INTERNET (responsabilità civile)

SOMMARIO

1. - LA RETE INTERNET

1.1. - *Una rivoluzione in atto*. - Negli ultimi dieci anni due fattori hanno determinato un cambiamento radicale nel nostro modo di vivere. Il primo è rappresentato dalla semplificazione delle modalità di utilizzazione dei *software* necessari per gestire le risorse informatiche; il secondo dalla diffusione capillare che la rete Internet ha avuto in tutto il mondo progredito. In ragione di ciò, si è detto che «la rivoluzione digitale deriva dalla rivoluzione informatica, ne è in qualche modo la sua evoluzione estrema» (ALPA, G., *Premessa*, in [10], XIII). Di vera e propria rivoluzione è dato parlare, senza tema di esagerazione; le due leve citate hanno infatti determinato una situazione per cui oggi a chiunque basta un computer collegato ad Internet per collocarsi nella società in modo completamente nuovo rispetto al passato. Cambia così il rapporto dell'uomo con il tempo, con lo spazio, con le altre persone e con le cose (tra i tanti, cfr. NAISBITT, J., *High Tech - High Touch*, New York, 1999; RAMPINI, F., *Una rivoluzione in corso*, Bari, 2000; AMOR, D., *E-Business. Vivere e lavorare in un mondo interconnesso*, Milano, 2000).

L'uso quotidiano del computer e la diffusione di Internet hanno modificato il nostro modo di vivere perché, ad esempio, oggi è possibile fare *shopping* in giro per il mondo senza muoversi da casa. Utilizzando il *mouse* e la tastiera del computer è semplicissimo collegarsi agli innumerevoli siti Internet che offrono *online* prodotti o servizi e dunque, attraverso le immagini che scorrono sul video, visitare magazzini (fisicamente ubicati in regioni, nazioni o continenti diversi) e paragonare prezzi e qualità; il tutto conoscendo in tempo reale la disponibilità dei prodotti che più interessano e, qualora lo si voglia, potendo acquistare direttamente senza fare un passo fuori dal proprio salotto. Oltre ad essere un nuovo foro «in cui si espongono merci su moderne bancarelle denominate siti, si guardano e si confrontano beni offerti, si concludono affari e quindi contratti» (MINNECI, U.-SCIARRONE ALIBRANDI, A., *Documento elettronico e contratto telematico*, in *Dig. civ.*, Aggiornamento, Torino, 2000, 344), Internet è un vero e proprio mercato delle informazioni, una piazza telematica in cui le notizie circolano a livello planetario in una quantità e con una velocità che non era possibile nemmeno immaginare sino a pochi lustri fa. Chiunque voglia sapere quello che è accaduto negli ultimi dieci minuti nel mondo, ovvero voglia consultare il catalogo di una biblioteca, o ancora, più semplicemente, abbia bisogno di conoscere l'orario in cui parte un determinato treno, deve solo pigiare qualche tasto e fare qualche piroetta con il *mouse*. Ma Internet è ancora di più. La grande rete, che oggi collega milioni di computer, è infatti anche, e forse soprattutto, un luogo di nuova concezione nel quale dialogare, lavorare, utilizzare elettrodomestici a distanza, organizzare e svolgere ricerche di gruppo, condividere esperienze, culture, progetti, timori. E ciò in quanto attraverso Internet è possibile spedire messaggi di posta elettronica — contenenti testi scritti, materiali audio, video e quant'altro — che giungono in pochi secondi al destinatario, ed è inoltre semplice comunicare in tempo reale da una parte all'altra del pianeta con uno o più interlocutori, utilizzando *forum* telematici, *chat*, servizi di videotelefono o videoconferenza (cfr., tra i tanti, PACCAGNELLA, L., *La comunicazione al computer*, Bologna, 2000; PIZZETTI, F.G., *Nell'era della rete*, Torino, 2000; CARBONE, P.-FERRI, P., *Le comunità virtuali*, Milano, 1999; e SHAPIRO, A.L., *The Control Revolution: How the Internet is Putting People in the Charge and Changing the World We Know*, New York, 1999).

1.2. - *Genesi, evoluzione e natura di Internet*. - Quando, nel 1946, presso l'Università della Pennsylvania veniva sperimentato il primo, lento e ingombrante, elaboratore elettronico, probabilmente nessuno, se non nei romanzi di fantascienza più immaginifici, poteva prevedere che, a distanza di pochi decenni, il computer sarebbe stato al centro di uno sviluppo delle tecnologie della comunicazione così imponente

da determinare cambiamenti sociali di portata epocale (v. FRANCESCHELLI, V., *Computer e diritto*, Rimini, 1989, 21).
La locuzione «era digitale», tanto di moda da qualche anno in ogni campo, bene sintetizza, e altrettanto bene testimonia, l'evoluzione generale in atto, nonché il ruolo che in essa hanno le nuove tecnologie informatiche (cfr. PASCUZZI, G, [15], 531). L'aggettivo digitale, nell'accezione oramai divenuta più comune, è proprio di tutto ciò che rappresenta dati in forma di numeri o lettere alfabetiche. La recente fortuna del termine si deve al fatto che ogni segnale trattato dal computer, anche il più complesso, è digitale perché espresso esclusivamente dalla combinazione dei valori 0 e 1 in sequenza, e dunque sulla base del sistema di scrittura definito binario; il che rende anche la logica sottesa ad ogni attività del computer di tipo binario (cfr. BORRUSO, R.-TIBERI, C., *L'informatica per il giurista*, Milano, 1990, 12). La parola «*bit*», con la quale si definisce l'unità informativa minima utilizzata dal computer, nasce proprio dalla crasi delle parole inglesi *binary* e *digit* (cfr. STIX, G-LACOB, M. *Who Gives a Gigabyte?, A Survival Guide for the Technologically Perplexed*, New York, 1999). In *bit* sono espresse tutte le informazioni che consentono ad Internet di operare e di essere ciò che è.
Ma cos'è realmente Internet? Dal punto di vista tecnico può dirsi, semplificando, che Internet non è una realtà fisica o tangibile, ma una rete globale che, interconnettendo un numero infinito di reti settoriali o locali, collega più computer o più *network* attraverso l'utilizzazione di protocolli comuni; si tratta, dunque, di una «rete di reti» (questa è la definizione che ne dà la Corte Federale degli Stati Uniti — Distretto Orientale della Pennsylvania, nella sentenza 11.6.1998, in *Dir. inf.*, 1996, 604, trad. e nota di ZENO-ZENCOVICH, V.), che si avvale, al fine di trasferire fisicamente i segnali, delle tradizionali reti di telecomunicazione, e in particolare della rete telefonica. Come è stato notato, l'idea realmente innovativa, dalla quale ha preso le mosse Internet, è quella di creare un protocollo comune tra computer. Non a caso, infatti, quando si parla di internet (con la lettera iniziale minuscola) ci si riferisce, non alla rete, ma alla «famiglia di protocolli per lo scambio di dati in forma digitale» che le consente di funzionare (cfr. PARODI, C.-CALICE, A., [26], 6). Il protocollo è un sistema di regole condivise che permettono a elaboratori di potenza e genere diversi di scambiarsi dati e, più in generale, di interagire. Il protocollo di comunicazione di base di Internet è denominato *TCP/IP* (acronimo di *Transmission Control Protocol/Internet Protocol*); esso, più precisamente, è una famiglia di protocolli (v. PASCUZZI, G., [15], 531).
Progenitore di Internet è la rete *Arpanet*, creata tra il 1965 e il 1969 da un'agenzia del governo statunitense che si occupava di ricerca militare nel campo informatico (*ARPA*). Essa, all'inizio, era destinata a collegare i computer della difesa americana, ma già nel 1970 viene messa a disposizione di un pubblico più ampio costituito da ricercatori e scienziati (cfr. BICKERSTAFF, S., *Shackles on the Giant: How the Federal Government Created Microsoft, Personal Computers, and the Internet*, 78 *Tex. L. Rev.* 1, 1999). Tra il 1974 e il 1980 si conducono esperimenti per consentire ad elaboratori elettronici appartenenti a reti specifiche o locali diverse di dialogare tra loro sulla base di linguaggi comuni. Nel 1980 Tim Berners-Lee, uno fisico inglese che operava in Svizzera presso il Centro Europeo per la ricerca Nucleare (CERN), crea un sistema — dallo sviluppo del quale, nel 1991, sempre presso il CERN, nasce l'attuale *World Wide Web* — che sfrutta l'ipertesto per collegare documenti sparsi nei vari computer dell'ente. Tra il 1981 e il 1982 il numero dei personal computer in uso nel mondo passa da 2 a 5,5 milioni. Nel 1981 solo 213 computer sono abilitati a offrire accessi ad altri computer; nel 1984 questo numero sale a 1000; nel 1989 a 80.000 e nel 1990 a 313.000. Nel 1989 si contano 500 *network*; nel 1990, 2300 (v. NESPOR, S.-DE CESARIS, A.L., [25], 3-14).
La nascita di Internet è convenzionalmente fatta risalire al 1° gennaio 1983, giorno in cui tutti i computer di *Arpanet* passano simultaneamente ad utilizzare il protocollo *TCP/IP*; nello stesso anno viene istituito l'*Internet Activities Board* (*IAB*) per guidare lo sviluppo del protocollo e per offrire assistenza tecnica alla comunità degli utenti di Internet. Nel 1984, agli indirizzi numerici con i quali vengono identificati i computer collegati alla rete (c.d. *Ip*, *Internet Protocol*) vengono associati indirizzi DNS (essi prendono il nome di *Domain Name*), i quali essendo costituiti da gruppi di lettere, acronimi, nomi o parole di senso compiuto, risultano di più semplice digitazione e più facile memorizzazione. In questi anni la IBM, società che sino ad allora operava in regime di monopolio nel mercato dei *personal computer*, affida alla sconosciuta e giovane società Microsoft il compito di lavorare alla ricerca di un linguaggio che consentisse agli utenti di interagire più facilmente con i computer. In poco tempo il linguaggio MS-DOS viene così sostituito dal sistema operativo *Windows*, il quale, svolgendo la funzione di interfaccia grafica tra macchina e utente, consente all'uomo, anche privo di specifiche competenze informatiche, di far funzionare il computer attraverso operazioni molto semplici. La rete *Arpanet*, intanto, viene sostituita da un altro *network* globale, creato e gestito da un'agenzia del governo federale americano, la *National Science Foundation* (NSF), che vieta lo sfruttamento commerciale della rete. Nel 1992, come detto, nasce il sistema «*www*» (*World Wide Web*), che permette una condivisione di informazioni tra computer basata sul linguaggio di programmazione HTML (*Hyper Text Markup Language*), con il quale si possono sviluppare documenti interattivi, creare pagine *web* e trasmettere informazioni multimediali, nonché sulla tecnologia ipertestuale che si avvale del protocollo HTTP (*Hyper Text Transmission Protocol*), il quale consente di passare, con un semplice *clic* del *mouse*, da una pagina all'altra dello stesso documento, oppure da una pagina *web* ad una completamente diversa attraverso i *link*, o collegamenti, disponibili. Per «*www*» si intende, dunque, il sistema ad ipertesto, con estensione planetaria, realizzato inserendo sulla rete documenti scritti nel linguaggio HTML, consultabili secondo il protocollo di trasmissione HTTP e raggiungibili attraverso gli indirizzi espressi secondo la sintassi di uno standard di indirizzamento delle risorse denominato *Url* (*Uniform Resource Locations*).
Nel 1993 viene realizzato il primo *browser* (e cioè il primo programma per leggere un ipertesto e spostarsi tra i materiali esistenti nel *www* potendoli vedere) concepito per un vasto pubblico, privo di conoscenze informatiche. L'abbassamento dei prezzi dei *personal computer*, il miglioramento delle prestazioni e la possibilità per chiunque di accedere ai materiali contenuti nel *www* anche senza avere conoscenze informatiche particolari, rappresentano le tre condizioni che determinano la diffusione sempre più globale della rete e l'aumento esponenziale del numero degli utenti. Nel 1992 viene emendato il *National Science Foundation Act* (Pub. L. No. 102-476, § 4, 106 Sat. 2300, 1992, codificato nel 42 U.S.C. § 1862) al fine di abolire il divieto di sfruttamento commerciale di Internet. Nel 1994, mentre il numero dei computer collegati alla rete delle reti sale a 5 milioni, e la posta elettronica raggiunge 160 paesi, l'Unione Europea pubblica il c.d. «rapporto *Bangemann*», in cui si parla di Internet come «autostrada dell'informazione». Tra il 1997 e il 1998 l'utilizzazione commerciale di Internet prende decisamente il sopravvento sulle finalità scientifiche, accademiche e, più in generale, culturali.
Nel 1998 scade il contratto con cui un ente nordamericano (la *Network Solutions, Inc.*) aveva gestito sino ad allora l'assegnazione dei *domain name*. Malgrado l'opposizione dell'Unione Europea, che vorrebbe istituire un organismo internazionale per svolgere tale funzione, il Governo degli Stati Uniti costituisce una società privata *non profit*, deno-

minata *Internet Corporation for Assigned Number and Names* (*ICANN*), alla quale viene affidata anche la responsabilità dello sviluppo dei nuovi *standard* per i protocolli. L'enorme potere che *ICANN* accentra nelle sue mani la espone alle critiche severe di quanti osservano come essa sia governata in maniera non trasparente da un consiglio provvisorio «nominato in modo misterioso» (così CLAUSING, J., *Critics See Internet Board Overstepping Its Authority*, in *New York Times*, 7.6.1999), né servono le elezioni, effettuate in rete tra il 1° e il 10 ottobre 2000 per nominare cinque dei nove rappresentanti della comunità di Internet nel Consiglio di *ICANN*, a superare le perplessità (cfr. WEIBERG, J., [116]). Se si pensa che anche gli altri organi di governo di Internet attualmente operativi sono direttamente riconducibili agli Stati Uniti, e che, sino ad ora, le regole preposte al funzionamento della grande rete sono state, per lo più, autoprodotte da tali enti, è facile comprendere quale sia il più grande problema politico di Internet: la mancanza di rappresentatività, di legittimazione e di democrazia in chi lo dirige (cfr. WEINSTOCK, N., [117]). Tale delicatissima questione, che si palesa cruciale anche nell'ottica di un delineamento dei futuri assetti giuridici di Internet, è aggravata da un'ulteriore osservazione: ogni cambiamento dei protocolli tecnologici della rete, che può avvenire al di fuori di procedure formalizzate, è in grado di produrre effetti di più forte impatto rispetto alla modifica delle regole giuridiche (cfr. LESSING, L., [7], 160-162).

Il dibattito sul tema è aperto ed acceso. Da una parte ci sono coloro che asseriscono l'opportunità di lasciare che Internet si governi da sé, tanto a livello legislativo quanto a livello giurisdizionale (cfr. LANIN, A., [114]), dall'altra quelli che invece sostengono la necessità di interventi statali (cfr. LEMLEY, M.A., [110], il quale contesta l'efficienza economica di una autoregolamentazione di Internet; nonché GOLDSMITH, J.L., [109]; E SHAPIRO, A.L., [111]), o quantomeno di una regolamentazione mista, in parte lasciata al mercato e in parte realizzata dagli Stati nazionali (v. LESSING, L., [112]; LITAN, R.E., [113]). Tra questi due opposti, si segnala anche una posizione ulteriore, che è quella di quanti sostengono che le novità introdotte da Internet possono essere regolate dai principi giuridici tradizionali, debitamente adattati a livello interpretativo (cfr. SOMMER, J.H., [115]). In proposito, occorre, altresì, evidenziare come la direttiva europea 2000/31/CE (v. *infra*, 2.4.) — relativa a taluni aspetti giuridici della società dell'informazione — agli artt. 16 e 17, faccia carico agli Stati di incoraggiare l'elaborazione di codici di autocondotta e raccomandi di non ostacolare il ricorso a forme stragiudiziali di composizione delle controversie (c.d. *Alternative Dispute Resolution*, ADR). Sul punto v. PIERANI, M., *La crisi del diritto internazionale privato ed i sistemi alternativi di risoluzione delle controversie on-line*, in *Commercio elettronico*, a cura di V. Franceschelli, Milano, 2001, 591.

1.3. - *Il futuro della «rete delle reti»*. - Internet, così come nel suo complesso l'era digitale, si caratterizza perché risultato della cooperazione tra tecnologie informatiche e tecnologie della comunicazione (v. PASCUZZI, G., [15], 532). È proprio dalla fusione delle parole telecomunicazione ed informatica che nasce il termine «telematica» con il quale si fa riferimento all'integrazione tecnologica che consente ai dati elaborati dai computer di essere trasferiti da un luogo fisico ad un altro, così permettendo ai computer di dialogare anche a distanza (cfr. FROSINI, G., *Telematica ed informatica giuridica*, in *Enc. dir.*, XLIV, Milano, 1992, 60; RICHERI, G., *Le autostrade dell'informazione*, in *Problemi dell'informazione*, 1995, 27; v. anche TELEMATICA). Può, in definitiva, dirsi che Internet è una rete di computer — *rectius* una rete di reti, basata sull'evoluzione della telematica applicata — tra le cui maglie trova la sua consacrazione la c.d. realtà virtuale, anche detta «ciberspazio» (termine coniato nel 1983 da GIBSON, W., *Neuromante*, Milano, 1984); una realtà, cioè, priva di fisicità, nel senso tradizionale del termine, perché tutta ridotta a segnali digitali.

In un futuro assai prossimo si assisterà ad una convergenza verso tale rete di tutti i più importanti strumenti di comunicazione. Telefonia, radio e televisione in particolare stanno mettendo a punto strategie per sfruttare al meglio le potenzialità di Internet, così da abbattere alcuni costi e migliorare la qualità di determinati servizi (cfr. PARDOLESI, R.-RENDA, A., *Appunti di un viaggio nel capitalismo digitale: reti e retaggi culturali nel diritto antitrust*, in LIPARI, N.-MUSU, I. (a cura di), *La concorrenza tra economia e diritto*, Bari, 2000, 147; YARBROUGH, T.L., *Connecting the World: The Development of the Global Information Infrastructure*, 53 *Federal Commission Law Journal* 315, 2001; PERRITT, H.H.Jr., *Law and the Information Superhighway*, II ed., Gaithersburg-New York, 2001). In considerazione di ciò, è stato sostenuto che nella nuova era i mercati cederanno il passo alle reti e la proprietà sarà progressivamente sostituita dall'accesso. Ciò in quanto, «nella *new economy* sono le idee, i concetti, le immagini — non le cose — i componenti fondamentali del valore» (RIFKIN, J., *L'era dell'accesso*, Milano, 2000, 6-7; cfr. FORRESTER, V., *Una strana dittatura*, Firenze, 2000; OHMAE, K., *Il continente invisibile*, Roma, 2001; O'ROURKE, M.A., *Property Rights and Competition on the Internet*, 16 *Berkeley Technology Law Journal* 561, 2001). Se tali previsioni si avvereranno, o al contrario si dimostreranno esagerate, non è dato saperlo. A chi prevede una rapida «internettizzazione» (v. *supra*), si contrappone, infatti, chi profetizza la fine di Internet e con essa una profonda depressione economica globale (v. MANDEL, M.J., *Internet depression*, Roma, 2001; cfr. BROWN, J.S.-DUGUID, P., *La vita sociale dell'informazione*, Milano, 2001). In ogni caso, e comunque la si pensi, dalle brevi osservazioni svolte, vien fatto di credere che Internet sia destinato nei prossimi anni, al di là di un suo possibile ridimensionamento commerciale, ad acquisire un'importanza sempre maggiore nella vita di ognuno. Uno dei padri della c.d. *information technology* ha, già da qualche tempo, avvertito che «la rivoluzione delle comunicazioni avrà luogo nel corso di parecchi decenni e sarà stimolata da nuove applicazioni, cioè da nuovi strumenti che spesso andranno incontro ad esigenze che non immaginiamo neppure» (GATES, B., *La strada che porta a domani*, Milano, 1997, 10). Se la televisione è stata il focolare domestico del ventesimo secolo, Internet sarà, dunque, qualcosa di simile, se non molto di più, nel prossimo futuro, con due sostanziali differenze: 1) in Internet l'uomo è soggetto attivo nell'esplorazione e nella consultazione dei materiali pubblicati in rete; 2) proprio la natura interattiva di Internet fa sì che esso resti, per lo più, uno strumento di utilizzazione personale, considerato che ognuno sente la rete come luogo nel quale poter affermare liberamente, ed in molti casi gratuitamente ed anonimamente, la propria personalità a riparo da sguardi indiscreti e giudizi morali. Le due circostanze, tra loro intrecciate e reciprocamente dipendenti, sollevano problemi giuridici di primaria importanza, in particolare nel campo della responsabilità civile.

2. - INTERNET E RESPONSABILITÀ CIVILE

2.1. - *Introduzione*. - Le c.d. autostrade telematiche (*supra*, 1.3.) rappresentano un mezzo di comunicazione dalle potenzialità divulgative enormi, capaci di moltiplicare vertiginosamente le possibilità di compiere attività dannose e gli effetti economici delle stesse. È proprio dal davanzale di chi voglia svolgere un'indagine sui profili di responsabilità civile del fenomeno Internet, dunque, che risultano maggiormente visibili quei nodi particolarmente intricati, e spesso non percepibili da altre prospettive, che rischierebbero di paralizzare il sistema qualora non fossero preventivamente

individuati e, per quanto possibile, sciolti. Malgrado qualcuno pensi che questo risultato sia perseguibile anche soltanto attraverso sapienti operazioni ermeneutiche compiute sui principi giuridici esistenti (*supra*, 1.2.), basta fare un semplice inventario delle problematiche emerse negli ultimi anni nel campo della responsabilità extracontrattuale e ricollegabili ad Internet (v. *infra*, 3.), per capire che una soluzione di tal fatta è ottimistica al punto da poter essere considerata semplicistica. Autorevole dottrina italiana, infatti, già più di tre lustri fa, riflettendo sull'incrocio tra computer e illecito civile, dopo aver sottolineato come in Italia su tale argomento regnasse «una atmosfera di tranquilla indifferenza, che rischia però di essere l'indifferenza dell'ignoranza», evidenziava le «difficoltà di incanalare la variegatezza delle ipotesi prospettabili nei binari delle regole tradizionali in materia di responsabilità civile» (BUSNELLI, F.D., *Introduzione*, in ALPA, G. (a cura di), *Computers e responsabilità civile*, Milano, 1985). Oggi che la situazione, con l'avvento e la diffusione di Internet, è notevolmente cambiata, gli stessi legislatori statali — soprattutto, come è ovvio, a livello transnazionale — manifestano una crescente sensibilità nei confronti delle problematiche in parola. I tempi sembrano oramai maturi perché le soluzioni adottate, ovvero soltanto proposte, approdino ad una dignitosa sistemazione che serva, se non altro, a tamponare le falle più diffuse e di maggiore incidenza pratica.

2.2. - *Globalità, multimedialità, immediatezza, delocalizzazione e immaterialità: le nuove categorie della comunicazione.* - Internet, come anticipato, consente di raggiungere in pochi istanti milioni di persone collegate ad un terminale ed ubicate in ogni parte del mondo, il che rende irrilevanti i confini geografici e, di conseguenza, illimitate le potenzialità lesive della comunicazione realizzata per mezzo delle nuove tecnologie. Chi è in grado di accedere ad un computer connesso alla grande rete può oggi entrare in contatto in tempo reale con altri utenti, così diventando parte di quella comunità c.d. virtuale (v. *supra*, 1.3.) nella quale la globalizzazione dei mercati, la multimedialità dell'informazione (giornalistica, culturale, ricreativa, personale o commerciale che sia) e l'abbattimento dei tempi sono tutt'altro che virtuali (nel senso filosofico della parola, per cui è virtuale tutto ciò che può avere in potenza, ma ancora non ha, realizzazione o manifestazione concreta). Queste peculiarità fanno di Internet un'entità, o un nuovo spazio, che le regole giuridiche di stampo tradizionale non riescono, per molti versi, a gestire, in quanto esse si giustificano soltanto in ragione di una concezione consolidata e millenaria — ma in rete superata — di spazio e tempo (v. DI CIOMMO, F., [43], 2033; cfr. IRTI, N., *Norma e luoghi. Problemi di geodiritto*. Bari-Roma, 2001). Ciò è a dire che nei manuali di diritto non è più possibile spiegare la dimensione spazio/temporale senza rilevare come oggi esistano nuove categorie — globalità, multimedialità, immediatezza — con cui il giurista si deve necessariamente confrontare (cfr. ALPA, G., *New economy e libere professioni: il diritto privato e l'attività forense nell'era della rivoluzione digitale*, in *Contratto e impr.*, 2000, 1175, il quale osserva che «come nell'antica tragedia greca, anche [nella *new economy*] si realizza — in forme affatto diverse — una unità di *tempo*, di *luogo* e di *azione*»: v. anche ID., *Cyber Law. Problemi giuridici connessi allo sviluppo di Internet*, in *Nuova giur. civ. comm.*, 1998, II, 385).

L'irrilevanza dei confini geografici fa il paio con altre due caratteristiche della comunicazione via Internet: la delocalizzazione e l'immaterialità. È possibile, infatti, osservare che l'internauta mentre naviga, o si limita ad immettere materiali in rete, rimane nella sua stanza, nel suo ufficio, ovvero nel luogo pubblico dal quale accede alla rete; e tuttavia egli non è nemmeno in quel posto, considerato che tale attività è realizzata attraverso un sistema che si basa sull'immaterialità ed è dunque essa stessa non geograficamente localizzabile. Come è stato notato, in Internet «il soggetto è flusso linguistico, parola testuale o segno grafico, un *essere là* che non è mai *là*, ma ovunque sono [...] accessibili le sue parole. L'estensione pratica del soggetto individuo, sociale, culturale o politica, è potenzialmente illimitata, mentre nello stesso tempo il suo centro di gravità resta virtualmente non identificabile e dunque del tutto imprendibile» (MATHIAS, P., *La Cité Internet*, Parigi, 1997, in MATHIAS, P.-PACIFICI, G.-POZZI, P.-SACCO, P., *La Polis Internet*, Milano, 2000, 27). La qual cosa significa, per il giurista, che l'individuazione — già di per sé tecnicamente difficile — del *locus* in cui il soggetto, responsabile del compimento di una certa attività illecita in Internet, si trovava al momento in cui i materiali oggetto della diffusione lesiva sono stati veicolati in rete, in teoria può non essere considerata sufficiente a ritenere di aver rintracciato il luogo in cui detta attività è compiuta ed ancor meno, come evidente, il luogo nel quale gli effetti dannosi della stessa si sono realizzati (v. *infra*, 2.5.).

Già dalle brevi considerazioni sin qui svolte, è possibile percepire la portata delle questioni pratiche con le quali si deve confrontare l'interprete che, in casi di illecito compiuto via Internet, voglia determinare il foro territorialmente competente o, peggio, si trovi a dover risolvere problemi di giurisdizione, ovvero di individuazione della legge statale applicabile, attraverso le norme di diritto internazionale privato. Difficoltà che si moltiplicano se solo si pensa che non è possibile svolgere un'unica riflessione per tutte le ipotesi di responsabilità in quanto, come è facile intuire, la gamma di tipologie di illecito e di tecnologie utilizzabili genera importanti variazioni sul tema. La dottrina nordamericana che ha studiato il fenomeno della c.d. delocalizzazione — tra l'altro, evidenziandone le differenze rispetto al fenomeno della internazionalizzazione — delle attività compiute su Internet, parla di «*glocalization*», termine derivato dalla fusione delle parole *globalization* e *localization* e coniato da SOJA, E., *Afterword*, 48 *Stanf. Law Rev.* 1427, 1996 (cfr. GROSSFELD, B., [42]). In Germania considerazioni in proposito sono svolte, tra gli altri, da MULLER-HENGSTENBERG, C., [35]; e KOCH, A.F., [37] 28.

2.3. - *La (difficile) individuazione di chi commette fatti illeciti tramite Internet.* - Tra i tanti che, al fine di risolvere le questioni esposte nel precedente paragrafo, si sono posti il problema della localizzazione delle attività compiute in Internet, vi è chi ha efficacemente notato come gli utenti della rete, «mentre sono in quel posto, il ciberspazio, sono anche qui. Siedono di fronte al video del terminale, mangiando patatine, ignorando il telefono» (LESSING, L., [34]). Se è vero che l'utente occupa un luogo fisico mentre naviga in rete (espressione convenzionale usata per indicare l'attività dello *user* che, visualizzando pagine del *web*, accede ai materiali contenuti in Internet), è altresì vero che non solo quel posto spesso non è, per il danneggiato, facilmente rintracciabile, come presto si chiarirà, ma anche che costituirebbe un grave problema per quest'ultimo dover incardinare la causa davanti al giudice, e sulla base del diritto, di quel luogo; ciò in quanto, il danneggiante accorto ed organizzato potrebbe decidere — ribadita l'irrilevanza dei confini geografici per le attività compiute in Internet — di utilizzare un computer ubicato in una località in cui non esistono norme in grado di perseguire concretamente l'autore del fatto illecito, così eludendo ogni pretesa risarcitoria del malcapitato danneggiato. Le difficoltà tecniche di rintracciare il luogo fisico dal quale l'autore del fatto illecito ha operato sono esasperate dalle analoghe difficoltà che si riscontrano per individuare la sua reale identità. Le une e le altre dipendono dalle modalità con cui il singolo utente (c.d. *user*) si collega alla rete. Modalità sulle quali giova soffermarsi.

Chiunque voglia navigare in Internet, deve avere stipulato un apposito contratto con un *access provider*, il quale gestisce un determinato numero di accessi alla rete al fine di concederli ai propri clienti (c.d. *client*). Questi, quando vogliono connettersi, lanciano, mediante segnali elettronici trasportati da linee telefoniche, tale richiesta al proprio *provider* che, sempre servendosi delle linee telefoniche (v. *supra*, 1.3.), fa, per tutto il corso della navigazione, da tramite tra essi e la rete, nella quale ogni sito è gestito da altri operatori che, se offrono un qualsivoglia servizio, vengono definiti *service provider*. Il cliente, per effettuare la registrazione (c.d. *login*), deve avere un nome di identificazione (c.d. *user Id*) e una parola segreta (c.d. *password*) che usa all'inizio di ogni connessione per farsi riconoscere dal proprio *access provider*. Quest'ultimo, da parte sua, ad ogni elaboratore connesso alla rete attribuisce un indirizzo, c.d. *Ip* (*Internet protocol*: composto da quattro serie di cifre, tra loro divise da tre punti), che in teoria dovrebbe consentire di individuare la paternità di tutti i segnali lanciati in rete e dunque di tutte le attività in essa realizzate dal singolo utente visto che lo *user*, muovendosi tra le pagine Internet, non lascia traccia del suo nome, né del suo *user Id*, bensì del suo *Ip*.

La questione merita di essere approfondita al fine di cogliere la portata dei problemi che in essa si annidano. Per prima cosa, va detto che soltanto alcuni enti, pubblici e privati, dispongono come utenti di un indirizzo fisso, mentre gli *Ip* normalmente sono assegnati temporaneamente in quanto vengono, di volta in volta, attribuiti dal *provider* al richiedente per la durata della singola sessione di collegamento alla rete. Questa scelta operazionale dipende dal fatto che ogni *provider*, come detto, gestisce un numero limitato di accessi alla rete e dunque di *Ip*, così che, per evitare l'esaurimento degli indirizzi a disposizione, esso, al fine di poter avere più clienti, preferisce attribuire al singolo utente, ad ogni richiesta di accesso, uno tra gli *Ip* in quell'istante disponibili. Ciò impedisce al *provider* di avere un registro stabile con l'indicazione nominativa dei propri clienti e l'*Ip* corrispondente. Tale situazione è aggravata da un'altra circostanza: molto spesso il contratto di accesso è oramai stipulato senza che vengano accertati i dati anagrafici spesi dell'utente, in quanto il relativo servizio, anche in Italia, da circa due anni, viene fornito gratuitamente, per cui il *provider*, che punta ad avere il più alto numero di clienti possibile, non ha interesse a controllarne l'identità.

Ulteriori complicazioni sorgono quando l'utente, al fine di garantirsi l'anonimato in rete, compie la sua navigazione utilizzando *software* o siti appositi (c.d. *anonymizer*) che svolgono una funzione di filtro ed evitano che rimanga traccia dell'*Ip* dello *user* nei registri elettronici (c.d. *file di log*) dei siti visitati. Sulla reale efficacia di tali *software* non vi è certezza: mentre il funzionamento dei siti *anonymizer* è semplice: essi raggiungono, utilizzando il proprio *Ip*, il sito di cui fa richiesta l'utente, così che nei *file di log* di tale sito rimane registrato solo l'*Ip* dell'*anonymizer*. Ciò consente allo *user* di godere di una certa *privacy on line*, ma non toglie che, in caso di illecito compiuto tramite l'*Ip* dell'*anonymizer*, quest'ultimo, attraverso i suoi *file di log*, possa essere in grado di associare all'attività illecita compiuta l'*Ip* del danneggiante.

Un discorso a parte va fatto per gli illeciti realizzati da chi gestisce o è titolare di un sito *web*. Ciò in quanto — mentre, come appena detto, il singolo navigante accede alla rete ottenendo normalmente, di volta in volta, un *Ip* mobile, e dunque variabile, a seconda delle disponibilità momentanee del suo *access provider* — l'apertura di siti Internet può avvenire con due modalità che, in ogni caso, attribuiscono a quel sito un indirizzo, o dominio, fisso. Il soggetto interessato ad avere un sito *web* può acquistare un determinato dominio attraverso il *provider* che gli fornisce l'accesso, il quale lo gestirà tecnicamente; ovvero può registrare autonomamente il sito presso le autorità competenti. Va subito detto che in entrambi i casi, per il fatto illecito commesso direttamente tramite un sito *web*, non sorgono significative difficoltà di individuazione formale del soggetto a cui è intestato il sito, e dunque potenzialmente responsabile, bensì problemi derivanti dalla possibilità di effettuare intestazioni false o di comodo, nonché di sfuggire, attraverso un'attenta localizzazione dell'attività effettuata in Internet, all'applicazione di determinate normative e alla giurisdizione, o alla competenza, di una determinata autorità giudiziaria (v. *infra*, 2.4. e 2.5.).

Tornando al fatto illecito commesso in rete dallo *user*, va evidenziato come, sia che l'*access provider* abbia un elenco nominativo attendibile dei propri clienti, sia che non lo abbia, ovvero (è il caso italiano) questo non sia attendibile, il problema dell'individuazione dell'autore del fatto illecito e quello della sua localizzazione persistono, giacché la prassi di non attribuire *Ip* fissi fa sì che comunque non esista un'autorità sovranazionale in grado di associare nomi di utenti e relativi indirizzi Internet. Se tale autorità ci fosse, l'utente danneggiato, per sapere contro chi agire in giudizio, dovrebbe soltanto rintracciare, con la collaborazione del *service provider* che gestisce la pagina o il servizio tramite il quale il fatto illecito è stato commesso (collaborazione, in verità, non sempre facile da ottenere, v. *infra*), l'*Ip* del danneggiante. In mancanza di questo elenco, invece, una volta rintracciato tale *Ip*, il danneggiato dovrà rivolgersi all'*access provider* che lo ha in gestione per sapere chi, tra i clienti di quest'ultimo, nel preciso momento in cui il fatto illecito è stato commesso, lo stava utilizzando. Lo *user* che voglia commettere attività illecite in Internet può avere buon gioco ad eludere ogni azione giudiziaria, se solo ha la accortezza di servirsi, per l'accesso alla rete, di un *provider* sottoposto a leggi che non lo obbligano a comunicare tali dati (in particolare, all'autorità giudiziaria straniera) o che sottopongo tale comunicazione a procedure lente e complicate. Unico onere che il malintenzionato dovrà sopportare a fronte di tali vantaggi — sempre che questi non voglia spostare fisicamente il computer dal quale accede alla rete nella località in cui si trova l'*access provider* — sarà rappresentato da un diverso regime di spesa. Più lontano si trova il *server* dell'*access provider*, più costoso risulta, infatti, il collegamento ad Internet. La logica è esattamente la stessa che regola le tariffe telefoniche perché, in questo caso, proprio di spese telefoniche si tratta.

A ben vedere, anche qualora esistesse un'autorità sovranazionale in grado di associare nomi ed *Ip*, ed anche qualora l'*access provider* del danneggiante fosse sottoposto a norme efficienti sul piano della cooperazione giudiziaria ed a precisi obblighi di diligenza nel conservare determinati dati e comunicarli agli interessati richiedenti, le difficoltà nell'individuazione nel danneggiante persisterebbero, se alle stesse regole non fosse sottoposto il *service provider* che gestisce il servizio tramite il quale l'illecito è stato compiuto. Ciò in quanto, se l'attività illecita è stata posta in essere, ad esempio, attraverso la pubblicazione di materiali offensivi per l'onore del danneggiato su una pagina *web* gestita da un *server* ubicato in una località dove il *service provider* non riceve dalla legge imposizioni di sorta, sarà difficile ottenere la collaborazione di quest'ultimo. Collaborazione che, invece, si palesa necessaria, considerato che soltanto dai *file di log* che ogni *provider* detiene per qualche tempo, al fine di memorizzare tutte le attività compiute tramite le proprie pagine o i propri servizi, è possibile ricavare le informazioni di cui il danneggiato avrebbe bisogno, a cominciare dall'*Ip* del danneggiante (cfr. PARODI, C.-CALICE, A., [26], 13-35). Una volta cancellati o segretati i *file* di *log*, per il danneggiato, non solo diventa impossibile ricercare il danneggiante, ma, quando gli impulsi elettronici ricevuti non siano stati memorizzati dal suo computer, diventa anche difficile dimostrare lo stesso fatto illecito e le modalità con cui esso è stato realizzato.

2.4. - *Problemi di giurisdizione e legge applicabile.* - La difficoltà tecnica di individuare e localizzare chi abbia commesso un fatto illecito servendosi di Internet (v. *supra*, 2.3.), considerata la vocazione sovranazionale del mezzo di comunicazione prescelto, crea questioni di diritto internazionale privato e di competenza territoriale di non poco momento (cfr. DRAETTA, U., [22]; DI CIOMMO, F., [43]).
Prendendo come riferimento la l. 31.5.1995, n. 218 (in *G.U.*, 3.6.1995, n. 68, suppl. ord.) è possibile svolgere qualche breve considerazione al fine di evidenziare la complessità dei problemi in parola. L'art. 62 di tale testo normativo (anche combinato con l'art. 24) afferma che in caso di astratta applicabilità di più normative nazionali al medesimo fatto, la legge applicabile in concreto si individua in base al criterio del *locus commissi delicti* (v. RESPONSABILITÀ CIVILE: IV- Diritto internazionale privato). La disposizione citata, in particolare, e in particolare prevede che la relativa responsabilità «è regolata dalla legge dello Stato in cui si è verificato l'evento. Tuttavia il danneggiato può chiedere l'applicazione della legge dello Stato in cui si è verificato il fatto che ha causato il danno». Lo stesso criterio è utilizzato per risolvere i conflitti di giurisdizione quando, in forza dell'art. 3, 2° comma, sia applicabile l'art. 5, 3° comma, della Convenzione di Bruxelles del 27.9.1968, che attribuisce la giurisdizione al giudice del «luogo in cui l'evento dannoso è avvenuto» (diversamente è a dirsi quando risulti applicabile il 1° comma di tale disposizione, ai sensi del quale la giurisdizione italiana sussiste sempre quando il convenuto è domiciliato o residente in Italia). Il nodo da sciogliere, come evidente, sarà costituito dall'esatta individuazione del posto in cui «si è verificato l'evento», visto che difficilmente — considerati i segnalati problemi di individuazione del luogo «in sui si è verificato il fatto» — il danneggiato si avvarrà della facoltà di chiedere l'applicazione della legge di tal ultimo stato. E ciò a meno che non si ritenga che si deve considerare avvenuto il fatto nel luogo di stabilimento del prestatore del servizio Internet, tramite il quale l'illecito è stato realizzato. In tal caso, infatti, viene in soccorso del danneggiato il considerando 19 della direttiva 2000/31/CE (in *G.U.C.E.*, L 178/1, 17.7.2000) — relativa a taluni aspetti giuridici dei servizi della società dell'informazione, in particolare il commercio elettronico, nel mercato interno — il quale afferma che «il luogo di stabilimento, per le società che forniscono servizi tramite Internet, non è né là dove si trova la tecnologia di supporto del sito né là dove esso è accessibile, bensì il luogo in cui tali società esercitano la loro attività economica». Il principio in parola, come evidente, non risolve il problema rappresentato dalla localizzazione del singolo utente che si sia reso responsabile del fatto illecito, bensì solo quello, pur rilevante, della localizzazione dei *provider*. La direttiva, peraltro, al «*Considerando*» n. 23. dichiara espressamente di non voler introdurre norme supplementari di diritto internazionale privato sui conflitti di legge e di non trattare della «competenza di organi giurisdizionali».
Se, al contrario, si considera luogo in cui «si è verificato l'evento» quello nel quale il danneggiato ha avuto per la prima volta conoscenza del fatto (per alcuni illeciti questo è il criterio utilizzato tradizionalmente), non sarà semplice per l'attore dimostrare di essersi trovato ad accedere alla rete da un certa località, piuttosto che da un'altra, quando ha avuto prima conoscenza dei contenuti dannosi; per riuscire in tale impresa dovrà sperare nella collaborazione dei *provider* coinvolti nella vicenda (v. *supra*, 2.3.). Ancora più complicata si rivela la questione qualora — invece di ritenere assodato che il luogo dell'evento sia quello in cui si trovava il danneggiato nel momento in cui ha preso, per la prima volta, coscienza dell'esistenza in rete dei materiali sgraditi — si osserva che ci sono ipotesi in cui l'evento si verifica indipendentemente dalla prima conoscenza del soggetto danneggiato. In tal caso, infatti, occorre individuare di volta in volta il luogo in cui può ritenersi che l'evento si sia verificato: attività ostacolata dal carattere essenzialmente immateriale del ciberspazio.
A questo punto giova richiamare il combinato disposto dell'art. 56 l. 21.6.1942, n. 929 (c.d. legge marchi), e dell'art. 3, 1° comma, l. n. 218/1995, che afferma la giurisdizione italiana, qualunque sia la cittadinanza, residenza o domicilio delle parti, per le azioni in materia di marchi, italiani o internazionali, già registrati o in corso di registrazione, ove estendenti «i loro effetti» in Italia (per una recente affermazione della giurisdizione italiana in applicazione dell'art. 56 l.m., v. Trib. Roma, ordinanza 9.3.2000, in *Foro it.*, 2000, I, 2334, con nota di G. Pascuzzi). L'art. 56 fornisce all'operatore, a differenza delle norme precedentemente richiamate, una regola in grado di operare senza problemi anche con riferimento agli atti illeciti realizzati via Internet. Non è detto, dunque, come da troppe parti si lascia intendere (cfr. BALLARINO, T., [3], 224), strizzando l'occhio all'autoregolamentazione (v. *supra*, 1.2.), che le regole giuridiche di derivazione statale siano per definizione inadeguate a gestire il fenomeno Internet. È vero, al contrario, che l'applicazione tradizionale dei principi consolidati si palesa, in molti casi, inadeguata alla nuova realtà, ma ciò non esclude che debbano essere proprio i legislatori statali a formularne di nuovi. A questo proposito, pare il caso di segnalare che vi sono diverse proposte di regolamentazione sovranazionale di tali problematiche, a tenore delle quali, per quanto riguarda la tutela del diritto d'autore, si prospettano criteri di collegamento che individuano la legge applicabile in quella dello Stato in cui avviene il c.d. *uploading* (caricamento sul *server* del *provider* delle pagine destinate ad essere visionate sul *web*) e, in subordine, quella dello Stato in cui si produce l'evento dannoso; mentre, per quanto riguarda la tutela dei diritti della personalità, si preferisce (e le ragioni alla base di tale scelta dovrebbero essere oramai chiare) promuovere l'applicazione della legge dello Stato in cui la vittima ha *subito* il danno, se questo era prevedibile da parte dell'autore dell'illecito e, in subordine, la legge dello Stato dello *uploading* dei dati che hanno causato il danno (v. GIURDANELLA, C., *Problemi di giurisdizione*, in [20], 373). Cfr. il regolamento CE n. 44/2001 (in *G.U.C.E.*, L 12, 16.1.2001), concernente la competenza giurisdizionale, il riconoscimento e l'esecuzione delle decisioni in materia civile e commerciale.

2.5. - *Problemi di foro territorialmente competente.* - Il problema della competenza territoriale del giudice chiamato a risolvere controversie riguardanti Internet — al pari delle questioni sulla legge applicabile e sulla giurisdizione di riferimento — coinvolge fattispecie molto eterogenee. Le incertezze concernono sia ipotesi di inadempimento contrattuale che di fatto illecito, sebbene, in relazione alle prime, il d. legisl. 22.5.1999, n. 185 (in *G.U.*, 21.6.1999, n. 143) — attuazione della direttiva 97/7/CE relativa alla protezione dei consumatori in materia di contratti a distanza — all'art. 14 disponga che «la competenza territoriale inderogabile è del luogo di residenza o di domicilio del consumatore, se ubicati nel territorio dello Stato» (cfr. DE MARZO, G., *I contratti a distanza*, Milano, 1999, 67; nonché DANOVI, F., *Il foro del consumatore nei contratti a distanza*, in *Riv. dir. proc.*, 2000, 430). La norma da ultimo citata è applicabile ai soli c.d. contratti *business to consumer* (tra imprenditore e consumatore) e non anche ai c.d. contratti *business to business* (tra imprenditori), ma certo contribuisce, con ciò smentendo quanti diffidano della possibilità per i legislatori nazionali di regolare le attività realizzate in Internet, a fissare — in ambito contrattuale e per fattispecie sottoposte alla legge di Stati facenti parte dell'Unione Europea — alcuni necessari punti fermi (cfr. GIOVA, S., *La conclusione del contratto via Internet*, Napoli, 2000, 92-96).

I maggiori dubbi riguardano, dunque, la competenza territoriale del giudice per il fatto illecito commesso in rete. In termini generali, tale competenza è disciplinata, nel nostro ordinamento, dal codice di procedura civile, a tenore del quale l'attore può scegliere di adire il giudice del luogo in cui il danneggiante ha la residenza, il domicilio o, in via residuale, la dimora (artt. 18 e 19), ovvero, alternativamente, quello del luogo in cui l'obbligazione «è sorta o deve eseguirsi» (art. 20). Ai sensi dell'articolo da ultimo citato, l'attore danneggiato da un fatto illecito può teoricamente scegliere tra due criteri alternativi: quello del *forum commissi delicti* e quello del *forum destinatae solutionis*. In concreto, tuttavia, questo secondo si rivela pressoché inutile, perché conduce a ritenere competente il giudice del luogo in cui ha domicilio il debitore al tempo della scadenza dell'obbligazione (in quanto questa ricade nell'ambito di applicazione dell'art. 1182, 4° comma, c.c.), così come, nella maggior parte dei casi, sarebbe ai sensi degli artt. 18 e 19 c.p.c. Il solo criterio adatto a rendere effettiva la disponibilità di un foro territoriale alternativo in caso di illecito è, dunque, quello del *locus commissi delicti*, in applicazione del quale, riguardo alla circostanza in cui vi sia diversità tra il luogo di commissione del fatto e quello di produzione dell'evento dannoso, la giurisprudenza si è tradizionalmente divisa tra chi sostiene che si debba aver riguardo a quest'ultimo (Cass., 5.6.1991, n. 6381, in *Foro it.*, 1992, I, 436) e chi ritiene il contrario (Cass., 29 marzo 1995, n. 3733, in *Foro it. Rep.*, 1995, voce cit., n. 8), mentre, se il danno si verifica in più luoghi, per orientamento costante si fa riferimento alla località di prima incidenza causale dell'azione nella sfera giuridica dell'attore (cfr. MANDRIOLI, C., *Diritto processuale civile*, XIII ed., I, Torino, 2000, 109). Anche l'art. 57 l.m. pone, come foro alternativo a quello della residenza, del domicilio o della dimora del convenuto (art. 56), il foro del luogo dove sono stati commessi i fatti che si assumono lesivi del diritto di marchio. Il problema ermeneutico consiste dunque — in relazione, tanto al fatto illecito in generale, quanto alla lesione del marchio — nel determinare cosa in concreto si debba intendere per *locus commissi delicti*, laddove, come già rilevato (v. *supra*, 1.1. e 2.3.), l'illecito commesso via Internet può sfuggire ai tentativi di definizione geografica e dispiega il suo potenziale lesivo contemporaneamente in tutta la rete, senza che sia possibile, nella maggioranza dei casi, individuare con certezza un luogo fisico di prima incidenza causale dell'azione.

L'imbarazzo interpretativo è confermato dall'incertezza manifestata dalla giurisprudenza italiana chiamata ad applicare il criterio in parola ad attività compiute via Internet. Mentre, infatti, secondo alcune pronunce, l'illecito è commesso dove è ubicato il computer dal quale partono i materiali diretti in rete, e non dove la lesione del diritto si manifesta (cfr. Trib. Lecce, 24.2.2001, e Trib. Verona, ordinanza 18.12.2000, entrambe in *Foro it.*, 2001, I, 2032); in altri casi si è ritenuto che siano territorialmente competenti tutti i tribunali italiani ubicati in luoghi dai quali è possibile accedere alla rete, perché in ognuno di tali fori si manifesta la lesione del diritto (v. Trib. Cagliari, ordinanza 28.2.2000, in *Nuova giur. civ.*, 2000, I, 535).

La problematica in esame si palesa ancora più complessa se solo si considera che ogni tipo di illecito deve essere trattato nel rispetto delle sue peculiarità. A tal proposito, giova osservare come, secondo la giurisprudenza di legittimità, quando si discuta una domanda di contraffazione del marchio e concorrenza sleale, per incardinare la causa davanti ad un giudice, occorre affermare la commercializzazione del prodotto nel territorio rientrante nella sua competenza (v. Cass., 28.10.1997, n. 10582, in *Riv. dir. ind.*, 1998, II, 273). Tale precisazione consente di reputare che, nel caso di specie, ogni tribunale italiano è competente a pronunciarsi quando i prodotti siano venduti a mezzo Internet. Ciò in quanto «Internet può essere inteso come un grande scaffale sul quale è collocata merce varia da guardare, comprare o consumare. Tra mettere in fila bottiglie con un marchio lesivo della privativa altrui in un supermercato tradizionale e pubblicare l'immagine delle stesse su un sito *web* attrezzato per la vendita *online* c'è, ai nostri fini, una sola sostanziale differenza: nel primo caso la commercializzazione ha un riferimento geografico preciso, nel secondo essa avviene in ogni posto dal quale è possibile accedere ad Internet» (DI CIOMMO, F., [43], 2041). Diversamente è a dirsi se si ritiene che, quando la produzione del danno sia disseminata sul territorio, l'esigenza di determinare un criterio oggettivo unico di individuazione della competenza territoriale imponga di tralasciare l'elemento della commercializzazione per far riferimento al luogo in cui il bene, che porta il marchio illegittimo, è prodotto. Attraverso tale espediente ermeneutico è, infatti, possibile aggirare il problema della competenza territoriale, in caso di illecito effettuato a mezzo Internet, semplicemente perché si evita di prendere in considerazione Internet. Anche questa soluzione (adottata, da ultimo, da Trib. Napoli, sezione di Pozzuoli, ordinanza 14.6.2000, in *Dir. inf.*, 2001, 231, con nota di P. Sammarco) non convince, in quanto finisce presumibilmente per incardinare la causa dinanzi al giudice del luogo in cui il convenuto ha la sede della propria impresa, così rendendo vana la ricerca di un foro «alternativo» a quello generale.

A ben vedere, nessuna delle soluzioni sinora passate in rassegna appare soddisfacente. Infatti, mentre quella che fa leva sul luogo in cui è collocato il computer dal quale l'utente accede alla rete o il sito viene gestito (nelle sue due varianti: luogo in cui è ubicato il *server*, ovvero luogo dal quale i dati vengono immessi in rete) si presta all'arbitrio del danneggiato che potrebbe, di volta in volta, scegliersi il giudice competente; quella che ritiene competenti tutti i tribunali italiani appare inaccettabile in quanto consente, non al danneggiante, ma al danneggiato, di realizzare il c.d. *forum shopping*, con ciò violando allo stesso modo il primo comma dell'art. 25 Cost., a tenore del quale il giudice naturale deve essere precostituito.

In definitiva, il criterio del *locus commissi delicti* non appare, almeno nella sua accezione tradizionale, idoneo ad essere applicato alle fattispecie in cui viene in rilievo l'uso di reti telematiche, e ciò in quanto entità «virtuali» non possono essere individuate materialmente (*id est*, dal punto di vista spaziale e temporale) come entità del mondo reale, «né va applicata la logica degli atomi ai byte» (NEGROPONTE, N., *Being Digital*, Knopf, 1995). Al contrario, una soluzione adatta a dirimere la questione in via definitiva ed equa sembra quella per cui, in caso di illecito realizzato a mezzo Internet, la competenza — in alternativa a quanto stabilito dagli artt. 18 e 19 c.p.c. — spetterebbe al giudice del foro in cui il danneggiato ha la propria sede, la propria residenza o il proprio domicilio (cfr. Trib. Messina, 6.11.2000, in *Foro it.*, 2001, I, 2032). In tal modo: 1) la causa viene incardinata dove l'illecito è giunto a compimento causando concretamente un danno; 2) si impedisce ad entrambe le parti in causa di compiere attività di *forum shopping* e si precostituisce il giudice naturale territorialmente competente; 3) si evita che il danneggiato debba sopportare spese legate alla necessità di individuare il luogo di gestione del sito nonché il rischio di non riuscire in tale individuazione. La soluzione proposta è perseguibile attraverso un'interpretazione dell'art. 20 c.p.c. (o, ad esempio, degli artt. 56 e 57 l.m.) che, in caso di illecito commesso in rete, faccia leva sulla realizzazione effettiva del danno. Basta, in altre parole, considerare *locus commissi delicti* quello dove il fatto illecito genera realmente il danno economico; luogo che, nel caso in cui l'offesa colpisca un imprenditore, coincide con quello in cui è ubicata la sede dell'impresa e, nel caso in cui colpisca una persona fisica, risulta quello della sua residenza o del suo domicilio, in quanto è lì che questa concretamente può essere pregiudicata da una condotta illecita altrui. Una simile

scelta ermeneutica — che, per inciso, rispetta l'opzione accolta dal legislatore in materia di contratti dei consumatori stipulati a distanza e dunque anche in rete — fa giustizia della singolarità e della peculiarità di Internet come strumento adatto a compiere attività dannose, ed inoltre, in un'ottica di *law and economics*, si rivela funzionale a riequilibrare il rapporto tra gestore del sito e terzi, altrimenti tutto sbilanciato a favore del primo, il quale gode di una vantaggio, se non sempre tecnologico, quantomeno logistico. La perseguibilità e l'efficienza della soluzione proposta trova ulteriore conferma se si considera che l'art. 30, 5° comma, l. 6.8.1990, n. 223 (in *G.U.*, 9.8.1990, n. 185, suppl. ord.) — disciplina del sistema radiotelevisivo pubblico e privato —, afferma, per il reato di diffamazione compiuto attraverso il mezzo radiotelevisivo, la competenza territoriale del giudice del luogo di residenza della persona offesa.

2.6. - *Gli «Internet provider»*. - Il pianeta Internet ruota intorno ad operatori che acquistano accessi alla rete dalle agenzie competenti e li distribuiscono agli utenti. Questa attività di intermediazione, a cui si aggiungono spesso servizi di varia natura, è svolta dagli *Internet Provider* (c.d. *ISP*). Con la generica qualifica di *provider* si fa generalmente riferimento ad una pluralità di soggetti che, ai fini della presente riflessione, devono essere distinti. Infatti, mentre l'*access provider* fornisce la connessione, il *service provider* fornisce servizi ulteriori (ospitalità di siti, caselle *e-mail*, *chat*, *forum* telematici, *newsgroup*, motori di ricerca, gestione di banche dati, bacheche elettroniche in cui gli utenti possono pubblicare i propri materiali, ecc.) ed il *content provider* veicola in rete propri contenuti (si pensi all'operatore che, ad esempio, pubblica in rete notizie di cronaca, collezioni di fotografie d'autore, racconti, barzellette e quant'altro). Tali differenze funzionali si rivelano importanti nell'ottica di un corretto inquadramento delle rispettive responsabilità, sebbene vada rilevato che la ripartizione sopra proposta è solo indicativa, visto che spesso accade che le qualifiche si sovrappongano in quanto un solo operatore fornisce l'accesso, offre servizi e veicola propri contenuti in rete. Ciò è a dire che l'esatta funzione, svolta dal *provider* in relazione alla fattispecie concreta, andrà indagata caso per caso.
Altra differenza da non sottovalutare, nell'economia della riflessione che si va conducendo, è quella tra *provider* che traggono profitti dalla loro attività, e *provider* c.d. amatoriali o istituzionali. Per *provider* istituzionali si intendono i centri di cultura, le scuole, gli enti pubblici preposti ad attività particolari, che abbiano strutture idonee a fornire il servizio di accesso alla rete; per *provider* amatoriali, singoli o associazioni che, senza alcun fine di lucro, né di ricerca, organizzano modeste strutture in grado di consentire il collegamento e la diffusione di materiali nel ciberspazio. A questi si contrappongono i *provider* professionisti, che sono persone fisiche, ma per lo più società, che curano tali servizi a fini di lucro e che, dunque, si presumono avere un'adeguata organizzazione. In virtù di tale prerogativa sono considerati, da una parte della dottrina, i soli soggetti in grado di risarcire i danni a terzi causati dagli illeciti compiuti dagli *user* (cfr. DONATO, B., [44]) visto che essi assumerebbero tale rischio a fronte di una remunerazione ed inoltre potrebbero, considerata l'organizzazione e la struttura di cui normalmente dispongono, apprestare sistemi di controllo sui contenuti che veicolano in rete.
Ai *provider* può essere astrattamente imputata una qualche responsabilità, per: 1) sospensione o interruzione dei servizi (l'ipotesi riguarda tutte e tre le categorie di *provider* sopra descritte); 2) fatto compiuto in rete da soggetti anonimi il cui *Ip* resta non individuato per colpa del *service provider* gestore del servizio tramite il quale l'illecito è stato realizzato; 3) illiceità di propri materiali veicolati in rete dal *content provider*; 4) fatto illecito compiuto da utenti che restano anonimi in quanto l'*access provider* non riesce ad impedire l'accesso abusivo ovvero a fornire la reale identità dei propri clienti. Alla trattazione di ognuna di tali questioni sono dedicati i paragrafi che seguono.

2.6.1. - *La responsabilità del «provider» per disservizi*. - Quando un *provider*, nello svolgimento delle sue attività (v. *supra*, 2.6.), si rende autore di un disservizio, si pone il problema di valutare se, e in presenza di quali circostanze, vi sia una responsabilità per i danni cagionati agli utenti. Certamente, nei confronti dei soggetti che sfruttano stabilmente i servizi in virtù di un apposito contratto, è sempre configurabile una responsabilità per inadempimento. Normalmente, in tali contratti, i *provider* hanno cura di inserire pattuizioni di esonero della responsabilità per disservizi, ritardi o sospensioni; l'efficacia di siffatte clausole, tuttavia, ai sensi dell'art. 1229 c.c., nel nostro ordinamento civile è limitata, e dunque il *provider* riuscirà a liberarsi da ogni tipo di responsabilità solo dimostrando che il disservizio è dipeso da circostanze sopravvenute, non prevedibili e non governabili, ovvero da sua colpa lieve (cfr., da ultimo, PONZANELLI, G., *Le clausole di esonero della responsabilità*, in *Danno e resp.*, 1998, 852; v. anche SIGNORELLI, F., *Profili di responsabilità del provider nell'e-commerce*, in *Commercio elettronico*, a cura di V. Franceschelli, Milano, 2001, 555 e, in particolare, 565-569). Nel tentativo di gestire il problema, i *provider* sono soliti far specificare contrattualmente al cliente se intende utilizzare il servizio per fini professionali o personali. Il più delle volte, il servizio viene prestato gratuitamente solo nei confronti di quanti dichiarano l'utilizzazione personale, e ciò al fine di incentivare tale scelta da parte dell'utente, il quale, tuttavia, di conseguenza, si troverà in difficoltà nel caso in futuro dovesse aver bisogno di dimostrare di aver subito ingenti danni a seguito di un eventuale disservizio. Negli Stati Uniti, per risolvere questi ed altri problemi, è stato recentemente elaborato lo *Uniform Computer Information Transaction Act*, *UCITA*, la cui adozione nei singoli Stati dell'Unione è attualmente ostacolata dalle perplessità, da più parti manifestate, circa alcuni punti nodali del testo normativo proposto (cfr. STEWART, M., *Commercial Access Contracts and the Internet: Does the Uniform Computer Information Transaction Act Clear the Air with Regard to Liabilities when an On-Line Access System Fails?*, 27 *Pepperdine Law Review* 597, 2000).
Più complessa è la situazione se si pensa ai danni procurati, dal medesimo disservizio di cui sopra, allo *user* che non abbia mai formalmente stipulato un contratto con il *provider* e che sia un semplice frequentatore, occasionale o abituale, del servizio. Il dubbio principale concerne la natura della responsabilità che si potrà delineare, in tale circostanza, in capo al *provider*, posto che in molti casi, al fine di registrare un numero più elevato di contatti sul proprio sito, essi lasciano appositamente a chiunque la possibilità di utilizzare gratuitamente e senza bisogno di alcun contratto, materiali o servizi messi a disposizione *online*. Una prima soluzione plausibile è quella di ritenere che, in presenza di colpa o dolo del *provider*, debitamente provati, quest'ultimo sia tenuto, in forza dell'art. 2043 c.c., a risarcire i danni effettivamente arrecati. Tale opzione presuppone il superamento di un problema che sta a monte e che consiste nel considerare come posizione giuridica qualificata e meritevole di tutela aquiliana quello dello *user* che, pur in assenza di contratto, ha riposto un certo affidamento nella possibilità di utilizzare il servizio in seguito sospeso. La seconda soluzione possibile fa leva sulla contestata teoria della c.d. responsabilità «da contatto» (cfr. CASTRONOVO, C., *L'obbligazione senza prestazione. Ai confini tra contratto e torto*, in AA.VV., *Scritti in onore di Mengoni*, I, Milano, 1995, 197), in applicazione della quale il *provider* risponderebbe per la mera indisponibilità del servizio, e dunque indipendentemente da colpa o dolo, a meno che non riesca a dimostrare

l'impossibilità oggettiva di impedire l'inconveniente, e ciò in quanto, pur in mancanza di un vero e proprio contratto, in presenza di determinate circostanze, opererebbe la disciplina generale dell'inadempimento.

2.6.2. - *La responsabilità del «service provider»*. - Sono comunemente definiti *service provider* gli operatori che forniscono in rete servizi di vario genere (v. *supra*, 2.6.). Quando, attraverso l'utilizzazione di tali servizi, un utente pone in essere un fatto illecito (ad esempio, formulando dichiarazioni in rete che poi si rivelano dannose per terzi, ovvero pubblicando materiali offensivi o diffamanti), ci si chiede chi sia il soggetto responsabile. Se il servizio è ontologicamente volto a realizzare tale illecito — situazione che, ad esempio, si verifica per quei siti che consentono agli *user* di violare i diritti d'autore scaricando gratuitamente dalla rete sul proprio personal computer opere protette —, non v'è dubbio che il fornitore debba rispondere direttamente dei danni causati. Viceversa, nel caso in cui il servizio di per sé non abbia una tale vocazione, sembra difficile individuare una precisa responsabilità in capo al *provider*, mentre sarà certamente responsabile l'utente che ha realizzato l'illecito, sempre che lo si individui.
In alcuni casi, tra *provider* e *user* esiste un contratto con il quale il primo declina ogni responsabilità in relazione ai contenuti veicolati in rete per conto del secondo, così attribuendo il ruolo di responsabile legale a quest'ultimo (cfr. ALBERTINI, L., *I contratti di accesso ad Internet*, in *Giust. civ.*, 1997, II, 95). In ogni caso, anche qualora tale accordo — che, del resto, non ha effetto nei confronti dei terzi danneggiati — manchi, al *service provider*, che sia in grado di comunicare a questi ultimi l'*Ip* del danneggiante e che si sia attivato per cancellare i materiali illeciti non appena ne abbia avuto conoscenza, non sembra imputabile alcuna responsabilità (v. *infra*, 2.6.4.).
La questione è stata oggetto, soprattutto negli Stati Uniti, di numerose vicende giudiziarie. Nel celebre caso *Cubby, Inc. v. CompuServe, Inc.* (776 *Fed. S.* 135, S.D.N.Y. 1991), in un *forum* telematico gestito dalla società *CompuServe* erano stati diffusi alcuni messaggi dal contenuto diffamatorio, tendenti a gettare discredito sulla società *Cubby*. La Corte escluse qualsiasi responsabilità da parte del gestore del *forum*, osservando che la velocità con cui i dati sono immessi in rete non consente un controllo sui loro contenuti, ed equiparando l'attività del *service provider* a quella del bibliotecario che non è tenuto a controllare il contenuto dei libri messi a disposizione del pubblico. Successivamente, nel caso *Stratton Oakmont, Inc. v. Prodigy Services, Co.* (per il cui epilogo v. la sentenza New York Supreme Court, 11.12.1995, in *West Law*, 1995, 323710), una società che gestiva un *bulletin board system* (una sorta di bacheca elettronica), in cui erano diffusi alcuni messaggi diffamatori per l'attore, veniva condannata in quanto, nella fattispecie, secondo i giudici, essa aveva assunto veri e propri poteri editoriali, visto che si era dotata di un sistema di filtraggio delle informazioni finalizzato ad evitare che fossero lanciati messaggi dannosi. Si andava così delineando una situazione paradossale che finiva per disincentivare l'adozione di filtri automatici, in quanto questi erano (e sono) tecnicamente in grado di ridurre, ma non di eliminare, i materiali illeciti o comunque lesivi di diritti altrui. Tale situazione suscitò la reazione del legislatore americano che nel 1996 emanò, all'interno del nuovo *Telecommunications Act* (47 *United State Code* 230c), il *Communication Decency Act* (*CDA*), il quale tra l'altro prevede che «nessun fornitore o utilizzatore di un servizio interattivo telematico sarà trattato come un editore nei confronti delle informazioni fornite da un altro fornitore di contenuto (*content provider*)» ed inoltre afferma la non responsabilità dei *provider* per gli eventuali danni causati quando, in buona fede, impediscano l'accesso ai materiali ritenuti potenzialmente lesivi di diritti altrui (c.d. *Good Samaritan Clause*). Le prime applicazioni giurisprudenziali di tale normativa confermarono la generale impossibilità di equiparare, a fini risarcitori, il *service provider* ad un editore (*contra*, però, *Blumenthal v. Drudge and AOL*, 992 *Fed. S.* 44, D.C. Cir. 1998, in cui la *AOL* fu ritenuta responsabile per i danni causati da una *e-mail* diffamatoria diffusa da un suo cliente).
Il 28 ottobre 1998, sempre negli Stati Uniti, è stato emanato il *Digital Millennium Copyright Act* (*DCMA*) (17 *United State Code* 1201), il quale, tra l'altro, disciplina la responsabilità dei *provider* per la diffusione in rete di materiali che violano le norme a tutela del *copyright* (cfr. GOLDSTEIN, M.P., [51]; YEN, A.C., [54]). La § 512, rubricata «*Limitations on liability relating to material online*», prevede che il fornitore di un servizio telematico, nel trasmettere o nel fornire accesso alla rete, non possa essere considerato responsabile qualora: 1) l'informazione sia propagata da un soggetto terzo; 2) la trasmissione, la connessione o lo stoccaggio delle informazioni rientri in un processo tecnico, senza che l'operatore abbia selezionato i contenuti da diffondere; 3) il soggetto intermediario non selezioni i destinatari; 4) il contenuto non sia registrato e non sia mantenuto per un periodo di tempo che ecceda quello strettamente necessario allo svolgimento delle finalità tecniche; 5) l'informazione non sia modificata (cfr. RICCIO, G.M., [52], 67-68). La stessa *section* prende in considerazione il caso del *provider* che, nel fornire un determinato servizio, non si limita a veicolare segnali, ma opera attraverso un procedimento di memorizzazione temporanea delle informazioni sul suo disco rigido (c.d. *caching*). Tale attività si differenzia dalla mera trasmissione in quanto consente l'intercettazione dei materiali memorizzati, e dunque permette al *provider* di intervenire per bloccarne l'ulteriore permanenza in rete, quando sia venuto a conoscenza di fatti o circostanze in base ai quali l'attività illecita è manifesta ovvero abbia ricevuto una apposita notificazione di un terzo (cfr. RICCIO, G.M., [52], 68).
In Italia, in assenza di un intervento legislativo, la dottrina, al fine di perseguire il *provider* quando non sia possibile individuare il reale autore dell'illecito, si è interrogata sulla possibilità di estendere analogicamente la disciplina riguardante la stampa agli illeciti informatici (cfr. V. ZENO ZENCOVICH, V., *La pretesa estensione alla telematica del regime della stampa: note critiche*, in *Dir. inf.*, 1998, 5). In materia penale, si è per lo più avversata tale prospettiva, in virtù della inderogabilità che caratterizza il principio di personalità della responsabilità (art. 27, 1° comma, Cost.), nonché il principio di legalità (art. 25, 2° comma, Cost.); mentre si discute in ordine alla applicabilità degli artt. 57, 261, 266, 302, 326, 414, 528, 595, 618 e 621 c.p. (cfr. SEMINARA, C., *La responsabilità penale degli operatori su Internet*, in *Dir. inf.*, 1998, 745; SIEBER, P., *Responsabilità penali per la circolazione di dati nelle reti internazionali di computer*, in *Riv. trim. dir. pen. econ.*, 743; PARODI, C.-CALICE, A., [26]). In ambito civile, la questione è stata affrontata (cfr. Trib. Roma, 4.7.1997, in *Dir. inf.*, 1998, 807; Trib. Roma, 22.3.1999, in *Dir. inf.*, 2000, 67; Trib. Teramo, ordinanza 11.12.1997, in *Dir. inf.*, 1998, 372; Trib. Napoli, decreto 18.3.1997, in *Foro it.*, 1997, I, 2307; Trib. Napoli, ordinanza 8.8.1997, in *Giust. civ.*, 1998, 1, 258) richiamando: l'art. 2050 c.c., in tema di responsabilità per attività pericolosa; l'art. 2048 c.c., nel caso, ad esempio, in cui l'illecito sia realizzato attraverso il computer della scuola da un minore; l'art. 2049 c.c., quando il fatto illecito sia commesso da un dipendente, durante l'orario di lavoro, attraverso il computer di servizio (cfr. TROIANO, O., [47], 405; TOSI, E., *Le responsabilità civili*, in [10], 297; PERON, S., [33]); ovvero gli artt. 11 e 12 l. 8.2.1948, n. 47, che riguardano la responsabilità civile dell'editore e la riparazione pecuniaria a carico dei diffamatori. A tale proposito, pare il caso di sottolineare che con la l. 7.3.2001, n. 62 (*Nuove norme sull'edito-*

ria e sui prodotti editoriali e modifiche alla l. 5.8.1991, n. 416; in *G.U.*, 21.3.2001, n. 67), è stata equiparata l'editoria elettronica a quella tradizionale ed è stata resa obbligatoria l'iscrizione nei registri della stampa per le pubblicazioni telematiche «diffus[e] al pubblico con periodicità regolare e contraddistint[e] da una testata» (cfr. ZENO-ZENCOVICH, V., *I «prodotti editoriali» elettronici nella L. 7 marzo 2001, n. 62*, in *Dir. inf.*, 2001, 153).

Nel vecchio continente il vuoto legislativo in materia (localmente attenuato da alcune normative, di carattere settoriale, quali il *Defamation Act*, emanato nel Regno Unito nel 1996, e il *Teledienstegesetz*, che dal 1° agosto 1997 è contenuto nell'art. 1 dell'*Informations- und Kommunikationsdienste Gesetz* tedesco) è stato parzialmente colmato dalla formulazione dei principi contenuti nella già citata direttiva 2000/31/CE (v. *supra*, 2.5.), che dell'esperienza nordamericana reca le stimmate. Questa dedica la sezione IV, rubricata «Responsabilità dei prestatori intermediari», al perseguimento di un difficile contemperamento tra gli interessi, spesso confliggenti, dei diversi soggetti che operano in Internet: da un parte, quelli dei *provider* che forniscono servizi di varia natura a non essere ritenuti responsabili per attività illecite compiute dai propri utenti; dall'altra, quelli della intera comunità internazionale, e delle imprese che temono le potenzialità lesive della rete, preoccupate che Internet rimanga uno spazio privo di regole, di controllori e, dunque, di responsabilità.

Né gli interventi legislativi d'oltreoceano, né la direttiva europea, a ben vedere, sembrano occuparsi del caso in cui il *service provider* non fornisca al danneggiato i dati di cui questi ha bisogno al fine di rintracciare l'autore dell'illecito. In particolare, come è stato notato, la direttiva «non crea una forma di responsabilità *ad hoc* per gli intermediari della rete» (RICCIO, G.M., [52], 78), in quanto ha preferito consentire l'applicazione a questi soggetti delle regole di diritto comune, salvo affermare che, quando in capo a tali operatori non è possibile individuare alcuna responsabilità specifica, gli stessi non rispondono del fatto illecito compiuto da chi utilizza i loro servizi. In particolare, all'art. 12, rubricato «Semplice trasporto», all'art. 13, rubricato «Memorizzazione temporanea detta *caching*», e all'art. 14, rubricato «*Hosting*», la normativa in parola prevede che i prestatori di servizi di rete, in presenza di condizioni che garantiscano la loro totale estraneità rispetto ai contenuti veicolati o memorizzati (temporaneamente o meno), non siano responsabili dell'illiceità di quei contenuti. In ogni caso, non appena l'operatore abbia notizia di tale illiceità, deve provvedere a rimuovere i materiali coinvolti (cfr. Trib. Grande Istance di Parigi, 20.11.2000, in *Dir. inf.*, 2001, 209, con nota di P. Costanzo). L'art. 15, infine, vieta agli Stati membri di imporre ai prestatori dei servizi di cui agli articoli 12, 13 e 14 «un obbligo generale di sorveglianza sulle informazioni che trasmettono o memorizzano [e] di ricercare attivamente fatti o circostanze che indichino la presenza di attività illecite». Tale previsione trova la sua giustificazione nell'impossibilità tecnica, avvertita soprattutto dagli operatori che forniscono più di un servizio, ovvero servizi caratterizzati dalla messa in rete in tempo reale dei materiali ricevuti dagli utenti, di realizzare un controllo preventivo sulla liceità dei contenuti. Di contro, la disposizione da ultimo citata consente agli Stati di stabilire, in sede di recepimento, «che i prestatori di servizi della società dell'informazione siano tenuti ad informare senza indugio la pubblica autorità competente di presunte attività o informazioni illecite dei destinatari dei loro servizi o a comunicare alle autorità competenti, a loro richiesta, informazioni che consentano l'identificazione dei destinatari dei loro servizi con cui hanno accordi di memorizzazione dei dati».

Sulla scorta di tali considerazioni, ed indipendentemente dalla formulazione letterale dell'art. 15 della direttiva, sembra dato ritenere che, anche in mancanza di un intervento *ad hoc* del legislatore nazionale, l'operatore incapace di fornire le informazioni utili all'identificazione dell'autore dell'illecito — informazioni che, invece, avrebbe dovuto conoscere e memorizzare per un certo periodo, stante la regola di diligenza professionale cui deve attenersi nell'esercizio della propria attività — risponda del danno che, con la sua condotta omissiva o negligente, contribuisce, se non a causare, a consolidare.

2.6.3. - *La responsabilità del «content provider»*. - Non è necessaria alcuna normativa speciale che consenta all'eventuale danneggiato di agire contro il *provider* che realizzi danni attraverso la messa in rete di propri contenuti. La direttiva 2000/31/CE, infatti, esonera da responsabilità gli operatori che forniscono servizi in Internet, ma a patto che questi non abbiamo in alcun modo inciso sui contenuti veicolati in rete o memorizzati per conto dei propri utenti. Si applicheranno, dunque, al *content provider* che abbia arrecato danni a terzi, i principi tradizionali che regolano il sistema della responsabilità aquiliana.

2.6.4. - *La responsabilità dell'«access provider»*. - Quando non sussistono i problemi tecnici, di cui si è diffusamente parlato in precedenza (v. *supra*, 2.3.), e dunque quando il danneggiato riesce, con la collaborazione del *service provider* interessato, ad individuare a quale *Ip* sia ricollegabile l'attività illecita, rimane il problema di risalire, mediante la collaborazione dell'*access provider* cui risulta intestato quell'indirizzo, dall'*Ip* all'identità reale dell'autore dell'illecito. Questa difficoltà può dipendere: 1) dalla falsa identità spesa dal cliente nel contratto con il suo *access provider*; 2) dalla mancata conservazione da parte di quest'ultimo dei registri elettronici dai quali risultano le combinazioni di *Ip* e *user ID* di volta in volta realizzate (v. *supra*, 2.3.); ovvero 3) dal fatto che mediante quel determinato *Id* possa aver agito una persona diversa dal titolare formale del contratto di accesso.

Riguardo alle prime due ipotesi, sembra lecito ritenere che — come il *service provider* (v. *supra*, 2.6.2.) — l'*access provider* sia tenuto a conservare i dati tecnici in suo possesso, quantomeno per il periodo sufficiente (bastano anche pochi giorni) a fornire all'eventuale danneggiato le informazioni necessarie a individuare il danneggiante, e debba altresì accertare l'identità dei propri clienti nel momento in cui con essi conclude contratti di accesso (cfr. RICCIO, G.M., [52], 98; *contra*, Trib. Grande Istance di Parigi, 22.5.2000, in *Gaz. Pal.*, 25.6.2000, jur., 41; Court d'Appel di Versailles, 8.6.2000, in *JCP*, éd. G 2000, act., 1412). Tali obblighi, considerato che Internet è uno strumento dalle potenzialità dannose enormi e che gli *access provider* sono, per lo più, società che svolgono tale attività a fini di lucro, scaturiscono direttamente dall'applicazione della regola di diligenza. Del resto, anche la direttiva 31/2000/Ce, al «*Considerando*» n. 48, dichiara di non voler pregiudicare «la possibilità per gli Stati membri di chiedere ai prestatori di servizi [...] di adempiere al dovere di diligenza che è ragionevole attendersi da loro ed è previsto dal diritto nazionale, al fine di individuare e prevenire alcuni tipi di attività illecite». L'utilità di un tale «richiesta» resta alquanto indecifrabile, posto che laddove esiste a livello normativo un generale dovere di diligenza da parte dei professionisti, questo deve essere rispettato indipendentemente da una sollecitazione del legislatore. Meglio allora intendere il «Considerando» in esame come un'esortazione rivolta agli Stati affinché chiariscano nel dettaglio il contenuto della clausola generale in parola.

Passando all'ultima delle tre ipotesi prospettate poc'anzi, occorre chiarire che essa può verificarsi quando uno stesso *user Id* e una stessa *password* siano utilizzati da più persone contemporaneamente (perché, ad esempio, appartenenti allo stesso nucleo familiare, alla stessa associazione, ecc.), ovvero quando essi vengano sottratti al legittimo detentore per

essere fraudolentemente utilizzati. In questi casi, ritenendo sia tenuto al risarcimento dei danni il soggetto a cui risulta intestato lo *user Id*, senza che gli sia in concreto rimproverabile alcunché, si finisce per creare una responsabilità oggettiva in capo a quest'ultimo, laddove, in alcuni casi, sarebbe preferibile che il regime fosse, al più, incentrato sull'inversione dell'onere della prova. Ciò in quanto, se nel nostro sistema civile le ipotesi di responsabilità oggettiva sono da considerarsi eccezionali, non è agevole crearne di nuove senza indagarne i fondamenti concettuali. Si potrebbe, allora, pensare di giustificare l'imputazione della responsabilità in capo al titolare dello *user Id* in virtù della presunta pericolosità dell'attività di navigazione in rete ovvero dello strumento utilizzato (il *computer* collegato alla rete tramite *modem* e *provider*). A ben vedere, non appare corretto applicare la tradizionale categoria della pericolosità ad attività e strumenti che, solo in un'accezione molto lata del termine, possono ritenersi pericolosi e che, inoltre, sono oramai diffusissimi. Allo stesso modo, a causa della natura sostanzialmente immateriale dei beni coinvolti nella vicenda, non sembra potersi parlare di responsabilità per danni causati da cose in custodia, posto che non è dato, al titolare cui siano sottratti fraudolentemente *user Id* e *password*, o a quello il cui *login* (v. *supra*, 2.3.) sia a disposizione di tutti i componenti della famiglia, accorgersi di aver subito la sottrazione o l'uso fraudolento, prima che il fatto illecito gli sia contestato; così come non gli è dato difendere il proprio *user Id* e la propria *password* da atti di pirateria informatica a suo danno. Inoltre, va considerato che *user Id* e *password* possono essere sottratti e illecitamente utilizzati, non solo senza che il titolare se ne accorga, ma anche senza che alcunché sia a quest'ultimo imputabile. Ciò accade quando la sottrazione a fini fraudolenti sia posta in essere da un esperto informatico direttamente dai *file di log* dell'*access provider*. In questo caso, va sicuramente esclusa la responsabilità del titolare dello *user Id* perché nulla è a lui rimproverabile. Tuttavia, se si riflette sulla difficoltà (*rectius*, impossibilità) che questo soggetto incontra, una volta convenuto in giudizio, per dimostrare tal ultima circostanza, si avverte quanto la sua posizione sia delicata.

Una soluzione che potrebbe evitare al titolare dello *user Id* l'imputazione puramente oggettiva della responsabilità, ed allo stesso tempo tutelare i terzi danneggiati dall'anonimo *user* che ha utilizzato un *Id* altrui, senza gravare eccessivamente l'*access provider* interessato, sembra quella di ritenere responsabile detto titolare solo quando: 1) questi si è assunto contrattualmente, verso il proprio *access provider*, il rischio costituito dalla possibilità che, in qualunque modo, il suo *user Id* e la sua *password* siano abusivamente utilizzati da terzi, e ciò, malgrado tale contratto abbia effetto diretto soltanto tra il *client* e il *provider*; ovvero 2) manchi l'assunzione del rischio, ma il convenuto non riesca a dimostrare di non aver avuto consapevolezza della sottrazione fraudolenta e di avere un controllo assoluto su chi accede al suo computer o ai dati necessari ad ottenere l'accesso alla rete. Se, al contrario, tale sforzo probatorio andrà a buon fine, la responsabilità dovrebbe essere attribuita al *provider*, dai cui *file di log* si potrà presumere siano stati sottratti *user Id* e *password*. La presunzione a carico dell'*access provider* si giustifica in quanto questi svolge in rete un'attività ben più delicata rispetto a quella del singolo *user*, lo fa spesso per finalità imprenditoriali e dunque deve avere un'organizzazione adeguata al suo ruolo, in grado di evitare fatti di terzi a danno dei suoi clienti (v. *supra*, 2.6.).

Riassumendo, può dirsi che il danneggiato — superati i problemi di individuazione dell'*Ip* — chiederà all'*access provider* competente a quale *user Id*, al momento del compimento del fatto illecito, era stato attribuito l'*Ip* incriminato e a quale identità reale corrisponde tale *Id*. Una volta che il *provider* avrà fornito quei dati, il danneggiato dovrà avere cura di citare in giudizio il titolare dello *user id* e, quando appaia probabile che quest'ultimo si possa liberare dalla presunzione di responsabilità, lo stesso *provider*. La soluzione proposta — se pure fondata su una responsabilità oggettiva residuale del *provider*, che in definitiva viene condannato per non aver impedito l'utilizzazione abusiva del *login* — appare maggiormente rispettosa dei principi operanti nel nostro ordinamento civile rispetto a quanto lo sarebbe quella che attribuisse un'analoga responsabilità a qualunque utente o, peggio, lasciasse privo di una effettiva tutela risarcitoria il terzo danneggiato (cfr. RESPONSABILITÀ CIVILE; RESPONSABILITÀ OGGETTIVA: I- Disciplina privatistica; RESPONSABILITÀ OGGETTIVA: II- Disciplina privatistica - diritto comparato e straniero -). Essa, inoltre, non rischia di porsi in antitesi con i principi sanciti dalla direttiva 31/2000/CE, in quanto questa, come già rilevato (v. *supra*, 2.6.2.), non sottrae i *provider* agli obblighi di diligenza che spettano loro in qualità di operatori professionali, e stabilisce semplicemente che, in presenza di alcuni presupposti, per il fatto illecito degli utenti, essi non sono responsabili (cfr. PONZANELLI, G., *Verso un diritto uniforme per la responsabilità degli internet service providers?*, in *Danno e resp.*, 2002, 5). A sostegno della tesi qui formulata ed esposta, viene la *loi* 1.8.2000, n. 719 (in *Journal Officiel*, 2.8.2000, 11903), con la quale in Francia, dopo l'emanazione della direttiva europea, si è legiferato in tema di responsabilità dei prestatori di servizi in Internet, introducendo il capitolo VI nel titolo II della l. n. 86-1067 del 30.9.1986. La legge in parola, all'art. 43-10, obbliga l'*access provider* e l'*host provider* a detenere e conservare i dati che consentono di identificare i soggetti che abbiano contribuito alla creazione dei contenuti dei siti (cfr. SCHOETTL, J.E., *La nouvelle modification de la loi 30 septembre 1986 relative a la liberté de communication: dernier épisode en date d'un feuilleton constitutionelle*, in *Petites affiches*, 31.7.2000, 12).

3. - UN INVENTARIO DELLE FATTISPECIE RICORRENTI

3.1. - *Diffamazione e altre aggressioni ai diritti della personalità.* - Internet, come anticipato, consente di diffondere in pochi attimi in tutto il mondo materiali di ogni tipo. La rete delle reti si candida ad essere, dunque, tanto il più potente, quanto il più pericoloso dei mezzi di informazione e di comunicazione. Anche perché l'unico davvero globale e a disposizione di centinaia di milioni di persone. Nonché l'unico che consente, a chi abbia minime conoscenze informatiche, non solo di attingere informazioni, ma anche di fornirle. Intesa in questo senso, ogni attività compiuta sulle reti telematiche è coperta dall'art. 21 Cost. (Internet, infatti, rientra senza meno nella nozione di «ogni altro mezzo di diffusione») nonché dall'art. 10 della Convenzione Europea dei diritti dell'uomo, che garantisce «la libertà di opinione e la libertà di ricevere o comunicare le informazioni o le idee, senza ingerenze da parte di pubbliche autorità e senza frontiere» come espressioni della libera manifestazione del pensiero.

Tanto l'attività di informazione quanto quella di comunicazione sono atte a causare danni, in particolare, ai diritti della personalità. Attraverso la diffusione in rete di determinate notizie o materiali è, dunque, possibile ledere il diritto al nome, all'immagine, all'onore, alla reputazione, alla riservatezza (v. *infra*, 3.2.), all'identità personale ed all'oblio, causando al danneggiato pregiudizi di gran lunga più gravi, attese le potenzialità e i bassi costi della connessione, rispetto ai mezzi tradizionali. Ciò implica che, dal punto di vista giuridico, tutte le problematiche tradizionalmente collegate alla libertà di manifestazione del pensiero si ripropongono, riguardo ad Internet, in maniera amplificata. Tuttavia, non si avverte nessuna necessità di norme *ad hoc* che si occupino di tali questioni, in quanto esse — al di là dei profili riguardanti la responsabilità dei *provider* (v. *supra*, 2.6.), il diritto

internazionale privato e il foro territorialmente competente (v. *supra*, 2.4. e 2.5.; cfr. Cass. pen., sez. V, 17.11.2000, in *Dir. inf.*, 2001, 21) — saranno efficacemente risolte mediante l'applicazione dalle comuni regole di responsabilità civile (cfr. AA.VV., [72]).

3.2. - *La violazione della «privacy»*. - Quando ci si collega ad un sito *web*, il *browser* dell'utente invia le seguenti informazioni al *server* dal quale tale sito è gestito: 1) tipo di sistema operativo istallato sul computer; 2) tipo di *browser* che si utilizza; 3) indirizzo *Ip*; 3) data e ora correnti; 4) *file* scaricati dal sito, tempo impiegato per completare il *download* (scaricamento) e componenti *software* e *hardware* utilizzate; 5) il sito da cui l'utente proviene e cioè l'ultimo sito visitato; 6) tutte le immagini che sono state automaticamente scaricate con la pagina; 7) ogni ulteriore attività compiuta dal navigante su quel sito; 8) il collegamento sul quale si è fatto *click* in seguito. Tutte queste informazioni sono contenute, e vengono conservate per qualche tempo, nei *file di log* del *server* del sito visitato (cfr. DANDA, M., *Online senza paura*, Milano, 2001, 155). Attraverso l'uso di tecnologie elementari è possibile aggregare questi dati e ottenere in poco tempo un profilo dello *user*, che comprende le sue preferenze culturali, culinarie, sessuali, ludiche, religiose, ed altro ancora, così da ledere il suo diritto alla *privacy* (cfr. MACCABONI, G., [74]; TASSONI, G., *Il trattamento dei dati personali nel commercio elettronico*, in *Commercio elettronico*, a cura di V. Franceschelli, Milano, 2001, 455). E ciò, mentre lo sprovveduto ed ignaro navigante, che di fronte allo schermo del suo computer si sente inosservato, crede di compiere in rete scelte in assoluta libertà, in quanto coperte dall'anonimato (cfr. GIANNANTONIO, E., *Introduzione all'informatica giuridica*, Milano, 1984, 215; cfr. RODOTÀ, S., [55]).
Ulteriori motivi di preoccupazione, per la dottrina americana che si occupa della *privacy* in Internet, sono rappresentati dal numero seriale (*Processor Serial Number*, *PSN*) che dal 1999 contraddistingue ogni computer dotato di un microprocessore *Intel Pentium III* (cfr. DERY, G.M.-FOX, J.R., [68]), e dalla scarsa segretezza della posta elettronica (cfr. Tar Lazio, 15.11.2001, n. 9425, in *Italia Oggi*, 27.12.2001, 28). Mentre eccessivi si sono rivelati i timori riguardanti i c.d. *cookie*: *file* depositati automaticamente durante la navigazione nella memoria del computer dell'utente (che può impedirne la ricezione disattivando l'apposita funzione del suo *browser*, o rimuoverli periodicamente attraverso semplici operazioni di manutenzione) e utilizzati dai programmi di gestione dei siti per riconoscere, quando il cibernauta torna su un sito già visitato, le preferenze da questo manifestate nel caso delle precedenti visite.
I dati raccolti via Internet sono oggetto di un fiorente commercio, nel senso che ci sono società interessate ad acquistarli — per realizzare, ad esempio, statistiche utili a perfezionare le tecniche di *marketing* e le strategie imprenditoriali — e società interessate a venderli o gestirli (cfr. Giudice di Pace di Roma, 29.3.1997, in *Contratti*, 1997, 608, con nota di R. Crocitto, e in *Foro it.*, 1997, I, 2345, con nota di P. Laghezza). È evidente come in questi casi vi siano precise responsabilità degli operatori che raccolgono ed utilizzano dati senza mai chiedere il consenso né avvertire l'utente. È allo stesso modo chiaro, però, che — al di là di ogni, pur rilevante, questione relativa ai problemi di diritto internazionale privato e, dunque, di legge applicabile — non è semplice, per il soggetto interessato, dimostrare la raccolta, la manipolazione o l'utilizzazione illegittima dei propri dati, spesso conservati su supporti digitali in forma criptata e codificata. Laddove manca un rapporto evidente tra gestore del sito ed utente, la possibilità per quest'ultimo di provare l'attività illecita del primo rimane, infatti, molto remota (cfr. BERMANN, J.-MULLIGAN, D., [63]; KOSTER, E.S., [66]). Diversa si presenta la situazione quando a raccogliere, trattare ed utilizzare i dati siano operatori che con lo *user* stipulano un contratto. In questo caso, infatti, chi detiene le informazioni personali dei clienti, onde evitare responsabilità, preferirà chiedere previamente il necessario consenso al trattamento (cfr. VILIANI, S., *Strategie contrattuali del consenso al trattamento dei dati personali*, in *Riv. crit. dir. priv.*, 1999, 159; CLARIZIA, R., *Contratto informativo per l'oggetto e per il mezzo*, in *Enc. dir.*, Aggiornamento II, Milano, 1998, 245).
La normativa italiana in materia di documento elettronico prevede esplicitamente l'applicazione delle norme a tutela della *privacy*, tanto in tema di misure di sicurezza per l'utilizzo dei documenti informatici (art. 3, 4° comma, d.P.R. 10.11.1997, n. 513, in *G.U.*, 13.3.1998, n. 60, recante criteri e modalità per la formazione, l'archiviazione e la trasmissione di documenti, con strumenti informatici e telematici; ora abrogato dall'art. 77, 2° comma, d.P.R. 28.12.2000, n. 445, in *G.U.*, 20.2.2001, n. 42, Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa) quanto a proposito degli obblighi delle autorità di certificazione (art. 9, 2° comma, lett. f), d.P.R. n. 513/1997, cit.; ora art. 28(R), 2° comma, lett. f, d.P.R. n. 445/2000, cit.). Tali richiami paiono, in verità, superflui atteso che l'art. 1 l. 31.12.1996, n. 675 (in *G.U.*, 8.1.1997, n. 5, suppl. ord.), c.d. legge sulla *privacy*, manifesta chiaramente la volontà di tutelare ogni trattamento di dati personali, effettuato con qualsiasi mezzo e da chiunque, nel territorio dello Stato (cfr. GIANNANTONIO, E., *Responsabilità civile e trattamento dei dati personali*, in *Dir. inf.*, 1999, 1035; BUTTARELLI, G., [57]; MAGLIO, M., [62]; FRANCHESCELLI, V., [60]; GRIPPO, V., [61]; CIACCI, G., [64]). Il responsabile del trattamento che violi la legge 675/96 è soggetto, ai sensi dell'art. 18, al regime di responsabilità di cui all'art. 2050 c.c. per cui, al fine di liberarsi dall'obbligo risarcitorio, dovrà dimostrare «di avere adottato tutte le misure idonee a evitare il danno». A fronte della prospettata parvenza di responsabilità semi-oggettiva, va qui segnalato come il non lieve onere di dimostrare il nesso causale tra danno e trattamento spetti al titolare dei dati personali. Nel tentativo di integrare, sebbene soltanto parzialmente, i contenuti del suddetto obbligo di correttezza, l'art. 15 prevede che «i dati personali oggetto del trattamento devono essere custoditi e controllati, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta».

3.3. - *«Download» di software difettoso e responsabilità del fornitore*. - Navigando su Internet è frequente incontrare siti nei quali è possibile scaricare (*to download*) ogni tipo di programma o applicazione che, in alcuni casi, provocano agli elaboratori perdite di dati o disfunzioni di altro genere (cfr. MC JOHN, S.M., *The Paradoxes of Free Software*, 9 *George Mason Law Review* 25, 2000). Le tutele dell'utente di fronte ad un prodotto difettoso, acquistato o scaricato gratuitamente, che arrechi danno al proprio sistema, non si possono fermare alla riduzione del prezzo o alla risoluzione del contratto, garantite dall'art. 1492 c.c.; il danno, infatti, non consiste soltanto nel cattivo acquisto, ma si estende alle conseguenze dannose cagionate dal prodotto acquistato, così come previsto dall'art. 1494, comma 2°, c.c. Fuori dall'ipotesi in cui vi sia responsabilità contrattuale del venditore, il soggetto danneggiato — nel caso in cui, ad esempio, abbia scaricato il *software* gratuitamente e in mancanza di un contratto — ha la possibilità di esperire il rimedio extracontrattuale, previsto dall'art. 2043 c.c., per azionare il quale, tuttavia, egli ha l'onere di provare tutti gli ele-

menti del fatto dannoso. Considerando il *software* come prodotto, è inoltre possibile prospettare l'applicazione del d.P.R. 24.5.1988, n. 224 (in *G.U.*, 23.6.1988, n. 146, suppl. ord.) — emanato in attuazione della direttiva 85/374/CEE — che pone, in capo al produttore, e in alcuni casi al distributore o al rivenditore al dettaglio una responsabilità c.d. oggettiva per i danni causati dal prodotto difettoso.

3.4. - *La responsabilità dei certificatori e dei titolari di firma digitale*. - Ipotesi particolari di fatto illecito, ricollegabili all'evoluzione delle nuove tecnologie informatiche, sono quelle che fanno capo ai certificatori e ai titolari di firma digitale. Per la definizione legislativa di firma digitale, v. l'art. 1, 1° comma, lett. b, d.P.R. 513/97 cit., nonché gli artt. 1(R), lett. n), 23(R) e 24(R), d.P.R. n. 445/2000 (cfr. CIACCI, G., *La firma digitale*, Milano, 1999; ROGNETTA, G., *La firma digitale e il documento informatico*, Napoli, 1999; SORRENTINO, F., *Firma digitale e firma elettronica: stato attuale e prospettive di riforma*, Milano, 2000; ZAGAMI, R., *Firma digitale e sicurezza giuridica*, Padova, 2000). I certificatori sono quei soggetti qualificati che conservano e gestiscono i registri di chiavi pubbliche, garantendo, tra l'altro, la corrispondenza biunivoca tra chiave pubblica e soggetto a cui essa appartiene, l'identità del titolare stesso, la sussistenza di eventuali poteri di rappresentanza o di altri titoli relativi all'attività professionale o a cariche rivestite, nonché il periodo di validità della chiave, il termine di scadenza del certificato, ed i suoi limiti di utilizzo (cfr. art. 11, d.P.C.M. 8.2.1999, in *G.U.*, 15.4.1999, n. 87; nonché artt. 22(R), lett. f), e 28(R), 2° comma, d.P.R. n. 445/2000). Poiché si tratta di attività destinata a garantire il corretto funzionamento del sistema, la legge richiede particolari requisiti per poterla svolgere (v. art. 27(R), d.P.R. n. 445/2000); tale attività è, peraltro, sottoposta alla l. n. 675/1996 (v. *supra*, 3.2.).

Per quanto concerne i profili di responsabilità, va detto che, mentre nei confronti dei soggetti richiedenti o titolari di firma il certificatore assume una responsabilità contrattuale, nei confronti dei terzi la negligente tenuta dei registri, o il mancato rispetto degli altri obblighi che deve rispettare, sono per lui fonte di responsabilità extracontrattuale (cfr. GRANIERI, M., *La responsabilità del certificatore nella disciplina della firma digitale*, in *Danno e resp.*, 1998, 513; v. altresì FIRMA DIGITALE - dir. civ. -). A tal proposito, occorre precisare che, quando il certificatore cagioni un danno violando direttamente obblighi di legge, per il danneggiato non è necessario dimostrarne la colpa, poiché tale condotta costituisce di per sé valido titolo di imputazione della responsabilità ai sensi dell'art. 28(R), d.P.R. n. 445/2000. E ciò, malgrado la direttiva del 13.12.1999 n. 1999/93/CE (in *G.U.C.E.*, L 13, 19.1.2000), «relativa ad un quadro comunitario per le firme elettroniche», all'art. 6 consenta al certificatore di liberarsi da responsabilità dimostrando di non essere stato negligente ed inoltre permetta allo stesso di inserire nel certificato qualificato i limiti di utilizzazione dello stesso. Tornando alla normativa italiana, al fine di completare il quadro, bisogna distinguere la responsabilità aquiliana del certificatore da quella di chi utilizza la firma digitale. Infatti, mentre — come detto — il primo risponde nei confronti dei terzi del proprio inadempimento a precisi obblighi di legge e, più in generale, della mancata corrispondenza alla realtà di tutti i dati contenuti nei certificati; il titolare di una coppia di chiavi è sempre responsabile dei danni derivanti dalla falsificazione della propria firma digitale, in quanto egli deve «conservare con la massima diligenza la chiave privata e il dispositivo che la contiene [nonché le informazioni di abilitazione all'uso della chiave privata] al fine di garantirne l'integrità e la massima riservatezza», e in più deve «richiedere immediatamente la revoca delle certificazioni relative alle chiavi contenute in dispositivi di firma di cui abbia perduto il possesso o difettosi» (art. 8, 4° comma, allegato tecnico al d.P.C.M. 8.2.1999, cit.). Quest'ultimo, dunque, non risponde delle obbligazioni nascenti dal contratto informatico siglato attraverso l'utilizzazione fraudolenta della sua firma digitale, ma risponde in via extracontrattuale del danno cagionato al terzo che ha confidato nella validità di tale contratto (ROMANO, U., *Firma digitale*, in *Dig. civ.*, Aggiornamento, Torino, 2000, 392-393).

3.5. - *La responsabilità dei c.d. istituti di moneta elettronica*. - Uno dei principali ostacoli al definitivo decollo del commercio elettronico è costituito dalla mancanza di sicurezza dei pagamenti effettuati in rete (cfr. FINOCCHIARO, G., *Il problema dei mezzi di pagamento*, in [10], 105; ROTUNNO, C., *Gli strumenti di pagamento*, in [17], 449; DE GRAZIA, L.M.-TAGLIAFERRI, M., *I mezzi di pagamento*, in [20], 129). Gli strumenti ad oggi utilizzabili per effettuare tali pagamenti possono, per comodità espositiva, essere classificati in tre categorie: 1) trasferimento elettronico di fondi mediante documento informatico siglato con firma digitale (art. 14 d.P.R. N. 513/1987); 2) accesso a distanza a proprie disponibilità esistenti su un conto, intrattenuto presso un depositario, tramite carta di credito tradizionale, conto corrente postale, bonifico bancario o contrassegno; 3) moneta elettronica. Le uniche forme di pagamento realmente innovative sono quelle rientranti in tal ultima categoria; su di esse è, dunque, opportuno svolgere qualche breve considerazione (per gli opportuni approfondimenti v. MONETA ELETTRONICA).

Per moneta elettronica, ai sensi dell'art. 1, 3° comma, lett. b), della direttiva 2000/46/CE del 18.9.2000 (in *G.U.C.E.*, L 275, 27.10.2000) — riguardante l'avvio, l'esercizio e la vigilanza prudenziale dell'attività degli istituti di moneta elettronica — 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». Gli istituti di moneta elettronica sono, dunque, soggetti che mettono sul mercato titoli di credito atipici destinati a circolare o a essere utilizzati in rete, secondo le peculiarità tecniche del sistema di volta in volta adottato (cfr. art. 1, 3° comma, lett. a), direttiva 2000/46/CE, cit.). L'operazione di pagamento mediante moneta elettronica funziona, per lo più, su base triangolare, in quanto l'istituto emittente *online* verifica i codici criptati della moneta spesa dal consumatore e certifica la bontà del pagamento al venditore, o al prestatore di un servizio a pagamento, mentre un apposito *software* scarica la somma spesa dalla disponibilità totale del consumatore. Nella fattispecie, vengono in rilievo almeno tre profili di responsabilità: il primo concerne il caso del consumatore che ha acquistato il titolo e, per avventura, non riesce ad utilizzarlo in quanto difettoso; il secondo afferisce al rapporto tra emittente ed operatore convenzionato, nell'*ambito* del quale possono sorgere problemi quando, ad esempio, a fronte dell'utilizzazione legittima del titolo da parte dello *user*, l'emittente si rifiuti di corrispondere quanto dovuto al venditore; ed il terzo riguarda il caso in cui il venditore o il prestatore di un servizio a pagamento, pur avendo concluso la convenzione con l'emittente, non accetti la moneta in parola. Tali questioni appaiono analoghe a quelle sollevate, nelle medesime circostanze, dalla carta di credito tradizionale, per cui si applicheranno i medesimi principi giuridici. Caso diverso è quello che si verifica quanto la carta di pagamento sia utilizzata da altri fraudolentemente; circostanza nella quale, ai sensi dell'art. 8, 2° comma, d. legisl. n. 185/99, l'istituto di emissione deve riaccreditare al consumatore i pagamenti che questi dimostra non essere a lui addebitabili (fatta salva l'applicazione dell'art. 12 , d. l. 3.5.1991, n. 143, convertito con modificazioni in l. 5.7.1991, n. 197), ma avrà, poi, in presenza di determinate circostanze, il diritto di addebitare

tali somme al fornitore del servizio o al venditore. Dunque, il rischio, in caso di frode, viene assunto dalle imprese di vendita a distanza, cui spetta un'azione risarcitoria nei confronti dell'autore della frode. Tuttavia, se il titolare del conto non denuncia l'indebita sottrazione dei suoi fondi, dovrà sopportare la perdita.

3.6. - *Violazione di proprietà intellettuale, industriale e segni distintivi altrui: in particolare il «cybersquatting» (o «domain grabbing»).* - Tra le pratiche illecite che è possibile compiere in Internet, un ruolo di primo piano hanno quelle volte a violare altrui diritti di privativa. In rete, infatti, sia per ragioni tecniche (non è facile distinguere l'originale dalla copia, manca il supporto, la riproduzione pirata si realizza e si distribuisce a costi bassissimi, sia per la carenza di norme adatte a disciplinare fenomeni di recente fioritura (ma in proposito cfr. la l. 18.8.2000, n. 248, in *G.U.*, 4.9.2000, n. 206, recante nuove norme di tutela del diritto d'autore; nonché la direttiva 2001/29/CE del 22.5.2001, in *G.U.C.E.*, L 167, 22.6.2001, sull'armonizzazione di taluni aspetti del diritto d'autore e dei diritti connessi nella società dell'informazione; per la legislazione statunitense, v. il *Digital Millennium Copyright Act*, cit., *supra*, 2.6.2.), risulta operazione semplice violare, tanto la proprietà intellettuale su brani musicali (cfr. PICKERING, L.-PAEZ, M.F., [88]; PASCUZZI, G., [89]), testi scritti, opere letterarie, immagini, *software* (cfr. CHIMIENTI, L., *La tutela del software nel diritto d'autore*, II ed., Milano, 2000; DE SANTIS, G., *La tutela giuridica del software tra brevetto e diritto d'autore*, Milano, 2000) opere multimediali (NIVARRA, L., [76]) e banche dati (cfr. MANSANI, L., [75]; AUTELITANO, F., [81]), quanto la proprietà industriale e gli altrui segni distintivi (cfr. PALAZZOLO, A.-TRIPODI, E.M., *Privative industriali, nomi di dominio, concorrenza, pubblicità on line*, in [17], 321; FIMIANI, C., [97]). Preferendo, per motivi di sintesi, non affrontare in questa sede tutte le problematiche ora elencate, si rinvia, per i relativi approfondimenti, ai lavori citati in questo paragrafo e nella sezione bibliografica. Sembra opportuno, invece, nell'economia della presente riflessione, svolgere alcune brevi considerazioni sui c.d. nomi di dominio (*domain name*).

I nomi di dominio non vengono decisi o scelti arbitrariamente dagli utenti, ma sono assegnati da apposite autorità, le quali per lo più accolgono il principio del «*first come, first served*», e dunque assegnano un determinato nome al primo in ordine di tempo che lo richiede (v. *supra*, 1.2.; cfr. COSTANZO, P., *Internet (diritto pubblico)*, in *Dig. Pubbl.*, Aggiornamento, Torino, 2000, 354). Poiché nel mondo virtuale un dominio, che è destinato a svolgere in rete la stessa funzione del marchio o dell'insegna, può essere assegnato una sola volta, marchi che nel mondo reale sono usati, con ricadute geografiche diverse, senza problemi, nel ciberspazio entrano in conflitto (cfr. PASCUZZI, G., [15], 536). La situazione è stata in questi anni aggravata dalla condotta di alcuni operatori che si sono affrettati a registrare presso le autorità competenti uno o più (c'è chi ha effettuato anche decine di migliaia di registrazioni) *domain name* corrispondenti a nomi di personaggi più o meno noti, ovvero a segni distintivi legittimamente utilizzati da altri. Questa pratica di accaparramento è definita *cybersquatting* o *domain grabbing* (per un tentativo di distinzione, v. CASSANO, G., [106]). In relazione a tali questioni, mentre la giurisprudenza di merito dominante in Italia — considerando il nome di dominio un segno distintivo atipico, e negando che l'attribuzione dell'autorità preposta possa fungere da elemento scriminante — applica la normativa a tutela dei segni distintivi e quella sulla concorrenza sleale; alcune pronunce hanno affermato che ai *domain name* sono applicabili esclusivamente le regole tecniche di *naming* (così Trib. di Firenze, sez. dist. di Empoli, ordinanza 23.11.2000, in *Disciplina comm.*, 2001, 280; Trib. Firenze, ordinanza 29.6.2000, in *Dir. inf.*, 2000, 675, con nota di P. Sammarco; cfr. Trib. Bari, 24 luglio 1996, in *Foro it.*, 1997, I, 2316, con nota di F. Cosentino). Parzialmente diversa si presenta la fattispecie quando, a seguito della registrazione abusiva, il sito recante tale nome di dominio non sia stato attivato. Non sembra, infine, configurabile una responsabilità dei *provider* che ospitano il sito individuato dal nome di dominio abusivo; salvo che questi, una volta che abbiano avuto notizia certa di tale abusività, non si attivino, per quanto è nelle loro possibilità, al fine di impedire che gli effetti dannosi derivanti dalla illecita registrazione si protraggano oltre (cfr. SAMMARCO, P., [53]). Per gli opportuni approfondimenti, cfr. AMBROSINI, A., [96]; ZICCARDI, G.-VITIELLO, P., [105]; VARÌ, P., [108]. Per una rassegna della giurisprudenza, v. GALLI, C., *I domain names nella giurisprudenza*, Milano, 2001. Per un tentativo italiano di regolamentare la materia, v. il disegno di l. A.S. n. 4594, presentato nella XIII Legislatura (cfr. SCIAUDONE, R., *Il disegno di legge sulla regolamentazione dei nomi a dominio su Internet*, in *Giust. civ.*, 2000, 493).

3.7. - *Il «deep-» e «surface-linking».* - Il valore commerciale di un sito dipende dal numero di accessi che esso può vantare; ciò in quanto, più naviganti transitano sulle pagine del sito in questione, più gli spazi pubblicitari (c.d. *banner*) da questo offerti risulteranno ambiti e redditizi. Il contatore di accessi è normalmente posto nella *home page* di ogni sito; questa è strutturata come una *directory* generale che offre la mappa del sito e la possibilità di raggiungere con un semplice *clic* le pagine interne. Sulla *home page* si concentra il maggior numero di *banner*, proprio perché essa, per sua natura, è destinata ad essere visitata da tutti gli *user* interessati ai materiali contenuti nel sito. Con la locuzione *deep-linking* si fa riferimento ad una diffusa pratica consistente nell'inserire nelle pagine del proprio sito *web* collegamenti ipertestuali (c.d. *link*) volti ad indirizzare e trasportare i navigatori della rete direttamente alle pagine interne di un altro sito senza passare per la *home page* di quest'ultimo e senza rendere manifesto tale trasferimento. Dal *deep-linking* occorre distinguere il *surface-linking* che si ha quando il trasferimento avviene da un sito all'altro senza però eludere la *home page* del sito verso il quale il navigante è veicolato.

La liceità della pratiche in parola va indagata tenendo presente che gli utenti, in mancanza delle dovute avvertenze, possono essere indotti a ritenere che la pagina, il servizio o la notizia a cui accedono attraverso il *link* siano forniti direttamente dal sito che lo ha predisposto, e comunque, in ogni caso, dopo il primo accesso possono preferire raggiungere i materiali di proprio interesse tramite quest'ultimo piuttosto che tramite il sito che li offre. Ciò consente di ritenere che il *deep-linking* sia idoneo a generare confusione e sviamento di clientela, ed in più che esso rappresenti un ingiusto e grave approfittamento dell'attività del sito di destinazione (art. 2598, n. 1 e 3, c.c.), oltre che un modo per sopprimere il marchio altrui sul prodotto messo in rete in violazione dell'art. 12 l.m., norma che sembra potersi applicare alla fattispecie per analogia (cfr. TOSI, E., *Le responsabilità civili*, in [10], 272; TONTODONATO, I.A., [102]). Un discorso diverso va fatto per il *surface-linking*, perché tale pratica consente la piena identificazione del titolare del sito di destinazione e dunque, quando l'informazione relativa al trasferimento sia corretta, non genera problemi di confusione e sviamento. Al contrario, la possibilità di configurare un approfittamento parassitario non sembra potersi escludere *a priori* e va, dunque, valutata di volta in volta in concreto. Sempre con riferimento al *surface-linking*, giova evidenziare che — se si rifiuta la tesi a tenore della quale ogni sito presente in Internet si offre consapevolmente ed implicitamente a tale attività (c.d. *implied license to link theory*) — esso potrebbe, al pari del *deep-linking*, essere ritenuto illecito anche sotto il profilo della violazione della proprietà industriale ed intellettuale altrui. In ogni caso, va ribadito il diritto per ogni sito

di vietare espressamente, mediante un avviso ben visibile in rete, l'attività di *linking* a suo carico. A causa del vuoto normativo e della mancanza di certezze in materia, al fine di evitare controversie, negli Stati Uniti è ormai invalsa la prassi di utilizzare appositi contratti aventi ad oggetto la licenza e le condizioni di utilizzo di *link* (c.d. *web-linking agreement*).

3.8. - *Il «framing»*. - Con il termine *framing* si fa riferimento ad un'ipotesi particolare di *linking*. La particolarità sta nel fatto che il sito contenente il *link*, non solo consente agli utenti di accedere alle pagine interne di un altro sito, ma visualizza tali pagine all'interno di una cornice (*frame*) sulla quale sono riprodotti i *banner* costituenti i suoi sponsor. Addirittura esistono siti, c.d. *framer*, che non offrono contenuti propri e che fungono soltanto da cornice di pagine altrui. Anche quando il *framing* metta in rilievo la fonte dell'informazione incorniciata ovvero sia posto in essere senza eludere l'*home page* del sito di destinazione, l'esistenza della cornice potrebbe indurre gli utenti a credere nell'esistenza di una associazione tra i due siti determinando così un rischio sviamento più alto rispetto al semplice *linking*. La pratica in parola, inoltre, integra certamente uno sfruttamento parassitario dell'attività del sito che fornisce involontariamente i contenuti alla cornice (questa è stata la conclusione a cui, nel primo caso giurisprudenziale italiano, è giunto Trib. Genova, ordinanza 22.12.2000, in *Dir. inf.*, 2001, 529). Ci sono, in definitiva, tutti gli estremi per affermare che il *framing* — salvo il caso in cui sia consentito da un precedente accordo tra i gestori dei siti interessati — viola sempre l'art. 2598 c.c., in quanto contrario ai principi di correttezza professionale e di leale concorrenza tra imprese, nonché l'art. 12 l.m. (v. *supra*, 3.7.), ed eventualmente le norme a tutela del diritto d'autore e delle banche dati.

3.9. - *I «meta tag»*. - I c.d. *meta-tag* possono essere considerati dei marcatori elettronici. Loro funzione precipua è quella di abbinare ad ogni pagina *web* una o più parole chiave, codificate in linguaggio HTML (v. *supra*, 1.2.) nei *file* sorgenti di programmazione di ogni pagina, in modo tale che non siano visibili all'utente e dunque operino come fossero un'etichetta nascosta. Queste parole interagiscono con i programmi automatici usati da alcuni motori di ricerca (servizi *online* che permettono agli utenti, digitando in un apposito spazio parole indicative dei propri interessi, di ottenere un elenco di indirizzi di pagine *web* che soddisfano la ricerca; cfr. ORLANDI, M., [78]), in quanto questi ultimi, una volta ricevuta una richiesta contenente una determinata parola, per offrire all'utente una risposta completa (che viene data in forma di *link*), cercano tra le prime parole dei siti conosciuti dal sistema, ovvero — laddove ci siano siti che utilizzano *meta-tag* — tra le parole usate come etichetta nascosta. I *meta-tag*, dunque, sono strumenti utili, tanto per i gestori dei siti, i quali desiderano evitare che le proprie pagine *web* non vengano rintracciate dai motori di ricerca soltanto perché i primi termini che compaiono sul singolo sito non sono evocative del contenuto, quanto per gli utenti, la cui ricerca, quando le etichette nascoste siano utilizzate correttamente, si rivela più proficua (cfr. CHINNOCK, A.S., [91]).
Dal punto di vista giuridico, la liceità dei *meta-tag* deve essere valutata dapprima in termini generali e poi in concreto. Ciò in quanto, si è sostenuto che l'uso di tali etichette potrebbe ritenersi in contrasto con l'art. 4, 1° comma, d. legisl. 25.1.1992, n. 74 (in *G.U.*, 13.2.1992, n. 36, suppl. ord.), che vieta la pubblicità nascosta (cfr. PEYRON, L., [92]). Non così, tuttavia, se si osserva che, quando l'uso delle parole chiave sia corretto, la funzione svolta dai *meta-tag* è sostanzialmente tecnica, si esaurisce nel rapporto con il motore di ricerca, e non è, per sua natura, adatta ad incidere, né direttamente, né indirettamente, sulla psiche del consumatore-navigatore. Diversa si presenta la situazione quando, da una valutazione in concreto, appaia che le etichette elettroniche nascoste vengono usate a fini confusori o ingannevoli, il che accade, ad esempio, quando il gestore del sito, invece che usare parole evocative dei propri contenuti curando di rispettare il marchio altrui e di evitare di confondere prima il motore di ricerca e poi gli utenti, appositamente si avvale di termini adatti a sfruttare passivamente la notorietà di un'impresa concorrente o di un certo personaggio (cfr. PRESSON, T.F.-BARNEY, J.R., [93]; MONAGAN, T., [107]). Tale condotta — i cui effetti possono essere molto gravi, considerando anche che non esistono limiti al numero di parole che un *meta-tag* può contenere — è certamente censurabile, a seconda dei casi, come violazione del marchio altrui e/o concorrenza sleale (cfr. GALBRAITH, C.D., [98]; TOSI, E., [103]; WARNER, J.R., [104]), ovvero come diffamazione, sfruttamento parassitario della notorietà altrui o altro fatto illecito. Per il primo caso giurisprudenziale italiano, che ha visto condannare l'utilizzatore dei *meta-tag* per concorrenza sleale, v. Trib. Roma, 18.1.2001, in *Corr. giur.*, 2001, 1087, con nota di G. Cassano, e in *Dir. inf.*, 2001, 551, con nota di P. Sammarco; v. anche Trib. Rovereto, 2.2.2001, in *Giur. merito*, 2001, II, 405, che ha ritenuto integri il reato di turbata libertà dell'industria o del commercio (art. 513 c.p.) la condotta di chi utilizza come *meta-tag* parole direttamente riferibili ad un'altra impresa, così «sfruttando la notorietà commerciale e la diffusione del prodotto concorrente».

3.10. - *Lo «spamming»*. - Lo *spamming* rappresenta una forma di pubblicità particolarmente invasiva che viene realizzata facendo pervenire nelle caselle postali elettroniche (*e-mail*) degli utenti di Internet messaggi promozionali da questi non richiesti e non voluti. Il vantaggio dello *spamming*, rispetto alla pubblicità effettuata tramite posta tradizionale, è rappresentato dai bassissimi costi, visto che non ci sono spese di carta, stampa, spedizione, consegna e quant'altro. In più, nel caso dello *spamming*, le spese maggiori sono sopportate dal *provider* che fornisce il servizio di posta elettronica, il quale deve inviare una gran quantità di messaggi a destinatari diversi, e dai titolari dei *box e-mail*, il cui collegamento alla rete risulta più lungo a causa dello scaricamento della pubblicità non voluta.
Negli Stati Uniti, lo *spamming* è avversato dai più, ma difeso da alcuni autori in nome della libertà di espressione e della libertà di iniziativa economica (cfr. GRAYDON, S.M., [69]). A fronte delle diverse pronunce che hanno condannato gli autori di tale forma di pubblicità, non si registra ancora un intervento legislativo federale volto a vietare l'attività in parola, mentre le leggi statali sul tema sono state ripetutamente dichiarate incostituzionali perché intervengono in materia di commercio interstatale, di competenza federale (NESPOR, S.-DE CESARIS, A.L., [25], 315).
In Europa, lo *spamming* è stato oggetto delle direttive 97/7/CE e 97/66/CE, per quanto riguarda il consenso dei destinatari a forme di comunicazione commerciale non sollecitate, nonché, da ultimo, della citata direttiva 2000/31/CE. Questa autorizza gli Stati a sottoporre a vincoli e limiti l'invio di posta elettronica contenente informazioni commerciali non sollecitate; mentre, agli Stati che non vogliano impedire tale pratica, essa impone di incoraggiare appropriate iniziative di filtraggio, rendere chiaramente identificabili le *e-mail* in questione e impedire che ci siano costi supplementari di comunicazione per il destinatario (v. il considerando n. 30 e l'art. 7, 1° comma). Infine, la direttiva prevede che, negli Stati dove lo *spamming* non è vietato, vengano predisposti «registri negativi» in cui possano iscriversi le persone fisiche che non desiderano ricevere tali comunicazioni commerciali; gli operatori interessati devono rispettare la volontà manifestata dai privati iscritti in tali registri (v. il «*Considerando*» n. 31 e l'art. 7, 2° comma). In

Italia, una soluzione a questi problemi, formulata con specifico riferimento alle «chiamate indesiderate», si trova nell'art. 10, d. legisl. 13.5.1998, n. 171 (in *G.U.*, 3.6.1998, n. 127) — recante disposizioni in materia di tutela della vita privata nel settore delle telecomunicazioni, in attuazione della direttiva 97/66/CE, ed in tema di attività giornalistica — il quale consente l'invio di materiale pubblicitario, senza intervento di un operatore o del *telefax*, solo con il consenso espresso del destinatario (cfr. anche l'art. 10, 1° comma, d. legisl. n. 185/1999). Del resto, già l'art. 13, lett. e), l. n. 675/1996, attribuisce all'interessato il diritto di opporsi al trattamento di dati personali per l'invio di materiale pubblicitario. In sintonia con tali principi sono le norme di buon uso dei servizi di rete (c.d. *Netiquette*) — emanate dalla *Naming Authority* italiana (che riprendono e sintetizzano le «*Netiquette guidelines*» valide a livello internazionale, pubblicate *online* all'indirizzo «*ftp://ftp.nic.it/rcf/ rcf1855.txt*») —, le quali, nella versione 2001, al punto 8, vietano l'invio, tramite posta elettronica, di messaggi pubblicitari o comunicazioni non sollecitati. Per l'illiceità di qualsiasi invio generalizzato di *e-mail*, v. la decisione adottata in data 11.1.2001 dal Garante per la protezione dei dati personali (in *Dir. Inf.*, 2001, 27).

4. - Fonti normative

Si rinvia alle fonti citate nel testo.

5. - Bibliografia

— Tra le opere generali che si occupano di Internet indagandone, se pure da diverse prospettive, i principali problemi giuridici, si segnalano: [1] Torrani, O.-Parise, S., *Internet e diritto*, Milano, 1997; [2] Hance, O., *Internet e la legge*, Milano, 1997; [3] Ballarino, T., *Internet nel mondo della legge*, Padova, 1998; [4] Ciampi, I., *Diritto e nuove tecnologie dell'informazione*, Firenze, 1998; [5] Brugaletta, F.-Landolfi, F.M., *Il diritto nel Cyberspazio*, Napoli, 1999; [6] Capolupo, S.-La Commara U., *Il commercio elettronico*, Roma, 1999; [7] Lessing, L., *Code and Other Laws of Cyberspace*, New York, 1999; [8] Nespor, S., *Internet e la legge*, I ed., Milano, 1999; [9] Sarzana Di Sant'Ippolito, C., *Profili giuridici del commercio via Internet*, Milano, 1999; [10] Tosi, E. (a cura di), *I problemi giuridici di Internet*, I ed., Milano, 1999; [11] Vaccà, C. (a cura di), *Il commercio elettronico*, Milano, 1999; [12] Wright, B.-Winn J.K., *The Law of Electronic Commerce*, New York, 1999; [13] Lemley, M.A.-Menell, P.S.-Mergers, R.P.-Samuelson, P., *Software and Internet Law*, New York, 2000; [14] Marini, L., *Il commercio elettronico*, Padova, 2000; [15] Pascuzzi, G., *Internet*, in *Dig. civ.*, Aggiornamento, Torino, 2000, 531; [16] Rognetta, G., *Il commercio elettronico*, Napoli, 2000; [17] Tripodi, E.M.-Santoro, F.-Missineo, S., *Manuale di commercio elettronico*, Milano, 2000; [18] AA.VV., *Internet e diritto. Problemi e soluzioni*, Bologna, 2001; [19] Antonucci, A., *E-Commerce. La direttiva 2000/31/CE e il quadro normativo della rete*, Milano, 2001; [20] Cassano, G. (a cura di), *Internet. Nuovi problemi e questioni controverse*, Milano, 2001; [21] Comandè, G.-Sica, S., *Il commercio elettronico. Profili giuridici*, Torino, 2001; [22] Draetta, U., *Internet e commercio elettronico. Nel diritto internazionale dei privati*, Milano, 2001; [23] Falabella, E.-Pedde, N., *Il giurista multimediale. Inquadramento giuridico, tributario e amministrativo dell'online*, Roma, 2001; [24] Giuseppini, S., *Principi di commercio elettronico*, Roma, 2001; [25] Nespor, S.-De Cesaris, A.L., *Internet e la legge*, II ed., Milano, 2001; [26] Parodi, C.-Calice, A, *Responsabilità penali e Internet*, Milano, 2001; [27] Santosuosso, G., *Il codice Internet e del commercio elettronico*, Padova, 2001; [28] Sirotti Gaudenzi, A. (a cura di), *Internet e diritto. Problemi e soluzioni*, Bologna, 2001; [29] Tosi, E. (a cura di), *I problemi giuridici di Internet*, II ed., Milano, 2001; [30] Valente, P.-Roccatagliata, F., *Internet. Aspetti giuridici e fiscali del commercio elettronico*, Novara, 2001.

— Oltre alle riflessioni tematiche contenute nelle opere sopra ricordate, v., tra gli scritti di carattere generale, sull'incrocio tra Internet e responsabilità civile: [31] Zeno-Zencovich, V., *I rapporti fra responsabilità civile e responsabilità penale nelle comunicazioni su Internet*, in *Dir. inf.*, 1999, 1049; [32] Olivier, F.-Barbry, E., *La responsabilité sur internet*, in *JCP*, 2000, 1739; [33] Peron, S., *Responsabilità extracontrattuale: problematiche giuridiche connesse all'utilizzo della rete Internet*, in *Resp. civ. prev.*, 2000, 822.

— Circa i problemi giuridici causati dalla natura extraterritoriale di Internet: [34] Lessing, L., *The Zones of Cyberspace*, 48 *Stanf. Law Rev.* 1403, 1996; [35] Müller, C.-Hengstenberg, C., *Nationale und internationale Rechtsprobleme im Internet*, in *NJW*, 1996, 1777; [36] Cerina, P., *Contraffazione di marchio sul world wide web e questioni di giurisdizione*, in *Il diritto industriale*, 1997, 299; [37] Koch, A.F., *Internet-Recht*, München, 1998, 28; [38] Picotti, L., *Profili penali delle comunicazioni illecite via Internet*, in *Dir. inf.*, 1999, 283; [39] American Bar Association (Report), *Achieving Legal and Business Order in Cyberspace: A Report on Global Jurisdiction Issues Created by the Internet*, in 55 *Bus. Law* 1801 (2000); [40] Shafer, D.P., *Canada's approach to jurisdiction over cybertorts: Braintech v. Kostiuk*, 27 *Pepper Law Review* 597 (2000); [41] Black, V.-Deturbide, M., *Braintech, Inc. v. Kostiuk: adjudicatory jurisdiction for Internet torts*, in 33 *Canadian Business Law Journal* 427 (2000); [42] Grossfeld, B., *Global accounting: Where Internet Meets Geography*, in 48 *AJCL* 261 (2000); [43] Di Ciommo, F., *Dispute sui «domain names», fatti illeciti compiuti via Internet ed inadeguatezza del criterio del «locus commissi delicti»*, in *Foro it.*, 2001, I, 2033.

— In tema di responsabilità aquiliana dei *provider*: [44] Donato, B., *La responsabilità dell'operatore di sistemi telematici*, in *Dir. inf.*, 1996, 135; [45] Franzoni, M., *La responsabilità del provider*, in *Annali it. Dir. autore*, 1997, 250; [46] Magni, S.-Spolidoro, M.S., *La responsabilità degli operatori in Internet: profili interni e internazionali*, in *Dir. inf.*, 1997, 61; [47] Troiano, O., *Gli illeciti attraverso Internet: problemi di imputazione e responsabilità*, in *Annali it. Dir. autore*, 1998, 405; [48] Di Ciommo, F., Internet, *diritti della personalità e responsabilità aquiliana del* provider, in *Danno e resp.*, 1999, 754; [49] Riccio, G.M., *La responsabilità del provider nell'esperienza francese: il caso Hallyday*, in *Dir. inf.*, 1999, 929; [50] Bugiolacchi, L., *Principi e questioni aperte in materia di responsabilità extracontrattuale dell'Internet provider. Una sintesi di diritto comparato*, in *Dir. inf.*, 2000, 829; [51] Goldstein, M.P., *Service Provider Liability for Acts Committed by Users: What You don't Know can Hurt You*, 18 *The John Marshall Journal of Computer & Information Law* 591 (2000); [52] Riccio, G.M., *Profili di responsabilità civile dell'Internet Provider*, Salerno, 2000; [53] Sammarco, P., *Assegnazione dei nomi a dominio su Internet, interferenze con il marchio, domain grabbing e responsabilità del Provider*, in *Dir. inf.*, 2000, 82; [54] Yen, A.C., *Internet Service Provider Liability for Subscriber Copyright Infringement, Enterprise Liability, and First Amendment*, in 88 *The Georgetown Law Journal* 1833 (2000).

— In tema di violazione della *privacy*, o altri diritti della personalità, tramite Internet: [55] Rodotà, S., *Tecnologie e diritti*, Bologna, 1995; [56] De Martini, C., *Telematica e diritti della persona*, in *Dir. inf.*, 1996, 847; [57] Buttarelli, G., *Banche dati e tutela della riservatezza*, Milano, 1997; [58] Comandè, G., *Privacy informatica: prospettive e pro-*

blemi, in *Danno e resp.*, 1997, 1997, 140; [59] CONIO, A., *La privacy naviga su Internet*, in *Riv. polizia loc.*, 1998, 545; [60] FRANCHESCELLI, V. (a cura di), *La tutela della privacy informatica*, Milano, 1998; [61] GRIPPO, V., *Analisi dei dati personali presenti su Internet. La legge 675/96 e le reti telematiche*, in *Riv. crit. dir. priv.*, 1998, 639; [62] MAGLIO, M., *Le misure di sicurezza nei sistemi informativi: il punto di vista di un giurista alla luce della legge sulla tutela dei dati personali*, in *Inf. e dir.*, 1998, I, 7; [63] BERMANN, J.-MULLIGAN, D., *Privacy in the digital age: work in progress (The Internet and the Law)*, in 23 *Nova Law Review* 551 (1999); [64] CIACCI, G., *Internet e diritto alla riservatezza*, in *Riv. trim. dir. proc. civ.*, 1999, 233; [65] GRIPPO, V., *Internet e dati personali*, in CLEMENTE, A., *Privacy*, Padova, 1999, 285; [66] KOSTER, E.S., *Zero privacy: personal data on the Internet*, 12 *The computer Lawyer* 10 (1999); [67] TOSI, E., *Prime osservazioni sull'applicabilità della disciplina generale della tutela dei dati personali a Internet e al commercio elettronico*, in *Dir. inf.*, 1999, 591; [68] DERY, G.M.-FOX, J.R, *Chipping Away at the Boundaries of Privacy: Intel's Pentium III Processor Serial Number and the Erosion of Fourth Amendment Privacy Expectations*, in 17 *Georgia State University Law Review* 331 (2000); [69] GRAYDON, S.M., *Much Ado About Spam: Unsolicited Advertising, the Internet, and You*, in 32 *St. Mary's Law Journal* 77, 2000; [70] LUGARESI, N., *Internet, privacy e pubblici poteri negli Stati Uniti*, Milano, 2000; [71] MEMMO, D., *La privacy informatica: linee di un percorso normativo*, in *Contratto e impr.*, 2000, 1213; [72] AA.VV., *Recent Developments in Media Law and Defamation Torts*, in 36 *Tort & Insurance Law Journal*, 431, 2001; [73] HAWKE, C.S., *Computer and Internet Use on Campus*, San Francisco, 2001; [74] MACCABONI, G., *La profilazione dell'utente telematico fra tecniche pubblicitarie* online *e tutela della privacy*, in *Dir. inf.*, 2001, 425.

Sui problemi suscitati dall'incrocio tra Internet e tutela della proprietà intellettuale: [75] MANSANI, L., *La protezione dei database in Internet*, in *Annali it. Dir. autore*, 1996, 149; [76] NIVARRA, L., *Le opere multimediali*, in *Annali it. Dir. autore*, 1996, 131; [77] AIMO, M., *Internet domain names e diritti di proprietà intellettuale sui segni distintivi: le prime decisioni italiane*, in *Contr. e impr. Europa*, 1998, 554; [78] ORLANDI, M., *Motori di ricerca e diritto d'autore*, in *Annali it. dir. autore*, 1998, 266; [79] PASCUZZI, G., *Il sampling*, in *Annali it. dir. autore*, 1998, 83; [80] SPADA, P., *La proprietà intellettuale nelle reti telematiche*, in *Riv. dir. civ.*, 1998, I, 635; [81] AUTELITANO, F., *La rilevanza delle banche dati nel sistema di «ciberlaw»*, in *Contratti*, 1999, 930; [82] MASSIMINI, A., *Cyberdiritto d'autore. Il diritto d'autore nell'era di Internet*, Napoli, 1999; [83] STABILE, S., *Internet e diritto d'autore: il cyberspace e la mondializzazione delle opere*, in *Il diritto industriale*, 1999, 87; [84] CENDALI, D.M.-FORSSANDER, C.E.-TURIELLO, R.J.Jr., *An overview of intellectual property issues relating to the Internet*, in 32 *Intellectual Property Law Review* 503 (2000); [85] KANE, M., *Copyright and the Internet: the balance between protection and encouragement*, in 22 *Jefferson Law Review* 183 (2000); [86] RICOLFI, M., *A copyright for cyberspace? The european dilemmas*, in *Annali it. Dir. autore*, 2000, 443; YEN, A.C., [54].

— In tema di riproduzione di brani musicali in rete: [87] JOLISH, B.D., *Scuttling the music pirate: protecting recordings in the age of the Internet*, in 17 *Entertainment & Sports Lawyer* 9 (1999); [88] PICKERING, L.-PAEZ, M.F., *Music on the Internet: how to minimize liability risks while benefiting from the music on the Internet*, in 55 *Bus. Law.* 409 (1999); [89] PASCUZZI, G., *Opere musicali su Internet: il formato MP3*, in *Foro it.*, 2001, IV, 102.

— Sulla tutela della proprietà industriale e sulla concorrenza sleale in Internet: [90] MAYR, S., *I domain names ed i diritti sui segni distintivi: una coesistenza problematica*, in *Annali it. Dir. autore*, 1996, V, 246; CERINA, P., [36]; [91] CHINNOCK, A.S., *Meta Tags: Another Whittle from the Stick of Trademark Protection?*, in 32 *University of California, Davis* 255 (1998); [92] PEYRON, L., *I «metatags» di Internet come nuovo mezzo di contraffazione del marchio e di pubblicità nascosta: un caso statunitense*, in *Giur. it.*, 1998, 739; [93] PRESSON, T.F.-BARNEY J.R., *Trademarks as Metatags: Infringement of Fair Use*, in 26 *AIPLA Quarterly Journal* 147 (1998); [94] CERASANI, C., *Il conflitto tra domain names e marchi di impresa nella giurisprudenza italiana*, in *Dir. comm. internaz.*, 1999, 645; [95] GAMBINO, A.M., *Il caso dei «nomi a dominio»*, in *Le nuove Res. Giurisprudenza sistematica*, fondata da W. Bigiavi, Torino, 1999; [96] AMBROSINI, A., *La tutela del nome di dominio*, Napoli, 2000; [97] FIMIANI, C., *Marchi e nomi a dominio*, in *Il diritto industriale*, 2000, 343; [98] GALBRAITH, C.D., *Electronic Billboards along the Information Superhighway: Liability under the Lanham Act for Using Trademarks to Key Internet Banner ADS*, in 41 *Boston College Law Review*, 847 (2000); [99] PALAZZOLO, A., *Il «domain name»*, in *Nuova giur. civ. comm.*, 2000, II, 167; [100] PALAZZOLO, A., *Nomi di dominio e gestione dei siti destinati al commercio elettronico*, in *Disciplina del commercio*, 2000, 15; [101] ROSSOTTO, R.-SINDICO, D., *Marchi e nomi di dominio: possibili rimedi contro i pirati cibernetici*, in *Il diritto industriale*, 2000, 132; SAMMARCO, P., [53]; [102] TONTODONATO, J.A., *Deep-linking: Sure You Can Exploit my Trademark, Weaken its Strength, and Make Yourself Money while Doing it*, 22 *Thomas Jefferson Law Review* 201 (2000); [103] TOSI, E., *Nomi di dominio e tutela dei segni distintivi in Internet tra «domain grabbing», «linking» e «meta-tag»*, *in Riv. dir. ind.*, 2000, II, 168; [104] WARNER J.R., *Trademark Infringement Online: Appropriate Federal Relief from the Illicit Use of Trademarked Material in Web Site Meta Tags*, in 22 *Thomas Jefferson Law Review* 133 (2000); [105] ZICCARDI, G.-VITIELLO, P. *La tutela giuridica del nome di dominio*, Modena, 2000; [106] CASSANO, G., *Cybersquatting*, in *Dir. inf.*, 2001, 83; [107] MONAGAN, T., *Can an Invisible Word Create Confusion? The Need for Clarity in the Law of Trademark Infringement through Internet Metatags*, in 62 *Ohio St. L. J.* 973 (2001); [108] VARÌ, P. *La natura giuridica dei nomi a dominio*, Padova, 2001.

— Per il dibattito nordamericano in tema di controllo e disciplina del fenomeno Internet: [109] GOLDSMITH, J.L., *Against Cyberanarchy*, in 65 *UCLR* 1199 (1998); [110] LEMLEY, M.A., *The Law and Economics of Internet Norms*, in 73 *Chicago-Kent Law Review* 1257 (1998); [111] SHAPIRO, A.L., *The Disappearance of Cyberspace and the Rise of Code*, in 8 *Seton Hall Constitutional Law Journal* 703 (1998); [112] LESSING, L., *The Law of the Horse: What Cyberlaw Might Teach*, in 113 *Harvard L. Rev.* 501 (1999); [113] LITAN, R.E., *Law and Policy in the Age of the Internet*, in 50 *Duke L. J.* 1045 (1999); [114] LANIN, A., *Who controls the Internet? States' Rights and the Reawakening of the Dormant Commerce Clause*, 73 *South Calif. L. Rev.* 1423 (2000); [115] SOMMER, J.H. *Against Cyberlaw*, 15 *Berkeley Technology Law Journal* 1145, 2000; [116] WEIBERG, J., *ICANN and the Problem of legitimacy*, 50 *Duke L.J.* 187 (2000); [117] WEINSTOCK, N., *Cyberspace Self-Governance: A Skeptical View from Liberal Democratic Theory*, 88 *Calif. L. Rev.* 395 (2000); [118] FRIED, C., *Perfect Freedom or Perfect Control*, 114 *Harvard L. Rev.* 606 (2000); [119] POST, D.G., *What Larry Doesn't Get: Code, Law and Liberty in Cyberspace*, 52 *Stan. L. Rev.* 1461 (2000); [120] RIBSTEIN, L.E.-KOBAYASHI, B.H., *State Regulation of Electronic Commerce*, in *Geroge Mason University*, 2001, *Law and Economics Working Paper Series* (disponibile alla pagina http://papers.ssrn.com/abstract=294466).

FRANCESCO DI CIOMMO