*. Il DeCCS era stato creato dall'allora quindicenne Jon Johansen, che è stato però citato in un giudizio penale dal Governo norvegese dietro pressione delle aziende discografiche. Fortunatamente i giudici norvegesi hanno stabilito che non è illegale utilizzare il DeCCS per visionare film legittimamente acquistati ed hanno assolto il giovane *hacker* da tutte le accuse, ma il fatto stesso che le pressioni di soggetti economicamente forti possano costituire la guida per le azioni della pubblica accusa è preoccupante, anche perché non sempre si potrà contare su giudici che non si faranno piegare dalle assurde pretese dei citati soggetti.

[76] Alcuni *software*, infatti, sono dotati di sistemi di protezione che ne impediscono la copia, per cui se il legittimo acquirente smarrisce il supporto sul quale il programma è memorizzato o se il supporto stesso viene danneggiato, e non è possibile effettuarne una copia, diventa necessario richiederne un'altra alla casa produttrice, previo pagamento di una cifra stabilita dalla stessa ditta (ammesso che esista ancora od offra questo servizio), oppure non è più possibile usufruire di un *software* per il cui uso è stato tuttavia pagato il corrispettivo. Del resto, è noto che, in linea generale, l'acquirente gode della facoltà di effettuare una copia di riserva di un programma

comunque vita a nessun allarme sociale, altrettanto non può dirsi per gli atti di *cracking*, come l'accesso abusivo ad un sistema informatico. Tuttavia, dinanzi allo scenario prima delineato, viene sempre più facile trovare una giustificazione addirittura giuridica per determinati atti di *cracking*, qualora siano finalizzati ad impedire violazioni di diritti fondamentali oppure si pongano come risposta a siffatte violazioni. Difatti, se lo Stato non tutela i propri cittadini, né dal punto di vista squisitamente politico né da quello giudiziario, cosa rimane a coloro i cui diritti sono calpestati[77]?

---

legittimamente comprato, ma i sistemi di protezione non consentono l'esercizio della facoltà medesima, per cui l'unico modo è aggirare questi sistemi, ma ciò potrebbe costituire un illecito se non addirittura un reato penale! Inoltre, è ovvio che una simile operazione richieda conoscenze non comuni, per cui in tali casi si potrebbe sostenere la liceità dei c.d. *crack*, ossia di quei *software* che aggirano le protezioni e che sono, tra l'altro, facilmente reperibili su Internet. Lo stesso problema, comunque, si pone per i comuni *compact disc* (cd) musicali, che rappresentano oggi il più utilizzato sistema di distribuzione musicale. Molti di essi, infatti, sono dotati di un sistema di protezione che non solo non ne consente la copia, ma che addirittura ne impedisce l'ascolto mediante i *personal computers*, e ciò costituisce una ingiustificata limitazione nel godimento di un bene legittimamente acquistato. Oltretutto, sulla confezione dei primi cd protetti non veniva neanche indicata la presenza della protezione, per cui si sono levate numerose voci di protesta, cui ha fatto seguito la scelta, da parte di alcune case discografiche, di continuare a vendere cd protetti e di porre sulle relative confezioni una etichetta, spesso microscopica in sé o comunque recante scritte assai piccole, in cui si avvisa il potenziale acquirente della presenza di un sistema di protezione. Non solo: alcune aziende del settore, infatti, hanno unilateralmente deciso di consentire di effettuare una sola copia non su supporto digitale bensì analogico, ossia sulle comuni audiocassette, che tuttavia garantiscono una qualità sonora assai minore, per cui non si può certo affermare che in tali casi viene lasciata la facoltà di effettuare una copia di *backup*, poiché la diversità strutturale del supporto incide in maniera decisiva sulle caratteristiche del bene che costituisce l'oggetto del contratto, sia per l'inevitabile deterioramento sonoro (dovuto alla conversione da digitale ad analogico nonché alle caratteristiche intrinseche della memorizzazione su un supporto della secondo tipologia) che per la differenziazione della modalità di ascolto (assai più rapida e flessibile nei cd).

[77] Del resto, "il problema non è solo il riconoscimento dei diritti dell'uomo – meraviglia negli ultimi decenni la proliferazione di lunghe liste di diritti – ma anche e soprattutto la realizzazione e la tutela reale dei diritti di base nel momento in cui essi

Questo interrogativo è ancor più inquietante ove si consideri che i diritti alla libera manifestazione del pensiero nonché al rispetto della segretezza della propria corrispondenza hanno fondamento costituzionale ed un'eventuale legge che ne disponesse una violazione indiscriminata sarebbe costituzionalmente illegittima. Tuttavia, sino alla relativa pronuncia da parte dell'Alta Corte, essa sarebbe vigente e ad essa tutti i cittadini dovrebbero orientare la propria condotta, nonostante la palese violazione dei propri diritti inviolabili. Si pensi, inoltre, ai citati casi Echelon ed Information Awareness Office: in tali casi, gli stati che li hanno realizzati costituiscono dei veri e propri *cracker* che, senza poter essere fermati, commettono illeciti in via continuativa, ledendo in primo luogo la riservatezza delle comunicazioni. Contro questi sistemi di intercettazione, l'unica arma a disposizione di ciascun individuo è costituito dagli strumenti di crittografia, non a caso considerati alla stregua delle armi vere e proprie nelle regolamentazioni di settore, che, quanto meno, oggi permettono maggiore libertà nel loro utilizzo. L'uomo comune è, dunque, un uomo di vetro, sottoposto agli indiscreti sguardi altrui. Gli Stati che lottano tanto aspramente contro la rivoluzione tecnologica, cercando di arrestarla, cercano di difendere i propri privilegi, la possibilità di controllare i propri sudditi, i quali, non avendo nella maggior parte coscienza di quanto avviene né dei possibili rimedi, si trovano totalmente indifesi. Inoltre, l'asse decisionale in ambito normativo si sposta progressivamente dalle autorità politiche alle autorità tecnocratiche, "meglio idonee a dialogare fra loro entro la società

---

si vanno a specificare e a calare nelle singole realtà culturali […, ma per] la realizzazione piena dei diritti degli esseri viventi si richiede qualcosa di più, vale a dire la pretesa del loro riconoscimento, che non è fatto solo teorico ma riguarda la loro azionabilità" (T. SERRA, *op. ult. cit.*, p. 41).

globale. Gli uomini più potenti della Terra oggi sono, probabilmente, i governatori delle banche centrali, che nelle rispettive società sono pure tecnocrazie, sprovviste di investitura popolare. Come ne sono sprovvisti i corpi giudiziari, neppure essi elettivi, e tuttavia disposti ad assumere compiti, di adeguamento del diritto ai mutamenti della realtà, che in passato si ritenevano riservati alla sede politica. Anche a questo riguardo si può ripetere che le attività politiche arretrano di fronte alle autorità tecnocratiche"[78].

Ovviamente, la liceità del fine perseguito non giustifica l'uso di alcuni mezzi, né da parte dei *cracker*, né da parte di altri soggetti privati, ma neanche da parte degli Stati (tanto più se i reali rappresentanti lo sono *sine titulo*, perché esercitano un potere di fatto senza esserne investiti[79]). Difatti, non si può pretendere di criminalizzare in maniera generalizzata una sola categoria di soggetti, indipendentemente dalle motivazioni che hanno spinto al compimento di determinate azioni nonché alle modalità realizzative delle singole condotte, quando altri soggetti possono ledere i diritti altrui per tutelare i propri, anche se di rango inferiore, con l'avallo di un potere statuale sempre meno forte e sempre più subordinato a poteri ben più forti, espressione, pertanto, di una egemonia

[78] F. GALGANO, *op. cit.*, p. 203.

[79] Oggi "la cultura *liberal* americana protesta per lo smisurato potere del presidente della Federal Reserve, le cui decisioni sono attese con ansia da imprese e dai governi di tutto il mondo. Denuncia la contraddizione con i principi della democrazia, che ricerca nella investitura popolare la legittimazione di ogni potere, secondo la ben nota formula di Rousseau. Ma è lecito domandarsi che senso avrebbe mai, per chi governa il mondo intero, essere eletto dai cittadini degli Stati Uniti. In una società che tende, come l'odierna società, a organizzarsi su basi planetarie, oltre la frammentazione dei singoli stati nazionali, la legittimazione del potere si sposta su basi diverse da quelle tradizionali. Democrazia significa pur sempre governo basato sul consenso dei governati; tecnodemocrazia è un concetto nuovo, che però sembra fare a meno della ricerca del consenso" (F. GALGANO, *ivi*, p. 203).

dell'economia sul diritto. Si è accennato alle iniziative della RIIA e delle *major* discografiche, che negli Stati Uniti hanno citato in giudizio migliaia di persone sospettate di aver scambiato *file* musicali su Internet; hanno inoltre dichiarato di essere in possesso degli indirizzi IP di altre migliaia di utenti, che saranno così identificati e, presumibilmente, convenuti innanzi ai giudici, a meno che non riconoscano le proprie colpe e, con una sorta di ravvedimento operoso, paghino un'ammenda alla RIIA[80]. A questo punto, sembra strano parlare dell'esistenza di uno «stato di diritto», visto che alcuni possono tutelarsi ledendo i diritti altrui, comportandosi allo stesso tempo come un organo di polizia giudiziaria (che effettua indagini ed intercettazioni) e di giustizia (che decide sull'innocenza o sulla colpevolezza altrui e addirittura consente l'oblazione!). Da questa succinta ricostruzione, emerge che i soggetti economicamente forti possono ledere i diritti di coloro che, se solo si azzardano a reagire, vengono accusati di atti di criminalità informatica e dunque incorrono in responsabilità di carattere penale: parafrasando George Orwell, si potrebbe dire che per il diritto tutti sono uguali, ma che alcuni sono più uguali degli altri.

Purtroppo, "il braccio di 'forza' tra il 'potere' (nazionale, sovranazionale, transnazionale, economico etc.) e il 'potere' che nasce dall'unione di coloro che condividono opinioni – secondo l'opinione di Tocqueville che sarà sviluppata da Hannah Arendt nel XX secolo –

[80] In più casi, tuttavia, la RIIA ha accusato ingiustamente soggetti che mai hanno violato le norme sul *copyright*, come nel caso della sig.ra Ward, anziana insegnate in pensione, che, sul *New York Times* del 25 settembre 2003, ha dovuto dar conto dei propri gusti musicali e spiegare che il suo utilizzo del *computer* è limitato all'invio di posta elettronica. Ciononostante, la RIIA ha minimizzato l'accaduto e la giustizia statunitense non si occupa di tali questioni.

dovrebbe rispondere alla dialettica democratica dell'ascolto e del dialogo, ma troppo spesso si risolve in un raffronto di forze non sempre pari. Si tratta anche di comprendere che il significato di politica deve essere rifondato e che dall'opinione condivisa nasce un potere che non può essere sottovalutato dai poteri istituzionalizzati, se questi non vogliono delegittimarsi. L'impegno politico del cittadino, del 'buon cittadino', si amplia a impegno dell'uomo cittadino del mondo e si manifesta anche come esigenza di esprimere il dissenso tutte le volte che le istituzioni democratiche prendono decisioni sull'avvenire del mondo sulla base di logiche chiuse. E si manifesta anche come pretesa che questo dissenso sia preso in considerazione dal potere istituzionalizzato"[81].

In questo quadro, gli *hackers* e, a volte, i *crackers*, potrebbero rappresentare un'importante risorsa contro uno strapotere statuale sempre maggiore, purché non si ecceda nel senso di considerarli quali baluardi a difesa della libertà, in lotta contro i moderni colossi dell'economia, ma neanche di criminalizzarli solo perché cercano di comprendere quanto non dovrebbe essere compreso dall'uomo comune. Ad esempio, il caso Zimmermann è significativo, in quanto dimostra come la possibilità di fornire un piccolo *software* finalizzato alla tutela della propria *privacy* possa intimorire addirittura gli Stati Uniti, la più grande potenza mondiale. Il progresso tecnologico nel settore informatico è stato reso possibile primariamente grazie all'apporto di scienziati come Douglas Engelbart, il quale è stato un *hacker*, come è emerso nella ricostruzione storica dell'evoluzione di Internet: le sue intuizioni, la sua sete di conoscenza e la volontà di superare i limiti attuali

[81] T. SERRA, *La disobbedienza civile.*, cit., p. 150.

della scienza hanno portato ad invenzioni assolutamente geniali, considerando l'età pionieristica (con riferimento all'informatica) nella quale ha operato. Oggi la figura di *hacker* non è in realtà incarnata dagli autori di *virus* informatici, ma da persone come Tim Berners-Lee, Linus Torvalds, e, soprattutto Richard Stallman[82], i cui rispettivi contributi al mondo informatico sono stati improntati all'ideale della condivisione della conoscenza, in modo che tutti possano giovarne e la scienza possa progredire.

In alcuni casi, tuttavia, anche il comportamento dei *cracker* potrebbe essere lecito qualora le condotte potenzialmente criminose siano poste in essere contro soggetti che a loro volta hanno realizzato e continuano a realizzare veri e propri reati anche con la complicità statuale, nonostante oggetto della lesione siano addirittura alcuni diritti fondamentali dell'uomo, la cui necessità di tutela potrebbe elidere l'antigiuridicità del fatto commesso dai primi. Si ripropone, pertanto, il menzionato problema della (im)possibilità di tutela per l'uomo comune, che, nonostante veda i propri diritti violati, non può tutelarli nelle sedi appropriate e non può neanche difenderli autonomamente. Alla molteplicità di problemi non si contrappongono, tuttavia, altrettante risposte, ma piuttosto la progressiva emersione di forme di disobbedienza civile elettronica, anche se alcuni atti possono concretizzarsi in forme di violenza informatica, per cui in tali ipotesi non potrebbe parlarsi di disobbedienza civile, atteso che la non violenza è uno dei suoi requisiti necessari[83]. Inoltre, "se fino a qualche anno fa

[82] Da più parti definito come l'ultimo vero *hacker*.
[83] Difatti, la violazione "deve essere fondamentalmente non violenta, in quanto, se vuole essere coerente con i principi che la sostengono, non può essere lesiva dei

l'ordinamento che l'eventuale disobbediente accettava era quello specifico nel quale si compiva il gesto, oggi con la transnazionalità del fenomeno si realizza un passo ulteriore che corre il rischio di far avvicinare sempre di più la disobbedienza civile alla rivolta, E non per il rischio della degenerazione, ma perché sembra che l'istanza partecipativa imponga un rispetto non tanto per gli ordinamenti in sé, quanto per il principio democratico che sembra scindersi dall'ordinamento stesso nel momento in cui il centro decisionale diventa una forza comune a cui le singole potenze partecipano ma con un atteggiamento che riscopre simboli e atteggiamenti di un potere che con la base non ha più alcun rapporto. Soprattutto il disobbediente civile dei tempi nuovi sembra avvertire la necessità di porsi come forza trasversale che risponde a logiche di carattere generale con riferimento anche al principio della vita e della sopravvivenza della vita interpretato come diritto umano fondamentale, in contrapposizione alla trasversalità di un potere che risponde a logiche parziali di tipo economico che col principio della vita nulla hanno a che fare"[84].

Il problema è che qualsiasi atto di *hacking* o di *cracking*, anche in base alle normative attuali, potrebbero essere connotato da violenza, ovviamente da intendersi in senso informatico; ma non sembra che attualmente ci siano altre possibilità di far sentire la propria voce *on line*

---

diritti degli altri e dei principi su cui si fonda la stessa istituzione. La non violenza è, in linea di principio, un requisito necessario perché la disobbedienza civile è basata sul rispetto dell'ordinamento in sé e l'ordinamento democratico ha tra i suoi principi costitutivi fondamentali il rispetto dei diritti di tutti e la razionalizzazione del conflitto attraverso l'eliminazione della violenza e della forza. Tra i fini di ogni associazione politica dei nostri giorni c'è la difesa della libertà, della vita e della proprietà, nel significato lockeano del termine, e quindi non si può pretendere di difendere questi principi attraverso mezzi che li contraddicano" (T. SERRA, *ivi*, p. 134).

[84] T. SERRA, *ivi*, p. 151.

se non mediante simili atti, che si caratterizzano, comunque, per una lesività di gran lunga inferiore a quelli posti in essere da parte degli eventuali destinatari di questi. L'impossibilità di tutelare sia in via preventiva che successiva un diritto fondamentale potrebbe pertanto elidere l'antigiuridicità di un fatto che costituisca una risposta ad un illecito altrui, proprio perché non può ritenersi che un diritto sancito in massimo grado possa rimanere sfornito di tutela, soprattutto nei casi di violazione palese.

9. CENNI SU DIRITTO D'AUTORE, INTERNET E DUPLICAZIONE ABUSIVA DEL *SOFTWARE*

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"[85].

Proprio il *boom* di Internet e la facilità di circolazione di qualsiasi

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

tipo di dato hanno messo in crisi il diritto d'autore[86], 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 gli enormi interessi coinvolti[87]. Ciò ha portato ad un frenetico susseguirsi di norme di diverso rango, che hanno reso assai confusionario il quadro normativo e della cui liceità si può in alcuni casi ampiamente dubitare[88].

Con precipuo riferimento alla situazione italiana, la legge sul diritto d'autore (legge 22 aprile 1941, n. 633, d'ora in poi l. aut.) è stata da ultimo modificata dal d. lgs. 9 aprile 2003, n. 68, di "attuazione della direttiva 2001/29/CE sull'armonizzazione di taluni aspetti del diritto d'autore e dei diritti connessi nella società dell'informazione", ma già la legge 18 agosto 2000, n. 248, recante "nuove norme di tutela del diritto

[86] Le problematiche derivanti dall'incidenza delle nuove tecnologie sulle normative vigenti sono assai numerose, ma in questa sede non possono essere affrontate nella loro globalità. Fra esse si possono qui ricordare la tutela dei programmi per elaboratore nonché dell'opera multimediale,

[87] Si ricordano: i trattati conclusi nel 1996 nell'ambito della *World Intellectual Property Organization* (WIPO), ossia il *"WIPO Copyright Treaty"* (WCT) ed il *"WIPO Performances and Phonograms Treaty"* (WPPT); il *"Libro verde della Commissione europea sul diritto d'autore e i diritti connessi nella Società dell'informazione"* del 27 luglio 1995, che fornisce le direttive da seguire nell'armonizzazione dei sistemi di controllo per la sicurezza in Internet, in modo da raggiungere una disciplina di tutela uniforme e standardizzata.

[88] 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" (*I giuristi e la società dell'informazione*, in *Dir. inf.*, 1996, 1, p. 18). Sulla tutela penale del *software* cfr., fra gli altri, G. CORRIAS LUCENTE, *Brevi note sulla tutela penale dei programmi informatici*, in *Dir. inf.*, 1999, 4-5, pp. 958-963.

d'autore", aveva fatto molto discutere per la nuova disciplina in tema di duplicazione abusiva di un *software*. L'art. 171 *bis* dispone che chiunque abusivamente duplica, *per trarne profitto*, "programmi per elaboratore o ai medesimi fini importa, distribuisce, vende, detiene a scopo commerciale o imprenditoriale o concede in locazione programmi contenuti in supporti non contrassegnati dalla Società italiana degli autori ed editori (SIAE), è soggetto alla pena della reclusione da sei mesi a tre anni e della multa da lire cinque milioni a lire trenta milioni"[89].

La l. 248/00 ha sostituito la dizione "a scopo di lucro" con la citata "per trarne profitto", così sanzionando penalmente anche il possesso non autorizzato di *software* e giungendo ad un ingiustificato inasprimento di regime[90], abbassando notevolmente la soglia di punibilità. Il legislatore non ha inoltre specificato che l'art. 171 *bis* non si applica "qualora la duplicazione abusiva di programmi sia posta in essere da privati al di fuori della loro attività professionale. Tale omissione rappresenta un concreto pericolo, atteso che, stante la lettera della norma (l'art. 171 *bis* apre con «chiunque»), anche il privato che duplica abusivamente software per tenerne presso di sé una copia, evitando così di spendere denaro per l'acquisto della copia autorizzata, potrà essere ritenuto penalmente responsabile. Si tenga presente, inoltre, che le pene edittali sono particolarmente elevate […], ed un «innocuo» duplicatore

[89] L'art. prosegue disponendo che "la stessa pena si applica se il fatto concerne qualsiasi mezzo inteso unicamente a consentire o facilitare la rimozione arbitraria o l'elusione funzionale di dispositivi applicati a protezione di un programma per elaboratori. La pena non è inferiore nel minimo a due anni di reclusione e la multa a lire trenta milioni se il fatto è di rilevante gravità".

[90] G. VACIAGO, *Il diritto d'autore e Internet*, in ID. (a cura di), *Internet e responsabilità giuridiche. Lineamenti, materiali e formulari in tema di diritto d'autore, nomi a dominio, Pubblica Amministrazione, privacy, reati informatici*, Piacenza, 2002, p. 20.

abusivo di software subirebbe un trattamento sanzionatorio affatto diverso da chi si macchi di reati particolarmente gravi quali, ad esempio, l'omicidio colposo"[91].

L'art. 171 *bis* l. aut. rende dunque palese l'intento di *deterrence* perseguito dal legislatore, che vuole scoraggiare chiunque dal porre in essere condotte lesive dei diritti delle grandi aziende del settore, mediante la minaccia di irrogazione di pene assolutamente non proporzionate alla gravità del fatto e pertanto in contrasto con i principi generali del diritto penale, che deve essere incentrato sul principio della stretta necessarietà (*nullum crimen, nulla poena sine necessitate*), circoscrivendo il ricorso alla sanzione penale nei rigorosi limiti della necessità di tutelare i diritti fondamentali della persona, direttamente o indirettamente. Tale principio comporta che la tutela penale debba essere riservata a beni fondamentali e contro offese di gravità intollerabile; ne consegue che il diritto penale ha carattere di sussidiarietà ed il suo ricorso è una *extrema ratio*, in ragione dell'inadeguatezza delle sanzioni extrapenali o per una più energica affermazione del valore tutelato[92].

Le considerazioni di cui sopra evidenziano che l'art. 171 *bis* si pone in stridente contrasto con il principio della proporzionalità della pena, che, "oltre a caratterizzare l'idea generale di giustizia, costituisce […] uno dei criteri-guida che presiedono allo stesso funzionamento dello Stato di diritto: è per questa ragione che il principio in parola costituisce

[91] G. ZICCARDI, *Il diritto d'autore nell'era digitale*, Milano, 2001, p. 75.

[92] F. MANTOVANI, *Diritto penale. Parte generale*, Padova, 1992, p. 24. Sulla depenalizzazione v., fra gli altri, A. ALBORGHETTI – BORGORTESE – M. MENEGHELLO, *Depenalizzazione e riforma del sistema sanzionatorio penale*, in A. ARTOSI – TOSIONGIOVANNI – NGIOIDA (a cura di), *Problemi della produzione e dell'attuazione normativa*, IV, *I diritti difficili nel sistema giuridico*, Bologna, 2001, pp. 209-222.

un parametro essenziale di qualsiasi teoria razionale e moderna sulla funzione della pena"[93]. Del resto, "l'obiettivo di impedire la commissione di reati non può mai giustificare l'inflizione di sanzioni «esemplari» o «terroristiche» manifestamente sproporzionate alla gravità del reato commesso"[94].

[93] G. FIANDACA – DACAUSCO, *Manuale di diritto penale. Parte generale*, Bologna, 1995, p. 638.
[94] G. FIANDACA – ANDAUSCO, *ivi*, p. 649.

CAPITOLO 7

IL DIRITTO ALLA PRIVACY

1. ORIGINE DEL DIRITTO ALLA PRIVACY

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

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

Già in alcuni procedimenti giudiziari, come Prince Albert *v.* Strange[2], i giudici avevano affermato la violazione, nel caso di specie, del diritto alla *privacy*, dunque riconoscendolo e rendendo palese la sua importanza non solo dal punto di vista teorico, ma soprattutto pratico, come dimostra la ricostruzione di Warren e Brandeis, nelle cui parole

[1] S. D. WARREN – RREN IVRANDEIS, *The right to privacy*, in *Harvard Law Review*, 1890, 4, p. 193, ora in *«Landmarks of Law»*, 1960, p. 261.
[2] Prince Albert *v.* Strange,1 McN & G. 25 (1849).

emerge la funzione della riservatezza quale argine contro gli attacchi di un giornalismo finalizzato non ad informare ma piuttosto a scandalizzare.

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

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

A detta degli autori, non ci si può esimere da responsabilità nel caso in cui si proceda alla pubblicazione di fatti o eventi caratterizzati da verità, poiché in tali ipotesi si verifica una lesione del *right to privacy*, il quale si trova su un differente piano logico, essendo ben distinto dal diritto all'identità personale. Parimenti, l'assenza di dolo e i motivi che hanno spinto a violare il diritto alla riservatezza non costituiscono una

[3] S. D. WARREN – RREN SVRANDEIS, *op. cit.*, p. 275.

scusante se il fatto si è verificato, visto che una volta che questo è stato compiuto non si può più tornare alla situazione *quo ante*. A queste conclusioni spinge un esame dell'intera *law of torts*, ai sensi della quale ciascuno è responsabile degli atti che compie intenzionalmente, anche se questi sono commessi in perfetta buona fede.

Secondo Warren e Brandeis, sarebbe necessario apprestare anche una tutela penale nei confronti del diritto alla riservatezza, soprattutto nei casi di estrema gravità della lesione che si realizzano, ad esempio, quando una eventuale pubblicazione abbia ampia diffusione[4]. Ovviamente, in tali eventualità è necessario un espresso intervento legislativo, poiché non si può procedere alla creazione di nuovi reati in via interpretativa. La necessità di una così forte forma di tutela è dovuta al fatto che, mediante una tutela individualizzata dei vari cittadini si riuscirebbe ad ottenere la tutela della società nel suo complesso[5].

Le tesi dei due giuristi statunitensi stupiscono ancor oggi per la loro modernità, soprattutto se si considera l'enorme divario tecnologico che separa gli Stati Uniti del finire dell'Ottocento dall'odierna società dell'informazione[6]. Oggi, all'acceleramento dei progressi in campo tecnico-scientifico e ai conseguenti benefici, si accompagna una pluralità di situazioni potenzialmente lesive della privacy di ciascuno di noi: basti pensare agli strumenti di acquisizione visiva e sonora, alla capillare diffusione dei *mass media*, all'avvento dell'informatica, alla diffusione di Internet.

---

[4] S. D. WARREN – RREN SVRANDEIS, *ibidem.*
[5] S. D. WARREN – RREN SVRANDEIS, *ibidem.*
[6] Sul diritto alla privacy v.: J. MICHAEL, *Privacy and human rights. An international and comparative study, with special reference to developments in information technology*, Aldershot-Paris, 1994; A. WESTIN, *Privacy and freedom*, New York, 1967.

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

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

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

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

Nella società odierna, tuttavia, in cui l'informazione assume sempre più rilevanza, anche e soprattutto da un punto di vista economico, sancire un diritto all'autodeterminazione informativa

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

permette di centralizzare il ruolo dell'uomo quale unico soggetto legittimato a decidere dell'uso di tutti i suoi dati personali. La vera essenza del diritto alla *privacy* non sta comunque nella sua eventuale patrimonialità potenziale, ma piuttosto nel suo carattere di diritto fondamentale ed inviolabile dell'uomo, che consente l'esercizio di altri diritti che sono legati alla possibilità di evitare inopportuni giudizi altrui, con riferimento a scelte di per sé insindacabili, come quelle legate a dati sensibili ed inerenti le scelte religiose e sessuali, le concezioni filosofiche, ecc. La lesione della riservatezza, inoltre, si riverbera anche sulla sfera psichica della soggetto che vede violato un suo diritto di rango costituzionale, che dovrebbe cedere solo dinanzi a casi concreti di particolare gravità ed in seguito all'effettuazione di un'operazione di bilanciamento fra diritti configgenti.

2. L'EVOLUZIONE DEL DIRITTO ALLA PRIVACY IN ITALIA

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

I primi contributi *in subiecta materia* risalgono agli anni trenta, periodo nel quale dobbiamo ricordare il contributo di Ravà[8], il quale individua, nel novero dei diritti della personalità, "un generale diritto alla

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

riservatezza"; pochi anni più tardi anche De Cupis[9] si mostra favorevole al riconoscimento di questo diritto. Inizia dunque un dibattito che coinvolge alcuni fra i più importanti studiosi italiani di diritto, divisi fra chi ritiene che la legge italiana tutela il diritto alla riservatezza[10] e fra chi sostiene il contrario[11].

Le discussioni in materia trovano nuovo vigore negli anni cinquanta, quando l'autorità giudiziaria viene investita di due procedimenti promossi per tutelare la riservatezza di due personaggi celebri, Enrico Caruso[12] e Claretta Petacci[13]. Nel «caso Caruso», in primo grado si afferma l'esistenza nel nostro ordinamento di un diritto alla riservatezza, tutelabile mediante l'applicazione analogica della disciplina del diritto all'immagine[14]. Tale diritto consiste "nel divieto di qualsiasi ingerenza estranea nella sfera della vita privata della persona, e di qualsiasi indiscrezione da parte di terzi, su quei fatti o comportamenti personali che, non pubblici per loro natura, non sono destinati alla

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

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

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

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

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

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

pubblicità delle persone che essi riguardano"[15]. Il giudizio prosegue poi innanzi la Corte di Cassazione[16], la quale ribalta l'impostazione seguita dai giudici di merito, e, seguendo la tesi prospettata da Pugliese[17], afferma che "il semplice desiderio di riserbo non è stato ritenuto dal legislatore un interesse tutelabile"[18] e quindi che nell'ordinamento italiano non esiste "un generale diritto alla «riservatezza», o «privatezza»"[19]. Questo orientamento non viene formalmente contraddetto dalla Suprema Corte sette anni più tardi[20], quando viene chiamata a pronunciarsi sul «caso Petacci»; come nel «caso Caruso», i giudici di merito[21] riconoscono l'esistenza del diritto alla riservatezza, ma stavolta viene invocata, come norma regolatrice del caso, l'art. 8[22] della Convenzione del Consiglio d'Europa per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali, ratificata in Italia con la legge 4 agosto 1955, n. 848. La Cassazione respinge questa tesi e nega ancora l'esistenza di un diritto alla riservatezza, purtuttavia "deve ammettersi la tutela nel caso di violazione del diritto assoluto di personalità inteso quale diritto *erga omnes* alla libertà di autodeterminazione nello svolgimento della personalità dell'uomo come singolo. Tale diritto è violato se si divulgano notizie della vita privata le quali, per tale loro natura, debbono ritenersi riservate"[23], e le quali trovano tutela nell'art. 2 Cost.

---

[15] Così Trib. Roma, *sent. ult. cit.*
[16] Cass., 22 dicembre 1956, n. 4487, in *Giust. Civ.*, 1957, I, p.5.
[17] Si veda G. PUGLIESE, *Il preteso diritto alla riservatezza e le indiscrezioni cinematografiche*, in *Foro It.*, 1954, c. 116, nota a Trib. Roma 14 settembre 1953.
[18] Cass., *sent. ult. cit.*, p.10.
[19] Cass., *sent. ult. cit.*, p. 5.
[20] Cass. 20 aprile 1963 n. 990, in *Foro It.*, 1963, I, c. 879.
[21] Corte d'appello di Milano, 26 agosto 1960, in *Foro It.*, 1961, I.
[22] *"Toute personne à droit au respect de sa vie privèe et familiale, de son domicile et de sa correspondance".*
[23] Cass., *sent. ult. cit.*, c. 879.

Nonostante questi contrasti, il legislatore interviene solo nel 1970 emanando la legge 20 maggio 1970 n. 300, il c.d. Statuto dei lavoratori, che contiene alcune previsioni a tutela della *privacy* dei lavoratori e pertanto applicabili solo nell'ambito del rapporto di lavoro. Più specificatamente, la legge vieta l'uso di impianti audiovisivi e di altre apparecchiature per finalità di controllo a distanza dell'attività dei lavoratori (art. 4) ed impedisce al datore di lavoro di effettuare accertamenti sulla idoneità e sulla infermità per malattia o infortunio del lavoratore dipendente (art. 5). Inoltre, l'art. 6 dispone che "le visite personali di controllo sul lavoratore sono vietate fuorché nei casi in cui siano indispensabili ai fini della tutela del patrimonio aziendale, in relazione alla qualità degli strumenti di lavoro o delle materie prime o dei prodotti. In tali casi le visite personali potranno essere effettuate soltanto a condizione che siano eseguite all'uscita dei luoghi di lavoro, che siano salvaguardate la dignità e la riservatezza del lavoratore e che avvengano con l'applicazione di sistemi di selezione automatica riferiti alla collettività o a gruppi di lavoratori". Infine, l'art. 8 vieta "al datore di lavoro, ai fini dell'assunzione, come nel corso dello svolgimento del rapporto di lavoro, di effettuare indagini, anche a mezzo di terzi, sulle opinioni politiche, religiose o sindacali del lavoratore, nonché su fatti non rilevanti ai fini della valutazione dell'attitudine professionale del lavoratore".

Le norme dello Statuto dei lavoratori fanno segnare dunque un passo avanti nella tutela della *privacy*, ma manca un intervento legislativo che esplicitamente lo riconosca e lo tuteli effettivamente. Fortunatamente, all'inerzia del legislatore fa seguito un intervento

suppletivo della giurisprudenza della Suprema Corte, che nel 1975, muta orientamento nella sua pronuncia sul c.d. «caso Soraya»[24], che rappresenta il *leading case* in materia e il formale riconoscimento dell'esistenza del diritto alla *privacy* nel nostro ordinamento, diritto "consiste[nte] nella tutela di quelle vicende strettamente personali e familiari le quali, anche se verificatesi fuori dal domicilio domestico, non hanno per i terzi un interesse socialmente apprezzabile, contro le ingerenze che, sia pure compiute con mezzi leciti, per scopi non esclusivamente speculativi e senza offesa per l'onore, la reputazione o il decoro, non siano giustificate da interessi pubblici preminenti"[25]. Le norme a fondamento del diritto alla riservatezza individuate dalla Cassazione sono assai numerose: gli artt. 2, 3, 14, 15, 27, 29, 41 Cost.; l'art. 1 legge 8 aprile 1974 n. 98; gli artt. 5, 6-10, 2105, 2622 cod. civ.; gli artt. 21, 24, 93 legge aut.; gli artt. 595 comma 2, 614, 616 cod. pen.; l'art. 48 legge fall.; l'art. 8 st. lav.; gli artt. 8 e 10 n. 2 della Convenzione del Consiglio d'Europa per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali; ed altre norme ancora cui sarebbe inutile accennare.

Risulta pertanto di palese evidenza che il diritto alla riservatezza ha trovato accoglimento in Italia grazie al lavorìo di dottrina e giurisprudenza, ed a parte alcuni disegni di legge mai approvati dalle

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

[25] Cass., *sent. ult. cit.*, c. 2905.

Camere per svariati motivi[26], il silenzio legislativo fino al 1996 (anno in cui viene emanata la legge 31 dicembre 1996, n. 675, ossia la c.d. legge sulla *privacy*) è rotto solo dalla legge 1 aprile 1981, n. 121 sull'amministrazione della pubblica sicurezza[27].

Negli anni successivi al «caso Soraya», la riflessione dottrinale e giurisprudenziale in tema di riservatezza non si è comunque arrestata, in virtù della sempre crescente problematicità del rapporto tra la tutela della vita privata dell'individuo e il diritto costituzionalmente garantito di libertà di manifestazione del pensiero, con riferimento soprattutto al diritto di cronaca[28]. Nel 1984 il dibattito in materia è diventato molto acceso, in seguito all'emanazione della nota sentenza della Corte di cassazione che ha stabilito il c.d. «decalogo dei giornalisti»[29], ossia

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

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

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

[29] Cass. 18 ottobre 1984, n. 5259, in *Dir. inf.*, 1985, 1, p. 143, con nota di S. FOIS – IS GIACOBBE – ACOBOROZZO DELLA ROCCA.

l'identificazione di quelle condizioni al verificarsi delle quali il diritto di cronaca può prevalere sul diritto alla riservatezza. Più precisamente, la Suprema Corte individua tre limiti:

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

Inoltre, in virtù dell'evoluzione delle concezioni in materia di rispetto della vita privata, parallelamente ai profili sinora citati, si registra la progressiva emersione di diritti che si pongono in condizione di complementarità rispetto alla *privacy*, come nel caso del diritto all'oblio, consistente nella pretesa dell'individuo che le vicende che lo riguardano non vengano più divulgate qualora la conoscenza di esse abbia perso il connotato dell'attualità[30].

Le riflessioni anzidette subiscono poi un ulteriore acceleramento, che ne rende ancor più manifesta l'importanza, perché l'avvento dei mezzi telematici ha consentito la trasmissione di informazioni in tempi prima impensabili, e già nel 1983 a queste ipotesi faceva acutamente riferimento Vincenzo Zeno-Zencovich, il quale ipotizzava una evoluzione tecnologica che nella sostanza si è oggi realizzata con la rete Internet [31], per mezzo della quale la violazione del diritto alla *privacy* può avvenire senza confini ed uscire totalmente fuori dal controllo del

[30] G. GIACOBBE, *op. cit.*, p. 112.
[31] V. ZENO-ZENCOVICH, *Telematica e tutela del diritto all'identità personale*, in *Pol. dir.*, 1983, 2, pp. 345 ss.

soggetto autore dell'illecito, con danni irreparabili per la persona la cui riservatezza è stata violata: Internet ha infatti una "formidabile capacità moltiplicatrice" [32]. Si conviene dunque con autorevole dottrina nell'affermare la necessità di rivedere ed aggiornare i criteri di valutazione degli strumenti di tutela della vita privata delle persone[33]. Con precipuo riferimento all'ordinamento italiano, è indispensabile che il progresso tecnologico, che nella pratica viene per lo più portato avanti da imprese private, venga instradato nel rispetto del disposto di cui all'art. 41 Cost., rispettando dunque quei diritti fondamentali della persona previsti dall'art. 2 Cost.

Proprio la disposizione da ultimo citata ha costituito la base per il riconoscimento della tutela di nuovi diritti che costituiscono l'attuazione concreta e il riconoscimento dei valori fondamentali della persona umana ed una giusta interpretazione del suddetto articolo ha contribuito a tutelare la *privacy* anche prima della legge n. 675/96 grazie all'apporto della giurisprudenza, che si è dimostrata molto più pronta del legislatore nel riconoscimento di un diritto fondamentale della persona umana, che inoltre assume un carattere di "garanzia-presupposto" dell'esercizio di altri diritti fondamentali perché violando la sfera intima si può dissuadere l'individuo dal compiere quelle scelte esistenziali per mezzo delle quali esercita il suo diritto di autodeterminarsi[34].

Il concreto soddisfacimento di queste istanze, a volte anche inconsce, della società, è dunque dovuto all'impegno di dottrina e giurisprudenza, che hanno più volte colmato i vuoti di tutela

[32] S. RODOTÀ, *Se non ci sono più confini qualche limite è necessario*, in *Telèma*, 1997, 8.
[33] G. GIACOBBE, *op. cit.*, p. 116.
[34] M. AIMO, *I «lavoratori di vetro»: regole di trattamento e meccanismi di tutela dei dati personali*, in *Riv. giur. prev. soc.*, 2002, 1, p. 48.

colpevolmente lasciati dal legislatore. Tuttavia, l'assenza di normative cogenti, ha in alcuni (rari) casi portato a posizioni indifendibili da una parte, seppur infinitesimale, della magistratura: basti pensare a quella sentenza del 1996 del Tribunale di Roma[35], nella quale si afferma che [se l'attore] "avesse davvero voluto tutelare la propria riservatezza, alla quale sembra tenere nel presente procedimento, avrebbe dovuto trovare una diversa forma di tutela dei propri diritti e non rivolgersi all'autorità giudiziaria"! Vi è di più: "nel caso di specie, non si tratta evidentemente di divulgazione di fatti gravi o riprovevoli, ma di una vicenda insolita e sotto certi aspetti stuzzicante perché collegata alla sfera sessuale". Questa è dunque "una visione nullificante dei diritti della personalità e della crescente arca di loro tutela"[36], e in merito (correttamente) Giuseppe Cassano afferma che "le poche affermazioni dell'organo giudicante sembrano aver mandato al macero intere biblioteche sul diritto alla riservatezza"[37].

Tuttavia, ferma restando l'inconcepibilità di una siffatta sentenza, con la quale il giudice romano sembra voler incentivare l'idea di farsi

[35] Trib. Roma 24 gennaio 1996, in *Dir. inf.*, 1996, 4-5, p. 572, con nota di V. ZENO-ZENCOVICH; il caso di specie riguardava l'ex-dirigente di un'azienda, che, a seguito del proprio licenziamento, aveva proposto azione avanti il Pretore di Frosinone per impugnare l'atto ed ottenere il risarcimento dei danni conseguenti, compreso il danno biologico in quanto l'attore lamentava disturbi alla sfera sessuale. Le parti giungevano poi ad una transazione, nella quale si riconosceva anche il risarcimento del danno biologico. Proprio quest'ultimo aspetto veniva ritenuto (oltre che stuzzicante dai giudici romani) anche interessante da quotidiani e periodici, i quali titolavano "Impotenza da licenziamento risarcita con 225 milioni – Perde lavoro e virilità" (La Repubblica) e "Un'insolita causa tra azienda e dipendente dimostra che il licenziamento fa male anche sotto le lenzuola – È vero: chi non lavora non fa l'amore" (Visto).

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

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

giustizia da sé, bisogna purtroppo ammettere che nel caso di violazione del diritto alla *privacy* il processo, per sua natura pubblico, potrebbe contribuire all'aggravamento della lesione suddetta. Si pensi al caso Soraya, il quale, come detto, costituisce il *leading case* in materia e che per tale motivo è citato in qualsiasi lavoro che si occupi della ricostruzione storica del diritto alla riservatezza, dunque ben al di fuori dei limiti della vicenda processuale. Sarebbe dunque auspicabile la predisposizione di una procedura *ad hoc* in tutti i casi in cui venga denunciata la violazione del diritto alla riservatezza, per evitare ulteriore pubblicità a vicende che dovrebbero invece essere private, anche se l'art. 128 cod. proc. civ. prevede che le udienze di discussione[38] possano svolgersi a porte chiuse ove ricorrano ragioni di ordine pubblico o buon costume.

Con riferimento alla diffusione delle sentenze e dei provvedimenti giudiziari, l'art. 52 comma 1 del Codice in materia di protezione di dati personali dispone che "l'interessato può chiedere per motivi legittimi, con richiesta depositata nella cancelleria o segreteria dell'ufficio che procede prima che sia definito il relativo grado di giudizio, che sia apposta a cura della medesima cancelleria o segreteria, sull'originale della sentenza o del provvedimento, un'annotazione volta a precludere, in caso di riproduzione della sentenza o provvedimento in qualsiasi forma, per finalità di informazione giuridica su riviste giuridiche, supporti elettronici o mediante reti di comunicazione elettronica, l'indicazione delle generalità e di altri dati identificativi del medesimo interessato riportati sulla sentenza o provvedimento". Ai sensi del successivo comma 5 della medesima norma, tali indicazioni vanno sempre omesse

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

se nel processo sono coinvolte persone vittime di reati di violenza sessuale o minori, oppure soggetti che sono parti in procedimenti in materia di rapporti di famiglia e di stato delle persone,

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

L'emanazione della legge n. 675/96 ha comunque posto termine alla lunga inerzia del legislatore italiano in materia di tutela del diritto alla riservatezza, in netto ritardo rispetto ai similari interventi normativi che in alcuni paesi (Svezia, Danimarca, Francia, ecc.) si erano avuti già negli anni settanta, ma appena in tempo per rispettare le prescrizioni dettate dall'Accordo di Schengen del 1985 e dalla direttiva della Comunità Europea 24 ottobre 1995, n. 46. Indipendentemente dalla valutazione qualitativa della legge in oggetto, è evidente che essa, anche grazie all'ottimo operato del Garante per la protezione dei dati personali, ha avuto grande risonanza a livello di riflessione scientifica, come dimostrano i numerosi contributi in materia[39], e, soprattutto, è stata

[39] Oltre alle opere già citate, cfr., fra gli altri: AA. VV., *Società dell'informazione tutela della riservatezza*, Atti del congresso di Stresa, 16-17 maggio 1997, Milano, 1998; R. ACCIAI, *Privacy e banche dati pubbliche. Il trattamento dei dati personali nelle pubbliche amministrazioni*, Padova, 2001; C. M. BIANCA – ANCA CHUSNELLI. (a cura di), *Tutela della privacy*, in *Nuove leggi civ. comm.*, 1999, 2-3; G. BUTTARELLI, *Banche dati e tutela della riservatezza. La privacy nella Società dell'Informazione*, Milano, 1997; V. CUFFARO – FFARICCIUTO – V. ZENO-ZENCOVICH (a cura di), *Trattamento dei dati e tutela della persona*, Milano, 1998;

progressivamente recepita dalla popolazione.

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

3.1 IL C.D. «CODICE DELLA PRIVACY»: ASPETTI GENERALI

In pochi anni la legge n. 675/96 ha subito numerose modifiche, effettuate mediante alcuni decreti legislativi che si sono succeduti sin dal 1997[41], che ne hanno modificato aspetti assai importanti, ed il suo contenuto è stato in gran parte trasfuso, seppur in alcuni casi con

---

E. GIANNANTONIO – ANNANTOOSANO – V. ZENO-ZENCOVICH, *Commentario alla legge 31 dicembre 1996, n. 675*, Padova, 1997; G. P. ZANETTA - ETTAASALEGNO, *La tutela della privacy nella sanità*, Milano, 1998.

[40] Cass. 25 marzo 2003, n. 4366, in *Dir. inf.*, 2003, 3, p. 523.

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

notevoli variazioni, nel d. lgs. 30 giugno 2003, n. 196, ossia il «**Codice in materia di protezione dei dati personali**» già detto «Codice della *privacy*» (d'ora in poi cod. priv.), la cui entrata in vigore è disposta per il 1° gennaio 2004[42]. Il codice, assai vasto, è diviso in tre parti: nella prima sono contenute le disposizioni generali e nella seconda quelle relative a specifici settori, mentre nella terza trovano posto le norme relative alle forme di tutela, alle sanzioni ed all'ufficio del Garante per la protezione dei dati personali (d'ora in poi Garante). La vastità del d.lgs. in oggetto rende palese la sempre maggiore importanza della tutela del diritto alla *privacy* in una molteplicità di situazioni, e sorprende come in pochi anni la normativa in tema di diritto alla riservatezza abbia fortunatamente colmato una pluridecennale lacuna legislativa, evolvendo da una legge approvata con poca cura per ottemperare ai citati obblighi internazionali dell'Italia ad un codice che "rappresenta il primo tentativo al mondo di conformare le innumerevoli disposizioni relative anche in via indiretta alla *privacy*"[43]. Esso costituisce, inoltre, il recepimento, oltre che di gran parte della legge n. 675/96 e delle norme che l'hanno modificata, anche delle pronunce emanate del Garante e dei pareri forniti dalla medesima *authority*, la cui attività è stata connotata da ragionevolezza e capacità di comprensione delle istanze avanzate da più parti nell'ambito dell'odierna società dell'informazione.

---

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

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

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

L'art. 2, ampliando la previsione di cui all'art. 1 comma 1 legge n. 675/96, dispone che il cod. priv. "garantisce che il trattamento dei dati personali si svolga nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali". Il riferimento esplicito sia al diritto alla riservatezza che al diritto alla protezione dei dati personali fa emergere il carattere di generalità del diritto alla *privacy*, del quale il diritto alla protezione dei dati personali costituisce, comunque, una specificazione.

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

trattamento dei dati personali effettuato da soggetti privati e pubblici".

La citata verifica di conformità dei codici deontologici alle leggi, operata dal Garante, riconosce loro "il valore di criterio di riferimento per determinare la legittimità del trattamento", per cui il rispetto delle regole ivi contenute costituisce elemento certo per la valutazione, eventualmente anche in sede giudiziaria, del rispetto dei suddetti principi di liceità e correttezza del trattamento. Ne consegue che "il codice deontologico assume valenza di norma, sebbene di grado secondario rispetto alla legge e ha l'innegabile pregio di penetrare meglio e più tecnicamente nei singoli settori di riferimento regolati"[44]. Al Garante è, dunque, affidato un compito assai delicato, perché, nella valutazione di ciascun codice, dovrà contemperare le opposte esigenze delle altre categorie coinvolte dalla creazione di siffatte disposizioni[45].

Il **trattamento di dati personali** consiste in "qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca di dati". Pertanto, tale amplissima definizione fa agevolmente comprendere che qualsiasi operazione compiuta sui dati personali rientra

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

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

nel campo di applicazione della normativa in oggetto.

I **dati personali** sono definiti come "qualunque informazione relativa 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). All'interno del novero dei dati personali la legge individua la categoria dei *dati identificativi*, ossia quei "dati personali che permettono l'identificazione diretta dell'interessato" (art. 4 comma 1 lett. c), e dei *dati sensibili*, il cui trattamento deve avvenire con modalità particolari, essendo quei "dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale" (art. 4 comma 1 lett. d).

L'art. 3, inoltre, impone un principio di carattere generale nell'ambito del trattamento dei dati personali, che deve avvenire secondo il **principio di necessità** del trattamento, con la conseguenza che bisogna configurare i sistemi informativi e i programmi informatici in modo da minimizzare l'utilizzazione di dati personali ed identificativi, così "da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi[46] od opportune modalità che permettano di identificare l'interessato solo in caso di necessità". Per quanto tale norma non sancisca un principio di

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

stretta necessità del trattamento, essa rappresenta comunque "una vera e propria rivoluzione nell'approccio alla protezione dei dati trattati con sistemi automatizzati, soprattutto nella sua applicazione al commercio elettronico e al funzionamento dei servizi di comunicazione"[47].

3.2 I SOGGETTI DEL CODICE DELLA PRIVACY

Il cod. priv., come già la legge n. 675/96, opera una tipizzazione dei soggetti che rilevano nell'ambito della attività di trattamento di dati personali. L'**interessato** è "la persona fisica, la persona giuridica, l'ente o l'associazione cui si riferiscono i dati personali" (art. 4 comma 1 lett. i). La legge fornisce una definizione onnicomprensiva, che tiene conto del fatto che la riservatezza non è un diritto proprio solo delle persone fisiche, ma anche di altri soggetti, cui viene dunque riconosciuto nella sua specifica accezione di diritto all'autodeterminazione informativa.

Il **titolare** del trattamento è, ai sensi dell'art. 4 comma 1 lett. f), "la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza". Questa definizione rende palese il ruolo apicale che il titolare occupa nella piramide gerarchica prospettata dal cod. priv., dato il particolare rilievo che rivestono i compiti attribuiti a questa figura, che, nel quadro dei soggetti che si occupano, in vario

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

modo, del trattamento, risulta l'unica assolutamente necessaria, in quanto è proprio il titolare a dar vita al trattamento. Rispetto alla normativa previgente, si rileva l'introduzione della possibilità espressa che vi siano più titolari.

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

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

Recependo un principio già sancito in via interpretativa dal Garante[48], il cod. priv. dispone che "quando il trattamento è effettuato da

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

una persona giuridica, da una pubblica amministrazione o da un qualsiasi altro ente, associazione od organismo, titolare del trattamento è l'entità nel suo complesso o l'unità od organismo periferico che esercita un potere decisionale del tutto autonomo sulle finalità e sulle modalità del trattamento, ivi compreso il profilo della sicurezza" (art. 28).

Il **responsabile** del trattamento di dati personali è "la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali" (art. 4 comma 1 lett. g); la nomina di questo soggetto è facoltativa, ai sensi dell'art. 29 comma 1, ed è espressione del potere di autonomia organizzativa del titolare, il quale, anche effettuando tale nomina, non viene comunque liberato da responsabilità. Il responsabile deve essere nominato tra soggetti che possano garantire, per esperienza, capacità ed affidabilità, il pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo della sicurezza dei dati; non deve necessariamente essere un unico soggetto, poiché l'art. 29 comma 3 permette la designazione di più responsabili, anche mediante suddivisione dei compiti, i quali devono sempre essere analiticamente specificati per iscritto (art. 29 comma 4). Quest'ultima disposizione non consente, quindi, che la designazione di tale figura avvenga in via implicita, ma la legge non pone preclusioni al cumulo di qualifiche all'interno della struttura del titolare, il quale può pertanto nominare responsabile anche un soggetto che ha già ulteriori qualifiche all'interno della predetta struttura, oltre a poterlo scegliere fra altre persone fisiche o servirsi di un organismo esterno incaricato di elaborare i dati.

---

anche S. FADDA, *Art. 1 comma 2*, in E. GIANNANTONIO – ANNANTOOSANO – V. ZENO-ZENCOVICH, cit, p. 19).

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

Nel caso in cui fra il responsabile ed il titolare intercorra un rapporto di lavoro subordinato, potrà trovare applicazione l'art. 2049 cod. civ., il quale sancisce la responsabilità dei padroni e committenti per i danni arrecati dal fatto illecito dei loro domestici e commessi nell'esercizio delle incombenze a cui sono adibiti. Nell'opposta eventualità in cui il responsabile non sia legato da un rapporto di lavoro subordinato, si renderà necessaria la conclusione di un contratto per mezzo del quale il titolare conferisca al responsabile l'incarico di gestire il trattamento; in dottrina è stata ipotizzata, in tal caso, l'applicazione delle norme che disciplinano l'appalto di servizi, con la conseguenza di spostare dal titolare al responsabile i rischi connessi allo svolgimento dell'attività[49].

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

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

[49] S. FADDA., *op. cit.*, p. 93.

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

3.3 IL TRATTAMENTO DI DATI PERSONALI (INFORMATIVA, CONSENSO, NOTIFICAZIONE)

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

dell'applicazione della disciplina sul trattamento dei dati personali.

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

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

Le operazioni che costituiscono trattamento ai sensi del cod. priv. possono essere suddivise in base alle seguenti fasi inerenti le banche dati[50]:

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

L'art. 11 detta i *principi qualitativi* circa la raccolta e i requisiti dei dati personali oggetto di trattamento[51], che devono essere:

[50] Si segue qui la divisione di M. AMBROSOLI, *La tutela dei dati personali e la responsabilità civile*, in *Riv. dir. priv.*, 1998, 2, p. 305.
[51] S. SICA, *Danno morale e legge sulla privacy informatica*, in *Danno e resp.*, 1997, 3, p. 283.

a) trattati in modo lecito e secondo correttezza[52];
b) raccolti e registrati per scopi determinati, espliciti e legittimi, ed utilizzati in altre operazioni del trattamento in termini compatibili con tali scopi;
c) esatti e, se necessario, aggiornati;
d) pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti o successivamente trattati;
e) conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati.

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

Prima di procedere al trattamento dei dati è necessario, innanzi tutto, fornire l'**informativa** al soggetto i cui dati potranno essere oggetto di trattamento. Queste informazioni possono essere rese oralmente o per iscritto[53] e, ai sensi dell'art. 13 e salvo diverse disposizioni, devono indicare:

a) le finalità e le modalità del trattamento cui sono destinati i dati;
b) la natura obbligatoria o facoltativa del conferimento dei dati;

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

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

c) le conseguenze di un eventuale rifiuto di rispondere;
d) 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;
e) i diritti dell'interessato previsti dall'art. 7;
f) gli estremi identificativi del titolare e, se designati, del responsabile[54] e del rappresentante nel territorio dello Stato di cui all'art. 5.

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

Prendendo atto della sempre maggiore diffusione dei *call centers*, il cod. priv. dispone che il Garante può individuare, con proprio provvedimento, modalità semplificate per l'informativa fornita in particolare da servizi telefonici di assistenza e informazione al pubblico[55].

Se i dati personali non sono raccolti presso l'interessato, l'informativa, comprensiva delle categorie di dati trattati, è a lui data al

[54] Quando il titolare ha designato più responsabili è indicato almeno uno di essi, indicando il sito della rete di comunicazione o le modalità attraverso le quali è conoscibile in modo agevole l'elenco aggiornato dei responsabili. Quando è stato designato un responsabile per il riscontro all'interessato in caso di esercizio dei diritti di cui all'art. 7, è indicato tale responsabile.
[55] In virtù dell'inciso "in particolare" dovrebbe comunque ritenersi che tale elencazione sia solo esemplificativa.

momento della registrazione dei dati o, quando è prevista la loro comunicazione, non oltre la prima comunicazione, fatte salve alcune eccezioni. Esse si verificano quando i dati sono trattati per ottemperare ad un obbligo previsto dalla legge, da un regolamento o dalla normativa comunitaria, o per lo svolgimento di investigazioni difensive o, comunque, per far valere o difendere un diritto in sede giudiziaria[56], o, ancora, se l'informativa all'interessato è, a giudizio del Garante, impossibile oppure troppo gravosa con riferimento al diritto tutelato.

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

L'art. 24, tuttavia, prevede numerose ipotesi nelle quali il trattamento può avvenire a prescindere dal consenso, qualora il trattamento stesso sia necessario per adempiere ad un obbligo previsto dalla legge, da un regolamento o dalla normativa comunitaria o per eseguire obblighi derivanti da un contratto del quale è parte l'interessato o per adempiere, prima della conclusione del contratto, a specifiche richieste dell'interessato. Il consenso non è altresì richiesto se il trattamento riguarda dati provenienti da pubblici registri, elenchi, atti o documenti conoscibili da chiunque, (fermi restando i limiti e le modalità

[56] "Sempre che i dati siano trattati esclusivamente per tali finalità e per il periodo strettamente necessario al loro perseguimento" (art. 13 comma 5 lett. b).

che le leggi, i regolamenti o la normativa comunitaria stabiliscono per la conoscibilità e pubblicità dei dati) oppure dati relativi allo svolgimento di attività economiche (trattati nel rispetto delle leggi di settore), o, ancora, se è necessario per la salvaguardia della vita o dell'incolumità fisica di un terzo[57].

Con esclusione dell'ipotesi di diffusione dei dati, il consenso non è richiesto se il trattamento è necessario ai fini, cui si è accennato, dello svolgimento delle investigazioni difensive o per far valere o difendere un diritto in sede giudiziaria, oppure se è necessario, nei casi individuati dal Garante sulla base dei principi sanciti dalla legge, per perseguire un legittimo interesse del titolare o di un terzo destinatario dei dati, anche in riferimento all'attività di gruppi bancari e di società controllate o collegate, qualora non prevalgano i diritti e le libertà fondamentali, la dignità o un legittimo interesse dell'interessato, e lo stesso vale per le associazioni *no profit* con riferimento ai propri soci ed aderenti, fatta eccezione per la comunicazione all'esterno e per la diffusione. Infine, il consenso non deve essere prestato nel caso in cui il trattamento sia necessario (in conformità ai rispettivi codici deontologici), per esclusivi scopi scientifici, statistici o storici (in quest'ultimo caso, presso archivi

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

privati dichiarati di notevole interesse storico).

Per i *dati sensibili* sono invece predisposte regole diverse, in ragione dell'importanza che tali dati rivestono, poiché essi riguardano i più intimi aspetti dell'uomo, e dunque essi possono essere trattati solo con il consenso scritto dell'interessato e previa autorizzazione del Garante. Tale regola non si applica, tuttavia, al trattamento dei dati relativo agli aderenti alle confessioni religiose e ai soggetti che con riferimento a finalità di natura esclusivamente religiosa hanno contatti regolari con le medesime confessioni, effettuato dai relativi organi, ovvero da enti civilmente riconosciuti, sempre che i dati non siano diffusi o comunicati fuori delle medesime confessioni; non si applica, inoltre, al trattamento dei dati riguardanti l'adesione di associazioni od organizzazioni a carattere sindacale o di categoria ad altre associazioni, organizzazioni o confederazioni a carattere sindacale o di categoria[58]. Infine, la tutela dei

[58] Art. 26 comma 4: "I dati sensibili possono essere oggetto di trattamento anche senza consenso, previa autorizzazione del Garante: a) quando il trattamento è effettuato da associazioni, enti od organismi senza scopo di lucro, anche non riconosciuti, a carattere politico, filosofico, religioso o sindacale, ivi compresi partiti e movimenti politici, per il perseguimento di scopi determinati e legittimi individuati dall'atto costitutivo, dallo statuto o dal contratto collettivo, relativamente ai dati personali degli aderenti o dei soggetti che in relazione a tali finalità hanno contatti regolari con l'associazione, ente od organismo, sempre che i dati non siano comunicati all'esterno o diffusi e l'ente, associazione od organismo determini idonee garanzie relativamente ai trattamenti effettuati, prevedendo espressamente le modalità di utilizzo dei dati con determinazione resa nota agli interessati all'atto dell'informativa ai sensi dell'articolo 13; b) quando il trattamento è necessario per la salvaguardia della vita o dell'incolumità fisica di un terzo. Se la medesima finalità riguarda l'interessato e quest'ultimo non può prestare il proprio consenso per impossibilità fisica, per incapacità di agire o per incapacità di intendere o di volere, il consenso è manifestato da chi esercita legalmente la potestà, ovvero da un prossimo congiunto, da un familiare, da un convivente o, in loro assenza, dal responsabile della struttura presso cui dimora l'interessato. Si applica la disposizione di cui all'articolo 82, comma 2; c) quando il trattamento è necessario ai fini dello svolgimento delle investigazioni difensive di cui alla legge 7 dicembre 2000, n. 397, o, comunque, per far valere o difendere in sede giudiziaria un diritto, sempre che i dati siano trattati

dati personali idonei a rivelare lo stato di salute è ancor più incisiva, considerando il divieto di diffusione di tali dati posto dall'art. 26 comma 5.

Sempre per garantire una maggiore tutela dei dati personali, nell'originario impianto normativo della legge n. 675/96 era previsto che il titolare che intendesse procedere ad un trattamento di dati personali ne avrebbe dovuto dare notificazione al Garante[59]. Da ultimo, il d.lgs. 467/01 aveva modificato tale disposizione prevedendo che "il titolare che intenda procedere ad un trattamento di dati personali soggetto al campo di applicazione della presente legge è tenuto a darne notificazione al Garante se il trattamento, in ragione delle relative modalità o della natura dei dati personali, sia suscettibile di recare pregiudizio ai diritti e alle libertà dell'interessato, e nei soli casi e con le modalità individuati con il regolamento di cui all'articolo 33, comma 3".

Il cod. priv., proseguendo sulla medesima linea del d.lgs. 467/01, innova profondamente nell'ambito dell'adempimento della **notificazione**, che, pertanto, di norma, non va effettuata, fatta eccezione per i casi espressamente previsti dal medesimo codice oppure per quelli individuati dal Garante. Le ipotesi già previste riguardano trattamenti di

---

esclusivamente per tali finalità e per il periodo strettamente necessario al loro perseguimento. Se i dati sono idonei a rivelare lo stato di salute e la vita sessuale, il diritto deve essere di rango pari a quello dell'interessato, ovvero consistente in un diritto della personalità o in un altro diritto o libertà fondamentale e inviolabile; d) quando è necessario per adempiere a specifici obblighi o compiti previsti dalla legge, da un regolamento o dalla normativa comunitaria per la gestione del rapporto di lavoro, anche in materia di igiene e sicurezza del lavoro e della popolazione e di previdenza e assistenza, nei limiti previsti dall'autorizzazione e ferme restando le disposizioni del codice di deontologia e di buona condotta di cui all'articolo 111".

[59] Art. 7 legge n. 675/96: "il titolare che intenda procedere ad un trattamento di dati personali soggetto al campo di applicazione della presente legge è tenuto a darne notificazione al Garante".

particolari dati sensibili, come i dati sanitari o relativi alla vita sessuale o riguardanti la solvibilità economica[60], ma si prende anche atto dell'evoluzione tecnologica, indicando, come primo caso, quello dei dati genetici, biometrici e di quelle informazioni che indicano la posizione geografica di persone od oggetti mediante una rete di comunicazione elettronica[61].

Tale elencazione può essere successivamente integrata da un provvedimento del Garante che individui altri trattamenti che possono recare pregiudizio ai diritti ed alle libertà dell'interessato, in ragione delle relative modalità o della natura dei dati personali. La medesima *authority*,

---

[60] Art. 37 comma 1: "Il titolare notifica al Garante il trattamento di dati personali cui intende procedere, solo se il trattamento riguarda: a) dati genetici, biometrici o dati che indicano la posizione geografica di persone od oggetti mediante una rete di comunicazione elettronica; b) 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; c) dati idonei a rivelare la vita sessuale o la sfera psichica trattati da associazioni, enti od organismi senza scopo di lucro, anche non riconosciuti, a carattere politico, filosofico, religioso o sindacale; d) dati trattati con l'ausilio di strumenti elettronici volti a definire il profilo o la personalità dell'interessato, o ad analizzare abitudini o scelte di consumo, ovvero a monitorare l'utilizzo di servizi di comunicazione elettronica con esclusione dei trattamenti tecnicamente indispensabili per fornire i servizi medesimi agli utenti; e) dati sensibili registrati in banche di dati a fini di selezione del personale per conto terzi, nonché dati sensibili utilizzati per sondaggi di opinione, ricerche di mercato e altre ricerche campionarie; f) dati registrati in apposite banche di dati gestite con strumenti elettronici e relative al rischio sulla solvibilità economica, alla situazione patrimoniale, al corretto adempimento di obbligazioni, a comportamenti illeciti o fraudolenti".

[61] In merito si rileva la pericolosità del *Total Information Awareness* (TIA), portato avanti negli Stati Uniti dal citato *Information Awareness Office*, il cui l'obiettivo è l'acquisizione della conoscenza di qualsiasi tipo di informazione. In tale ambito si può ricordare il programma *HumanID*, finalizzato allo "sviluppo di tecnologie automatizzate di identificazione biometrica per rilevare, riconoscere e identificare persone a grandi distanze". La violazione della *privacy* che si realizza in tali casi è dunque tanto palese da non richiedere, purtroppo, ulteriori commenti (sul punto sia consentito rinviare a G. FIORIGLIO, *La privacy e i sistemi di controllo di intercettazione globale: il caso dell'Information Awareness Office*, in *L'ircocervo*, 2003, 2, sez. leg.).

inoltre, può sottrarre all'obbligo di notificazione, nell'ambito dei trattamenti sopra elencati, eventuali trattamenti che ritenga non siano suscettibili di recare detto pregiudizio.

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

Nella normativa previgente, la notificazione doveva essere effettuata a mezzo di lettera raccomandata o con altro mezzo idoneo a certificarne la ricezione: oggi l'art. 38 comma 2 dispone che "la notificazione è validamente effettuata solo se è trasmessa per via telematica utilizzando il modello predisposto dal Garante e osservando le prescrizioni da questi impartite, anche per quanto riguarda le modalità di sottoscrizione con firma digitale e di conferma del ricevimento della notificazione", mentre il comma 4 prevede che "il Garante può individuare altro idoneo sistema per la notificazione in riferimento a nuove soluzioni tecnologiche previste dalla normativa vigente". In tal modo si prende correttamente atto dell'utilità degli strumenti informatici e telematici, che consentono di rendere assai più celeri le attività di trasmissione delle informazioni.

Nel caso di **cessazione**, per qualsiasi causa, di un trattamento, l'art. 16 prevede che i dati personali oggetto del trattamento medesimo possono essere distrutti, ceduti ad altro titolare[62], conservati per fini esclusivamente personali[63] oppure conservati o ceduti ad altro titolare,

[62] Purché destinati ad un trattamento in termini compatibili agli scopi per i quali i dati sono raccolti.
[63] Ma non destinati ad una comunicazione sistematica o alla diffusione.

per scopi storici, statistici o scientifici, in conformità alla legge, ai regolamenti, alla normativa comunitaria e ai codici deontologici.

3.4 I DIRITTI DELL'INTERESSATO

Il titolo II della I parte del cod. priv. è dedicato ai **diritti dell'interessato**. In particolare, l'art. 7 dispone che "l'interessato ha diritto di ottenere la conferma dell'esistenza o meno di dati personali che lo riguardano, anche se non ancora registrati, e la loro comunicazione in forma intelligibile".

Inoltre, l'interessato ha diritto di ottenere l'indicazione:

a) dell'origine dei dati personali;
b) delle finalità e modalità del trattamento;
c) della logica applicata in caso di trattamento effettuato con l'ausilio di strumenti elettronici;
d) degli estremi identificativi del titolare, dei responsabili e del rappresentante designato ai sensi dell'art. 5 comma 2;
e) dei soggetti o delle categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di rappresentante designato nel territorio dello Stato, di responsabili o incaricati (art. 7 comma 2).

L'interessato ha diritto di ottenere:

a) l'aggiornamento, la rettificazione oppure, quando vi ha interesse, l'integrazione dei dati;

b) la cancellazione, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge, compresi quelli di cui non è necessaria la conservazione in relazione agli scopi per i quali i dati sono stati raccolti o successivamente trattati;

c) l'attestazione che le operazioni di cui alle lettere a) e b) sono state portate a conoscenza, anche per quanto riguarda il loro contenuto, di coloro ai quali i dati sono stati comunicati o diffusi, eccettuato il caso in cui tale adempimento si rivela impossibile o comporta un impiego di mezzi manifestamente sproporzionato rispetto al diritto tutelato (art. 7 comma 3).

L'interessato ha diritto di opporsi, in tutto o in parte: a) per motivi legittimi al trattamento dei dati personali che lo riguardano, ancorché pertinenti allo scopo della raccolta; b) al trattamento di dati personali che lo riguardano a fini di invio di materiale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato o di comunicazione commerciale.

I diritti di cui si è detto[64] possono essere esercitati mediante

[64] L'art. 8 comma 2 prevede comunque alcune eccezioni al principio appena detto, disponendo che "I diritti di cui all'articolo 7 non possono essere esercitati con richiesta al titolare o al responsabile o con ricorso ai sensi dell'articolo 145, se i trattamenti di dati personali sono effettuati: a) in base alle disposizioni del decreto-legge 3 maggio 1991, n. 143, convertito, con modificazioni, dalla legge 5 luglio 1991, n. 197, e successive modificazioni, in materia di riciclaggio; b) in base alle disposizioni del decreto-legge 31 dicembre 1991, n. 419, convertito, con modificazioni, dalla legge 18 febbraio 1992, n. 172, e successive modificazioni, in materia di sostegno alle vittime di richieste estorsive; c) da Commissioni parlamentari d'inchiesta istituite ai sensi dell'articolo 82 della Costituzione; d) da un soggetto pubblico, diverso dagli enti pubblici economici, in base ad espressa disposizione di legge, per esclusive finalità inerenti alla politica monetaria e valutaria, al sistema dei pagamenti, al controllo degli

richiesta rivolta senza formalità al titolare o al responsabile, anche per il tramite di un incaricato, alla quale è fornito idoneo riscontro senza ritardo. Se la richiesta riguarda i diritti di cui all'art 7, commi 1 e 2, può essere effettuata anche oralmente, mentre in tutti gli altri casi può essere proposta tramite raccomandata, fax, posta elettronica o altro sistema idoneo individuato dal Garante in base all'evoluzione tecnologica, e può essere riproposta, salvo giustificati motivi, non prima di novanta giorni dalla prima richiesta. Quando i dati trattati non hanno carattere oggettivo, non può tuttavia essere chiesta la rettificazione o l'integrazione di dati personali di tipo valutativo, relativi a giudizi, opinioni o ad altri apprezzamenti di tipo soggettivo, nonché l'indicazione di condotte da tenersi o di decisioni in via di assunzione da parte del titolare del trattamento.

L'interessato può esercitare personalmente (anche con l'assistenza di una persona di fiducia) i diritti di cui all'art. 7, o per mezzo di altri soggetti (persone fisiche, enti, associazioni od organismi) cui viene conferita, per iscritto, delega o procura. Qualora i diritti in oggetto si

---

intermediari e dei mercati creditizi e finanziari, nonché alla tutela della loro stabilità; e) ai sensi dell'articolo 24, comma 1, lettera f), limitatamente al periodo durante il quale potrebbe derivarne un pregiudizio effettivo e concreto per lo svolgimento delle investigazioni difensive o per l'esercizio del diritto in sede giudiziaria; f) da fornitori di servizi di comunicazione elettronica accessibili al pubblico relativamente a comunicazioni telefoniche in entrata, salvo che possa derivarne un pregiudizio effettivo e concreto per lo svolgimento delle investigazioni difensive di cui alla legge 7 dicembre 2000, n. 397; g) per ragioni di giustizia, presso uffici giudiziari di ogni ordine e grado o il Consiglio superiore della magistratura o altri organi di autogoverno o il Ministero della giustizia; h) ai sensi dell'articolo 53, fermo restando quanto previsto dalla legge 1 aprile 1981, n. 121". Il comma 3, inoltre, dispone che "il Garante, anche su segnalazione dell'interessato, nei casi di cui al comma 2, lettere a), b), d), e) ed f) provvede nei modi di cui agli articoli 157, 158 e 159 e, nei casi di cui alle lettere c), g) ed h) del medesimo comma, provvede nei modi di cui all'articolo 160".

riferiscano a dati personali concernenti persone decedute, essi possono essere esercitati da chi ha un interesse proprio, o agisce a tutela dell'interessato o per ragioni familiari meritevoli di protezione.

Salvo specifica richiesta, il **riscontro** comprende tutti i dati personali che riguardano l'interessato e che sono trattati dal titolare, il quale deve, da un lato, adottare tutte le misure idonee ad agevolare all'interessato l'accesso ai propri dati, dall'altro, semplificare le modalità ed ottimizzare i tempi per il riscontro di cui sopra (art. 10). Il responsabile o gli incaricati si occupano dell'estrazione dei dati, che possono poi essere comunicati al richiedente in via orale oppure essere offerti in visione mediante strumenti elettronici, purché non ne venga pregiudicata la comprensibilità. Inoltre, è possibile, dietro richiesta, provvedere alla loro trasposizione su supporto cartaceo o informatico, oppure alla loro trasmissione per via telematica. Se l'estrazione dei dati risulta particolarmente difficoltosa, il riscontro può avvenire anche attraverso l'esibizione o la consegna in copia di atti e documenti contenenti i dati personali richiesti[65].

[65] L'art. 10, ai commi successivi, prevede, poi, che "il diritto di ottenere la comunicazione in forma intelligibile dei dati non riguarda dati personali relativi a terzi, salvo che la scomposizione dei dati trattati o la privazione di alcuni elementi renda incomprensibili i dati personali relativi all'interessato. La comunicazione dei dati è effettuata in forma intelligibile anche attraverso l'utilizzo di una grafia comprensibile. In caso di comunicazione di codici o sigle sono forniti, anche mediante gli incaricati, i parametri per la comprensione del relativo significato. Quando, a seguito della richiesta di cui all'articolo 7, commi 1 e 2, lettere a), b) e c) non risulta confermata l'esistenza di dati che riguardano l'interessato, può essere chiesto un contributo spese non eccedente i costi effettivamente sopportati per la ricerca effettuata nel caso specifico. Il contributo di cui al comma 7 non può comunque superare l'importo determinato dal Garante con provvedimento di carattere generale, che può individuarlo forfettariamente in relazione al caso in cui i dati sono trattati con strumenti elettronici e la risposta è fornita oralmente. Con il medesimo provvedimento il Garante può prevedere che il contributo possa essere

3.5 LE MISURE DI SICUREZZA

Alla sicurezza dei dati e dei sistemi è dedicato il titolo V della I parte del cod. priv. Nel capo I trovano posto le norme in tema di misure di sicurezza, mentre nel II sono disciplinate le misure minime di sicurezza. Questa tematica ha un ruolo centrale nella regolamentazione del trattamento dei dati personali, anche in considerazione del fatto che l'omessa adozione delle misure minime di sicurezza costituisce un illecito penale. Si consideri, inoltre, che "la sicurezza dei dati costituisce una garanzia «esterna» diretta, in via preventiva, a ridurre al minimo il rischio di interazioni di situazioni patologiche estranee con le libertà e i diritti sottesi al trattamento" e da ciò risulta "l'*indisponibilità* della disciplina da parte dei soggetti coinvolti nel trattamento dei dati, che verosimilmente si potrebbe tradurre nella rinuncia da parte dell'interessato alle misure di sicurezza, […ma] la mancata predisposizione delle stesse potrebbe comportare una lesione alla dignità umana, […che] costituisce l'asse portante ed inviolabile di equilibrio tra gli interessi contrapposti"[66].

L'art. 31 stabilisce, in linea generale, gli **obblighi di sicurezza**: "i dati personali oggetto di trattamento sono custoditi e controllati, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo

---

chiesto quando i dati personali figurano su uno speciale supporto del quale è richiesta specificamente la riproduzione, oppure quando, presso uno o più titolari, si determina un notevole impiego di mezzi in relazione alla complessità o all'entità delle richieste ed è confermata l'esistenza di dati che riguardano l'interessato. Il contributo di cui ai commi 7 e 8 è corrisposto anche mediante versamento postale o bancario, ovvero mediante carta di pagamento o di credito, ove possibile all'atto della ricezione del riscontro e comunque non oltre quindici giorni da tale riscontro".

[66] S. PARDINI, *Art. 15*, in C. M. BIANCA – AN D. BUSNELLI (a cura di), *Tutela della privacy*, in *Nuove leggi. civ. comm.*, 1999, 2-3, II, p. 439.

da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta". L'art. 32, invece, disciplina il caso in cui il titolare è un fornitore di un servizio di comunicazione elettronica accessibile al pubblico[67].

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

In particolare, l'art. 34 prevede che "il trattamento di dati personali effettuato con strumenti elettronici è consentito solo se sono adottate,

[67] "Il fornitore di un servizio di comunicazione elettronica accessibile al pubblico adotta ai sensi dell'articolo 31 idonee misure tecniche e organizzative adeguate al rischio esistente, per salvaguardare la sicurezza dei suoi servizi, l'integrità dei dati relativi al traffico, dei dati relativi all'ubicazione e delle comunicazioni elettroniche rispetto ad ogni forma di utilizzazione o cognizione non consentita. Quando la sicurezza del servizio o dei dati personali richiede anche l'adozione di misure che riguardano la rete, il fornitore del servizio di comunicazione elettronica accessibile al pubblico adotta tali misure congiuntamente con il fornitore della rete pubblica di comunicazioni. In caso di mancato accordo, su richiesta di uno dei fornitori, la controversia è definita dall'Autorità per le garanzie nelle comunicazioni secondo le modalità previste dalla normativa vigente. Il fornitore di un servizio di comunicazione elettronica accessibile al pubblico informa gli abbonati e, ove possibile, gli utenti, se sussiste un particolare rischio di violazione della sicurezza della rete, indicando, quando il rischio è al di fuori dell'ambito di applicazione delle misure che il fornitore stesso è tenuto ad adottare ai sensi dei commi 1 e 2, tutti i possibili rimedi e i relativi costi presumibili. Analoga informativa è resa al Garante e all'Autorità per le garanzie nelle comunicazioni".

nei modi previsti dal disciplinare tecnico contenuto nell'allegato B), le seguenti misure minime:

a) autenticazione informatica;
b) adozione di procedure di gestione delle credenziali di autenticazione;
c) utilizzazione di un sistema di autorizzazione;
d) aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici;
e) protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di dati, ad accessi non consentiti e a determinati programmi informatici;
f) adozione di procedure per la custodia di copie di sicurezza, il ripristino della disponibilità dei dati e dei sistemi;
g) tenuta di un aggiornato documento programmatico sulla sicurezza;
h) adozione di tecniche di cifratura o di codici identificativi per determinati trattamenti di dati idonei a rivelare lo stato di salute o la vita sessuale effettuati da organismi sanitari".

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

a) aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unità organizzative;

b) previsione di procedure per un'idonea custodia di atti e documenti affidati agli incaricati per lo svolgimento dei relativi compiti;
c) previsione di procedure per la conservazione di determinati atti in archivi ad accesso selezionato e disciplina delle modalità di accesso finalizzata all'identificazione degli incaricati".

Pertanto, nell'allegato B del cod. priv. sono contenute le norme che stabiliscono le misure minime di sicurezza che devono essere adottate dal titolare, dal responsabile e dagli incaricati per non essere responsabili penalmente *ex* art. 169 cod. priv.. L'allegato in oggetto è suddiviso in ventinove punti, nei quali si regolamentano il sistema di autenticazione informatica[68], il sistema di autorizzazione[69], le ulteriori misure di sicurezza[70], il documento programmatico sulla sicurezza[71], le

[68] Il trattamento di dati personali con strumenti elettronici è consentito agli incaricati dotati di credenziali di autenticazione che consentano il superamento di una procedura di autenticazione. Tali credenziali consistono in un codice identificativo personale associato ad una parola chiave (o *password*) oppure in un dispositivo di autenticazione (usato esclusivamente dall'incaricato) , che può essere associato ad un codice identificativo, ad una *password* o ad una caratteristica biometrica dell'interessato (eventualmente associata ad un codice identificativo o ad una parola chiave). La componente riservata di ciascuna credenziale deve essere tenuta segreta, utilizzando particolari cautele; inoltre, i dispositivi di autenticazione devono essere custoditi con la dovuta diligenza.

[69] I profili di autorizzazione, da assegnare a ciascun incaricato, sono individuati e configurati anteriormente all'inizio del trattamento, al fine di limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento.

[70] Si dispone che l'aggiornamento della lista degli incaricati e degli addetti alla manutenzione od alla gestione degli strumenti informatici sia effettuato quanto meno annualmente; lo stesso vale gli aggiornamenti *software* relativi sia alla vulnerabilità che alla rimozione dei c.d. *bugs* dei programmi utilizzati, fatta eccezione in caso di trattamento di dati sensibili o giudiziari: in tali casi l'aggiornamento deve essere quanto meno semestrale, così come deve avvenire, in linea generale, per le protezioni contro il rischio di intrusione e di azione di "programmi diretti a danneggiare o interrompere un sistema informatico", di cui all'art. 615 *quinquies* cod. pen., che devono essere aggiornate con la medesima cadenza. Infine, si prevede che i dati

misure da adottare in caso di trattamento di dati sensibili e giudiziari[72], nonché quelle da adottare per trattamenti senza l'ausilio di strumenti elettronici[73].

3.6 IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Con l'emanazione della legge n. 675/96 è stata creata una nuova *authority*, il **Garante per la protezione dei dati personali**, che ha sinora confermato la bontà della scelta legislativa, "conseguendo il non semplice obiettivo di affermare la «cultura» della riservatezza, senza cedimenti o

devono essere salvati quanto meno ogni settimana. Bisogna tuttavia rilevare l'imprecisione di quest'ultima disposizione, da intendersi, probabilmente, come obbligo di effettuare una copia di riserva (o copia di *backup*) dei dati con cadenza settimanale: del resto, se i dati non vengono salvati una volta presenti nella memoria dell'elaboratore, al suo spegnimento essi vengono irrimediabilmente persi.

[71] Il documento programmatico sulla sicurezza deve essere redatto dal titolare di un trattamento di dati sensibili o di dati giudiziari (anche attraverso il responsabile) entro il 31 marzo di ogni anno. In esso sono indicati, fra l'altro, l'elenco dei trattamenti, la distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati, l'analisi dei rischi che incombono sui dati, le misure da adottare per garantirne l'integrità e la disponibilità.

[72] I dati sensibili e giudiziari devono essere protetti contro eventuali accessi abusivi, di cui all'art. 615 *ter* cod. pen., mediante l'utilizzo di idonei strumenti elettronici. Inoltre, se memorizzati su supporti rimovibili, devono essere impartite istruzioni tecniche ed organizzative per impedirne accessi non autorizzati e trattamenti non consentiti, e se tali supporti non sono utilizzati, devono essere distrutti o resi inutilizzabili, ma possono essere riutilizzati, anche da altri incaricati, qualora le informazioni ivi contenute non siano intelligibili e tecnicamente in alcun modo ricostruibili. Particolari cautele sono previste per i dati relativi all'identità genetica, che, difatti, sono trattati esclusivamente in locali protetti accessibili unicamente agli incaricati ed a soggetti all'uopo autorizzati, possono essere trasportati all'esterno di tali locali solo se inseriti in contenitori sicuri e possono essere trasmessi in via elettronica solo proteggendoli mediante la loro cifratura.

[73] In linea generale, agli incaricati sono impartite istruzioni scritte che si riferiscono all'intero ciclo del trattamento. Sui medesimi soggetti grava l'obbligo di custodia degli atti e dei documenti che gli vengono affidati, qualora questi contengano dati sensibili o giudiziari. Infine, si prescrive che l'accesso agli archivi contenenti dati sensibili o giudiziari debba essere controllato.

«sterilizzazioni» della legge, e, al contempo, di porsi in un atteggiamento dialogico con i soggetti concretamente chiamati a dare applicazione alla disciplina"[74].

Alla regolamentazione dell'*authority* in oggetto è dedicato il titolo II della III parte del cod. priv. Riprendendo l'art. 30 comma 2 della legge n. 675/96, l'art. 153 dispone che "il Garante opera in piena autonomia e con indipendenza di giudizio e di valutazione". Esso è un organo collegiale, costituito da quattro componenti[75], nel cui ambito viene eletto il Presidente, il cui voto prevale in caso di parità. I componenti durano in carica quattro anni e possono essere rieletti solo una volta.

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

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;
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'art. 143, e di adottare gli altri provvedimenti previsti dalla disciplina applicabile al trattamento dei dati personali;

[74] S. SICA, *D. Lgs. n. 467/01 e «riforma» della privacy: un vulnus al «sistema» della riservatezza*, in *Dir. inf.*, 2002, 2, p. 264.
[75] I componenti sono eletti per una metà dalla Camera dei deputati e per l'altra metà dal Senato della Repubblica con voto limitato.

e) promuovere la sottoscrizione di codici di deontologia e buona condotta;
f) segnalare al Parlamento e al Governo l'opportunità di interventi normativi richiesti dalla necessità di tutelare i diritti, le libertà fondamentali e la dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali;
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, dei quali viene a conoscenza nell'esercizio o a causa delle funzioni;
j) tenere il registro dei trattamenti formato sulla base delle notificazioni;
k) predisporre annualmente una relazione sull'attività svolta e sullo stato di attuazione del cod. priv., che è trasmessa al Parlamento e al Governo entro il 30 aprile dell'anno successivo a quello cui si riferisce.

La **tutela dell'interessato** è affidata, in primo luogo, al Garante. Ad esso l'interessato può rivolgersi in tre modi. Innanzi tutto, può proporre un *reclamo* circostanziato, per rappresentare una violazione della disciplina rilevante in materia di trattamento di dati personali; può inoltre effettuare una *segnalazione*, se non è possibile presentare un reclamo circostanziato, al fine di sollecitare un controllo da parte del Garante

sulla disciplina medesima; infine, può presentare un *ricorso*, se intende far valere gli specifici diritti di cui al citato art. 7.

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

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

3.7 LA RESPONSABILITÀ CIVILE NEL CODICE DELLA PRIVACY

La delicatezza delle informazioni contenute nelle banche dati ha spinto il legislatore a riprodurre nel cod. priv. il testo dell'art. 18 della legge n. 675/96, per cui, ai sensi dell'art. 15 del cod. priv., "chiunque cagiona danno ad altri per effetto del trattamento di dati personali è tenuto al risarcimento ai sensi dell'art. 2050 del codice civile", il quale a sua volta dispone che "chiunque cagiona danno ad altri nello svolgimento di un'attività pericolosa, per sua natura o per la natura dei mezzi adoperati, è tenuto al risarcimento, se non prova di avere adottato tutte le misure idonee a evitare il danno". Per l'interpretazione dell'art. 15 è possibile far riferimento alla produzione dottrinale relativa all'art. 18 della legge n. 675/96, poiché, come detto, le due norme coincidono.

In merito si registra una divergenza di opinioni fra chi ritiene che il legislatore abbia qualificato *ipso iure* il trattamento dei dati come attività pericolosa[76] e chi sostiene invece che tramite il rinvio all'art. 2050 cod. civ. sia stata sancita l'applicabilità del regime relativo alla prova liberatoria prevista in materia di attività pericolose[77]. A sostegno della prima tesi è

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

[77] F. D. BUSNELLI, *Il "trattamento dei dati personali" nella vicenda dei diritti alla persona: la tutela risarcitoria*, in V. CUFFARO – FFARICCIUTO – CCIUENO-ZENCOVICH (a cura di), *Trattamento dei dati e tutela della persona*, Milano, 1998, p. 185; G. COMANDÈ, *Art. 18*, in C. M. BIANCA – ANCA CHUSNELLI (a cura di), *Tutela della privacy*, cit., p. 488; V. FRANCESCHELLI, *La tutela della privacy informatica. Problemi e prospettive*, Milano, 1998,

stato affermato che è possibile considerare pericolosa l'attività di trattamento dei dati personali per sua natura, "in relazione al rischio che essa presenta di ledere i diritti fondamentali dell'interessato"[78]; pertanto, il rischio tipico dell'attività di trattamento di dati personali appare essere quello di ledere posizioni particolari, particolarmente qualificate, dell'interessato, rischio che sussiste anche al di fuori dell'ipotesi di trattamento concernente dati sensibili[79]. Nel caso in cui si propenda per questa tesi, la disciplina di cui all'art. 2050 cod. civ. risulterà applicabile solo in caso di lesione di diritti fondamentali dell'interessato, mentre per eventuali altri pregiudizi (come la perdita economica determinata dalla distruzione della banca dati) la norma invocabile sarà l'art. 2043 cod. civ.[80]; ciò in base alla regola secondo la quale si risponde in base alla disciplina speciale di responsabilità oggettiva per i danni cagionati a causa, e non in occasione, dell'attività pericolosa. Qualora si accetti la seconda teoria, il regime della prova liberatoria *ex* art. 2050 cod. civ. sarà sempre applicabile, anche quindi se il danno non sia collegato alla lesione di un diritto fondamentale[81]. In ogni caso, non si può assolutamente ritenere che la normativa configuri un'ipotesi di semplice inversione dell'onere della prova, poiché ciò comporterebbe la liberazione da responsabilità se colui sul quale grava il suddetto onere riuscisse a dimostrare la mancanza di colpa, ossia di aver agito con prudenza,

---

p. 54; M. FRANZONI, *Dati personali e responsabilità civile*, in *Resp. civ.*, 1988, 4-5, p. 903; M. GRANIERI, *Una proposta di lettura sulla tutela risarcitoria nella vicenda del trattamento di dati personali*, in *Danno e resp.*, 1998, 3, p. 222; G. VISINTINI, *Trattato breve della responsabilità* civile, Padova, 1999, p. 404.

[78] P. ZIVIZ, *ibidem.*

[79] P. ZIVIZ, *ibidem.*

[80] P. ZIVIZ, *ivi*, p. 1301.

[81] P. ZIVIZ, *ibidem.*

diligenza, perizia.

La seconda teoria poggia invece sulla considerazione che, secondo la *communis opinio*, l'attività dovrebbe dirsi pericolosa in quanto ne possano derivare danni all'incolumità delle persone; orbene, qualificare l'attività di trattamento di dati personali in termini di pericolosità comporterebbe un'applicazione forse troppo ampia del suddetto attributo; inoltre, rileva giustamente Comandè, l'attività di trattamento di dati personali sarebbe stata esplicitamente classificata come attività pericolosa "senza l'inutile *fictio* del rinvio"[82].

La presunzione di responsabilità prevista dall'art. 2050 cod. civ. (e quindi anche dall'art. 15 del cod. priv.) può essere vinta solo con una prova alquanto rigorosa, dal momento che il danneggiante deve dimostrare di aver adottato tutte le misure idonee ad evitare il danno. Non è quindi sufficiente la prova negativa di non aver violato alcuna disposizione di legge o di regolamento o comunque le norme di comune prudenza: per liberarsi dalla responsabilità occorre la prova positiva di aver impiegato ogni cura o misura valida ad impedire l'evento dannoso[83], ragion per cui sovente solo la dimostrazione della dipendenza causale del danno da un caso fortuito (che consiste in un "elemento imprevisto ed imprevedibile che, inserendosi in un determinato processo causale e soverchiando ogni possibilità di resistenza da parte delle forza dell'uomo, rende inevitabile il compiersi dell'evento[84]") o dal fatto esclusivo del danneggiato viene considerata quale prova liberatoria ai sensi dell'art. 2050 cod. civ. In ogni caso, la giurisprudenza è molto rigorosa in questa

[82] G. COMANDÈ, *op. cit.*, p. 488.
[83] Cass. 29 aprile 1991, n. 4710, in *Mass. Foro It.*., 1991, c. 397.
[84] S. MERZ, *Manuale pratico della liquidazione del danno*, Padova, 1999, p. 5.

operazione interpretativa e richiede che il caso fortuito abbia provocato un effetto interruttivo del nesso causale tra il danno e l'attività pericolosa[85].

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

Risulta evidente l'importanza di questa norma, perché i principi da essa sanciti, se non rispettati, comportano l'obbligo di risarcire il danno. Essa, pertanto, assume valenza centrale nell'ambito del risarcimento del danno cagionato per effetto del trattamento di dati personali: soprattutto la clausola generale della liceità e correttezza del trattamento ben si presta a sopperire ad eventuali carenze delle lettere b) – e) del medesimo articolo[86]. Dunque la sfera di responsabilità appare tanto vasta, che risulterebbe possibile, in ipotesi, chiedere il risarcimento del danno anche al di fuori di una specifica violazione di legge, purché il trattamento sia

[85] Cass. 21 novembre 1984, n. 5960, in *Mass. Foro It.*., 1984, c. 1176.
[86] S. SICA, *Danno morale e legge sulla privacy informatica*, cit., p. 283.

avvenuto infrangendo le regole della *lawfulness and correctness*[87].

3.8 LE SANZIONI PREVISTE DAL CODICE DELLA PRIVACY

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

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

[87] G. VETTORI, *Privacy e diritti dell'interessato*, in *Resp. civ.*, 1998, 4-5, p. 898.

CAPITOLO 8

IL DOCUMENTO INFORMATICO E LA FIRMA DIGITALE

1. CENNI PRELIMINARI

L'enorme diffusione degli strumenti informatici ha fatto emergere con sempre maggior forza l'esigenza di sostituzione dei tradizionali documenti cartacei con documenti informatici, in maniera da facilitare l'utilizzo a qualsiasi scopo delle informazioni. L'interconnessione dei computer consente infatti una velocità prima impensabile di interscambio dei dati e i documenti possono essere trasferiti da una parte all'altra del globo in pochi secondi. I benefici sono di tutta evidenza, perché le informazioni elettroniche, in ragione della loro immaterialità e della gestione elettronica da parte degli elaboratori, consentono di superare i già visti problemi connessi all'utilizzo di documenti cartacei, in particolar modo con riferimento agli aspetti dell'archiviazione, del reperimento e del trasferimento.

Proprio l'immaterialità costituisce tuttavia il problema principale che si è posto sin da subito con riferimento al valore giuridico da attribuire ai documenti informatici. Essi costituiscono entità immateriali, potenzialmente modificabili od eliminabili senza lasciar tracce. Ovviamente gli strumenti informatici consentono di superare questi problemi, consentendo di proteggere i documenti da successive

modifiche o impedendo la cancellazione di determinati *file*[1]. "Il documento informatico, in sé, è «astratto». Esiste sempre un supporto (perché l'informazione elettronica consiste sempre nel cambiamento di uno stato fisico della materia) ma la natura di questo supporto è irrilevante per la natura del documento, anche se in determinati casi può essere essenziale per la produzione degli effetti propri del documento stesso"[2].

Altri problemi assai rilevanti sono connessi alla certezza della provenienza dei documenti, in modo che chi li abbia redatti non possa disconoscerli, e alla necessità di stabilire metodologie che consentano la prova della manifestazione della volontà per via telematica, anche con riferimento alla determinazione dei momenti in cui si realizzano le fasi dell'invio delle dichiarazione di volontà e della loro rispettiva conoscenza o conoscibilità.

Questi aspetti hanno importanza fondamentale in ambito giuridico, poiché nei negozi giuridici bilaterali o plurilaterali il negozio si perfeziona al momento dell'incontro delle parti, in quelli unilaterali recettizi al momento della conoscenza, da parte del destinatario, della dichiarazione, infine in quelli unilaterali non recettizi al momento della manifestazione di volontà[3].

---

[1] La cancellazione di dati contenuti su un supporto ottico non è invece possibile, perché essi sono supporti che consentono solo la lettura dei dati, ma non la scrittura (fatta eccezione per quelli riscrivibili). L'unico modo per eliminare tali informazioni è, dunque, la distruzione del supporto che le contiene.

[2] M. CAMMARATA – MMARACCARONE, *La firma digitale sicura. Il documento informatico nell'ordinamento italiano*, Milano, 2003, p. 59.

[3] La veridicità dei documenti prodotti in copia fotostatica o trasmessi via *fax* non è, comunque, maggiore di quanto astrattamente effettuabile per via elettronica, in quanto tali strumenti ben si prestano ad attività di alterazione o falsificazione delle informazioni.

Le regolamentazione della materia è dunque finalizzata alla scelta ed alla disciplina dei requisiti di validità del documento informatico e della firma digitale, così da rendere equipollenti i documenti in forma elettronica a quelli in forma cartacea.

2. IL DOCUMENTO INFORMATICO NELLA EVOLUZIONE (O INVOLUZIONE) DELLA NORMATIVA ITALIANA E COMUNITARIA

Prima di accennare alla normativa italiana e comunitaria in tema di documento informatico, bisogna considerare che il documento (non informatico) non è definito, in linea generale, nel codice civile, nonostante tale termine sia utilizzato più volte (fra gli altri, agli artt. 1262, 1477, 2961, ecc.). La definizione di documento è stata pertanto fornita dalla dottrina[4], per cui non è univoca, ma nella molteplicità di contributi *in subiecta materia* bisogna menzionare il celebre contributo di Francesco Carnelutti. L'illustre autore afferma che "il documento ha in sé la virtù del far conoscere; questa virtù è dovuta a ciò che noi chiamiamo il *contenuto rappresentativo*"[5]. Natalino Irti, invece, ritiene che il documento sia

[4] Sul documento, in generale, v. anche: L. BOVE, *Documento (storia del diritto)* (voce), in *Dig. disc. priv. – sez. civ.*, VII, Torino, 1991, pp. 13-26; S. PATTI, *Documento* (voce), in *Dig. disc. priv. – sez. civ.*, VII, Torino, 1991, pp. 1-13.

[5] F. CARNELUTTI, *Documento (teoria moderna)* (voce), in *Novissimo Digesto Italiano*, VI, Torino, 1960, p. 86. Sul punto, Natalino Irti afferma che "la rappresentazione si svolge e determina nella sfera dello spirituale, ed esige un soggetto che torni a conoscere e rievochi in sé le parole del passato. La rappresentazione non è un dato obiettivo, racchiuso nel documento, ma è questo interiore rivivere, che accoglie e consuma l'opaca impenetrabilità dei segni fisici. E, perciò essa è sempre individuale, e relativa al soggetto che la compie. La percezione dei segni è il momento primario o filologico, che viene superato mercé il passaggio al momento dell'interpretare. Qui i segni scompaiono nella loro fisicità, e nasce l'immagine del fatto e con essa il giudizio

"una *res signata* (un oggetto percepibile, recante segni), onde è dato pronunciare il giudizio di esistenza di un fatto, che sia sussumibile sotto un tipo normativo"[6].

Ciò premesso, si può ora ripercorrere per sommi capi il percorso legislativo seguito nell'ambito della regolamentazione del documento informatico e della firma digitale, percorso tracciato in primo luogo da una bozza di disegno di legge presentata il 18 settembre 1996 dall'Autorità per l'Informatica nella Pubblica Amministrazione[7] (AIPA, oggi divenuta Centro Nazionale per l'Informatica nella Pubblica Amministrazione) e pubblicata sul proprio sito Internet, con l'espresso invito, rivolto a tutti i navigatori, di effettuare commenti e suggerimenti. Il *modus operandi* dell'AIPA ha costituito in tale frangente un chiaro esempio di come il progresso informatico, se ben sfruttato, possa dare nuova linfa alla democrazia, mediante il dialogo fra rappresentanti e rappresentati.

L'anno successivo viene emanata la l. 15 marzo 1997, n. 59 (c.d. l. Bassanini), che dà origine a tutto il sistema normativo sulla firma digitale; norma cardine è l'art. 15 comma 2, il quale stabilisce che "gli atti, dati e documenti formati dalla pubblica amministrazione e dai privati con strumenti informatici o telematici, i contratti stipulati nelle medesime forme, nonché la loro archiviazione e trasmissione con strumenti

---

storiografico" (N. IRTI, *Sul concetto giuridico di documento*, in *Riv. trim. dir. proc. civ.*, 1969, 2, p. 502).

[6] N. IRTI, *ivi*, p. 502. Un'altra definizione è fornita da Aurelio Candian, secondo il quale "il documento è una cosa corporale, semplice o composta, idonea a ricevere, conservare, trasmettere, la rappresentazione descrittiva o emblematica o fonetica di un dato ente, giuridicamente rilevante" (*Documentazione e documento (teoria generale)* (voce), in *Enc. dir.*, XIII, Milano, 1964, p. 579).

[7] La bozza rappresenta il risultato del lavoro compiuto dalla commissione creata *ad hoc* dall'AIPA e coordinata da Donato A. Limone.

informatici, sono validi e rilevanti a tutti gli effetti di legge".

Nel frattempo, la bozza pubblicata su Internet dall'AIPA viene sottoposta a modifiche e rielaborata, arrivando poi all'emanazione del d.p.r. 10 novembre 1997, n. 513, "recante criteri e modalità per la formazione, l'archiviazione e la trasmissione di documenti con strumenti informatici e telematici". In tal modo l'Italia diventa la prima nazione a porre in essere una regolamentazione di carattere generale in materia di documento informatico e firma digitale, perché il d.p.r. trova applicazione sia negli atti dei privati che in quelli della pubblica amministrazione e si può così affermare che "il *diritto* contribuisce in modo diretto ed efficace a transitare verso una reale *società delle tecnologie e dell'informazione*"[8]. Negli altri stati, compresi gli Stati Uniti, sino a quel momento si era invece legiferato solo in ambiti settoriali.

Un quadro normativo chiaro ed espressione di una politica legislativa finalmente seria e recettiva delle istanze del corpo sociale inizia tuttavia ad ingarbugliarsi progressivamente, a partire dal 13 novembre 1999, quando viene emanata la direttiva CE n. 93, nella quale sorge l'inspiegabile distinzione fra "firma elettronica" e "firma elettronica avanzata". Dopo poco più di un anno viene varato il "testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa" (d.p.r. 28 dicembre 2000, n. 445, d'ora in poi "t.u."), poi modificato dal d. lgs. 23 gennaio 2002, n. 10 ("Attuazione della direttiva 1999/93/CE relativa ad un quadro comunitario per le firme elettroniche") e dal d.p.r. 7 aprile 2003, n. 137 ("Regolamento recante disposizioni di coordinamento in materia di firme elettroniche a norma

[8] D. A. LIMONE, *La validità giuridica dei documenti informatici. La firma digitale*, in AA.VV., *Liber amicorum in onore di Vittorio Frosini*, II, *Studi giuridici*, Milano, 1999, p. 165.

dell'articolo 13 del decreto legislativo 23 gennaio 2002, n. 10")[9]. Nel

[9] Il quadro regolamentativo della materia è tuttavia ben più ampio, in quanto, oltre ai testi fondamentali ora citati, bisogna aggiungere (fra gli altri): i d.p.r. 13 febbraio 2001, n. 123 ("Regolamento recante disciplina sull'uso di strumenti informatici e telematici nel processo civile, nel processo amministrativo e nel processo innanzi alle sezioni giurisdizionali della Corte dei conti"); 8 marzo 1999, n. 70 ("Regolamento recante disciplina del telelavoro nelle pubbliche amministrazioni, a norma dell'articolo 4, comma 3, della legge 16 giugno 1998, n. 191"); 20 ottobre 1998, n. 428 ("Regolamento recante norme per la gestione del protocollo informatico da parte delle amministrazioni pubbliche"); 23 dicembre 1997, n. 522 ("Regolamento recante norme per l'organizzazione ed il funzionamento del Centro tecnico per l'assistenza ai soggetti che utilizzano la Rete unitaria della pubblica amministrazione, a norma dell'articolo 17, comma 19, della Legge 15 maggio 1997, n. 127"); le deliberazioni AIPA: n. 51/00 ("Regole tecniche in materia di formazione e conservazione di documenti informatici delle pubbliche amministrazioni ai sensi dell'art. 18, comma 3, del Decreto del Presidente della Repubblica 10 novembre 1997, n. 513") e n. 42/01 ("Regole tecniche per la riproduzione e conservazione di documenti su supporto ottico idoneo a garantire la conformità dei documenti agli originali - articolo 6, commi 1 e 2, del Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa, di cui al decreto del Presidente della Repubblica 28 dicembre 2000, n. 445"); le circolari AIPA: n. AIPA/CR/31 del 21 giugno 2001 ("Art. 7, comma 6, del decreto del Presidente del Consiglio dei ministri del 31 ottobre 2000, recante "Regole tecniche per il protocollo informatico di cui al decreto del Presidente della Repubblica 20 ottobre 1998, n. 428" - requisiti minimi di sicurezza dei sistemi operativi disponibili commercialmente"); n. AIPA/CR/29 del 18 maggio 2001 ("Art. 14, comma 2, del decreto del Presidente del Consiglio dei ministri dell'8 febbraio 1999: codici identificativi idonei per la verifica del valore della chiave pubblica della coppia di chiavi del Presidente dell'Autorità per l'informatica nella pubblica amministrazione"); n. AIPA/CR/28 del 7 maggio 2001 ("Articolo 18, comma 2, del decreto del Presidente del Consiglio dei ministri 31 ottobre 2000, pubblicato nella Gazzetta Ufficiale 21 novembre 2000, n. 272, recante regole tecniche per il protocollo informatico di cui al decreto del Presidente della Repubblica 28 dicembre 2000, n. 445 - Standard, modalità di trasmissione, formato e definizioni dei tipi di informazioni minime ed accessorie comunemente scambiate tra le pubbliche amministrazioni e associate ai documenti protocollati"); n. AIPA/CR/27 del 16 febbraio 2001 ("Art. 17 del decreto del Presidente della Repubblica 10 novembre 1997, n. 513: utilizzo della firma digitale nelle Pubbliche Amministrazioni"); n. AIPA/CR/26 del 13 luglio 2000 ("Art. 8, comma 3, del decreto del Presidente della Repubblica 10 novembre 1997, n. 513: elenco delle Società individuate dall'Autorità per l'informatica nella Pubblica Amministrazione, alla data del 6 luglio 2000, ai fini dell'attività di certificazione"); n. AIPA/CR/24 del 19 giugno 2000 ("Art. 16, comma 1, dell'allegato tecnico al decreto del Presidente del Consiglio dei Ministri 8 febbraio 1999, pubblicato sulla Gazzetta Ufficiale del 15 aprile 1999, serie generale, n. 87 – Linee guida per l'interoperabilità tra i certificatori iscritti nell'elenco pubblico di cui

prosieguo risulterà purtroppo palese lo stato di confusione ingenerato da interventi legislativi non ponderati e realizzati frettolosamente e con poca cura, col risultato di minare le fondamenta di una regolamentazione che aveva per una volta posto l'Italia all'avanguardia in un settore in cui il connubio fra informatica e diritto può produrre grandi risultati, sia con riferimento alla semplificazione dell'attività amministrativa che per le numerose attività private (commerciali e non) che possono trarre giovamento da una circolazione delle informazioni allo stesso tempo rapida e giuridicamente certa.

Ciò premesso, è ora possibile analizzare la normativa vigente in tema di documento informatico e firma digitale, alla luce delle modifiche che si sono sin qui succedute. La definizione di **documento informatico** è rimasta immutata a partire dal d.p.r. 513/97: la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti.

---

all'articolo 8, comma 3, del decreto del Presidente della Repubblica 10 novembre 1997, n. 513"); n. AIPA/CR/22 ("Art. 16, comma 1, dell'allegato tecnico al decreto del Presidente del Consiglio dei Ministri 8 febbraio 1999, pubblicato sulla Gazzetta Ufficiale del 15 aprile 1999, serie generale, n. 87 – Modalità per presentare domanda di iscrizione nell'elenco pubblico dei certificatori di cui all'articolo 8, comma 3, del decreto del Presidente della Repubblica 10 novembre 1997, n. 513"); i d.p.c.m.: 20 aprile 2001 ("Differimento del termine che autorizza l'autocertificazione della rispondenza ai requisiti di sicurezza nelle regole tecniche di cui al decreto del Presidente del Consiglio dei Ministri dell'8 febbraio 1999"); 7 dicembre 2000 ("Proroga del termine che autorizza l'autocertificazione della rispondenza ai requisiti di sicurezza nelle regole tecniche di cui al decreto del Presidente del Consiglio dei Ministri dell'8 febbraio 1999"); 31 ottobre 2000 ("Regole tecniche per il protocollo informatico di cui al decreto del Presidente della Repubblica 20 ottobre 1998, n. 428"); 22 ottobre 1999 ("Regolamento recante caratteristiche e modalità per il rilascio della carta di identità elettronica e del documento di identità elettronico, a norma dell'articolo 2, comma 10, della legge 15 maggio 1997, n. 127, come modificato dall'articolo 2, comma 4, della legge 16 giugno 1998, n. 191"); 8 febbraio 1999 ("Regole tecniche per la formazione, la trasmissione, la conservazione, la duplicazione, la riproduzione e la validazione, anche temporale, dei documenti informatici ai sensi dell'articolo 3, comma 1, del Decreto del Presidente della Repubblica, 10 novembre 1997, n. 513").

Esso è per il giurista un *quid novi*, è un documento la cui esistenza e la cui rilevanza prescindono dalla presenza, prima necessaria, di un supporto fisico, con la conseguenza che le normative e le novità della materia non possono essere sempre lette alla luce delle tradizionali teorie sul documento[10], ma impongono quesiti nuovi cui lo studioso del diritto deve accostarsi ben sapendo di dover in alcuni casi trovare risposte altrettanto nuove ed attentamente ponderate, in virtù dell'amplissimo raggio di applicazione della normativa. L'art. 8 t.u., infatti, dispone che "il documento informatico da chiunque formato, la registrazione su supporto informatico e la trasmissione con strumenti telematici, sono validi e rilevanti a tutti gli effetti di legge, se conformi alle disposizioni del presente testo unico"[11].

Inoltre, poiché le pubbliche amministrazioni, *ex* art. 3 comma 1 del d. lgs. 12 febbraio 1993, n. 39 ("Norme in materia di sistemi informativi automatizzati delle amministrazioni pubbliche"), devono di norma adottare gli atti amministrativi di competenza utilizzando i sistemi informativi automatizzati e, considerando che ai sensi dell'art. 9 t.u. i documenti informatici delle p.a. costituiscono informazione primaria ed originale da cui è possibile effettuare, su diversi tipi di supporto, riproduzioni e copie per gli usi consentiti dalla legge, il documento

[10] M. CAMMARATA – MMARACCARONE, *op. cit.*, p. 7.

[11] L'utilizzo, nella norma in oggetto, sia dei termini "validità" che "rilevanza" non costituisce, secondo Cammarata e Maccarone, una inutile ridondanza, atteso che "si tratta di due aspetti completamente diversi: la validità del documento è la sua capacità di produrre determinati effetti giuridici, stabiliti caso per caso dalla legge, mentre la rilevanza è, più in generale, la qualità che determina la presa in considerazione di una fattispecie da parte dell'ordinamento giuridico. A voler essere pignoli, la dizione più rilevante sarebbe «rilevanti» e «validi», ponendo prima l'aspetto generale e poi quello specifico, oppure si potrebbe dire che la validità implica la rilevanza, ma tutto questo non cambia il senso della disposizione" (*op. cit.*, p. 81).

informatico assume ancora maggiore rilievo dal punto di vista del diritto amministrativo, dal momento che dalla combinata lettura delle disposizioni in esame si può evincere che esso rappresenta la regola secondo la quale le p.a. dovrebbero creare i documenti[12].

Affinché un documento informatico sia valido a tutti gli effetti di legge è in ogni caso necessaria l'apposizione o l'associazione ad esso di una firma elettronica o digitale, creata nel rispetto delle prescrizioni legislative. Il susseguirsi degli interventi normativi ha tuttavia portato alla creazione di più tipi di firme, di cui si dirà in seguito: per ora è sufficiente affermare che la firma elettronica è «insicura», mentre la firma elettronica avanzata o digitale è «sicura». Una volta che si appone la firma al documento, questo può essere attribuito con certezza al sottoscrittore (*attribuibilità*), che non potrà dunque negare di averlo firmato (*non ripudiabilità*); dalla firma si potranno inoltre evincere le generalità del firmatario e del certificatore, oltre a potersi verificare il certificato e l'*integrità* del documento.

Ai sensi dell'art. 10 t.u., un documento informatico formato validamente, in linea generale, forma piena prova dei fatti e delle cose rappresentate, se la parte contro cui sono prodotte non ne disconosce la conformità ai fatti o alle cose medesime. Già quello sottoscritto con una firma elettronica generica è equiparato alla riproduzioni meccaniche e soddisfa il requisito legale della forma scritta e tale tipologia di firma viene equiparata a quella autografa.

Invece, se il documento è sottoscritto con firma digitale o con un altro tipo di firma elettronica avanzata, e la firma è basata su di un

[12] M. CAMMARATA – MMARACCARONE, *op. cit.*, p. 83.

certificato qualificato ed è generata mediante un dispositivo per la creazione di una firma sicura, fa inoltre piena prova, fino a querela di falso[13], della provenienza delle dichiarazioni da chi l'ha sottoscritto. In merito, in dottrina si è osservato che, "presumibilmente, l'intenzione del legislatore è stata quella di voler eliminare i dubbi sull'esperibilità degli istituti del disconoscimento e del procedimento di verificazione della scrittura privata "digitale", oggetto di accessi dibattiti in dottrina, dotando al contempo la firma elettronica cd sicura di un regime di stabilità molto ampio"[14].

[13] La querela di falso è una istanza proposta innanzi il Tribunale e diretta ad ottenere l'accertamento della falsità di un atto pubblico o di una scrittura privata riconosciuta, autenticata o verificata, proponibile sia in via principale che incidentale in qualunque stato e grado del giudizio.

[14] F. SARZANA DI SANT'IPPOLITO, *Il legislatore italiano e le firme elettroniche: la crisi del principio di unitarietà della sottoscrizione*, in *Corr. giur.*, 2003, 10, p. 1381. L'a. prosegue affermando che la norma sembra aver recepito quell'orientamento dottrinale che, anche nella previgente normativa, attribuiva il valore di prova legale al documento sottoscritto con firma digitale. Il presupposto di tale teoria consiste nella considerazione che il procedimento di certificazione consentirebbe di porre una presunzione assoluta di riferibilità della firma apposta al titolare della coppia di chiavi o del dispositivo di firma, mentre la proposizione della querela di falso consentirebbe di attribuire la firma apposta ad un documento al sottoscrittore, escludendone un uso fraudolento da parte di terzi. Inoltre, l'autenticazione della firma da parte del pubblico ufficiale permetterebbe "di accertare la validità della chiave privata, di controllare la reale volontà del soggetto interessato e di accertare la liceità del documento sottoscritto secondo i principi generali. Non è chi non veda, però, come questa ricostruzione pecchi di farraginosità in quanto impone agli interpreti di effettuare "artifici" dialettici per spiegare una pluralità di istituti posti a presidio dell'unico fatto sinora riconosciuto dai nostri codici: l'apposizione di una sottoscrizione ed il controllo (del pubblico ufficiale o dell'organo giudiziario) precedente o successivo alla stessa apposizione. Questa ricostruzione non spiega poi come sia possibile che un soggetto esercitante un'attività economica privata non riconducibile a quella del pubblico ufficiale (il certificatore qualificato o accreditato) possa attribuire al documento sottoscritto con firma sicura la forza probatoria *"sino a querela di falso"*. […Tale interpretazione] potrebbe incidere inoltre sul diritto alla difesa delle parti presenti nel giudizio: anche volendo ipotizzare che il certificatore si limiti a mettere in relazione un dispositivo di firma con il sottoscrittore, appare difficile che, con gli ordinari strumenti processuali, un soggetto dotato di una "identità digitale",

Al documento informatico, sottoscritto con firma elettronica, in ogni caso non può essere negata rilevanza giuridica né ammissibilità come mezzo di prova unicamente a causa del fatto che è sottoscritto in forma elettronica oppure in quanto la firma non è basata su di un certificato qualificato o su di un certificato qualificato rilasciato da un certificatore accreditato o, infine, perché la firma non è stata apposta avvalendosi di un dispositivo per la creazione di una firma sicura.

L'efficacia cui si è fatto riferimento è quella del documento informatico in sé e per sé: bisogna ora analizzare il regime in tema di copie e duplicati. Se la copia o il duplicato di un documento cartaceo costituiscono comunque entità ben distinte da questo, la forma binaria del documento informatico fa sì che non sia possibile distinguere, in linea di principio, fra quello originale e i suoi duplicati o le sue copie, proprio perché tecnicamente sono identici, essendo il primo costituito dalla stessa sequenza in codice binario di cui sono composti i secondi, a meno di aggiungere l'espressa dicitura di «duplicato» o di «copia». L'art. 20 t.u. dispone che i duplicati, le copie e gli estratti del documento informatico, se conformi alle disposizioni dello stesso t.u., sono giuridicamente validi anche se riprodotti su altri supporti, che devono comunque necessariamente essere informatici, non essendo possibile apporre una firma digitale su un documento cartaceo ed in mancanza di essa non si può validamente creare un documento conforme alle prescrizioni del t.u.; il comma 2 della medesima disposizione, inoltre, prevede che i documenti informatici contenenti copia o riproduzione di

---

che egli ritiene di essere stata falsificata, possa dimostrare la propria estraneità al processo di apposizione della firma di fronte ad un documento che gli attribuisce con la forza della scrittura privata autenticata o dell'atto pubblico la paternità dell'atto" (p. 1382).

qualsiasi tipo di documento, spediti o rilasciati dai depositari pubblici autorizzati e dai pubblici ufficiali, hanno piena efficacia se ad essi è apposta o associata, da parte di chi li spedisce o rilascia, una firma elettronica qualificata; infine, ai sensi del comma 3, le copie su supporto informatico di documenti, formati in origine su supporto cartaceo o, comunque, non informatico, sostituiscono, ad ogni effetto di legge, gli originali da cui sono tratte se la loro conformità all'originale è autenticata da un notaio o da altro pubblico ufficiale a ciò autorizzato, con dichiarazione allegata al documento informatico e asseverata secondo le regole tecniche di cui all'articolo 8, comma 2, consentendo così la «smaterializzazione» dei documenti.

L'art. 38 t.u. dispone poi che tutte le istanze e le dichiarazioni da presentare alla pubblica amministrazione o ai gestori o esercenti di pubblici servizi possono essere inviate anche per fax e via telematica, equiparando pertanto, a tali fini, il documento informatico ad un comune fax, nonostante la medesima norma stabilisca anche che le istanze e le dichiarazioni inviate per via telematica sono valide se sottoscritte mediante la firma digitale (basata su di un certificato qualificato, rilasciato da un certificatore accreditato, e generata mediante un dispositivo per la creazione di una firma sicura) oppure se l'autore è identificato dal sistema informatico con l'uso della carta d'identità elettronica o della carta nazionale dei servizi. Inoltre, le istanze e le dichiarazioni sostitutive di atto di notorietà da produrre agli organi della amministrazione pubblica o ai gestori o esercenti di pubblici servizi sono sottoscritte dall'interessato in presenza del dipendente addetto ovvero sottoscritte e presentate unitamente a copia fotostatica non autenticata di un documento di

identità del sottoscrittore, che viene poi inserita nel fascicolo. Le istanze e la copia fotostatica del documento di identità possono essere inviate per via telematica.

Ai sensi dell'art. 41 t.u., i certificati rilasciati dalle pubbliche amministrazioni attestanti stati, qualità personali e fatti non soggetti a modificazioni hanno validità illimitata, mentre per le restanti certificazioni si prevede una validità di sei mesi dalla data di rilascio, salvo speciali disposizioni legislative o regolamentari. Si stabilisce anche una sorta di «elasticità» in riferimento alla validità temporale dei certificati anagrafici, delle certificazioni dello stato civile, degli estratti e delle copie integrali degli atti di stato civile, che sono ammessi dalle pubbliche amministrazioni nonché dai gestori o esercenti di pubblici servizi anche oltre i termini di validità a seguito di una dichiarazione dell'interessato, apposta in fondo al documento, dalla quale risulti che le informazioni contenute nel certificato stesso non hanno subito variazioni dalla data di rilascio. Tale dichiarazione consente la prosecuzione del procedimento per il quale gli atti certificativi sono richiesti, ovviamente ferma restando la facoltà di verificare la veridicità e la autenticità delle attestazioni prodotte. In caso di falsa dichiarazione si applicano le disposizioni di cui all'art. 76, ai sensi del cui comma 1 "chiunque rilascia dichiarazioni mendaci, forma atti falsi o ne fa uso nei casi previsti dal presente testo unico è punito ai sensi del codice penale e delle leggi speciali in materia"(comma 1)[15].

[15] I successivi commi dispongono, poi, che "l'esibizione di un atto contenente dati non più rispondenti a verità equivale ad uso di atto falso. Le dichiarazioni sostitutive rese ai sensi degli articoli 46 e 47 e le dichiarazioni rese per conto delle persone indicate nell'articolo 4, comma 2, sono considerate come fatte a pubblico ufficiale. Se i reati indicati nei commi 1, 2 e 3 sono commessi per ottenere la nomina ad un

In alcuni casi non è tuttavia possibile far ricorso a documenti informatici, ossia quando la materialità o l'unicità del documento sono requisiti indispensabili per la produzione di effetti legali[16], come nel caso della procura speciale, che deve essere unica e deve essere apposta o allegata all'atto cui si riferisce, mentre se fosse solamente una sequenza in codice binario sarebbe duplicabile e potrebbe essere utilizzata per un numero potenzialmente illimitato di atti uguali.

Una volta che il documento informatico è stato validamente formato, esso può essere trasmesso per via telematica. In tal caso si intende inviato e pervenuto al destinatario, se trasmesso all'indirizzo elettronico da questi dichiarato. La data e l'ora di formazione, di trasmissione o di ricezione di un documento informatico, redatto in conformità alle disposizioni del t.u. nonché alle regole tecniche di cui agli articoli 8, comma 2 e 9, comma 4, sono opponibili ai terzi, mentre la trasmissione del documento informatico per via telematica, con modalità che assicurino l'avvenuta consegna, equivale alla notificazione per mezzo della posta nei casi consentiti dalla legge. In queste eventualità si pone, tuttavia, il problema della sicurezza dei dati inviati per via telematica, cui si può comunque ovviare mediante l'utilizzo di sistemi di crittazione, oltre a quello, più grave, relativo alla prova che la spedizione telematica del documento sia andata a buon fine. Nelle normali spedizioni a mezzo raccomandata, l'avviso di ricevimento fa prova dell'esito positivo della consegna del documento, ma fornire una simile prova nelle trasmissioni in forma elettronica è ben più difficile, dovendo affidarsi ad ulteriori

---

pubblico ufficio o l''autorizzazione all'esercizio di una professione o arte, il giudice, nei casi più gravi, può applicare l'interdizione temporanea dai pubblici uffici o dalla professione e arte".

[16] M. CAMMARATA – MMARACCARONE, *op. cit.*, p. 98.

messaggi che certifichino l'arrivo a destinazione del documento, messaggi la cui veridicità può essere riscontrata nei *file* di *log* dei *provider*. In tal modo, tuttavia, la procedura diventa assai complicata e può facilmente prestarsi ad abusi, a meno di creare una forma di spedizione più sicura che tenga conto anche di tale aspetto.

3. LA FIRMA DIGITALE

La firma autografa consente di risalire all'identità del sottoscrittore di un documento cartaceo, in quanto la calligrafia è un elemento distintivo della persona. Inoltre, al fine di garantire maggiore certezza, l'ordinamento giuridico prevede che essa possa essere apposta innanzi ad un pubblico ufficiale, facendo così fede sino a querela di falso.

All'identità di chi appone una firma elettronica su un documento informatico non si può invece risalire, a meno che non venga utilizzata una **firma digitale**, ossia una informazione che viene aggiunta ad un documento elettronico proprio per garantirne l'integrità e l'autenticità[17]. In base al disposto dell'art. 1 lett. b) del d.p.r. 513/97, la firma digitale consiste nel risultato della procedura informatica (validazione) basata su

[17] "La firma digitale non è una firma. La firma digitale non è la sottoscrizione autografa, ma è *come* la sottoscrizione autografa, ovvero è *equivalente* alla sottoscrizione autografa. Ed è proprio il *come* ad attestare che tra firma e firma digitale non c'è identità, e a confermare la diversità. Sebbene il termine utilizzato sia «firma» in entrambi i casi, tuttavia con riguardo alla firma digitale esso non ha la funzione di designare il medesimo oggetto (firma) specificandone una qualità (digitale). Firma e firma digitale sono due entità ontologicamente diverse. L'attributo «digitale» muta la natura della «firma». […] La firma digitale è il risultato di una procedura tecnologica, mentre la sottoscrizione è il risultato di un gesto umano" (G. FINOCCHIARO, *La firma digitale. Formazione, archiviazione e trasmissione di documenti con strumenti informatici e telematici*, in F. GALGANO (a cura di), *Commentario del codice civile Scialoja – Branca*, Art. 2699-2720, Supplemento (d.p.r. 10 novembre 1997 n. 513), Bologna, 2000, p. 1).

un sistema di chiavi asimmetriche a coppia, una pubblica e una privata, che consente al sottoscrittore tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici. La chiave privata deve essere conosciuta solo dal soggetto titolare, perché mediante essa si appone la firma digitale sul documento informatico o si decifra il documento informatico in precedenza cifrato mediante la corrispondente chiave pubblica, che è invece l'altro elemento della coppia, finalizzato alla verifica della firma digitale apposta sul documento informatico dal titolare delle chiavi asimmetriche o alla cifratura dei documenti informatici da trasmettere al titolare delle predette chiavi. Le due chiavi sono generate nel corso di un procedimento unico e sono inscindibili, ma, per garantire maggiore sicurezza, dall'una non si può risalire all'altra.

I successivi interventi normativi hanno tuttavia complicato il chiaro quadro delineato dal d.p.r. 513/97: la *firma digitale* è ora definita come "un particolare tipo di firma elettronica qualificata basata su un sistema di chiavi asimmetriche a coppia, una pubblica e una privata, che consente al titolare tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici"[18]. Dunque oggi la firma digitale è una *species*

[18] Art. 23 t.u.: "La firma digitale deve riferirsi in maniera univoca ad un solo soggetto ed al documento o all'insieme di documenti cui è apposta o associata. Per la generazione della firma digitale deve adoperarsi una chiave privata la cui corrispondente chiave pubblica sia stata oggetto dell'emissione di un certificato qualificato che, al momento della sottoscrizione, non risulti scaduto di validità ovvero non risulti revocato o sospeso. L'apposizione ad un documento informatico di una firma elettronica basata su un certificato elettronico revocato, scaduto o sospeso

all'interno del *genus* della firma elettronica, secondo discutibili, per usare un eufemismo, conoscenze informatiche. La *firma elettronica* è, ai sensi dell'art. 2, comma 1, lett. a), del d. lgs. 10/02, l'insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di autenticazione informatica; la *firma elettronica avanzata* è, ai sensi dell'art. 2, comma 1, lett. g), del d. lgs. 10/02, la firma elettronica ottenuta attraverso una procedura informatica che garantisce la connessione univoca al firmatario e la sua univoca identificazione, creata con mezzi sui quali il firmatario può conservare un controllo esclusivo e collegata ai dati ai quali si riferisce in modo da consentire di rilevare se i dati stessi siano stati successivamente modificati; infine, la *firma elettronica qualificata* è la firma elettronica avanzata che sia basata su un certificato qualificato e creata mediante un dispositivo sicuro per la creazione della firma, ossia la firma digitale di cui al d.p.r. 513/97[19].

---

equivale a mancata sottoscrizione. La revoca o la sospensione, comunque motivate, hanno effetto dal momento della pubblicazione, salvo che il revocante, o chi richiede la sospensione, non dimostri che essa era già a conoscenza di tutte le parti interessate. L'apposizione di firma digitale integra e sostituisce, ad ogni fine previsto dalla normativa vigente, l'apposizione di sigilli, punzoni, timbri, contrassegni e marchi di qualsiasi genere. Attraverso il certificato elettronico si devono rilevare, secondo le regole tecniche di cui all'articolo 8, comma 2, la validità del certificato elettronico stesso, nonché gli elementi identificativi del titolare e del certificatore".

[19] In dottrina si è comunque sostenuto che, nonostante l'intervento definitorio sia probabilmente inopportuno e talvolta ambiguo dal punto di vista semantico, esso non debba essere sopravvalutato, "in primo luogo perché l'impianto che ne esce non è qualitativamente diverso da quello precedente: infatti già l'innesto della direttiva europea 1999/93/CE sul sistema italiano fondato originariamente sul D.P.R. 513/1997 aveva portato ad un sistema incentrato su un *genus*, la firma elettronica, del quale la *firma elettronica avanzata* costituiva *species*, connotata per i più rigidi requisiti funzionali cui doveva assolvere; ed in tale impianto la *firma digitale* costituiva null'altro che un particolare tipo di firma elettronica avanzata, caratterizzata dal raggiungimento di tali requisiti funzionali con una specifica tecnologia, quella della crittografia asimmetrica o a doppia chiave. In secondo luogo, perché il nuovo

Anche nella nuova regolamentazione si intende per chiavi asimmetriche la coppia di chiavi crittografiche, una privata ed una pubblica, correlate tra loro, utilizzate nell'ambito dei sistemi di validazione di documenti informatici; la chiave privata è quell'elemento della coppia di chiavi asimmetriche, che deve essere conosciuto soltanto dal soggetto titolare, mediante il quale si appone la firma digitale sul documento informatico, mentre la chiave pubblica è l'altro elemento della coppia di chiavi asimmetriche destinato ad essere reso pubblico, con il quale si verifica la firma digitale apposta sul documento informatico dal titolare delle chiavi asimmetriche.

La firma elettronica può essere creata sia con un programma informatico adeguatamente configurato (*software*) che con un apparato strumentale (*hardware*); la firma digitale sicura deve essere invece creata con un "dispositivo sicuro", ossia con un apparato strumentale rispondente ai requisiti di cui all'articolo 10 del citato decreto n. 10 del 2002, nonché del t.u.

Una volte ottenuta la coppia di chiavi asimmetriche è possibile procedere alla **certificazione**, consistente nel risultato della procedura informatica, applicata alla chiave pubblica e rilevabile dai sistemi di validazione, mediante la quale si garantisce la corrispondenza biunivoca tra chiave pubblica e soggetto titolare cui essa appartiene, si identifica quest'ultimo e si attesta il periodo di validità della predetta chiave ed il termine di scadenza del relativo certificato, in ogni caso non superiore a

---

concetto introdotto – quello di *firma elettronica qualificata* – poteva in via implicita ricavarsi già dalla disciplina complessivamente introdotta con il D.Lgs 10/2002, che menzionava, alle lettere e) ed f) dell'art. 2.1, i concetti di «certificato qualificato» e di «dispositivo sicuro» per la creazione della firma" (F. DELFINI, *Il D.P.R. n. 137/2003 in materia di firme elettroniche*, in *I contratti*, 2003, 8-9, p. 832).

tre anni.

Il *certificatore* è il soggetto pubblico o privato che effettua la certificazione, rilascia il certificato della chiave pubblica, lo pubblica unitamente a quest'ultima, pubblica ed aggiorna gli elenchi dei certificati sospesi e revocati. *Ex* art. 1 comma 1 lett. u) t.u., il certificatore, ai sensi dell'art. 2, comma 1, lett. b), del d.lgs. 10/02, è il soggetto che presta servizi di certificazione delle firme elettroniche o che fornisce altri servizi connessi con queste ultime[20]. La medesima norma, alle lett. v) e z), delinea rispettivamente le figure del certificatore qualificato e accreditato. Il primo è colui che rilascia al pubblico certificati elettronici conformi ai requisiti indicati nel t.u. e nelle regole tecniche di cui all'art. 8, comma 2[21];

[20] Art. 26 t.u.: "L'attività dei certificatori stabiliti in Italia o in un altro Stato membro dell'Unione europea è libera e non necessita di autorizzazione preventiva, ai sensi dell'articolo 3 del decreto legislativo 23 gennaio 2002, n. 10. Detti certificatori o, se persone giuridiche, i loro legali rappresentanti ed i soggetti preposti all'amministrazione, devono inoltre possedere i requisiti di onorabilità richiesti ai soggetti che svolgono funzioni di amministrazione, direzione e controllo presso le banche di cui all'articolo 26 del testo unico delle leggi in materia bancaria e creditizia, approvato con decreto legislativo 1° settembre 1993, n. 385. L'accertamento successivo dell'assenza o del venir meno dei requisiti di cui al comma 1 comporta il divieto di prosecuzione dell'attività intrapresa. Ai certificatori qualificati e ai certificatori accreditati che hanno sede stabile in altri Stati membri dell'Unione europea non si applicano le norme del presente decreto e le relative norme tecniche di cui all'articolo 8, comma 2, e si applicano le rispettive norme di recepimento della direttiva 1999/93/CE".

[21] Art. 27 t.u.: "I certificatori che rilasciano al pubblico certificati qualificati devono trovarsi nelle condizioni previste dall'articolo 26. […Essi] devono inoltre: a) dimostrare l'affidabilità organizzativa, tecnica e finanziaria necessaria per svolgere attività di certificazione; b) impiegare personale dotato delle conoscenze specifiche, dell'esperienza e delle competenze necessarie per i servizi forniti, in particolare della competenza a livello gestionale, della conoscenza specifica nel settore della tecnologia delle firme elettroniche e della dimestichezza con procedure di sicurezza appropriate, e che sia in grado di rispettare le norme del presente testo unico e le regole tecniche di cui all'articolo 8, comma 2; c) applicare procedure e metodi amministrativi e di gestione adeguati e tecniche consolidate; d) utilizzare sistemi affidabili e prodotti di firma protetti da alterazioni e che garantiscano la sicurezza tecnica e crittografica dei procedimenti, in conformità a criteri di sicurezza riconosciuti in ambito europeo e

il secondo è, ai sensi dell'art. 2, comma 1, lett. c), del d.lgs 10/02, il certificatore accreditato in Italia ovvero in altri Stati membri dell'Unione europea ai sensi del t.u. nonché dell'art. 3, par. 2, della direttiva n. 1999/93/CE.

I certificati qualificati, ai sensi dell'art. 2, comma 1, lett. e), del d.lgs. 10/02, sono certificati elettronici conformi ai requisiti di cui all'allegato I della direttiva n. 1999/93/CE, rilasciati da certificatori che rispondono ai requisiti di cui all'allegato II della medesima direttiva. Più specificatamente, *ex* art. 27 *bis* t.u., "i certificati qualificati devono contenere almeno le seguenti informazioni:

a) indicazione che il certificato elettronico rilasciato è un certificato qualificato;
b) numero di serie o altro codice identificativo del certificato;
c) nome, ragione o denominazione sociale del certificatore e lo Stato nel quale è stabilito;
d) nome, cognome e codice fiscale del titolare del certificato o uno pseudonimo chiaramente identificato come tale;

---

internazionale e certificati ai sensi dello schema nazionale di cui all'articolo 10, comma 1, del decreto legislativo 23 gennaio 2002, n. 10; e) adottare adeguate misure contro la contraffazione dei certificati, idonee anche a garantire la riservatezza, l'integrità e la sicurezza nella generazione delle chiavi, nei casi in cui il certificatore generi tali chiavi. I certificatori di cui al comma 1 devono comunicare, prima dell'inizio dell'attività, anche in via telematica, una dichiarazione di inizio di attività al Dipartimento dell'innovazione e le tecnologie della Presidenza del Consiglio dei Ministri, attestante l'esistenza dei presupposti e dei requisiti previsti dal presente testo unico, ai sensi dell'articolo 4, comma 1, del decreto legislativo 23 gennaio 2002, n. 10. Il Dipartimento procede, d'ufficio o su segnalazione motivata di soggetti pubblici o privati, a controlli volti ad accertare la sussistenza dei presupposti e dei requisiti previsti dal presente testo unico e dispone, se del caso, con provvedimento motivato da notificare all'interessato, il divieto di prosecuzione dell'attività e la rimozione dei suoi effetti, salvo che, ove ciò sia possibile, l'interessato provveda a conformare alla normativa vigente detta attività ed i suoi effetti entro il termine prefissatogli dall'amministrazione stessa."

e) dati per la verifica della firma corrispondenti ai dati per la creazione della stessa in possesso del titolare;
f) indicazione del termine iniziale e finale del periodo di validità del certificato;
g) firma elettronica avanzata del certificatore che ha rilasciato il certificato.

In aggiunta alle informazioni di cui al comma 1, fatta salva la possibilità di utilizzare uno pseudonimo, per i titolari residenti all'estero cui non risulti attribuito il codice fiscale, si deve indicare il codice fiscale rilasciato dall'autorità fiscale del Paese di residenza o, in mancanza, un analogo codice identificativo, quale ad esempio un codice di sicurezza sociale o un codice identificativo generale. Il certificato qualificato può inoltre contenere, su domanda del titolare o del terzo interessato, le seguenti informazioni, se pertinenti allo scopo per il quale il certificato è richiesto: a) le qualifiche specifiche del titolare, quali l'appartenenza ad ordini o collegi professionali, l'iscrizione ad albi o il possesso di altre abilitazioni professionali, nonché poteri di rappresentanza; b) limiti d'uso del certificato, ai sensi dell'articolo 28-bis, comma 3; c) limiti del valore degli atti unilaterali e dei contratti per i quali il certificato può essere usato, ove applicabili".

L'art. 29 *septies* t.u. prevede le ipotesi di *revoca* e *sospensione* dei certificati qualificati: "il certificato qualificato deve essere a cura del certificatore:

a) revocato in caso di cessazione dell'attività del certificatore;
b) revocato o sospeso in esecuzione di un provvedimento dell'autorità;

c) revocato o sospeso a seguito di richiesta del titolare o del terzo dal quale derivano i poteri del titolare;
d) revocato o sospeso in presenza di cause limitative della capacità del titolare o di abusi o falsificazioni.

Il certificato qualificato può, inoltre, essere revocato o sospeso nei casi previsti dalle regole tecniche di cui all'articolo 8, comma 2. La revoca o la sospensione del certificato qualificato, qualunque ne sia la causa, ha effetto dal momento della pubblicazione della lista che lo contiene. Il momento della pubblicazione deve essere attestato mediante adeguato riferimento temporale. Le modalità di revoca o sospensione sono previste nelle regole tecniche di cui all'articolo 8, comma 2".

Ex art. 24 comma 2, l'autenticazione consiste invece nell'attestazione, da parte del pubblico ufficiale, che la firma digitale è stata apposta in sua presenza dal titolare, previo accertamento della sua identità personale, della validità della chiave utilizzata e del fatto che il documento sottoscritto risponde alla volontà della parte e non è in contrasto con l'ordinamento giuridico ai sensi dell'art. 28, comma 1, n. 1 della legge 6 febbraio 1913, n. 89. La firma digitale così apposta non può essere ripudiata.

La responsabilità del certificatore trova oggi spazio nel nuovo art. 29 *bis* t.u., ai sensi del quale "il certificatore che rilascia al pubblico un certificato qualificato o che garantisce al pubblico l'affidabilità del certificato è responsabile, se non prova d'aver agito senza colpa, del danno cagionato a chi abbia fatto ragionevole affidamento: a) sull'esattezza delle informazioni in esso contenute alla data del rilascio e sulla loro completezza rispetto ai requisiti fissati per i certificati

qualificati; b) sulla garanzia che al momento del rilascio del certificato il firmatario detenesse i dati per la creazione della firma corrispondenti ai dati per la verifica della firma riportati o identificati nel certificato; c) sulla garanzia che i dati per la creazione e per la verifica della firma possano essere usati in modo complementare, nei casi in cui il certificatore generi entrambi. Il certificatore che rilascia al pubblico un certificato qualificato è responsabile, nei confronti dei terzi che facciano ragionevole affidamento sul certificato stesso, dei danni provocati per effetto della mancata registrazione della revoca o sospensione del certificato, salvo che provi d'aver agito senza colpa. Il certificatore può indicare, in un certificato qualificato, i limiti d'uso di detto certificato ovvero un valore limite per i negozi per i quali può essere usato il certificato stesso, purché i limiti d'uso o il valore limite siano riconoscibili da parte dei terzi. Il certificatore non è responsabile dei danni derivanti dall'uso di un certificato qualificato che ecceda i limiti posti dallo stesso o derivanti dal superamento del valore limite".

L'art. 29 *bis* t.u. disciplina gli obblighi del titolare e del certificatore: "il titolare ed il certificatore sono tenuti ad adottare tutte le misure organizzative e tecniche idonee ad evitare danno ad altri. Il certificatore che rilascia, ai sensi dell'articolo 27, certificati qualificati è tenuto inoltre a: a) identificare con certezza la persona che fa richiesta della certificazione; b) rilasciare e rendere pubblico il certificato elettronico nei modi e nei casi stabiliti dalle regole tecniche di cui all'articolo 8, comma 2, nel rispetto della legge 31 dicembre 1996, n. 675, e successive modificazioni; c) specificare, nel certificato qualificato su richiesta dell'istante, e con il consenso del terzo interessato, i poteri di

rappresentanza o di altri titoli relativi all'attività professionale o a cariche rivestite, previa verifica della sussistenza degli stessi; d) attenersi alle regole tecniche di cui all'articolo 8, comma 2; e) informare i richiedenti in modo compiuto e chiaro, sulla procedura di certificazione e sui necessari requisiti tecnici per accedervi e sulle caratteristiche e sulle limitazioni d'uso delle firme emesse sulla base del servizio di certificazione; f) adottare le misure di sicurezza per il trattamento dei dati personali, ai sensi dell'articolo 15, comma 2, della legge 31 dicembre 1996, n. 675; g) non rendersi depositario di dati per la creazione della firma del titolare; h) procedere alla pubblicazione della revoca e della sospensione del certificato elettronico in caso di richiesta da parte del titolare o del terzo dal quale derivino i poteri di quest'ultimo, di perdita del possesso della chiave, di provvedimento dell'autorità, di acquisizione della conoscenza di cause limitative della capacità del titolare, di sospetti abusi o falsificazioni; i) garantire il funzionamento efficiente, puntuale e sicuro dei servizi di elencazione, nonché garantire un servizio di revoca e sospensione dei certificati elettronici sicuro e tempestivo; l) assicurare la precisa determinazione della data e dell'ora di rilascio, di revoca e di sospensione dei certificati elettronici; m) tenere registrazione, anche elettronica, di tutte le informazioni relative al certificato qualificato per dieci anni in particolare al fine di fornire prova della certificazione in eventuali procedimenti giudiziari; n) non copiare, nè conservare le chiavi private di firma del soggetto cui il certificatore ha fornito il servizio di certificazione; o) predisporre su mezzi di comunicazione durevoli tutte le informazioni utili ai soggetti che richiedono il servizio di certificazione, tra cui in particolare gli esatti termini e condizioni relative all'uso del

certificato, compresa ogni limitazione dell'uso, l'esistenza di un sistema di accreditamento facoltativo e le procedure di reclamo e di risoluzione delle controversie; dette informazioni, che possono essere trasmesse elettronicamente, devono essere scritte in linguaggio chiaro ed essere fornite prima dell'accordo tra il richiedente il servizio ed il certificatore; p) utilizzare sistemi affidabili per la gestione del registro dei certificati con modalità tali da garantire che soltanto le persone autorizzate possano effettuare inserimenti e modifiche, che l'autenticità delle informazioni sia verificabile, che i certificati siano accessibili alla consultazione del pubblico soltanto nei casi consentiti dal titolare del certificato e che l'operatore possa rendersi conto di qualsiasi evento che comprometta i requisiti di sicurezza. Su richiesta, elementi pertinenti delle informazioni possono essere resi accessibili a terzi che facciano affidamento sul certificato.

Il certificatore che rilascia certificati al pubblico raccoglie i dati personali solo direttamente dalla persona cui si riferiscono o previo suo esplicito consenso, e soltanto nella misura necessaria al rilascio e al mantenimento del certificato, fornendo l'informativa prevista dalla disciplina in materia di dati personali. I dati non possono essere raccolti o elaborati per fini diversi senza l'espresso consenso della persona cui si riferiscono".

CAPITOLO 9

IL COMMERCIO ELETTRONICO

1. ASPETTI GENERALI

Internet si presta ad una molteplicità di utilizzi: è un'inesauribile fonte di informazioni, è un luogo virtuale di incontro e di dibattito, ma è anche «sede» di un «mercato» assai particolare, nel quale vengono svolte attività di commercio elettronico (*e-commerce*). La particolarità del mercato in oggetto è connaturata all'essenza della Rete, che muta la tradizionale configurazione dello spazio e del tempo, poiché non esistono le distanze tipiche del mondo «materiale» e, generalmente, non esistono i relativi orari. Questo singolare mercato sfugge, pertanto, a qualsiasi tradizionale catalogazione nei due sensi citati e consente di creare una propria dimensione in ragione del particolare mezzo utilizzato, ossia il *computer*[1]. L'informatica consente di svolgere una serie di attività e prestazioni con una velocità ed una produttività prima impensabili, come risulta anche dalla semplice osservazione empirica della strutturazione dei vari luoghi di lavoro[2].

Il commercio elettronico in sé e per sé presenta sia vantaggi che

[1] R. CLARIZIA, *Il commercio via* Internet: *gli aspetti giuridici generali e le problematiche contrattuali*, in R. RINALDI (a cura di), *La fiscalità del commercio via Internet: attualità e prospettive*, Torino, 2001, p. 3.
[2] B. INZITARI, *Contratti via* Internet: *aspetti della dematerializzazione*, in R. RINALDI (a cura di), *op. cit.*, p. 119.

svantaggi per i soggetti coinvolti. Per le imprese è infatti molto più economico predisporre un servizio di vendita *on line* che non aprire un nuovo punto vendita: diminuiscono i costi sia legati al locale che al personale, non essendo necessario predisporre un contatto diretto con il pubblico. Del resto, la tradizionale espansione economica di un'attività commerciale passa necessariamente attraverso una sua espansione fisica, mediante l'apertura, ad esempio, di nuovi punti vendita, con i relativi costi. La predisposizione di un punto vendita *on line*, dunque virtuale, richiede cifre ben minori ed una visibilità astrattamente ben maggiore, potendo coinvolgere una cerchia di acquirenti potenzialmente illimitata.

I vantaggi sono evidenti anche per il potenziale cliente: non è necessario spostarsi fisicamente, ma in pochi *click* è possibile raggiungere negozi virtualmente vicini e materialmente lontani. Inoltre, la comparazione dei prezzi praticati e dei servizi offerti dalle varie aziende concorrenti risulta assai rapida, perché non viene richiesto proprio lo spostamento fisico. Ancora, è possibile reperire merce, anche assai rara, in ogni momento della giornata, indipendentemente dagli orari di apertura delle tradizionali attività commerciali.

Dall'altro lato bisogna tuttavia considerare che predisporre un proprio punto vendita virtuale non è sempre remunerativo, in quanto "tra i maggiori ostacoli che l'e-commerce ha incontrato nel suo sviluppo sicuramente hanno giocato un ruolo dominante quelli socio-culturali come la scarsa familiarità con le tecnologie informatiche o la diffidenza verso le stesse"[3]. Inoltre, se per i beni immateriali legati proprio agli strumenti informatici (come il *software*) il commercio effettuato per via

[3] G. CASSANO, *Il commercio elettronico: una premessa*, in ID. (a cura di), *Diritto delle nuove tecnologie informatiche e dell'INTERNET*, Milano, 2002, p. 361.

telematica è la forma forse più naturale di distribuzione, per altre tipologie merceologiche il contatto diretto con la merce assume in molti casi una rilevanza essenziale, come nel settore tessile, soprattutto con riferimento alle transazioni fra professionisti e consumatori (c.d. B2C, sulle quali v. *infra*)[4].

Il **commercio elettronico** "consiste nello svolgimento di attività commerciali per via elettronica. Basato sull'elaborazione e la trasmissione di dati […] per via elettronica, esso comprende attività disparate quali: commercializzazione di merci e servizi per via elettronica; distribuzione on-line di contenuti digitali; effettuazione per via elettronica di operazioni quali trasferimenti di fondi, compravendita di azioni, emissione di polizze di carico, vendite all'asta, progettazione e ingegneria in cooperazione; *on-line sourcing*; appalti pubblici per via elettronica, vendita diretta al consumatore e servizi post-vendita. Il commercio elettronico comprende prodotti (ad es., prodotti di consumo, apparecchiature specialistiche per il settore sanitario), servizi (ad es., servizi d'informazione, servizi giuridici e finanziari), attività di tipo tradizionale (ad es., assistenza sanitaria ed istruzione) e di nuovo tipo (ad es., "centri commerciali virtuali")"[5]. Del resto, qualora si limitasse il commercio elettronico alle sole reti aperte quali Internet, le parti

[4] Anche nelle transazioni fra professionisti (B2B) può sussistere il problema relativo al contatto con la merce, per saggiarne le eventuali qualità, ma il problema è facilmente risolvibile ricorrendo alla c.d. vendita a campione, per cui basta inviare una piccola quantità del prodotto offerto, che costituirà poi il referente qualitativo degli altri prodotti venduti.

[5] COM(97) 157, *Un'iniziativa europea in materia di commercio elettronico. Comunicazione al Parlamento europeo, al Consiglio, al Comitato economico e sociale e al Comitato delle regioni*, p. 9. Secondo l'Associazione Italiana Internet Providers, il commercio elettronico è l'attività "di compravendita di beni e servizi svolta completamente o in parte attraverso la Rete" (*Codice di Autoregolamentazione per i servizi Internet*, http://www.aiip.it/autoreg.html).

contrattuali potrebbero stabilire una connessione diretta per negoziare tramite i propri *computers* creando così una rete «chiusa», al fine di aggirare le eventuali regolamentazioni in tema di commercio elettronico.

La specificità del commercio elettronico consiste non solo nel fatto che la transazione si perfeziona per via telematica[6], ma anche che le attività a tal fine necessarie avvengono *on line*: basti pensare alla ricerca del contraente, allo svolgimento delle trattative, al versamento del corrispettivo e, in alcuni casi, addirittura alla distribuzione e alla consegna di beni immateriali[7].

Il **commercio elettronico** può essere **diretto** o **indiretto**. Nel primo caso, il negozio si svolge interamente *on line*, perché il suo oggetto è un bene immateriale, dunque trasmissibile per via telematica, come un *software* oppure un servizio di consultazione di banca dati. L'immaterialità costituisce, pertanto, il carattere distintivo di questa tipologia di commercio elettronico, perché intrinseco sia all'oggetto del contratto che al suo intero svolgimento; sarebbe inoltre illogico il mancato sfruttamento delle potenzialità dei mezzi telematici, dal momento che in taluni casi sarebbe necessario fissare il bene immateriale su un supporto fisico per poi procedere al suo invio a destinazione, con relativi aggravio dei costi e aumento dei tempi[8]. Nelle ipotesi di commercio elettronico indiretto, invece, il negozio ha ad oggetto uno o più beni materiali, la cui

---

[6] Sulle tipologie contrattuali *on line* v.: I. IASELLI – SELLASELLI, *I contratti informatici*, Piacenza, 2003; C. ROSSELLO, *Profili giuridici relativi ai contratti conclusi via Internet*, in W. G. SCOTT – OTT URTULA – RTULTECCO (a cura di), *Il commercio elettronico. Verso nuovi rapporti tra imprese e mercati*, Torino, 1999, pp. 285-305; F. SARZANA DI S. IPPOLITO, *I contratti di Internet e del commercio elettronico*, Milano, 2001.

[7] A. DI AMATO, *La qualificazione delle transazioni in etere come contratti di massa e i diritti dei consumatori. Le clausole vessatorie*, in G. CASSANO (a cura di), *Il commercio via Internet. Profili giuridici, fiscali, tributari, comunitari, sociali, filosofici, normativi*, Piacenza, 2002, p. 55.

[8] G. ROGNETTA, *Il commercio elettronico*, Napoli, 2000, p. 9.

trasmissione non può ovviamente avvenire via Internet, ma deve essere effettuata mediante i normali mezzi di spedizione. In tal caso, dunque, l'*iter* contrattuale si svolge in più fasi, alcune *on line*, come l'incontro delle volontà, altre *off line*, come nel caso della consegna della merce[9].

2. BUSINESS TO BUSINESS (B2B), BUSINESS TO CONSUMER (B2C), PERSON TO PERSON (P2P)

Nell'ambito del commercio elettronico bisogna distinguere fra *Business to Business* (B2B), *Business to Consumer* (B2C) e *Person to Person* (P2P), che rappresentano i macrosegmenti del mercato[10].

Nella prima categoria rientrano tutte le transazioni che coinvolgono due o più professionisti, che non hanno come parte il consumatore finale. L'acquirente di alcuni servizi è, allo stesso tempo, anche il venditore per altre tipologie di beni e l'utilizzo di Internet può consentire rilevanti vantaggi economici, ma sussiste la necessità di una interazione reciproca fra le imprese, dove c'è una elevata disponibilità di risorse economiche[11]. Il B2B ha "un volume di gran lunga superiore rispetto al B2C: esso individua il commercio elettronico all'ingrosso, con

[9] È bene ricordare che nel nostro ordinamento si distingue fra contratti consensuali e reali: i primi si perfezionano nel momento in cui si incontrano le manifestazioni di volontà delle parti, i secondi con la consegna del bene. Ciò assume rilievo con riferimento al rischio di perimento della cosa, poiché nella prima ipotesi la proprietà si trasferisce indipendentemente dalla consegna, mentre nella seconda ciò avviene solo con la *traditio*.

[10] Su B2B e B2C v. A. DONÀ DALLE ROSE, *B2B e B2C*, in G. CASSANO (a cura di), *Diritto delle nuove tecnologie informatiche e dell'INTERNET*, cit., p. 386.

[11] F. DE LEO, *L'electronic business e le prospettive per i nuovi mercati*, in W. G. SCOTT – M. MURTULA – RTULTECCO (a cura di), *Il commercio elettronico. Verso nuovi rapporti tra imprese e mercati*, Torino, 1999, p. 69.

categorie merceologiche predefinite, e si realizza quando l'impegno diretto di un'impresa in Rete trova risposta da parte di un'azienda o comunque di un individuo che opera nell'ambito della propria attività professionale, sottoponendo a questa regolamentazione anche i contratti in cui una parte contraente sia un provider"[12]. A livello di regolamentazione giuridica, la maggiore differenza con il B2C consiste nella non applicabilità delle norme dettate a tutela del consumatore[13].

Nel B2C, invece, le transazioni coinvolgono il professionista ed il consumatore. Tale mercato rappresenta, potenzialmente, il maggior ambito di interesse per le attività di commercio elettronico da un punto di vista quantitativo, cioè riferito al numero complessivo di transazioni, che tuttavia si connotano, per lo più, per essere microtransazioni. Le imprese che operano in tale settore, pertanto, devono essere in grado di sostenere e gestire un notevole numero di collegamenti[14] e devono inoltre rendere assai semplice l'intero svolgimento della transazione, a partire dall'offerta dei beni o dei servizi per giungere alla conclusione del contratto, in modo da richiedere al potenziale acquirente solo le conoscenze di base all'uopo necessarie e dunque rivolgersi ad un mercato che sia il più ampio possibile. Nel B2C il problema principale è però costituito dalla tutela del consumatore, che costituisce la parte debole del

[12] F. TESAURO – SAURANESSA, *Economia digitale. Aspetti civilistici e fiscali*, Milano, 2002, p. 49.
[13] A. STRACUZZI, *Il commercio elettronico e l'impresa. Contratti di vendita conclusi tramite Internet. Sistemi di pagamento e misure di sicurezza*, Milano, 1999, p. 41. Infatti, "molte delle norme che riguardano il commercio elettronico sono volte a garantire ai consumatori almeno lo stesso livello di protezione di cui essi godono relativamente ad operazioni commerciali che non si svolgono on line, se non ad un livello maggiore" (U. DRAETTA, *Internet e commercio elettronico nel diritto internazionale dei privati*, Milano, 2001, p. 31).
[14] F. DE LEO, *op. cit.*, p. 69.

contratto, per cui è stata progressivamente predisposta una normativa a sua tutela. Si possono qui ricordare il d.lgs. 15 gennaio 1992, n. 50 (di attuazione della direttiva n. 85/577/CEE in materia di contratti negoziati fuori dei locali commerciali), il d.lgs. 22 maggio 1999, n. 185 (di attuazione della direttiva 97/7/CE relativa alla protezione dei consumatori in materia di contratti a distanza), gli artt. 1469 *bis* e ss. cod. civ. (introdotti dalla l. 6 febbraio 1996, n. 52, recante "disposizioni per l'adempimento di obblighi derivanti dall'appartenenza dell'Italia alle Comunità europee"), il d.lgs. 2 febbraio 2002, n. 24 (di attuazione della direttiva 1999/44/CE su taluni aspetti della vendita e delle garanzie di consumo).

Nel P2P, invece, le transazioni avvengono fra due o più privati, le cui volontà si esprimono per mezzo di quei siti finalizzati al commercio da privato a privato e che dunque svolgono una mera funzione di mezzo, più o meno evoluta, che consente l'effettuazione delle transazioni.

Infine, si possono qui ricordare altre due categorie di commercio elettronico di rilievo, ossia *Public Agencies to business* e *Public Agencies to citizens*, la prima inerente i rapporti tra impresa e consumatori[15], la seconda riguardante l'erogazione elettronica dei servizi al cittadino[16].

[15] "Il ruolo delle pubbliche amministrazioni è molto importante per l'espansione del sistema: si consideri da un lato, e solo per fare un esempio, il potere di gestire gli appalti pubblici e, dall'altro, la possibilità di applicare le tecnologie del commercio elettronico trasmettendo fiducia e sicurezza agli operatori privati del mercato virtuale" (G. ROGNETTA, *op. cit.*, p. 11).
[16] A. STRACUZZI, *op. cit.*, p. 4.

3. LA REGOLAMENTAZIONE DEL COMMERCIO ELETTRONICO: IN PARTICOLARE IL D.LGS. 70/03

In linea generale, ciascun ordinamento pone delle regole che disciplinano lo svolgimento delle attività commerciali nell'ambito del proprio territorio, che dunque variano da stato a stato, investendo una molteplicità di aspetti giuridicamente rilevanti. La diffusione dell'*e-commerce* mette tuttavia in crisi le relative, tradizionali categorie giuridiche in conseguenza del carattere di a-territorialità della Rete, per cui sorge l'esigenza di regolamentazione di una materia nella quale bisogna necessariamente tendere ad una progressiva "uniformazione progressiva e sovranazionale delle regole, non foss'altro per ragioni di efficienza e competitività delle imprese del settore, interessate *naturaliter* da meccanismi di globalizzazione delle dinamiche di mercato"[17].Ciò ha portato, in primo luogo, all'approvazione, da parte del Parlamento europeo, della direttiva 8 maggio 2000, n. 31, "relativa a taluni aspetti giuridici dei servizi della società dell'informazione, in particolare il commercio elettronico, nel mercato interno", ossia la c.d. «Direttiva sul commercio elettronico»[18].

Nell'ordinamento italiano, la direttiva 2000/31/CE è stata recepita mediante il d.lgs. 9 aprile 2003, n. 70, volto a "promuovere la libera circolazione dei servizi della società dell'informazione, fra i quali il

[17] S. SICA, *Recepita la direttiva sul commercio elettronico*, in *Corr. giur.*, 2003, 9, p. 1247.
[18] Sulla dir. 2000/31/CE v.: DE MAGISTRIS F., La direttiva comunitaria in materia di commercio elettronico, in CASSANO G. (a cura di), Diritto delle nuove tecnologie informatiche e dell'INTERNET, Milano, 2002, p. 369; G. DE NOVA – F. DELFINI, *La direttiva sul commercio elettronico: prime considerazioni*, in *Riv. dir. priv.*, 2000, 4, pp. 693-704; F. SARZANA DI S. IPPOLITO, *Approvata la direttiva sul commercio elettronico*, in *Corr. giur.*, 2000, 10, pp. 1288-1294.

commercio elettronico" (art. 1 comma 1). Nel testo sono presenti numerosi errori, anche grammaticali, ed imprecisioni, puntualmente segnalati da autorevole dottrina al fine di "evidenziare i guasti di una legislazione delegata affidata a procedure opache di una pubblica amministrazione che anziché essere consapevole delle proprie specifiche competenze (amministrare è compito diverso dal legiferare) agisce come un apprendista stregone"[19].

Ai sensi dell'art. 1 comma 2, nel campo di applicazione di questo decreto non rientrano:

a) i rapporti fra contribuente e amministrazione finanziaria connessi con l'applicazione, anche tramite concessionari, delle disposizioni in materia di tributi nonché la regolamentazione degli aspetti tributari dei servizi della società dell'informazione ed in particolare del commercio elettronico;
b) le questioni relative al diritto alla riservatezza, con riguardo al trattamento dei dati personali nel settore delle telecomunicazioni, con riferimento alla disciplina vigente;
c) le intese restrittive della concorrenza;
d) le prestazioni di servizi della società dell'informazione effettuate da soggetti stabiliti in Paesi non appartenenti allo spazio economico europeo;
e) le attività, dei notai o di altre professioni, nella misura in cui implicano un nesso diretto e specifico con l'esercizio dei pubblici poteri;

[19] V. ZENO-ZENCOVICH, *Note critiche sulla nuova disciplina del commercio elettronico dettata dal d.lgs. 70/03*, in *Dir. inf.*, 2003, 3, p. 506.

f) la rappresentanza e la difesa processuali;
g) i giochi d'azzardo, ove ammessi, che implicano una posta pecuniaria, i giochi di fortuna, compresi il lotto, le lotterie, le scommesse i concorsi pronostici e gli altri giochi come definiti dalla normativa vigente, nonché quelli nei quali l'elemento aleatorio è prevalente.

La normativa di cui al d.lgs. 70/03 non si applica però a tutti i contratti, in virtù della disposizione di cui all'art. 11, che esclude quelli:

a) che istituiscono o trasferiscono diritti relativi a beni immobili, diversi da quelli in materia di locazione;
b) che richiedono per legge l'intervento di organi giurisdizionali, pubblici poteri o professioni che implicano l'esercizio di pubblici poteri;
c) di fideiussione o di garanzie prestate da persone che agiscono a fini che esulano dalle loro attività commerciali, imprenditoriali o professionali;
d) disciplinati dal diritto di famiglia o di successione.

La libera circolazione dei servizi, tuttavia, non basta a contraddistinguere la disciplina che ci occupa come finalizzata all'attuazione di una strategia di stampo totalmente liberale, atteso che "sono fatte salve le disposizioni comunitarie e nazionali sulla tutela della salute pubblica e dei consumatori, sul regime autorizzatorio in ordine alle prestazioni di servizi investigativi o di vigilanza privata, nonché in materia di ordine pubblico e di sicurezza, di prevenzione del riciclaggio del denaro, del traffico illecito di stupefacenti, di commercio, im portazione ed esportazione di armi, munizioni ed esplosivi e dei materiali

d'armamento" (art. 1 comma 3), per cui Internet non costituisce una «zona franca», priva di regole, nella quale effettuare traffici illeciti[20].

I primi due commi dell'art. 3 traducono "in norme complementari il c.d. principio del «paese di origine», di cui all'art. 3 della direttiva, per il quale l'attività del prestatore è sottoposta alle norme del paese di stabilimento ed i servizi da questo erogati nel rispetto di esse possono liberamente circolare negli altri Stati membri. La piena applicazione del principio, tuttavia, può trovare un primo ostacolo, nella materia in esame, quanto alla individuazione del paese «di origine», cioè del paese ove si trova il luogo di stabilimento del prestatore del servizio, posto che, come emerge dall'art. 2, lett. c) ult. parte, esso non coincide necessariamente con il luogo ove si trovano i mezzi tecnici e le tecnologie necessarie per prestare il servizio medesimo"[21]. A tali commi deroga il successivo art. 4, ai sensi del quale tali disposizioni non si applicano nei seguenti casi:

a) diritti d'autore, diritti assimilati, diritti di cui alla l. 21 febbraio 1989, n. 70 (recante "norme per la tutela giuridica delle topografie dei prodotti a semiconduttori") e al d.lgs. 6 maggio 1999, n. 169 (di "attuazione della direttiva 96/9/CE relativa alla tutela giuridica delle banche di dati") nonché diritti di proprietà industriale;
b) emissione di moneta elettronica da parte di istituti per i quali gli Stati membri hanno applicato una delle deroghe di cui all'art. 8, par. l, della dir. 2000/46/CE del Parlamento

[20] Così S. SICA, *op. cit.*, p. 1248.
[21] F. DELFINI, *Il D.Lgs. 70/2003 di attuazione della direttiva 2000/31/CE sul commercio elettronico*, in *I contratti*, 2003, 6, p. 613.

europeo e del Consiglio riguardante l'avvio, l'esercizio e la vigilanza prudenziale dell'attività degli istituti di moneta elettronica;

c) l'art. 44, par. 2, della dir. 85/611/CEE, in materia di pubblicità degli organismi di investimento collettivo in valori mobiliari;
d) all'attività assicurativa di cui all'art. 30 e al titolo IV della dir. 92/49/CEE, terza direttiva sulle assicurazioni sui danni, agli articoli 7 e 8 della dir. 88/357/CEE, seconda direttiva sulle assicurazioni sui danni; al titolo IV della dir. 92/96/CEE, terza direttiva sulle assicurazioni sulla vita, e all'art. 4 della dir. 90/619/CEE, la seconda direttiva sulle assicurazioni sulla vita, come modificate dalla dir. 2002/83/CE;
e) facoltà delle parti di scegliere la legge applicabile al loro contratto;
f) obbligazioni contrattuali riguardanti i contratti conclusi dai consumatori;
g) validità dei contratti che istituiscono o trasferiscono diritti relativi a beni immobili nei casi in cui tali contratti devono soddisfare requisiti formali;
h) ammissibilità delle comunicazioni commerciali non sollecitate per posta elettronica.

L'art. 5 pone invece una serie di deroghe di carattere generale, prevedendo che la libera circolazione di un determinato servizio della società dell'informazione proveniente da un altro Stato membro può

essere limitata, con provvedimento dell'autorità giudiziaria o degli organi amministrativi di vigilanza o delle autorità indipendenti di settore, per motivi di:

a) ordine pubblico, per l'opera di prevenzione, investigazione, individuazione e perseguimento di reati, in particolare la tutela dei minori e la lotta contro l'incitamento all'odio razziale, sessuale, religioso o etnico, nonché contro la violazione della dignità umana;
b) tutela della salute pubblica;
c) pubblica sicurezza, compresa la salvaguardia della sicurezza e della difesa nazionale;
d) tutela dei consumatori, ivi compresi gli investitori.

I provvedimenti ora citati possono essere adottati se, nel caso concreto, si palesano necessari se un determinato servizio della società dell'informazione lede o presenti un rischio serio e grave di ledere l'ordine pubblico, la salute pubblica, la pubblica sicurezza, la tutela dei consumatori[22].

Particolare rilievo assume, poi, l'art. 7, che prevede l'obbligo, per il prestatore, di fornire determinate informazioni generali, che non

[22] Art. 5 commi 3 e 4: "Fatti salvi i procedimenti giudiziari e gli atti compiuti nell'ambito di un'indagine penale, l'autorità competente, per il tramite del Ministero delle attività produttive ovvero l'autorità indipendente di settore, deve, prima di adottare il provvedimento: a) chiedere allo Stato membro di cui al comma 1 di prendere provvedimenti e verificare che essi non sono stati presi o che erano inadeguati; b) notificare alla Commissione europea e allo Stato membro di cui al comma 1, la sua intenzione di adottare tali provvedimenti. Dei provvedimenti adottati dalle autorità indipendenti, è data periodicamente comunicazione al Ministero competente. In caso di urgenza, i soggetti di cui al comma 3 possono derogare alle condizioni poste nello stesso comma. I provvedimenti, in tal caso, sono notificati nel più breve tempo possibile alla Commissione e allo Stato membro, insieme ai motivi dell'urgenza".

sostituiscono, ma si aggiungono agli obblighi informativi già previsti in relazione ai beni forniti ed ai servizi offerti. Le informazioni di cui alla norma citata devono essere aggiornate e facilmente accessibili, in modo diretto e permanente, ai destinatari del servizio e alle Autorità competenti. Esse consistono in:

a) nome, denominazione o ragione sociale;
b) domicilio o sede legale;
c) estremi che permettono di contattare rapidamente il prestatore e di comunicare direttamente ed efficacemente con lo stesso, compreso l'indirizzo di posta elettronica;
d) numero di iscrizione al repertorio delle attività economiche (REA) o al registro delle imprese;
e) elementi di individuazione ed estremi della competente autorità di vigilanza qualora l'attività sia soggetta a concessione, licenza od autorizzazione;
f) per quanto riguarda le professioni regolamentate: 1) l'ordine professionale o istituzione analoga, presso cui il prestatore sia iscritto e il numero di iscrizione; 2) il titolo professionale e lo Stato membro in cui è stato rilasciato; 3) il riferimento alle nonne professionali e agli eventuali codici di condotta vigenti nello Stato membro di stabilimento e le modalità di consultazione dei medesimi;
g) numero della partita IVA o altro numero di identificazione considerato equivalente nello Stato membro, qualora il prestatore eserciti un'attività soggetta ad imposta;

h) indicazione in modo chiaro ed inequivocabile dei prezzi e delle tariffe dei servizi forniti, evidenziando se comprendono le imposte, i costi di consegna ed altri elementi aggiuntivi da specificare;
i) indicazione delle attività consentite al consumatore e al destinatario del servizio ed estremi del contratto qualora l'attività sia soggetta ad autorizzazione o l'oggetto della prestazione sia fornito sulla base di un contratto di licenza d'uso.

In aggiunta a tali obblighi informativi, l'art. 8 prevede che le comunicazioni commerciali[23] che costituiscono un servizio della società dell'informazione o ne sono parte integrante devono contenere anche, sin dal primo invio, una specifica informativa che ne chiarisce la natura di comunicazione commerciale ed indica la persona fisica o giuridica per conto della quale essa è effettuata. L'informativa deve inoltre evidenziare che si tratta di un'offerta promozionale, come sconti, premi, o omaggi e le relative condizioni di accesso, e che si tratta di concorsi o giochi promozionali, se consentiti, e le relative condizioni di partecipazione.

L'art. 12 comma 1, disciplinando le informazioni dirette alla conclusione del contratto, dispone che, oltre agli obblighi informativi previsti per specifici beni e servizi, nonché a quelli stabiliti dall'art. 3 del

[23] Con riferimento alle comunicazioni commerciali non sollecitate trova applicazione l'art. 9, ai sensi del quale, fatti salvi gli obblighi previsti dal d.lgs. 22 maggio 1999, n. 185 e dal d.lgs. 13 maggio 1998, n. 171, "le comunicazioni commerciali non sollecitate trasmesse da un prestatore per posta elettronica devono, in modo chiaro e inequivocabile, essere identificate come tali fin dal momento in cui il destinatario le riceve e contenere l'indicazione che il destinatario del messaggio può opporsi al ricevimento in futuro di tali comunicazioni. La prova del carattere sollecitato delle comunicazioni commerciali è onere del prestatore".

d.lgs. 22 maggio 1999, n. 185, il prestatore, salvo diverso accordo tra parti che non siano consumatori, deve fornire in modo chiaro, comprensibile ed inequivocabile, prima dell'inoltro dell'ordine da parte del destinatario del servizio, le seguenti informazioni:

a) le varie fasi tecniche da seguire per la conclusione del contratto;
b) il modo in cui il contratto concluso sarà archiviato e le relative modalità di accesso;
c) i mezzi tecnici messi a disposizione del destinatario per individuare e correggere gli errori di inserimento dei dati; prima di inoltrare l'ordine al prestatore;
d) gli eventuali codici di condotta cui aderisce e come accedervi per via telematica;
e) le lingue a disposizione per concludere il contratto oltre all'italiano;
f) l'indicazione degli strumenti di composizione delle controversie.

Questa disposizione non è tuttavia applicabile ai contratti conclusi esclusivamente mediante scambio di messaggi di posta elettronica o comunicazioni individuali equivalenti. Le clausole e le condizioni generali del contratto proposte al destinatario devono essere messe a sua disposizione in modo che gli sia consentita la memorizzazione e la riproduzione .

"La lett. c) dell'art. 12. 1. […] non si limita ad imporre un obbligo informativo ma, ancor più a monte, impone al prestatore di predisporre idonei strumenti di rilievo e correzione di errori nella manifestazione di

volontà, che con lessico più tradizionale, diremmo errori *ostativi*. Si tratta di previsione opportuna, perché la predisposizione di una tutela *di fatto* (ed *ex ante*) rispetto agli errori nella dichiarazione o nella sua trasmissione – per usare le parole della rubrica dell'art. 1433 Codice civile – potrà sopperire alla pratica inapplicabilità al commercio elettronico (nel quale pur possono essere frequenti tali errori) della tradizionale tutela *giuridica* (ed *ex post*) dell'annullamento, che ruota attorno al requisito della riconoscibilità dell'errore (art. 1431 Codice civile), di difficile ricorrenza (o quantomeno di ardua prova) nella contrattazione telematica"[24].

L'art. 12 comma 1 "ha definitivamente superato qualsiasi suggestione di dettare un *modello speciale* (derogatorio all'ordinaria disciplina codicistica) *per la conclusione dei contratti telematici*"[25]. Il comma 2 del medesimo articolo, ponendo un obbligo particolarmente qualificato a carico del prestatore, consente di "porre rimedio al rischio, caratteristico della contrattazione telematica mediante accesso al sito, che l'incauto navigatore, con la semplice pressione di un tasto, si vincoli senza avere neppure consapevolezza del vincolo assunto"[26].

Infine, con riferimento all'inoltro dell'ordine, ai sensi dell'art. 13, "le norme sulla conclusione dei contratti si applicano anche nei casi in cui il destinatario di un bene o di un servizio della società dell'informazione inoltri il proprio ordine per via telematica. Salvo differente accordo tra parti diverse dai consumatori, il prestatore deve, senza ingiustificato ritardo e per via telematica, accusare ricevuta dell'ordine del destinatario contenente un riepilogo delle condizioni

[24] F. DELFINI, *op. cit.*, p. 614.
[25] R. TARICCO, *Volontà e accordo nella contrattazione telematica*, in *Nuova giur. civ. comm.*, 2003, 2, II, p. 228.
[26] R. TARICCO, *op. cit.*, p. 229.

generali e particolari applicabili al contratto, le informazioni relative alle caratteristiche essenziali del bene o del servizio e l'indicazione dettagliata del prezzo, dei mezzi di pagamento, del recesso, dei costi di consegna e dei tributi applicabili. L'ordine e la ricevuta si considerano pervenuti quando le parti alle quali sono indirizzati hanno la possibilità di accedervi. Le disposizioni di cui ai commi 2 e 3 non si applicano ai contratti conclusi esclusivamente mediante scambio di messaggi di posta elettronica o comunicazioni individuali equivalenti".

4. I SISTEMI DI PAGAMENTO

Nelle transazioni *on line* sussiste primariamente il problema relativo ai metodi di pagamento utilizzabili[27]. Se nelle fattispecie di compravendita aventi ad oggetto beni materiali, l'utilizzo di sistemi di pagamento tradizionali (come il contrassegno) non provoca particolari problemi ed è generalmente consentito dalla maggioranza delle aziende che svolgono attività di *e-commerce*, nelle ipotesi di commercio elettronico diretto tali strumenti palesano la loro inadeguatezza, poiché non consentono il completamento della transazione *on line*, ma necessitano di una ulteriore fase che si svolge, per forza di cose, *off line*, dunque aggiungendo un carattere di materialità ad un procedimento che si connota, all'opposto, per la sua immaterialità.

Inoltre, in linea generale, un sistema di pagamento elettronico deve soddisfare alcuni requisiti, che possono così elencarsi:

[27] Su questi aspetti v. M. TIDONA, *I pagamenti elettronici in Internet. La circolazione elettronica della ricchezza. Gli aspetti fiscali delle transazioni in rete*, Rimini, 2001.

a) *riservatezza* e *sicurezza* dei dati: le transazioni devono avvenire senza che sia possibile per soggetti terzi venire a conoscenza dei contenuti delle comunicazioni. Le informazioni relative al negozio, con riferimento ai suoi elementi soggettivi ed oggettivi, devono essere conoscibili solo dalle parti e non devono essere esposti ad ingerenze esterne. Bisogna pertanto assicurare l'anonimato e la non tracciabilità: il nome del compratore non solo non deve comparire, ma lo stesso non deve poter essere identificato così come non deve essere possibile collegare differenti pagamenti dello stesso compratore. L'anonimato può essere raggiunto mediante la sostituzione del nome con uno pseudonimo, mentre la non tracciabilità può essere assicurata dalla crittazione delle comunicazioni;
b) *autenticità* ed *identificabilità* delle parti: la loro identità non deve essere conoscibile da soggetti terzi rispetto alla transazione, ma è necessario che ciascuna conosca l'identità dell'altra, per poter garantire la genuinità dei messaggi nonché la rispettiva rintracciabilità; ovviamente tali informazioni non devono essere comunicate ad altri soggetti, incombendo su ciascuna parte un obbligo di riservatezza, cui corrisponde il relativo diritto della controparte;
c) *non ripudiabilità* delle informazioni: la volontà negoziale delle parti riguardo al pagamento non deve poter essere disconosciuta e deve essere opponibile ai terzi in un

eventuale giudizio. Pertanto, l'autore di ciascun messaggio non deve poter ripudiare il contenuto di quanto affermato;

d) *inalterabilità* dei documenti ed *integrità* dei dati: il contenuto delle transazioni deve essere pienamente conforme alla volontà delle parti e non deve sussistere la possibilità di alterare il documento informatico sul quale si fonda la transazione, sia prima che dopo la sua conclusione;

e) *interoperabilità* delle applicazioni e delle tecnologie: la possibilità di utilizzare gli strumenti di pagamento elettronico andrebbe assicurata a tutti, indipendentemente dalla piattaforma *hardware* e *software* utilizzata. In caso contrario, il mercato potrebbe trainare esclusivamente gli *standard* attuali e contribuire al mantenimento dei monopoli *de facto*, impedendo lo sviluppo tecnologico e l'emersione di nuovi soggetti in tale ambito[28].

Inoltre, affinché gli strumenti di pagamento elettronico possano essere comunemente utilizzati è necessario che essi siano semplici da

[28] Oggi il settore informatico è dominato da poche aziende, soprattutto con riferimento all'ambito dei sistemi operativi (s.o.), dove si registra una posizione di monopolio da parte della Microsoft. Se la diffusione dell'*e-commerce* sarà sempre maggiore, sarà ovvio predisporre nei s.o. (e volendo anche nell'*hardware* dei nuovi *computer*) dominanti una implementazione diffusa, in maniera nativa, dei vari strumenti di pagamento, senza garantire ad altri soggetti la possibilità di essere effettivamente concorrenti e ciò potrebbe costituire un nuovo fattore di consolidamento delle attuali posizioni predominanti del mercato e, al contempo, di indebolimento di chi occupa un settore di nicchia, perché, chiunque volesse effettuare acquisti *on line*, non potrebbe rivolgersi a soluzioni alternative allo *standard*, come Linux. Bisognerebbe imporre, pertanto, agli attuali monopolisti, l'obbligo di contribuire alla diffusione delle nuove tecnologie anche nei confronti dei propri concorrenti che occupano fasce di mercato ridotte, al fine di contribuire ad uno sviluppo tecnologico, che, per quanto sia *market-based*, contribuisca a lasciare a ciascuno quanto meno la libertà di scelta.

utilizzare, soprattutto con riferimento al B2C, il cui *target* deve necessariamente essere il più ampio possibile.

Bisogna tuttavia considerare che non tutti questi elementi sono necessariamente richiesti in una normale transazione o comunque si atteggiano in maniera diversa a seconda delle caratteristiche della singola transazione, sia in ragione della tipologia del bene fornito o del servizio offerto che del loro costo. Il sistema di pagamento elettronico «ideale» dovrebbe dunque rispettare in modo flessibile ciascuno dei requisiti sopra esposti, adattandosi alla molteplicità delle situazioni concrete e garantendo, in ogni caso, un livello minimo di rispetto dei suddetti requisiti. Per avere una nozione di "pagamento informatico", si è dovuto attendere il d.p.r. 10 novembre 1997, n. 513, che ha introdotto la nozione di *electronic payments* rinviando però alle regole tecniche da emanarsi successivamente con decreto del Presidente del Consiglio dei ministri, poi emanato in data 8 febbraio 1999, il quale pur disciplinando puntualmente la formazione, la trasmissione, la conservazione, la duplicazione, la riproduzione e la validazione, anche temporale, dei documenti informatici attraverso la firma digitale non contiene alcun accenno ai pagamenti elettronici.

Una valida definizione di strumento di pagamento elettronico è riscontrabile nella raccomandazione della Commissione europea n. 97/489/CE del 30 luglio 1997, che si riferisce alle operazioni mediante strumenti di pagamento elettronico, con particolare riferimento alle relazioni tra gli emittenti ed i titolari di tali strumenti. In essa lo strumento di pagamento elettronico è definito come uno strumento che consente al titolare di effettuare le operazioni di trasferimento di fondi,

ad eccezione dei trasferimenti conferiti su istruzione ed eseguiti da istituzioni finanziarie, nonché le operazioni di ritiro di denaro contante e caricamento o scaricamento di tali strumenti presso attrezzature come le casse automatiche e gli sportelli automatici, nonché presso l'emittente o presso un ente obbligato contrattualmente ad accertare detti strumenti di pagamento.

Operare una classificazione dei sistemi di pagamento non è però agevole, in virtù della progressiva stratificazione di proposte e di progetti relativi ad una materia profondamente influenzata dallo sviluppo tecnologico, che ha portato non solo alla creazione di nuovi sistemi di pagamento, ma anche al miglioramento di quelli già esistenti, che in taluni casi costituiscono in realtà la fusione di più sistemi diversi, rendendo oltremodo difficoltosa un'eventuale distinzione generalizzata fra gli stessi[29]. I sistemi di pagamento, del resto, devono essere caratterizzati da versatilità ed adattabilità, per poter essere adeguati sia alle esigenze delle differenti tipologie contrattuali sia all'incessante progresso in ambito informatico.

La classificazione, pertanto, può essere effettuata secondo alcune macro-categorie che si caratterizzano per la loro non esaustività e in alcuni casi per una relativa complementarietà, atteso che uno stesso sistema può rientrare in più categorie, per cui la singola specificità risulta dovuta alla combinazione di più aspetti. Possiamo così distinguere fra **sistemi di pagamento**:

[29] Si pensi, ad esempio, alle carte di pagamento a doppia natura rilasciate dagli istituti bancari, che sono contemporaneamente carte di debito e carte di credito a seconda dell'utilizzo che se ne vuole fare, oppure alle numerose ed eterogenee tipologie di pagamento effettuabili tramite telefoni cellulari (sulle quali v. *infra*).

a) *mediante accesso a distanza* e *di moneta elettronica*: tale distinzione è operata nella citata raccomandazione n. 97/489/CE, che però esclude dal suo ambito di applicazione le reti chiuse. I primi comprendono tutti i mezzi di pagamento tradizionali applicati alla Rete, ivi comprese le carte di credito, mentre i secondi costituiscono uno strumento di pagamento in cui il valore monetario è memorizzato su un dispositivo elettronico;
b) *diretti* e *indiretti*: i primi richiedono l'interazione tra il compratore e il venditore, mentre i secondi consentono l'avvio della procedura di pagamento senza richiedere la contemporanea presenza delle parti;
c) *on line* e *off line*: nei primi lo scambio dei dati avviene in tutte le fasi sempre per mezzo di Internet, mentre nei secondi anche una sola fase può essere svolta senza l'utilizzo della Rete;
d) *tradizionali*, *elettronici* e *virtuali*[30]: i primi sono tuttora utilizzati nell'ambito del commercio elettronico indiretto, quando il pagamento viene effettuato mediante contrassegno o denaro contante (inviato tramite posta ordinaria). Nei sistemi di pagamento elettronici (o di seconda generazione), invece, le carte di pagamento[31] sostituiscono il denaro contante, mentre in quelli virtuali (o di terza generazione) si

[30] Questa distinzione, in realtà cronologica, non trova corrispondenza in ambito normativo, ma permette di cogliere l'evoluzione in materia.
[31] Ossia le carte di credito e le carte di debito e tutti i servizi di pagamento bancario che si sono informatizzati, come il bonifico bancario effettuato *on line*.

concretizzano quasi esclusivamente nella moneta elettronica;

e) *hardware* e *software*: i primi sono classificati in *stored value cards* e si suddividono a loro volta in sottocategorie a seconda di una classificazione tecnica o giuridica. Questa categoria comprende tutti gli strumenti riconducibili alla tipologia delle «carte»[32], e delle loro evoluzioni. Nella realtà la maggior parte dei sistemi *hardware* utilizza per le transazioni via Internet le fasi e i protocolli delle transazioni effettuate tramite strumenti *software* e viceversa gli strumenti di pagamento *software* risiedono inevitabilmente su diversi supporti *hardware*. Gli strumenti di pagamento *software* si

[32] Le carte possono essere *ordinarie* o *telematiche*. Le prime sono plastificate o in cartoncino e in esse i dati necessari all'identificazione in alcuni casi possono essere celati sotto una striscia argentata da rimuovere oppure espressi nei codici a barre (che devono essere letti in appositi lettori per autorizzare la transazione). Le seconde danno luogo ad una trasmissione diretta, tramite un canale telematico, dei dati dell'utente e della transazione in corso; possono essere magnetiche od elettroniche e a loro volta si dividono in altre categorie. Le *carte magnetiche* presentano sul retro una striscia di materiale magnetico, mentre le *carte elettroniche* sono carte telematiche che contengono uno o più microcircuiti con funzione di memorizzazione e di elaborazione. A differenza di quelle magnetiche, si presentano *standard* solo per quanto attiene alle caratteristiche fisiche, le dimensioni, la disposizione geometrica dei contatti e il significato da assegnare a ciascun contatto, mentre l'*hardware* (i microcircuiti utilizzati) e il *software* (i programmi) cambiano a seconda delle case produttrici e della funzione data alla carta. Le carte elettroniche sono dunque più costose di quelle magnetiche, ma sono anche più sicure, perché sono corredate da un codice personale segreto detto PIN (*Personal Identification Number*), e sono duplicabili solo con un procedimento estremamente complesso e costoso. Le carte elettroniche vanno poi distinte in *carte a memoria* e *carte intelligenti*. Le prime contengono solo i circuiti di memoria (che immagazzinano i dati) e i circuiti necessari per comunicare con la macchina lettrice contenente il *software* di controllo; le seconde invece contengono dei veri e propri microelaboratori e, con essi, anche il *software* di controllo. Le carte elettroniche sono più costose di quelle magnetiche, ma anche più resistenti e sicure, perché non possono essere lette se non si conosce la chiave di accesso alla memoria interna della carta o PIN, e la loro duplicazione è inoltre molto più complicata e costosa di quella delle carte magnetiche.

suddividono in tre sottocategorie: *debit based*, *credit based* e *token based*. Più specificatamente, i sistemi *credit based*, sono protocolli e servizi basati sull'uso di carte di credito, che prevedono l'invio del numero attraverso sistemi di crittografia, finalizzati alla protezione delle informazioni scambiate. Sono stati così ideati protocolli di sicurezza[33],

[33] I protocolli di comunicazione si avvalgono anche di altre componenti ed i relativi sistemi possono essere suddivisi in tre categorie: a) *sistemi a pagamento diretto con utilizzo di SSL* (*Secure Socket Layer*), nei quali i dati della carta di credito sono comunicati direttamente al venditore. Il protocollo utilizzato è l'SSL (adottato da Netscape e Microsoft), che prevede un sistema sicuro, basato sulla crittazione preventiva delle informazioni da inviare *on line*. L'utilizzo dell'SSL avviene in maniera trasparente per l'utente, che deve solamente utilizzare un *browser* predisposto, mentre l'implementazione dell'SSL nel *merchant system* richiede la presenza di un certificato SSL, che viene rilasciato da una delle tante *Certification Authority* presenti su Internet. L'autenticazione degli interlocutori e lo stabilimento della connessione avvengono mediante l'uso di certificati digitali, la cui validità può essere verificata risalendo la catena delle autorità di certificazione; tale verifica, in linea generale, viene svolta automaticamente dai normali *browser*, che avvertono l'utente della sussistenza di eventuali problemi. Tuttavia, anche se l'SSL garantisce la sicurezza delle comunicazioni tra venditore e compratore, quest'ultimo dovrà fidarsi del *merchant* per quanto riguarda la gestione dei dati della propria carta, perché i codici PAN (*Personal Account Number,* costituiscono i numeri identificativi delle carte di credito, sulle quali v. *infra*) delle carte saranno custoditi proprio dal *merchant*, che oltretutto sarà responsabile della loro segretezza. Dall'altro lato, però, il *merchant* non ha garanzie circa l'identità del compratore, che potrebbe utilizzare numeri di carta di credito rubati oppure compiere realmente un acquisto per poi ripudiarlo in seguito. Questa tipologia di sistemi di pagamento è alquanto diffusa all'estero e in particolare negli Stati Uniti, mentre in Italia essi sono utilizzati soltanto dai siti di *e-commerce* più importanti, per i quali già la notorietà del proprio marchio garantisce l'acquirente; b) *sistemi basati su payment gateway*, che utilizzano il protocollo SSL con *redirection*. Il *payment gateway* è un componente che si interpone in Internet tra le parti negozianti una compravendita, e un *network* interbancario, durante la fase della transazione con carta di credito. Pertanto, al momento della digitazione del numero di carta di credito, il sistema automaticamente reindirizza l'acquirente dal sito di *e-commerce* al *payment gateway*, utilizzando un canale di comunicazione crittografato. Il *merchant* non viene mai a conoscenza dei dati della carta e delega la ricezione dei pagamenti completamente al *payment gateway*, mentre l'acquirente sa che il numero della propria carta viene inviato direttamente ed esclusivamente al *payment gateway*, che nel caso di specie è un istituto bancario. Il *payment gateway* inoltra la richiesta al circuito autorizzativo e ne comunica l'esito sia al compratore che al venditore; c) *sistemi non*

alcuni prodotti in collaborazioni tra più soggetti e istituzioni, altri invece creati e sviluppati *ad hoc* per singoli casi. I sistemi *debit based* si basano sull'impiego di assegni elettronici[34]. Il funzionamento teorico di un pagamento tramite assegno digitale segue un *iter* procedurale sostanzialmente analogo a quello del corrispettivo titolo in formato cartaceo. Il traente compila l'assegno su un elaboratore elettronico e la sottoscrizione elettronica viene apposta da un apposito *software*. L'assegno elettronico, salvato come *file*, viene poi inviato al prenditore tramite posta elettronica o direttamente via *web* mediante una connessione protetta al sito di *e-commerce*. All'assegno viene apposta la firma digitale, a titolo di girata per l'incasso, dal beneficiario (o dall'ultimo giratario) e quindi inoltrato all'Istituto finanziario gestore del servizio, che ha il ruolo di *stanza di compensazione (Clearing House*) per consentire il

---

ripudiabili, che assicurano l'autenticazione di tutti gli attori, dal *payment gateway* al compratore. Essi richiedono, dunque, che il compratore disponga di un mezzo con cui autenticarsi e, generalmente, viene utilizzata la firma digitale con crittografia a chiave pubblica (sulla quale v. *infra*), per cui l'utente deve dotarsi di un *software* specifico per potersi autenticare agli altri attori. Per quanto tali sistemi offrano eccellenti garanzie di sicurezza, sono tuttavia poco diffusi, a causa della loro complessità, che incide poi sui costi e sulla facilità di utilizzo.

[34] Tali sistemi presuppongono l'apertura di un conto presso una banca *on line*, sul quale verrà poi tratto l'assegno che rappresenta il corrispettivo, in formato digitale, di un tradizionale assegno bancario cartaceo, la cui normativa si applica anche all'assegno digitale, il quale ha la forma di un'immagine riprodotta sullo schermo di un elaboratore elettronico, nella quale sono predisposti appositi spazi in cui inserire le informazioni necessarie, identiche a quelle che devono essere scritte su un normale assegno cartaceo, mentre, non potendosi ovviamente apporre una firma autografa, l'assegno digitale viene autenticato con la *firma digitale* del soggetto autorizzato alla tratta. Inoltre, la banca dell'emittente può sottoscrivere tale assegno, attestando che l'emittente è un suo correntista, in grado di assolvere al pagamento.

dialogo tra le banche coinvolte, la convalida del titolo di credito nonché l'autorizzazione al trasferimento dei fondi. In alternativa l'assegno può essere depositato presso l'istituto bancario ove il beneficiario è correntista e l'istituto stesso effettua poi la richiesta di riscossione alla *Clearing House*. I sistemi *token based* si basano sulla creazione di una vera e propria moneta virtuale (*e-cash*) e sono generalmente impiegati in transazioni di modico valore. Una moneta elettronica consiste in una ricevuta in formato digitale, oppure di un semplice *file*, che attesta l'avvenuta precostituzione di una somma di denaro presso un ente di provata affidabilità e liberamente circolabile, in quanto garantita dal deposito stesso, fino alla richiesta di riconversione all'istituto emittente (zecca virtuale, *e-mint*). La valuta digitale costituisce, pertanto, una fattispecie di moneta fiduciaria, assimilabile al mezzo di scambio vigente in un sistema monetario fondato sul regime di convertibilità;

f) *macropagamenti* e *micropagamenti*: tale distinzione è quantitativa e fa riferimento al valore della transazione. Nelle transazioni di modico valore vengono generalmente utilizzati sistemi di sicurezza alquanto blandi, al fine di ridurre le spese di commissione, che altrimenti renderebbero antieconomica la stessa transazione;

g) di *e-commerce* e di *mobile commerce*: nel più generale ambito del commercio elettronico, il telefono cellulare si presta ad una

molteplicità di utilizzi nell'ambito del commercio elettronico. Esso può essere utilizzato come strumento di più tipologie di pagamenti elettronici dalla natura eterogenea, mediante i noti sistemi SMS (*Short Message System*) e WAP (*Wireless Application Protocol*)[35], oppure scalando l'importo dal credito residuo disponibile presso il proprio gestore del servizio di telefonia mobile, o, ancora, come semplice strumento di comunicazione per la conferma di un pagamento[36].

Dalle classificazioni generali sopra esposte si possono evincere l'eterogeneità e la complessità degli strumenti di pagamento elettronico. In tale ambito assumono particolare rilievo, per la loro diffusione, le carte di credito, di debito e prepagate, cui si è accennato. In particolare,

[35] Il WAP rappresenta una forma ridotta ed adattata alle specifiche peculiarità dei terminali mobili del protocollo HTTP. Esso consente la visualizzazione delle pagine *web* in un formato adatto al *display* del telefono cellulare, che deve essere dotato del necessario software per la visualizzazione di contenuti remoti (*microbrowser*). Il collegamento tra il telefono (*client*) ed il sito (*server*) necessita poi del *WAP gateway*, che converte il formato e la struttura dei pacchetti di dati per consentire il transito dei dati fra due reti eterogenee (Internet e la rete di telefonia mobile).

[36] Nell'abbinamento tra negoziazioni di commercio elettronico e dispositivi di telefonia mobile si possono individuare due distinti ambienti di realizzazione, in base alle caratteristiche tecniche del substrato comunicativo nel quale trovano collocazione gli scambi negoziali e del livello di intensità con cui il cellulare ne costituisce elemento peculiare. In un primo ambiente, la transazione di commercio elettronico viene realizzata per mezzo dell'abbinamento, da parte dell'acquirente, del proprio telefono cellulare al *computer* con il quale l'utente stesso accede ad Internet e si collega al sito di *e-commerce*. Il terminale mobile, che in tal caso svolge la propria naturale funzione di dispositivo di comunicazione vocale, viene integrato nel sistema quale mezzo con cui il compratore identifica se stesso presso il proprio istituto creditizio ed ottiene l'autorizzazione a disporre da remoto degli strumenti di pagamento a lui facenti capo, tra i quali spicca la carta di credito. In un secondo ambiente, invece, il telefono cellulare è lo strumento per mezzo del quale viene effettuata la connessione ad Internet e viene inoltre realizzata, in tutte le sue fasi, la negoziazione commerciale. In tal caso si verifica una peculiare fattispecie di commercio elettronico, nota come *mobile commerce* (commercio elettronico mobile).

la *carta di credito* (che può essere prodotta su diversi supporti, come carte a banda magnetica e *smart card*[37]) è un documento che abilita il titolare, in base a un rapporto contrattuale con l'emittente, a effettuare acquisti di beni o servizi presso qualsiasi esercizio convenzionato con l'emittente stesso. In ogni sistema di carte di credito operano tre soggetti: l'emittente, il titolare e l'esercente. L'*emittente* (ente od istituto bancario), è chi emette e consegna al titolare una carta di credito ed, al tempo stesso, associa un esercente per l'accettazione della stessa. In questo modo, il *titolare*, per l'acquisto di un bene o per il pagamento di un servizio, deve rivolgersi all'esercente convenzionato col circuito cui appartiene la carta di credito del titolare. Una volta effettuato l'acquisto o pagato il servizio, l'*esercente* dovrà sottoscrivere al titolare della carta un documento o *voucher*

[37] Le *smart card* sono dotate di un *chip* che contiene un microprocessore, una memoria RAM, una memoria ROM nonché l'interfaccia per l'alimentazione e il dialogo con altri sistemi. Grazie alla propria capacità elaborativa autonoma e all'elevata capienza di memorizzazione di informazioni, la carta con microprocessore è in grado di ospitare al suo interno un insieme di procedure di autenticazione e i sistemi crittografici per la protezione dei dati in essa contenuti. La tecnologia attuale permette quindi al *chip* di contenere più applicazioni, garantendo la piena separazione dei relativi ambienti operativi (dati e procedure). Tale possibile coesistenza, peraltro, consente di offrire, per mezzo di un unico supporto, molteplici servizi di diversa natura. L'identificazione del portatore di una *smart card* può essere eseguita interamente all'interno della carta stessa, grazie ai dati contenuti nell'area di memoria ed all'inserimento di un codice PIN. Per essere in grado di produrre *smart card* contraffatte, bisognerebbe dunque ottenere un *chip* avente le identiche caratteristiche di quello originale ed in tal caso è necessario conoscere le specifiche di costruzione e della struttura dei dati memorizzati sulla *smart card* autentica, tra cui la chiave e gli algoritmi utilizzati per la gestione della carta; inoltre, sono necessari strumenti altamente tecnologici e specializzati, assai costosi. A questo vantaggio va aggiunta la possibilità di programmare il microcircuito in modo tale da riconoscere eventuali attività fraudolente, tramite la previsione di un limite di spesa non superabile o la disabilitazione della carta in caso di iterazione del tentativo di inserimento del codice d'accesso utilizzato tramite il lettore di *smart card*. Tuttavia, a differenza delle carte tradizionali, l'utilizzo di *smart card* richiede un apposito lettore (*smart card reader*) collegato al *computer*, mentre l'inserimento del PIN avviene in locale direttamente sull'elaboratore e consente l'accesso alle informazioni.

(tagliando) con il quale lo riconosce debitore dell'importo relativo alla sua spesa, per ottenere, successivamente, il corrispettivo in denaro con la presentazione presso la propria banca dei *voucher*, o sottoscrizioni di debito, raccolte nell'arco di uno o più giorni[38]. A questo punto, attraverso l'inoltro delle «memorie di spesa» dalla banca dell'esercente a quella dell'emittente, quest'ultimo provvederà ad addebitare sul conto corrente del titolare il corrispondente importo[39]. Il pagamento da parte del titolare è differito e normalmente avviene a cadenze predefinite, di solito mensilmente in unica soluzione oppure, se è stato previsto, anche in forma rateale.

Nelle *carte di debito*, l'addebito avviene entro un breve periodo di tempo a decorrere dall'acquisto. Esse sono utilizzabili per transazioni nelle quali si provvede automaticamente all'immediato pagamento del

[38] Questa procedura è spesso automatizzata e i *voucher* servono solo come prova in caso di controversia.

[39] Normalmente le carte di credito sono emesse da istituti bancari, da società specializzate o direttamente dagli esercenti di catene di distribuzione commerciale. Ogni carta di credito è identificata da un numero (*Personal Account Number,* PAN), con cui è possibile risalire alla banca e al conto corrente dal quale andranno prelevati gli importi. Le carte di credito tradizionali sono dotate di una banda magnetica, per accelerare la lettura elettronica dei dati già impressi in rilievo sulla medesima (PAN e scadenza). I meccanismi di costruzione della sequenza di cifre attribuita a ciascuna carta riducono sia i rischi di errori in caso di digitazione del numero presso un elaboratore (per evitare che ad un numero errato corrisponda un numero di carta esistente) che la possibilità di compiere frodi mediante la generazione fortuita di numeri di carte di credito. I numeri vengono inoltre attribuiti ad ogni carta in base ad un algoritmo matematico denominato *Luhn Check Digit Algorithm*, in base al quale la sequenza di cifre che costituisce il numero deve rispettare determinate proprietà, verificabili attraverso una successione di calcoli svolti dall'elaboratore. Tuttavia, alcuni *software* (illegali ma facilmente reperibili su *Internet*) permettono di calcolare il numero della carta di credito mediante l'applicazione dell'algoritmo di Luhn, creando numeri che hanno una buona probabilità di risultare validi. Oltre al numero di carta di credito, sul retro della stessa viene posto un secondo numero (chiamato *AVS, Address Verification System* o *Address Verification Service*), che consente di verificare l'effettivo possesso della *credit card*..

commerciante attraverso un punto di vendita automatizzato (*Point of Sale*, P.O.S.), addebitando direttamente la relativa somma di denaro sul conto corrente bancario dell'acquirente, nel cui conto, in linea generale, deve essere depositata una cifra quanto meno pari a quella oggetto di transazione. L'accesso al sistema avviene con l'abbinamento della tessera magnetica e dell'inserimento di un codice segreto (*Personal Identification Number*, P.I.N.)[40]. Il terminale avvia un procedimento di accredito e addebito nei conti correnti di acquirente e venditore. Le carte di debito possono inoltre essere utilizzate per effettuare prelevamenti di denaro contante dal proprio conto corrente attraverso gli appositi sportelli automatici (*Automatic Teller Machines*, A.T.M.)[41]. Oggi le carte di debito sono dotate anche del servizio *Fastpay*, che, similmente a quanto avviene con le carte di credito, consente al titolare di acquistare negli esercizi convenzionati senza utilizzare il PIN e di ricevere l'addebito ad una determinata scadenza.

Nelle *carte prepagate*, il valore monetario è immagazzinato, per cui, prima di ricevere la carta o contestualmente al suo ricevimento, il proprietario paga il corrispettivo al distributore della medesima. Esse operano, pertanto, secondo il principio del pagamento anticipato, e possono essere utilizzate per un limitato numero di transazioni, molto spesso in un ridotto numero di punti vendita. Nel caso di una carta prepagata monouso, poi, il distributore della carta e il distributore del servizio possono coincidere. Ci sono inoltre carte prepagate che possono

[40] Esse sono essenzialmente riconducibili alla tipologia «Pago Bancomat», attraverso la quale si può accedere sia al «servizio Bancomat» funzionante come A.T.M.(*Automatic Teller Machines*) , sia al «servizio Bancomat-P.O.S. ».

[41] Con l'adesione al circuito *Cirrus-Maestro* è possibile effettuare prelevamenti anche in stati esteri.

essere utilizzate per un gran numero di scopi e su scala nazionale o internazionale, sempre però ristrettamente ad una certa aree, come nel caso delle schede telefoniche.

Alla *moneta elettronica* sono riconducibili solo alcuni dei sistemi di carte prepagate, le cui caratteristiche (anonimato, idoneità ai micropagamenti, rischio limitato all'importo residuo, possibilità di smobilizzo della somma non utilizzata) sono comunque estensibili anche alla moneta elettronica propriamente detta. Le carte prepagate, tuttavia, non conducono alla creazione di un nuovo bene fungente da moneta, dotato di potere d'acquisto autonomo, poiché con la digitazione del numero della carta viene impartito un ordine di trasferimento di un importo dal conto precostituito, e il ricevente può solo, eventualmente, richiederne l'accredito sul proprio conto corrente bancario. La moneta elettronica è, invece, uno strumento di pagamento in cui il valore monetario è memorizzato su un dispositivo elettronico in possesso del cliente ed il cui ammontare caricato diminuisce o aumenta, a seconda dell'operazione effettuata, ogni volta che il proprietario del dispositivo lo utilizza per un'operazione di acquisto, vendita, carico o scarico utilizzando sistemi all'uopo predisposti. Essa è, pertanto, un titolo di credito al portatore[42], che non richiede un preesistente rapporto di conto

[42] «Digicash» costituisce la soluzione caratterizzata dalla massima verosimiglianza con il denaro cartaceo. Proposto nel 1994 da David Chaum, Digicash (denominazione poi mutata in «Ecash») ha rappresentato il primo prodotto per lo scambio di moneta elettronica tramite reti telematiche. Il sistema prevede l'attivazione di un deposito presso un ente creditizio abilitato alla distribuzione della valuta Ecash ed il successivo *download*, da parte di ciascun utente, di un applicativo *software* di portafoglio digitale (*Ecash wallet*), destinato allo stoccaggio, presso l'elaboratore del correntista, della moneta digitale di cui è richiesta l'emissione alla banca. La peculiarità del metodo Digicash consiste nel totale anonimato del denaro elettronico generato. Una particolare applicazione crittografica, nota come firma cieca (*blind signature*), consente

corrente bancario, offrendo così una ulteriore garanzia di anonimato. La disciplina della moneta elettronica è dettata dalla direttiva 2000/46/CE, del Parlamento europeo e del Consiglio del 18 settembre 2000, "riguardante l'avvio, l'esercizio e la vigilanza prudenziale dell'attività degli istituti di moneta elettronica". La direttiva in oggetto definisce la moneta elettronica come un surrogato elettronico di monete metalliche e banconote, memorizzato su un dispositivo elettronico come una carta a microprocessore o una memoria di elaboratore[43]. La previsione comunitaria non richiede una spendibilità generalizzata della moneta elettronica, essendo, al contrario, sufficiente che detto strumento sia accettato anche solo da un limitato numero di imprese e finanche dai soli componenti del gruppo di appartenenza dell'emittente. L'emissione deve avvenire dietro ricezione di fondi il cui valore non sia inferiore al valore monetario emesso[44], e, dunque, l'emissione di moneta elettronica non crea moneta.

La moneta elettronica è caratterizzata dalla rimborsabilità, per cui

---

l'apposizione, da parte della banca emittente, della propria firma digitale su ciascun esemplare coniato, occultando tuttavia alla zecca virtuale il numero di serie di ogni stringa di bit autenticata. Il codice di identificazione di ogni singola moneta digitale diviene visibile alla banca solo al momento della riconversione, rendendo in tal modo fattibile l'impedimento della doppia spesa, ma non la ricostruzione dell'identità del soggetto che aveva domandato la creazione di *electronic cash*.

[43] Con l'espressione "moneta elettronica", contenuta nell'art.1, par.3, lett.b) della direttiva 2000/46/CE si intende "un valore monetario rappresentato da un credito nei confronti dell'emittente che sia: i) memorizzato su un dispositivo elettronico; ii) emesso dietro ricezione di fondi il cui valore non sia inferiore al valore monetario emesso; iii) accettato come mezzo di pagamento da imprese diverse dall'emittente".

[44] In particolare, costituiscono attività di emissione di moneta elettronica tutte quelle operazioni elementari attraverso le quali l'emittente riceve da parte del richiedente l'emissione una somma di denaro; procede a memorizzare nel dispositivo elettronico del richiedente una posizione di disponibilità monetaria di entità non superiore alla somma previamente ricevuta («caricamento»); mette il titolare del dispositivo in condizione di disporre della moneta elettronica in esso caricata.

il detentore di moneta elettronica può, durante il periodo di validità, esigere dall'emittente il rimborso del valore nominale o in denaro contante oppure mediante un versamento su un conto corrente senza altre spese che non siano strettamente necessarie per l'esecuzione di tali operazioni, con un limite minimo per il rimborso non superiore a dieci euro.

Nonostante ciascun sistema di moneta elettronica sia contraddistinto da proprie specificità funzionali, è possibile individuare alcune caratteristiche di sicurezza comuni e per evitare azioni fraudolente (falsificazione, alterazione in aumento del valore nominale, doppia spesa), vengono utilizzati sistemi di crittografia a chiave pubblica e si fa ricorso alla firma digitale[45].

Nell'ambito della moneta elettronica si può distinguere fra due tipologie, a seconda del dispositivo di memorizzazione e conservazione della stessa: *network money* (*moneta virtuale in senso stretto*), che è una valuta digitale residente sull'*hard disk* di un elaboratore, e *card money* (*borsellino elettronico* o *e-purse*), consistente in un valore elettronico caricato su una *smart card*. In particolare, la moneta caricata sulle *smart card* è idonea alla sostituzione del denaro circolante in ogni ambiente, anche al di fuori

[45] La sequenza di cifre in formato binario alla quale corrisponde una dato importo monetario viene digitalmente firmata dell'emittente. La sottoscrizione elettronica, apposta dalla zecca virtuale tramite la propria chiave segreta, oltre a contrastare efficacemente la falsificazione (*autenticità*) e la modifica del valore nominale caratterizzante ciascuna specifica stringa di bit (*integrità*), garantisce che il soggetto richiedente il conio della moneta abbia preventivamente disposto la necessaria copertura finanziaria. La generazione di una somma di denaro in formato elettronico prevede inoltre il legame con un identificatore univoco, analogo al numero di serie presente sulle banconote tradizionali. Nel corso della fase di estinzione dell'*electronic cash*, o di trasferimento del relativo importo sul conto corrente bancario del riscossore, la verifica del numero identificativo consente di appurare l'eventuale tentativo di riutilizzo di un medesimo valore elettronico presso prenditori diversi.

delle transazioni *on line*, posto che in tal caso è necessario che solo il *merchant* abbia il lettore di *smart card*, similmente a quanto avviene nei POS, incentivando, potenzialmente, la futura diffusione globale di tale strumento. Il relativo procedimento viene svolto senza l'intervento di intermediari aggiuntivi durante lo scambio di dati digitali, poiché, una volta emesse regolarmente le carte in oggetto, non è richiesta alcuna fase di autorizzazione al pagamento. Ne consegue una riduzione dei costi, dovuto al minore impiego complessivo di risorse, cui tuttavia si accompagna la necessaria presenza di un lettore di *smart card*. Inoltre, per garantire una interoperabilità globale allo strumento in oggetto, è stato costituito un organismo internazionale volto alla definizione di procedure funzionali *standard* di *card money*, denominato CEPS (*Common Electronic Purse Specifications*), al quale hanno attualmente aderito trenta nazioni, nel cui ambito è stato emesso oltre il 90% delle *smart card* prepagate sinora create.

5. ASPETTI PROBLEMATICI DELLA SICUREZZA DELLE TRANSAZIONI ELETTRONICHE

Il problema forse più rilevante nell'ambito delle transazioni elettroniche è costituito dalla sicurezza dei dati: la diffusione del commercio elettronico e degli strumenti di pagamento elettronico dipende in buona parte dalla concreta possibilità di garantire la piena riservatezza delle informazioni circolanti, soprattutto con riferimento a dati di diretta valenza economica, come i numeri di carta di credito. Alla garanzia di sicurezza si deve accompagnare una corretta informazione in

merito, al fine di consentire il superamento dei diffusi dubbi in merito all'opportunità di utilizzare tali sistemi *on line*, dovuti al timore di subire frodi informatiche. Del resto, la sicurezza di un bene materiale viene raggiunta mediante la predisposizione di sistemi ben visibili e tangibili, come stanze e porte blindate, mentre la sicurezza di un bene immateriale è necessariamente altrettanto immateriale e dunque è ben più difficile convincere della sicurezza di determinati sistemi chi non ha un'ottima conoscenza dei sistemi informatici. Ne consegue che per conseguire la fiducia dei potenziali utilizzatori e dunque contribuire allo sviluppo del commercio elettronico, è necessario sviluppare metodologie che forniscano garanzie relative alla sicurezza dei dati, regolamentando la materia in modo da consentire la piena ed effettiva protezione delle relative informazioni.

La progressiva smaterializzazione della ricchezza rende sempre più importante la problematica in oggetto, soprattutto a causa della interconnessione globale dei sistemi resa possibile da Internet, che, paradossalmente, è al tempo stesso l'elemento che ha consentito, di fatto, lo sviluppo del commercio elettronico, e che tuttavia può ostacolarne l'incremento. Il fatto stesso che i canali di distribuzione elettronica siano basati, direttamente o indirettamente, proprio su Internet, ha importanti conseguenza sul piano della sicurezza dell'informazione, poiché un canale di comunicazione, per quanto possa essere protetto da strumenti di crittografia, subisce un rischio di intrusione proporzionale al numero di persone che accedono al canale stesso. L'accesso ad Internet, difatti, può essere effettuato da stati differenti, ciascuno con una propria legislazione, per cui la commissione di illeciti *on line* può essere facilitata

da più fattori. Una condotta umana può essere lecita in una nazione ed illecita in un'altra; inoltre, l'utilizzo di determinate tecniche può rendere praticamente impossibile risalire all'autore di un eventuale illecito; inoltre, è di tutta evidenza che perseguire un soggetto che si trova dall'altra parte del mondo rispetto al soggetto leso è impresa tutt'altro che facile.

6. QUESTIONI FISCALI

Internet mette in crisi i singoli stati in virtù dei suoi caratteri di immaterialità e di a-territorialità, in quanto la sovranità di ciascun paese è legata al suo territorio; parimenti problematico diventa anche l'esercizio della loro sovranità tributaria[46] e la composizione degli eventuali contrasti in merito. "È infatti innegabile che i concetti fondamentali del diritto tributario siano stati elaborati in relazione ad un commercio formato essenzialmente da transazioni tra presenti con oggetti dotati di una ben determinata soglia di riconoscibilità sensoriale"[47]; Sinora, infatti, gli ordinamenti tributari si sono ispirati al principio della tassazione del reddito mondiale (*world wide principle*) nei confronti dei soggetti residenti[48] ed al principio della fonte[49] (*source principle*) nei confronti di quelli non

[46] Sullo specifico problema dell'IVA v. S. SAMMARTINO, *Commercio elettronico internazionale ed IVA: la qualificazione delle operazioni alla luce della normativa italiana*, in RINALDI R. (a cura di), *op. cit.*, pp. 157-168.
[47] E. MARELLO, *Le categorie tradizionali del diritto tributario ed il commercio elettronico*, in R. RINALDI (a cura di), *op. cit.*, p. 169.
[48] In tal caso "si tiene in considerazione la pretesa dello Stato di residenza del soggetto passivo, beneficiario della fattispecie in questione" (G. CORABI, *Il commercio elettronico e la crisi della fiscalità internazionale*, Milano, 2000, p. 59).
[49] Qui, invece, "si tiene in considerazione la pretesa dello Stato in cui è situata la fonte effettiva del reddito" (G. CORABI, *ivi*, p. 59).

residenti, applicandoli congiuntamente o disgiuntamente[50]; lo svolgimento di attività commerciali nell'ambito di Internet è tuttavia caratterizzato dalla dematerializzazione delle singole operazioni nelle quali è possibile suddividere i singoli negozi nei quali si concretizzano tali fattispecie, rendendo problematica l'imposizione tributaria da parte dei singoli stati, tradizionalmente legata ai criteri della residenza o della stabile organizzazione.

In particolare, la stabile organizzazione, in senso materiale, è generalmente intesa come la sede fissa di affari in cui l'impresa non residente esercita in tutto o in parte la sua attività: bisognerebbe dunque valutare l'ubicazione del *server* per mezzo del quale l'attività è svolta, a meno di non ritenere che la predisposizione di un sito *web* costituisca un'offerta al pubblico e sia dunque da ritenere come l'effettuazione di un'attività, pertanto sufficiente a giustificare la tassazione del relativo reddito. In senso personale, invece, tale criterio prevede la possibilità di tassare l'impresa straniera nello stato della fonte anche qualora non agisca in proprio ma piuttosto attraverso un agente che concluda contratti per suo conto. Sul punto, in dottrina si è ritenuto che, al fine di esercitare la potestà impositiva, l'agente debba necessariamente essere una persona fisica e non possa invece essere un *software agent*[51]. Nel caso dei redditi d'impresa costituiti da interessi, dividendi o *royalty*[52] che non

[50] P. ADONNINO, *Il commercio via* Internet *e la fiscalità: gli aspetti generali delle attività transnazionali e nazionali*, in R. RINALDI (a cura di), *op. cit.*, p. 30.
[51] L. HINNEKENS, *L'applicazione del concetto di stabile organizzazione e degli altri principi di giurisdizione all'imposizione del reddito derivante dal commercio elettronico*, tr. it., in R. RINALDI (a cura di), *op. cit.*, pp. 51-55.
[52] La *royalty* è il compenso di qualsiasi natura ricevuto come remunerazione per l'uso o la concessione in uso di diritti d'autore su opere letterarie, artistiche o scientifiche, e

siano conseguiti da una stabile organizzazione all'interno dello stesso stato, lo stato di residenza può generalmente esercitare la potestà impositiva, mentre lo stato della fonte mantiene un certo diritto di prelievo[53].

Tali considerazioni sono valide per il nostro ordinamento, poiché, ai sensi dell'attuale normativa italiana, al fine di stabilire la localizzazione del reddito in Italia, è necessario che lo svolgimento di un'attività avvenga in Italia oppure che ivi esista una stabile organizzazione a mezzo della quale sia svolta l'attività[54].

Un ulteriore problema è relativo al c.d. *transfer pricing*, ossia ai prezzi di trasferimento, che costituiscono uno strumento essenziale nella tassazione dei redditi transnazionali allo scopo di garantirne la corretta attribuzione ai singoli stati[55]. La crescente frammentazione dei processi produttivi in più fasi, svolte da soggetti operanti in luoghi diversi, pone il problema di stabilire in termini di valore il loro impatto sull'intero processo, rendendo assai arduo quantificare della tassazione.

In considerazione dei problemi suesposti, in dottrina è stata proposta la "creazione di un luogo d'imposizione unico all'interno della Comunità per gli operatori di Paesi terzi, accompagnato da un controllo interamente elettronico delle prestazioni di servizio da essi effettuate e da una semplificazione totale dei loro obblighi dichiarativi onde incitare gli

---

di informazioni relative ad esperienze di carattere industriale, commerciale o scientifico.

[53] B. WESTBERG, *Tassazione del reddito derivante dal commercio elettronico internazionale*, tr. it., in R. RINALDI (a cura di), *op. cit.*, pp. 88-106

[54] G. C. CROXATTO, *Commercio elettronico internazionale ed imposte sul reddito: la localizzazione e la residenza alla luce dell'ordinamento italiano*, in R. RINALDI (a cura di), *op. cit.*, p. 109.

[55] P. ADONNINO, *op. cit.*, p. 33.

operatori a rispettare tali obblighi"[56].

7. I META TAGS

Il «*meta tag*» è una parola inserita all'interno del codice HTML di una pagina *web*, non visibile al suo fruitore, ma presa invece in considerazione dai motori di ricerca (come Google, HotBot, ecc.). I *meta tags* vengono utilizzati al fine di farsi pubblicità: difatti, essere inclusi nei cataloghi creati dai vari motori di ricerca consente di aumentare in maniera considerevole il proprio numero di contatti, soprattutto se in posizione di visibilità, con la possibilità di ottenere un maggior numero di introiti pubblicitari. Ad esempio, una ditta (Liberia Alfa S.p.A.) inserisce, tramite un *meta tag*, le parole «Libreria Beta S.p.A.», in modo che chiunque digiti, nella interrogazione di un motore di ricerca, i termini «Libreria Beta S.p.A.», giunga non nel sito di quest'ultima, ma piuttosto in quello della Libreria Alfa.[57]

L'utilizzo di marchi, generalmente celebri e sui quali non si detengono i diritti, come parole chiave ricercate dai motori di ricerca, costituisce una nuova modalità di attuazione della concorrenza sleale. Già la legge attribuisce al solo titolare del marchio la possibilità di farne uso esclusivo, ma nel caso di specie si verifica un abusivo ed indebito sfruttamento della notorietà raggiunta da un altro concorrente, perché il motore di ricerca, «ingannato» dai *meta tags*, potrebbe indicare come sito più rilevante non quello del titolare del marchio ma piuttosto di chi lo

[56] M. AUJEAN, *Il commercio elettronico internazionale e l'IVA*, tr. it., in R. RINALDI (a cura di), *op. cit.*, p. 155.
[57] L'esempio, parafrasato, è ripreso da M. BESSONE, E-economy *e commercio elettronico: quale diritto per i tempi di internet?*, in *Il diritto dell'informazione e dell'informatica*, 2002, 1, p. 48.

usa surrettiziamente!

Come afferma il Tribunale di Napoli, "la registrazione su Internet come nome a dominio di un marchio protetto e l'uso di quest'ultimo all'interno di *meta tags* o di pagine web da parte del non titolare per uno scopo commerciale e promozionale integrano una condotta illecita che rientra nella concorrenza sleale, di cui il provider deve rispondere come corresponsabile, qualora esista già la conoscenza dell'abuso ed il provider stesso non intervenga per eliminarlo."[58] La qualificazione giuridica di siffatte condotte è pertanto abbastanza semplice, in quanto esse rappresentano condotte di concorrenza sleale, dunque sottoposte alla relativa disciplina.

8.1 IL NOME DI DOMINIO E LA TUTELA DEL MARCHIO. ASPETTI GENERALI

Il nome di dominio (detto anche nome a dominio o *domain name* o *host name*) è l'indirizzo di un sito in formato alfabetico (ad esempio, www.parlamento.it), dunque potenzialmente assai semplice da ricordare, al contrario dell'indirizzo IP (*IP Address*), che è espresso in forma numerica. Come si è visto, un altro *computer* presente su Internet (il c.d.

[58] Trib. Napoli 28 dicembre 2001, in *Dir. inf.*, 2002, 1, pp. 94-100, con nota di P. SAMMARCO, *Atti di concorrenza sleale attraverso Internet e responsabilità del provider*, pp. 100-108. Il caso portato innanzi al giudice partenopeo riguardava la predisposizione di un sito Internet, denominato «www.philipsitaliaservice.it», nel quale si pubblicizzava un elenco di centri di assistenza domiciliare (posti in vari città italiane), contattabili mediante l'indirizzo *e-mail* «philipservice@libero.it» (nei quali, tra l'altro, era possibile riparare anche prodotti di altre aziende!). La pagina *web*, inoltre, conteneva un *meta-tag*, consistente nella denominazione del marchio della «Philips S.p.A.», nonché alcuni collegamenti ipertestuali volti ad ingenerare nell'utenza la convinzione che tale attività commerciale fosse svolta proprio dalla Philips.

Domain Name Server, DNS) permette di risalire, in maniera trasparente per l'utente, da un nome a dominio ad un indirizzo IP e viceversa.

È di tutta evidenza che assicurarsi un buon *domain name*, facile da memorizzare, aumenta il numero di connessioni al proprio sito, soprattutto per chi non sa districarsi bene all'interno della Rete. I problemi giuridici sorgono allorché venga registrato un nome di dominio coincidente ad un marchio, soprattutto se celebre[59], perché sinora il principio base della registrazione di un *host name* è consistito nella tempestività della registrazione, risultando di proprietà di chi per primo lo ha registrato (*first come, first served*). Ciò ha portato solo pochi anni fa ad un acquisto selvaggio dei nomi di dominio più semplici da ricordare, perché costituiti da parole di uso comune o da marchi celebri, al fine di rivenderne in un secondo tempo la proprietà ai soggetti interessati e ad un prezzo assai più elevato di quanto corrisposto per la registrazione (c.d. *cybersquatting* o *domain grabbing*). Nel secondo caso ciò costituisce una sorta di ricatto per le aziende, che per avere una efficace presenza *on line* sono costrette a dover acquistare il nome di dominio corrispondente al proprio marchio a prezzi anche assai elevati.

In assenza di una specifica disciplina legislativa *in subiecta materia*, dottrina e giurisprudenza concordano nell'equiparare il mondo virtuale a quello fisico, applicando la regola per cui il titolare dei diritti di uso

[59] Il marchio può consistere tanto in un emblema (c.d. marchio emblematico), quanto in una denominazione o in un segno, purché presenti carattere distintivo (A. FIALE, *Diritto commerciale*, Napoli, 2002, p. 109). Esso è tradizionalmente considerato il segno distintivo più importante, in quanto contraddistingue prodotti e servizi, e consente le scelte di mercato mediante la differenziazione e la individuazione dei prodotti. Pertanto, esso è, al contempo, strumento di comunicazione, informazione e concorrenza (G. SENA, *Marchio di impresa (natura e funzione)* (voce), in *Dig. disc. priv.*, *sez. comm.*, IX, Torino, 1993, p. 292).

esclusivo del segno tipico può inibire a terzi l'uso di quest'ultimo come nome di dominio[60]. In particolare, la giurisprudenza ritiene che la registrazione di un *domain name* che riproduce o contiene il marchio altrui costituisce una contraffazione del marchio poiché permette di ricollegare l'attività a quella del titolare del marchio, sfruttando la notorietà del segno e traendone, quindi, un indebito vantaggio[61]. Ne consegue che solo il titolare di un marchio registrato potrebbe legittimamente usarlo sul proprio sito o come nome di dominio. In dottrina si afferma che "la funzione principale di un nome a dominio contenente un marchio denominativo è di consentire l'individuazione dell'offerta commerciale

[60] La produzione dottrinale in materia è oramai assai ampia; oltre ai testi citati, cfr. anche: A. ANTONINI, *La tutela giuridica del nome di dominio*, in *Dir. inf.*, 2001, 6, pp. 813-825; E. BASSOLI, Domain grabbing *e tutela inibitoria*, in *Dir. inf.*, 2001, 3, pp. 522-528; G. CASSANO, *Cybersquatting*, in *Dir. inf.*, 2001, 1, pp. 83-94; G. CASSANO, *In tema di domain name*, in *Dir. inf.*, 2000, 3, pp. 494-499; G. CASSANO, *Una «giurisprudenza toscana» sui nomi a dominio?*, in *Dir. inf.*, 2001, 3, pp. 511-520; C. GALLI, *I domain names nella giurisprudenza*, Milano, 2001; N. GATTA, *Problemi in tema di* domain names: *le ipotesi di regolamentazione comunitaria*, in A. ANTONUCCI (a cura di), *E-commerce. La direttiva 200/31/CE e il quadro normativo della rete*, Milano, 2001, pp. 377-404; A. IMPRODA, *Segni distintivi e domain names: un rapporto conflittuale*, in *Dir inf.*, 2000, 2, pp. 366-370; A. PALAZZOLO – LAZZOLORIPODI, *Privative industriali, nomi di dominio, concorrenza, pubblicità* on line, in E. M. TRIPODI – IPODANTORO – NTORISSINEO, *Manuale di commercio elettronico*, Milano, 2000, pp. 321-373; P. SAMMARCO, *Assegnazione dei nomi a dominio su Internet, interferenze con il marchio,* domain grabbing *e responsabilità del provider*, in *Dir. inf.*, 2000, 1, pp. 67-83; P. SAMMARCO, *Competenza territoriale in materia di illecita utilizzazione di nome a dominio*, in *Dir. inf.*, 2001, 2, pp. 236-242; P. SAMMARCO, *Il giudizio di confondibilità applicato ai nomi a dominio con particolare riferimento alla testata di giornale*, in *Dir. inf.*, 2001, 1, pp. 45-50; SAMMARCO P., *La riconducibilità a nome a dominio di marchi complessi e la loro tutela*, in *Dir. inf.*, 2001, 4-5, pp. 736-742; T. SOGARI, *Domain name: quale tutela?*, in AA. VV., *Proprietà intellettuale e cyberspazio*, Atti del Congresso internazionale, Stresa 4-5 maggio 2001, Milano, 2002, pp. 169-177; G. TARIZZO, *L'applicabilità della disciplina sui marchi ai nomi di dominio: certezze e dubbi*, in *Dir. inf.*, 2000, 3, pp. 500-507; G. ZICCARDI – CCARITIELLO, *La tutela giuridica del nome di dominio*, Modena, 2000.

[61] Così Trib. Roma 2 agosto 1997, in *Foro it.*, 1998, I, c. 923; Pret. Valdagno 27 maggio 1998, in *Giur. it.*, 1998, c. 1875; Trib. Verona 25 maggio 1999, in *Foro it.*, 1999, I, c. 3061.

contenuta nel sito. Da ciò deriva che la confondibilità prevista dall'ordinamento italiano in tema di marchi deve essere valutata in modo concreto nei diversi casi specifici, dato che, in base al funzionamento di Internet, non possono esistere due domain name uguali, mentre nella legge marchi è prevista la possibilità di avere due segni distintivi identici, almeno in alcuni casi (settore merceologico differente o ambito territoriale diverso). Il risultato è che l'esclusiva che deriva ad un titolare di un marchio deve essere considerata con particolare attenzione nei giudizi riguardanti i nomi a dominio"[62].

Il riferimento alla confondibilità è stato però correttamente ricostruito in dottrina con precipuo riferimento alle caratteristiche essenziali della rete Internet. Difatti, il navigatore che già conosce un segno distintivo e lo digita nella barra degli indirizzi del *browser*, al fine di raggiungere il titolare del segno medesimo, "è normalmente consapevole dei limiti territoriali e merceologici della protezione di quel segno e quindi della possibilità che anche altri soggetti si avvalgano sulla rete del medesimo segno in relazione ad attività o a territori diversi. Il navigatore, in altri termini, si trova nella stessa condizione di chi, conoscendo soltanto la denominazione sociale del soggetto con il quale intende mettersi in contatto telefonicamente, sa bene che nell'elenco alfabetico della guida telefonica può trovare anche altri soggetti, operanti in settori diversi, che hanno la medesima denominazione", per cui l'eventuale errore del navigatore rileva (o dovrebbe rilevare) sotto il profilo del pericolo di confusione solo se il contenuto del sito stesso (e in primo

[62] N. LASORSA, *Domain name*, in G. VACIAGO (a cura di), *Internet e responsabilità giuridiche. Lineamenti, materiali e formulari in tema di diritto d'autore, nomi a dominio, Pubblica Amministrazione, privacy, reati informatici*, Piacenza, 2002, p. 119.

luogo della *home page*) può indurre a ritenere di trovarsi effettivamente nel sito del titolare del segno considerato[63].

Nel caso specifico dei marchi celebri, "il giudizio di "affinità" di un prodotto rispetto ad un altro coperto da un marchio notorio o rinomato deve essere formulato […] secondo un criterio più largo di quello adoperato per i marchi comuni. In relazione ai marchi cosiddetti "celebri", infatti, deve accogliersi una nozione più ampia di "affinità", la quale tenga conto del pericolo di confusione in cui il consumatore medio può cadere attribuendo al titolare del marchio celebre la fabbricazione anche di altri prodotti non rilevantemente distanti sotto il piano merceologico e non caratterizzati di per sè da alta specializzazione."[64] L'art. 1 comma 2 legge marchi prevede che il titolare del marchio ha il diritto di vietare a terzi l'utilizzo di un segno identico o simile anche per prodotti o servizi non affini, qualora l'uso del segno consenta di trarre senza giusto motivo un indebito vantaggio dal carattere distintivo o dalla rinomanza del marchio qualora possa recare un pregiudizio al legittimo titolare.

Il riconoscimento di tale forma di tutela richiede però lo svolgimento di un giudizio di accertamento sulla notorietà e celebrità del marchio, che viene necessariamente rimesso alla discrezionalità dell'interprete. Ne consegue, pertanto, che un marchio ritenuto celebre da un Tribunale, al punto da inibirne l'uso come «nome a dominio» utilizzato da soggetti che su tale denominazione non possono vantare alcun diritto, possa essere ritenuto, da altro Tribunale, non dotato di quella particolare forza evocativa che i segni notori posseggono, con

[63] C. GALLI, *op. cit.*, p. 40.
[64] Cass. 20 dicembre 1999, n. 14315.

l'effetto di considerare legittima la sua utilizzazione come *domain name* da parte di terzi[65].

8.2 LA GIURISPRUDENZA IN TEMA DI NOME DI DOMINIO

L'assegnazione dei nomi di dominio non è disciplinata da leggi, ma piuttosto da consuetudini invalse nei pochi anni in cui si è verificato lo sviluppo di Internet nonché da normative di autoregolamentazione emanate dalle organizzazioni che gestiscono tale attività. L'assenza di prescrizioni legislative ha portato a svariate pronunce giudiziali, talora contrastanti, a partire dal 1996, con l'emanazione dell'ordinanza del Tribunale di Bari che costituisce la prima decisione giudiziale italiana in tema di nomi a dominio. In essa si afferma che la legge marchi si applica anche in questo ambito solo ove sussista un pericolo di confusione per il pubblico, dovuto all'identicità dei prodotti commercializzati sul sito raggiungibile mediante il *domain name* contestato. Nel caso di specie, inoltre, la ricorrente non poteva vantare alcun diritto di esclusiva sul dominio contestato.

Nel 1997 si registrano tre importanti casi, il primo deciso con ordinanza del Tribunale di Pescara del 9 gennaio (c.d. caso «Nautilus»)[66], il secondo con le ordinanze del Tribunale di Milano del 9 giugno e del 22

[65] Così P. SAMMARCO, *Il regime giuridico dei "nomi a dominio"*, Milano, 2002, p. 83. Il riferimento dell'autore è al c.d. caso Miss Italia, sul quale v. *infra*.

[66] Trib. Pescara 9 gennaio 1997, in *Dir. inf.*, 1997, 6, p. 952, con nota di L. LIGUORI, *Osservazioni in tema di tutela dei segni distintivi su Internet*, pp. 962-969. Nel caso di specie, il ricorrente aveva registrato il marchio «Nautilus» per lo svolgimento della propria attività di agente pubblicitario anche su Internet, ma ne lamentava l'utilizzo da parte di un'altra società allo scopo di pubblicizzare servizi e programmi di comunicazione attraverso un sito *web* riportante proprio la denominazione Nautilus.

luglio (c.d. caso «Amadeus»)[67], il terzo con ordinanza del Tribunale di Roma del 2 agosto (c.d. caso «Porta Portese»)[68]. In tutti e tre i procedimenti le ricorrenti hanno chiesto la tutela inibitoria sulla base dell'art. 2598 cod. civ., sostenendo che l'utilizzo di un nome di dominio o di una sua parte che riporti un marchio di titolarità di un altro soggetto, per la prestazione di determinati servizi *on line*, possa creare confusione negli utenti di questo, qualora tali servizi abbiano natura uguale od affine. Nel caso Nautilus, il giudice abruzzese ha affermato che "non costituisce contraffazione di marchio l'adozione dello stesso segno come *domain name* di un sito Internet quando non vi sia prova concreta di confusione, con conseguente sviamento di clientela, rischio che va escluso in quanto il segno imitato non presenti caratteri di originalità e creatività, come provato dall'enorme numero di siti Internet identificati dallo stesso nome e dalla notoria diffusione dello stesso in numerosi settori; in quanto le attività dei titolari dei rispettivi segni differiscano in modo significativo; e in quanto tali attività siano rivolte ad una clientela specializzata". Nel caso Amadeus, il Tribunale di Milano ha affermato che "l'inibitoria

[67] Trib. Milano 22 luglio 1997, in *Dir. inf.*, 1997, 6, p. 957, con nota di L. LIGUORI, *cit.* Nel caso portato all'attenzione dei giudici milanesi, la società spagnola Amadeus Marketing SA e la sua controllata Amadeus Marketing Italia s.r.l. ricorrevano ex art. 700 cod. proc. civ. per lamentare la contraffazione del proprio marchio (Amadeus) da parte della Logica s.r.l., che utilizzava quale nome di dominio la denominazione «Amadeus.it ». Le società ricorrenti, operanti nel settore turistico a livello internazionale, risultavano utilizzare il sito denominato «Amadeus.net» e chiedevano pertanto che venisse inibito alla resistente l'uso di tale denominazione, perché idonea ad ingenerare confusione anche in virtù della affinità dei servizi resi dalle parti in causa.

[68] Trib. Roma 2 agosto 1997, in *Dir. inf.*, 1997, 6, p. 961, con nota di L. LIGUORI, *cit.* La Sege s.r.l., titolare del marchio «Porta Portese» e proprietaria della omonima testata giornalistica per la diffusione di servizi di informazione economica, ne lamentava l'utilizzo da parte della Starnet s.r.l., che, utilizzando il nome di dominio «Portaportese.it», forniva servizi *on line* della medesima natura.

dell'ulteriore uso di un *domain name* simile ad un anteriore marchio registrato, che sia usato per contraddistinguere un sito dal quale è possibile accedere anche a servizi dello stesso genere di quelli per cui il marchio è stato registrato, deve essere disposta esclusivamente in relazione all'accessibilità dal sito dei servizi per i quali si verifica l'interferenza tra i due segni e non per l'offerta di servizi diversi". Nel caso Porta Portese, il giudice romano ha stabilito che "l'utilizzazione di un *domain name* identico ad un marchio e ad un titolo di pubblicazione anteriori altrui implica oggettivamente e per se stessa una situazione di confondibilità per gli utenti e quindi una violazione dei diritti in questione, anche tenendo conto della sostanziale assimibilità dei servizi resi al pubblico dai titolari dei segni in conflitto" ed ha inoltre affermato che la violazione del marchio non viene meno né per effetto dell'assegnazione del nome a dominio da parte della *Naming Authority* né a causa della mancata registrazione del proprio dominio presso tale organizzazione.

L'anno successivo, nell'ordinanza 27 maggio 1998, il Pretore di Valdagno afferma che "la rete Internet costituisce, tra l'altro, un modello di comunicazione tra imprese, nonché tra imprese e pubblico di consumatori, ulteriore ed aggiuntivo rispetto a quelli tradizionali. Ma è evidente che i possibili soggetti del dialogo virtuale sono in ipotesi i medesimi delle anteriori forme di comunicazione-incontro sul mercato. Di tal che si palesa insopprimibile il diritto di ciascuna impresa di presentarsi sul mercato ed al pubblico secondo ogni modello di comunicazione, ed utilizzando, evidentemente, sempre il proprio nome ed i marchi a disposizione". Questa ordinanza è stata poi reclamata

innanzi al Tribunale di Vicenza, nella cui ordinanza del 6 luglio 1998 (che dichiara l'infondatezza del reclamo) si legge che "l'utilizzazione di un altrui marchio che gode di rinomanza come *domain name* di un sito Internet relativo a prodotti non affini a quelli per cui il marchio è registrato costituisce contraffazione del marchio in questione, in quanto consente all'utilizzatore di trarre indebitamente vantaggio dalla rinomanza del marchio e comporta per esso un pericolo di pregiudizio".

I contrasti giurisprudenziali sono invece evidenti nel caso «Miss Italia». In merito, il Tribunale di Modena, con ordinanza 23 maggio 2000, dispone che "l'adozione del *domain name* «missitalia.it» per un sito in cui è svolta un'attività di vendita di componenti elettronici non costituisce contraffazione del marchio «Miss Italia» della società che gestisce l'omonimo concorso di bellezza, né sotto il profilo confusorio, poiché la radicale diversità di attività impedisce ogni possibilità di associazione, né sotto quello dell'impedimento alla registrazione di un *domain name* identico, perché le possibilità di idonea differenziazione sono pressoché infinite". Il Tribunale di Reggio Emilia, invece, con ordinanza del 30 maggio 2000, dispone che "la registrazione dei *domain names* «missitalia.com», «missitalia.net», «missitalia.org», «miss-italia.com», «miss-italia.net» e «miss-italia.org», con l'intenzione, dichiarata dal registrante, di vendere in rete prodotti (alimentari) italiani deve ritenersi univocamente finalizzata ad una condotta costituente violazione del diritto al marchio rinomato «Miss Italia» e giustifica l'emanazione di un'inibitoria cautelare dell'utilizzazione di tali *domain names* per la pubblicità, l'immissione nella rete Internet di informazioni commerciali e l'offerta di beni e servizi di qualsiasi natura". Poco più tardi, il Tribunale

di Modena, rigettando il reclamo avverso l'ordinanza del 23 maggio 2000, con ordinanza del 27 luglio 2000 afferma che "il *domain name*, a seconda delle circostanze del caso, può essere un mero indirizzo o numero di telefono informatico, oppure, in relazione al contenuto e alla configurazione dello stesso, può invece avere un senso applicare ad esso la normativa sui marchi". Il Tribunale non ritiene sussistente, nel caso di specie, il *periculum in mora* necessario al fine di ottenere l'inibitoria cautelare dell'utilizzazione del nome di dominio in oggetto, atteso che le due attività non sono affini e dunque difficilmente può realizzarsi uno "sviamento definitivo degli utenti della rete, che, anche quando siano stati sviati dal nome del sito, una volta verificatone l'oggetto, plausimibilmente ed agevolmente possono lasciarlo, in quanto del tutto privo di interesse per loro, per indirizzarsi al sito del titolare del marchio".

Il Tribunale di Firenze, con l'ordinanza 8 luglio 2000, resa nel c.d. caso «Sabena», andando in contrasto con la giurisprudenza prevalente, afferma che "poiché funzione del *domain name* è di consentire a chiunque di raggiungere una pagina *web*, il *domain name*, in quanto mezzo operativo e tecnico-logico, non può costituire violazione di un marchio di impresa o di altri segni distintivi"[69].

In senso contrario è la sentenza del Tribunale di Napoli del 26 febbraio 2002, il c.d. caso «Playboy»[70]. Il giudice partenopeo aderisce all'orientamento dominante in dottrina e in giurisprudenza, affermando "che Internet costituisce in primo luogo una forma di comunicazione,

[69] Trib. Firenze 29 giugno 2000, in Dir. inf., 2000, p. 672, con nota di P. SAMMARCO, *Aspetti problematici relativi al rapporto tra nome a dominio e marchio altrui*, in *Dir. inf.*, 2000, 4-5, pp. 675-682.
[70] In http://www.interlex.it/testi/na020226.htm.

anche di impresa, nonché un veicolo pubblicitario […e] da qui allora l'applicabilità delle regole in materia di segni distintivi: questi ultimi a loro volta mezzi di comunicazione d'impresa". Inoltre, si sancisce, ancora una volta, l'irrilevanza del principio *first come, first served*, per cui "l'uso di un domain name pur correttamente attribuito dal punto di vista tecnico può ben integrare gli estremi - a seconda dei casi - della lesione del diritto al nome, o della concorrenza sleale, o della legge marchi; il fatto che si sia ottenuto il domain name seguendo le regole del sistema non vuol dire che si sia sottratti dalle norme giuridiche vigenti, che spiegano la loro efficacia anche in Internet". Con riferimento al caso di specie, il Tribunale afferma che trovano applicazione gli artt. 65 e 66 l. marchi, nonché - per i profili di concorrenza sleale - gli artt. 2598 ss cod. civ. e dichiara, in primo luogo, che l'uso del termine Playboy da parte del convenuto come *domain name*, "identificante il sito Internet www.PlayBoy.it, costituisce contraffazione dei marchi registrati PlayBoy, della PlayBoy Enterprises International, inc. e della omonima denominazione sociale. Tale uso integra altresì gli estremi della concorrenza sleale confusoria a danno della medesima società". Si inibisce, inoltre, al convenuto l'uso del termine in oggetto, in qualsiasi forma ed ambito.

Da ultimo bisogna segnalare il c.d. caso Armani. Già la nota azienda di abbigliamento non risulta titolare del nome a dominio "armani.com", perché già registrato dal sig. A.R. Mani, cittadino canadese, di cui non si è riuscita a dimostrare la mala fede al momento dell'acquisto; la poca considerazione delle potenzialità della Rete è stata forse all'origine della tardività di registrazione dei nomi di dominio

corrispondenti o simili al marchio, per cui l'impresa è stata preceduta anche nella registrazione del *domain name* «armani.it», stavolta da un'altra ditta, il «Timbrificio Armani». Il Tribunale di Bergamo, con sentenza del 3 marzo 2003[71], ha dichiarato "l'illiceità della registrazione e della utilizzazione da parte del convenuto del domain name "armani" ai sensi della legge marchi" e per l'effetto ha ordinato "la cancellazione della parola "armani" nel nome a dominio registrato in favore del convenuto ed inibisce al convenuto stesso l'uso della parola "armani" come nome a dominio, ove non accompagnata da elementi idonei a differenziala dal marchio Armani". Il giudice bergamasco giustifica la sua decisione affermando che "la qualificazione del marchio Armani come marchio registrato che gode di rinomanza comporta che il titolare benefici della tutela ampliata, che esorbita cioè il limite dell'identità o affinità tra prodotti e servizi, potendo egli - ai sensi dell'art. 1, comma 1 lett. c) l. marchi - vietare a terzi l'uso di un segno identico o simile, a prescindere dal rischio di confusione, laddove l'uso del segno consenta, alternativamente, di trarre indebitamente vantaggio dal carattere distintivo o dalla rinomanza del marchio o reca ad esso pregiudizio. La tutela merceologicamente ampliata riconosciuta dalla legge del marchio celebre - quindi al di là della confondibilità in quanto, in tale ipotesi, il bene protetto non è l'interesse alla non confondibilità, bensì l'interesse di chi ha reso rinomato il segno a non vedersi sottratte o pregiudicate le utilità economiche che possono derivare da tale rinomanza - ogni volta che ricorra una delle condizioni previste dal citato art. 1 l. marchi

[71] In http://www.interlex.it/testi/armani.htm. Su di essa v. R. MANNO, *Il caso armani.it: domini, marchi e diritti assoluti*, in http://www.interlex.it/nomiadom/r_manno3.htm; A. MONTI, *Armani.it. Un dominio "su misura"*, in http://www.interlex.it/nomiadom/amonti66.htm.

sgombera il campo dalla rilevanza delle ulteriori difese del convenuto". Nel caso di specie, inoltre, si ritiene sussistente "il pregiudizio per l'attrice che, in ragione della condotta del convenuto, non può presentarsi sulla rete Internet proprio attraverso il celebre marchio che costituisce indiscutibile richiamo per un numero elevatissimo di consumatori, con conseguente perdita di tutti quegli utenti meno esperti delle rete Internet che limitino la propria ricerca al dominio «armani.it»"[72]. In dottrina si avverte però "il timore che, come sembra abbia fatto il giudice, si operi una aprioristica qualificazione del domain name in termini di segno distintivo atipico suscettibile di valutazione ai sensi della legge marchi: ciò vorrebbe dire riservare alle imprese titolari di marchio, ancorché rinomato, una precedenza nella registrazione e uso del corrispondente dominio, tutelabile anche in giudizio contro ogni abuso. Riteniamo che, quando la registrazione e l'utilizzazione di un dominio sia strumentale all'esercizio di un diritto (assoluto o costituzionale) e non vi sia la prova della malafede o della confondibilità, non ricorrano i presupposti per la tutela giurisdizionale di quelle che restano solo scomode, ancorché legittime, situazioni di fatto"[73].

Tenendo presente i succinti richiami alla giurisprudenza nella materia che ci occupa, in linea generale, sarebbe comunque opportuno distinguere in relazione a ciascun caso concreto, perché se nei casi di *domain grabbing* non si dubita della invocabilità della tutela[74], in altri casi più sfumati, come il citato caso Armani, bisogna ben distinguere e

[72] Tale considerazione viene corroborata dal fatto che, il numero di utenti che, in un trimestre, hanno visitato il sito del convenuto, è pari a tre volte il numero dei navigatori che si è recato su «giorgioarmani.it».
[73] R. MANNO, *op. cit.*
[74] C. GALLI, *op. cit.*, p. 63.

decidere contemperando sia le regole già poste a disciplina di determinati settori che le specificità di Internet, per evitare che anche in questo settore la protezione delle attività economiche divenga eccessiva e costituisca il parametro in base al quale effettuare la valutazione di liceità di fattispecie che tuttavia hanno carattere ben più generale e riguardano, in molti casi, la libera manifestazione del pensiero[75], che è, indubbiamente, un diritto di rango superiore a quello di libertà di iniziativa economica privata, il quale può prevaricare quei diritti di libertà, connaturati alla stessa essenza dell'individuo, che dovrebbero essere caratterizzati sempre e comunque da una inviolabilità concreta. Internet si presta ad una molteplicità di utilizzi, ma non può essere riduttivamente considerata un enorme mercato virtuale e sottoposta *esclusivamente* alle regole del diritto commerciale: una simile considerazione non sembra giustificabile, mentre è difficilmente controvertibile la considerazione che la sua eterogeneità contenutistica non esclude, in attesa di una regolamentazione *ad hoc*, l'applicazione in via analogica delle normative dettate per altri settori, purché ciò avvenga tenendo presente le peculiarità della Rete e non pretendendo di partire da una concezione aprioristica della Rete stessa, slegata dalla realtà fattuale, ma partendo dalla sua considerazione concreta per poi effettuare l'eventuale l'applicazione delle normative suddette. Inoltre, il principio *first come, first served* potrebbe ritenersi consuetudinario ed essere pertanto seguito sino

[75] "Infatti è opportuno ricordare come il dominio internet permetta di esercitare diritti assoluti, azionabili *erga omnes*, non solo alle imprese (diritto di marchio), ma anche alle persone fisiche, come il diritto al nome (diritto della personalità) e i diritti costituzionali della persona, come la libertà di espressione. Nel conflitto tra questi diritti, il dominio internet si colloca in una posizione di assoluta neutralità" (R. MANNO, *op. cit.*).

ad una eventuale regolamentazione normativa, fatta comunque eccezione per i casi di *domain grabbing*, della cui illiceità, come si è visto, non si dubita. Negli altri casi la valutazione andrebbe pertanto rimessa all'apprezzamento dell'autorità giudiziaria, tenendo presente che ci si dovrebbe trovare dinanzi ad un giudizio sul fatto, dunque precluso, sotto questo aspetto, ad una eventuale cognizione del giudice di legittimità.

BIBLIOGRAFIA ESSENZIALE

AA.VV., *Filosofia e diritto nell'era di Internet*, Atti della giornata di studio, Roma 21 novembre 2002, Roma, 2003

AA.VV., *Proprietà intellettuale e cyberspazio*, Atti del Congresso internazionale, Stresa 4–5 maggio 2001, Milano, 2002

AA.VV., *Verso un sistema esperto giuridico integrale*, Atti del Convegno celebrativo del venticinquennale dell'Istituto per la Documentazione Giuridica del Consiglio Nazionale delle Ricerche (Firenze, 1–3 dicembre 1993), Padova, 1996

AMATO MANGIAMELI A. C., *Diritto e cyberspace. Appunti di informatica giuridica e filosofia del diritto*, Torino, 2000

BAADE H. W. (edited by), *Jurimetrics*, New York–London, 1963

BERNERS–LEE T., *L'architettura del nuovo web*, trad. it., Milano 2001

BERNERS–LEE T., HENDLER J., LASSILA O., *The Semantic Web*, in *Scientific American*, 2001, pp. 35–43

BIAGIOLI C., MERCATALI P., SARTOR G., *Elementi di legimatica*, Padova, 1993

BIAGIOLI C., MERCATALI P., SARTOR G. (a cura di), *Legimatica. Informatica per legiferare*, Napoli, 1995

BOOLE G., *Indagine sulle leggi del pensiero su cui sono fondate le teorie matematiche della logica e della probabilità*, trad. it., Torino, 1976

BORRUSO R., *Computer e diritto*, Tomo I, *Analisi giuridica del computer*, Milano, 1988

BORRUSO R., *Computer e diritto*, Tomo II, *Problemi giuridici dell'informatica*, Milano, 1988

BUTTARELLI G., *Banche dati e tutela della riservatezza. La privacy nella Società dell'Informazione*, Milano, 1997

CAMMARATA M., MACCARONE E., *La firma digitale sicura. Il documento informatico nell'ordinamento italiano*, Milano, 2003

COMANDÈ G., SICA S., *Il commercio elettronico. Profili giuridici*, Torino, 2001

CORASANITI G., *Esperienza giuridica e sicurezza informatica*, Milano, 2003

CORTESE R., JACOBAZZI C., LIMONE D. A. (a cura di), *Manuale di informatica giudiziaria*, Rimini 1985

COTTA S., *La sfida tecnologica*, Bologna 1968

FINOCCHIARO G., *Diritto di Internet. Scritti e materiali per il corso*, Bologna, 2001

FROSINI V., *Informatica diritto e società*, Milano, 1988

FROSINI V., *L'orizzonte giuridico dell'Internet,* in *Il diritto dell'informazione e dell'informatica*, 2000, 2, pp. 271–280

FROSINI V., LIMONE D. A. (a cura di), *L'insegnamento dell'informatica giuridica*, Napoli, 1990

GALLI C., *I domain names nella giurisprudenza*, Milano, 2001

GIANNANTONIO E., *Introduzione all'informatica giuridica*, Milano, 1984

GIANNANTONIO E., *Manuale di diritto dell'informatica*, Padova, 2001

GIANNANTONIO E., LOSANO M. G., ZENO–ZENCOVICH V.,

Commentario alla legge 31 dicembre 1996, n. 675, Padova, 1997

HIMANEN P., *L'etica hacker e lo spirito dell'età dell'informazione*, trad. it., Milano, 2003

IRTI N., *Norma e luoghi. Problemi di geo–diritto*, Roma–Bari, 2001

LÉVY P., *Il virtuale*, trad. it, Milano 1997

LÉVY P., *L'intelligenza collettiva. Per un'antropologia del cyberspazio*, trad. it., Milano 2002

LIMONE D. A. (a cura di), *Dalla giuritecnica all'informatica giuridica. Studi dedicati a Vittorio Frosini*, Milano 1995

LOEVINGER L, *Jurimetrics. The Next Step Forward*, in *Minnesota Law Review*, 1949, 33, pp. 455–493

LOSANO M. G., *Corso di informatica giuridica*, 1, *L'elaborazione dei dati non numerici*, Milano, 1984

LOSANO M. G., *Corso di informatica giuridica*, 2, *Il diritto dell'informatica*, Milano, 1984

LOSANO M. G., *Corso di informatica giuridica*, 3, *L'analisi delle procedure giuridiche*, Milano, 1984

LOSANO M. G., *Giuscibernetica: macchine e modelli cibernetici nel diritto*, Torino, 1969

LYON D., *La società sorvegliata. Tecnologie di controllo della vita quotidiana*, trad. it., Milano, 2002

MARTINO A. A., *La progettazione legislativa nell'ordinamento inquinato, in*

Studi parlamentari e di politica costituzionale, 1977, 38, pp. 1–21.

NANNUCCI R. (a cura di), *Lineamenti di informatica giuridica*, Napoli, 2002

PAGANO R., *Introduzione alla legistica. L'arte di preparare le leggi*, Milano, 1999

PALAZZOLO N. (a cura di), *Corso di informatica giuridica*, Catania, 1998

PASCUZZI G. (a cura di), *Diritto e informatica. L'avvocato di fronte alle tecnologie digitali*, Milano, 2002

PÉREZ–LUÑO A. E., *Saggi di informatica giuridica*, trad. it., Milano, 1998

RODOTÀ S., *La «privacy» tra individuo e collettività*, in *Politica del diritto*, 1974, pp. 545–563

RODOTÀ S., *Tecnopolitica*, Roma–Bari, 1997

SAMMARCO P., *Il regime giuridico dei "nomi a dominio"*, Milano, 2002

SARTOR G., *Intelligenza artificiale e diritto. Un'introduzione*, Milano, 1996

SARTOR G., *Le applicazioni giuridiche dell'intelligenza artificiale. La rappresentazione della conoscenza*, Milano 1990

SARZANA DI S. IPPOLITO C., *Informatica, internet e diritto penale*, Milano, 2003

SCOTT W. G., MURTULA M., STECCO M. (a cura di), *Il commercio elettronico. Verso nuovi rapporti tra imprese e mercati*, Torino, 1999

SIMITIS S., *Crisi dell'informazione giuridica ed elaborazione elettronica dei dati*, trad. it., Milano, 1977

TADDEI ELMI G., *Corso di informatica giuridica*, Napoli, 2003

TADDEI ELMI G., *Dimensioni dell'informatica giuridica*, Napoli, 1990

TARANTINO A., *Elementi di informatica giuridica*, Milano 1998

TISCORNIA D., *Il diritto nei modelli dell'intelligenza artificiale*, Bologna 1996

TOSI E. (a cura di), *I problemi giuridici di Internet. Dall'E–Commerce all'E–Business*, Milano 2001

WARREN S. D., BRANDEIS L. D., *The right to privacy*, in *Harvard Law Review*, 1890, 4, p. 193 e in *Landmarks of Law*, 1960, pp. 261–283

WESTIN A., *Privacy and freedom*, New York, 1967

WIENER N., *La cibernetica. Controllo e comunicazione nell'animale e nella macchina*, trad. it., Milano, 1968

ZICCARDI G., *Il diritto d'autore nell'era digitale*, Milano, 2001