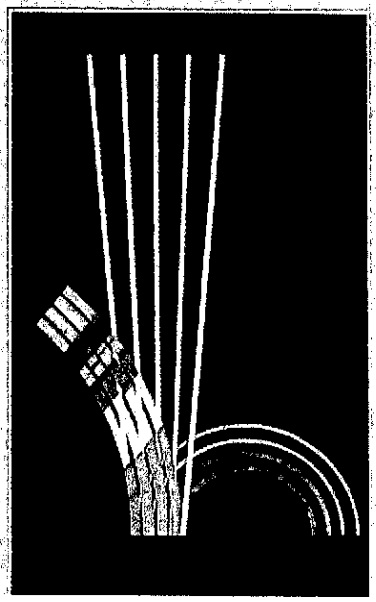
LA RESPONSABILITÀ CIVILE

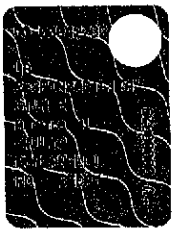
Tredici variazioni sul tema

a cura di

GIULIO PONZANELLI

Danno ambientale - Danno biologico - Danno da emotrasfusione - Danno da handicap da procreazione - Danno da computer - Responsabilità civile per [illegible]
Responsabilità civile per [illegible] - Responsabilità civile degli Stati - Danno da [illegible]
Danno da consumo di sigarette - Danno da prodotti difettosi - Responsabilità [illegible]





La responsabilità civile. Tredici variazioni sul tema, a cura di Giulio Ponzanelli

LA RESPONSABILITÀ CIVILE

Tredici variazioni sul tema

A cura di
GIULIO PONZANELLI

CEDAM
CASA EDITRICE DOTT. ANTONIO MILANI
2002

ISBN 88-13-24053-8

La Casa Editrice CEDAM S.p.A.
opera con un Sistema Qualità conforme alle norme
UNI EN ISO 9001 certificato da CISQ CERT con numero 1.354

Stampato in Italia - Printed in Italy

GRAFICHE FIORINI - VIA ALTICHIERO, 11 - VERONA

INDICE

Francesco Di Ciommo (*)

LA RESPONSABILITÀ CIVILE NELL'ERA DI INTERNET

Sommario: 1. Il diritto dell'era digitale. – 2. Internet e responsabilità civile. – 3. La difficile individuazione di chi commette fatti illeciti via Internet. – 4. L'inadeguatezza del criterio del *locus commissi delicti* per risolvere questioni di legge applicabile, giurisdizione e competenza territoriale. – 5.1. Le fattispecie di responsabilità civile più diffuse in Internet: la diffamazione *on-line*. – 5.2. (continua) La violazione della *privacy*. – 5.3. (continua) La responsabilità dei certificatori e dei titolari di firma digitale. – 5.4. (continua) La responsabilità dei c.d. istituti di moneta elettronica. – 5.5. (continua) La tutela in rete della proprietà intellettuale, industriale e dei segni distintivi dell'impresa: in particolare, il *cybersquatting* (o *domain name grabbing*). – 5.6. (continua) Il *deep-* e il *surface- linking*. – 5.7. (continua) Il *framing*. – 5.8. (continua) I *meta-tag*. – 5.9. (continua) Lo *spamming*.

1. Il diritto dell'era digitale

Non è certo scoperta dell'ultima ora che il diritto positivo – inteso come sistema di organizzazione sociale, basato su norme effettivamente esistenti ed applicate in una società, in quanto poste e fatte valere dagli organi o autorità che in tale comunità sono competenti a farlo [1] – nel tentativo di rispondere alle nuove istanze di regolamentazione, sia destinato, per sua natura, a subire frequenti

(*) Il presente scritto riproduce ed integra alcune delle riflessioni svolte dall'autore nella voce *Internet (responsabilità civile)*, attualmente in corso di pubblicazione per l'aggiornamento 2002 della Enciclopedia giuridica Treccani.

(1) Per questa definizione, v. G. Visentini, *Lezioni di teoria generale del diritto*, II ed., Padova, 2000, 18.

operazioni di *maquillage*, ed eccezionalmente, al mutare di determinate circostanze storiche, addirittura a cambiar pelle, per assicurare nel tempo la convivenza pacifica tra gli uomini. È, tuttavia, evidente come nel secolo appena trascorso, più che nei precedenti, i giuristi «abbiano dovuto [...] confrontarsi con problematiche sempre nuove, generate – con un'abbondanza forse mai conosciuta in passato – soprattutto dall'accelerazione del pensiero scientifico» ([2]). Il che ha reso, in molti casi, manifeste le difficoltà che il diritto incontra nel perseguire la propria vocazione primaria, che è quella di essere strumento efficiente di regolamentazione dei fenomeni sociali. E ciò in quanto, mentre il dato reale si evolve a ritmi sempre più sostenuti, il diritto tenta un inseguimento nel corso del quale i legislatori nazionali palesano spesso ritardi e scarse competenze specifiche.

Tra le novità, e le eredità, più importanti del XX secolo va senza dubbio registrato lo sviluppo vorticoso delle tecnologie della comunicazione a distanza: in pochi decenni, infatti, si è passati dalla scoperta del telefono a quella della radio, dalla diffusione della televisione a quella delle reti telematiche ([3]). Ognuna delle tappe di questa evoluzione si è meritata l'attenzione dei giuristi, e segnatamente dei civilisti, in quanto ha sollevato, anche nei rapporti tra i privati, problematiche nuove che il diritto non può trascurare.

Il fenomeno Internet rappresenta, in questo momento, il fronte più avanzato dello sviluppo delle tecnologie della comunicazione e, in definitiva, l'emblema stesso della società che, proprio per il *medium* che sempre più utilizza per comunicare, viene definita digitale ([4]). Tale definizione dà conto di una trasformazione epocale che il

---

([2]) Così F. DI CIOMMO, *L'informazione giuridica nell'era informatica: un* trade-off *inevitabile tra quantità e attendibilità?*, in ID. (a cura di), *Le banche di dati giuridici*, Milano, 2002, XIII.

([3]) Circa l'impatto dello sviluppo delle tecnologie della comunicazione e dell'informazione, c.d. *media*, sulla realtà socio-economica, sui comportamenti umani e sui rapporti tra individui, particolarmente interessanti sono le recenti considerazioni svolte da S. MOORES, *Il consumo dei media*, tradotto da U. Livini, Bologna, 1998; nonché da R. SILVERSTONE, *Televisione e vita quotidiana*, con traduzione di N. Rainó, Bologna, 2000.

([4]) Per definire Internet può dirsi che, dal punto di vista tecnico, esso non è una realtà fisica o tangibile, ma una rete globale che, interconnettendo un numero infinito di reti settoriali o locali, collega più computer e più *network* attraverso l'utilizzazione di

mondo progredito ha subìto negli ultimi dieci anni. Parlare di era digitale – moda oramai invalsa in ogni campo del sapere – serve ad evidenziare le radicali trasformazioni che hanno, in tale breve lasso di tempo, coinvolto il nostro modo di relazionarci con le cose, con gli eventi, con le informazioni e con gli altri ([5]). La rivoluzione in atto non trova le sue radici in movimenti culturali, filosofici o politici (sebbene, come era facile prevedere, abbia dato luogo a movimenti di tal fatta), in quanto essa è determinata, più semplicemente, dall'utilizzazione diffusa del nuovo strumento di comunicazione (il *medium*, per l'appunto) ([6]). È forse la prima volta nella storia recente dell'umanità che un'innovazione di processo influenza in modo tan-

---

protocolli comuni. Internet è dunque una "rete di reti" (questa è la definizione che ne dà la Corte Federale degli Stati Uniti – Distretto Orientale della Pensylvania, nella sentenza 11 giugno 1998, in *Dir. inf. e inform.*, 1996, 604, traduzione e nota di V. ZENO ZENCOVICH) che si avvale, al fine di trasferire fisicamente i segnali, delle tradizionali reti di telecomunicazione, e in particolare della rete telefonica. Per una recente riflessione in tema di ricadute economiche e sociali dello sviluppo delle nuove tecnologie della comunicazione e dell'informazione, v. P. GARRONE-S. MARIOTTI (a cura di), *L'economia digitale*, Bologna, 2001.

([5]) Internet ha influenzato significativamente il nostro modo di vivere. A mo' di esempio, può notarsi come chiunque oggi possa far *shopping* in giro per il mondo senza muoversi da casa. Utilizzando il *mouse* e la tastiera del computer è, infatti, semplicissimo collegarsi agli innumerevoli siti web che offrono *on-line* prodotti e servizi ed è dunque possibile, 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 del prodotto che più interessa e, qualora lo si voglia, potendo acquistare direttamente senza fare un passo fuori dal proprio salotto. Ma, 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» (così U. MINNECI-A. ALIBRANDI SCIARRONE, *Documento elettronico e contratto telematico*, in *Dig. civ.*, Aggiornamento, Torino, 2000, 344), Internet è un vero e proprio mercato delle informazioni, uno sportello di servizi sempre aperto, un luogo di incontro di amici vecchi e nuovi, una lavagna su cui scrivere quello che si vuole e leggere quello che altri hanno scritto, uno strumento per inviare e ricevere in tempo reale lettere, fotografie, grafici, materiali audio, video e quant'altro. Per gli opportuni approfondimenti e per notizie sulla genesi e sull'evoluzione di Internet, sia consentito rinviare a F. DI CIOMMO, *Internet (responsabilità civile)*, voce dell'*Encicl. giur. Treccani*, Roma, 2002; nonché a G. PASCUZZI, *Internet*, in *Dig. civ.*, Aggiornamento, Torino, 2000, 531.

([6]) Cfr. J.NAISBITT, *High Tech - High Touch*, New York, 1999; A.L. SHAPIRO, *The Control Revolution: How the Internet is Putting in the Charge and Changing the World We Know*, New York, 1999; L. PACCAGNELLA, *La comunicazione al computer*,

to diretto i comportamenti umani al punto da determinare così importanti trasformazioni culturali e sociali.

L'uso quotidiano, da parte di milioni di persone in tutto il mondo, di computer collegati alle reti locali che condividono i protocolli utilizzati in Internet ha creato le condizioni per la nascita di quella che viene definita la comunità globale o comunità cibernetica. Questa comunità è diversa da ogni altra sotto tanti punti di vista. Per prima cosa, riassumendo, può notarsi come la comunicazione in Internet non risenta delle distanze o delle barriere geografiche dato che ogni utilizzatore della rete, da qualunque parte del mondo, può comunicare con altri utenti che accedono ad Internet da qualsiasi altro luogo, o sfruttare un servizio prestato *on-line* da un server fisicamente ubicato ovunque, come se i suoi interlocutori si trovassero, in quel preciso istante, di fronte a lui ([7]). In questo senso si suole affermare che la comunicazione via Internet ha tra le sue principali caratteristiche la "globalità", in quanto coinvolge utenti di qualunque nazionalità, cultura, lingua, tradizione e religione, e la "realità", poiché consente di comunicare in tempo reale, e cioè senza tempi morti di attesa, salvo quelli eventuali che dipendono da difficoltà tecniche di collegamento o dall'eccesso di traffico sulle reti telematiche utilizzate ([8]).

La realità della comunicazione in Internet, tuttavia, a prima vista non distingue il nuovo *medium* dal telefono, dalla televisione o dalla radio. E ciò in quanto, per comprendere sino in fondo la portata in-

---

Bologna, 2000; F. RAMPINI, *Una rivoluzione in corso*, Bari, 2000; D. AMOR, *E-Business. Vivere e lavorare in un mondo interconnesso*, Milano, 2000.

([7]) Per una riflessione di qualche anno fa, ma ancora interessante ed attuale, sulla "morte" delle distanze causata dall'utilizzazione delle nuove tecnologie della comunicazione, v. R. CAIRNCROSS, *The Death of Distance: How the Communications Revolutions Will Change Our Lives*, Boston, 1997, il quale, per inciso, sembra voler evocare G. GILMORE, *The Death of Contract*, versione it., Milano, 1997.

([8]) Il termine "telematica" nasce dalla fusione della parole "telecomunicazione" e "informatica"; con esso si fa riferimento alla integrazione tecnologica che consente ai dati elaborati dai computer di essere trasferiti da un luogo fisico ad un altro, così permettendo ad elaboratori elettronici ubicati a distanza di dialogare. Cfr. G. FROSINI, *Telematica ed informatica giuridica*, in *Enc. dir.*, XLIV, Milano, 1992, 60; nonché G. RICHIERI, *Le autostrade dell'informazione*, in *Problemi dell'informazione*, 1995, 27.

novativa del fenomeno in parola, occorre far riferimento ad altre caratteristiche tecniche del *cyberspace* ([9]). In particolare, giova evidenziare come attraverso Internet possano essere trasferiti materiali di vario tipo (testi, suoni, disegni, fotografie, filmati, ecc.), circostanza questa che rende la comunicazione in rete più complessa e completa rispetto ad ogni altra forma di comunicazione a distanza sinora conosciuta ([10]). Si parla a tal proposito di "multimedialità". Inoltre, in Internet è possibile costruire spazi virtuali (c.d. siti web), che offrono servizi o prodotti perennemente a disposizione di utenti che li vogliano visitare con finalità informative, ludiche, commerciali e quant'altro ([11]). All'interno del web l'utente, sfruttando la tecnologie ipertestuale, può muoversi liberamente scegliendo cosa fare e come farlo, cosa cercare e attraverso quali traiettorie ([12]); proprio per questo la c.d. navigazione in Internet è definita "interattiva": l'utente non subisce, più o meno, passivamente la comunicazione che gli ar-

([9]) Di *cyberspace* parlò per la prima volta nel 1983 W. GIBSON – nel suo celeberrimo romanzo pubblicato in Italia con il titolo *Neuromante*, Milano, 1984 – facendo riferimento ad una realtà priva di fisicità, nel senso tradizionale del termine, perché tutta ridotta a segnali digitali.

([10]) A conferma di quanto Internet sia destinato nei prossimi anni ad invadere la nostra quotidianità, modificandola sempre più profondamente, v. il decreto del Ministero della Giustizia del 13 febbraio 2001, n. 123, in *G.U.R.I.* n. 89 del 17 aprile 2001, che rappresenta uno dei passi effettuati nel nostro ordinamento verso il c.d. processo telematico. Ad oggi manca ancora il decreto ministeriale contenente le regole tecniche operative, cosicché la data di entrata in vigore di tale nuova forma di processo, fissata originariamente per il 1° gennaio 2002, è inesorabilmente slittata; in ogni caso, la strada sembra oramai segnata. Per gli opportuni approfondimenti, tra gli altri, v. S. GATTAMELATA, *Un nuovo tassello per un processo telematico (riflessioni sul decreto del Ministero della Giustizia 13 febbraio 2001, n. 123)*, in *Nuove leggi civ. comm.*, 2001, 532.

([11]) V. sul punto la precedente nota n. 5.

([12]) Il *World Wide Web* (indicato comunemente con l'acronimo "www", o con il diminutivo "web") nasce nel 1991 come sistema 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 (*Hiper Text Transmission Protocol*), che 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, di volta in volta disponibili.

riva dal *medium*, come accade per la televisione o per la radio (almeno intese in senso tradizionale), ma muove egli stesso alla ricerca dei contenuti di cui ha bisogno e può addirittura partecipare all'offerta in rete dei contenuti considerato che è molto semplice per chiunque pubblicare (*rectius*, immettere) materiali in Internet ([13]).

Bastino, nell'impossibilità di dilungarci in questa sede sul punto, le veloci considerazioni sin qui svolte per cogliere la portata epocale dell'avvento di Internet nella nostra quotidianità. A rischio di ripeterci, giova evidenziare come oggi, ogni navigatore che trascorra anche soltanto poche ore alla settimana in rete si colloca, anche se spesso inconsapevolmente, nella società in modo nuovo rispetto al passato; cambia il suo rapporto con il tempo, con lo spazio, con le informazioni, con la propria identità nazionale, con la propria lingua, con le altre persone, con i mercati e con le cose ([14]). Parlare di svolta epocale e di nuova era non è, dunque, esagerato. Il punto per il giurista, e da qui aveva preso le mosse questa riflessione, è capire come (e se) il diritto è realmente pronto per svolgere, nei confronti del "ciberspazio", la sua funzione ordinatrice ([15]).

([13]) H.M. ENZENSBERGER nel suo ultimo libro (*Die Elixiere der Wissenschaft*, Surkamp Verlag, Frankfurt am Main, 2002), che è uscito ad aprile in Germania e presto verrà pubblicato anche in italiano (*Gli elisir della scienza*, Einaudi), dopo aver osservato che «i media giocano un ruolo centrale nella esistenza umana e il loro impressionante sviluppo porta a dei cambiamenti che nessuno può realmente prevedere», evidenzia come nell'era di Internet «la pubblicazione, nell'era gutenberghiana privilegio di pochi, diventa un diritto umano elettronico».

([14]) È stato recentemente sostenuto che nella nuova era i mercati tradizionali cederanno il passo alle reti e il diritto di proprietà sarà progressivamente sostituito dal diritto di accesso. Ciò in quanto «nella *new economy* sono le idee, i concetti, le immagini – non le cose – i componenti fondamentali del valore» (così J. RIFKIN, *L'era dell'accesso*, Milano, 2000, 6-7; cfr. K. OHMAE, *Il continente invisibile*, Roma 2001; M.A. O'ROURKE, *Property Rights and Competition on the Internet*, 16 *Berkeley Technology Law Journal* 561, 2001).

([15]) Tra le oramai numerosissime opere dedicate ai problemi giuridici di Internet, oltre a quelle citate nelle altre note, v. O. TORRANI-S. Parise, *Internet e diritto*, Milano, 1997; O. HANCE, *Internet e la legge*, Milano, 1997; I. CIAMPI, *Diritto e nuove tecnologie dell'informazione*, Firenze, 1998; S. CAPOLUPO-U. LA COMMARA, *Il commercio elettronico*, Roma, 1999; S. NESPOR, *Internet e la legge*, I ed., Milano, 1999; [9] SARZANA DI SANT'IPPOLITO, C. e F., *Profili giuridici del commercio via Internet*, Milano, 1999; C. VACCÀ (a cura di), *Il commercio elettronico*, Milano, 1999; B. WRIGHT-J.K.

La regolamentazione giuridica di Internet, oltre ad essere assai complessa, in quanto pone capo a una vasta e variegata gamma di questioni, crea problemi nuovi, e allo stato dell'arte in gran parte insuperati, ai legislatori nazionali, che pure hanno dimostrato negli ultimi anni una spiccata sensibilità a riguardo ([16]). Prima di discorrere di questioni specifiche – sulle quali verterà la parte restante del presente scritto –, occorre qui brevemente occuparsi di un argomento di teoria generale: chi è legittimato a regolare Internet, nonché ogni attività che in esso si compie, e quale efficacia sono destinate ad avere le regole eventualmente poste da un'autorità piuttosto che da un'altra?

La questione, come evidente, è nodale. Il dubbio che la alimenta dipende da un'osservazione di fondo: se Internet oggi (ma la sua posizione è destinata a consolidarsi in futuro) ([17])

WINN, *The Law of Electronic Commerce*, New York, 1999; M.A. LEMLEY-P.S. MENELL-R.P. MERGERS-P. SAMUELSON, *Software and Internet Law*, New York, 2000; L. MARINI, *Il commercio elettronico*, Padova, 2000; G. ROGNETTA, *Il commercio elettronico*, Napoli, 2000; G. COMANDÉ, *Le regole giuridiche nel commercio elettronico. Un'analisi di diritto comparato*, Pisa, 2000; AA.VV., *Internet e diritto. Problemi e soluzioni*, Bologna, 2001; A. ANTONUCCI, *E-Commerce. La direttiva 2000/31/CE e il quadro normativo della rete*, Milano, 2001; G. COMANDÉ-S. SICA, *Il commercio elettronico. Profili giuridici*, Torino, 2001; E. FALABELLA-N. PEDDE, *Il giurista multimediale. Inquadramento giuridico, tributario e amministrativo dell'online*, Roma, 2001; S. GIUSEPPINI, *Principi di Commercio Elettronico*, Roma, 2001; G. SANTOSUOSSO, *Il codice Internet e del commercio elettronico*, Padova, 2001; A. SIROTTI GAUDENZI (a cura di), *Internet e diritto. Problemi e soluzioni*, Bologna, 2001; P. VALENTE-F. ROCCATAGLIATA, *Internet. Aspetti giuridici e fiscali del commercio elettronico*, Novara, 2001.

([16]) Sull'argomento piace ricordare la bella relazione tenuta a Roma il 7 marzo 2002, presso l'Accademia dei Lincei, da Paolo Grossi. Chi scrive non è al corrente di un'eventuale pubblicazione, o diffusione mediante altre forme, della stessa.

([17]) Nell'immediato futuro si assisterà ad una convergenza verso la rete Internet di tutti i più importanti strumenti di comunicazione attualmente in uso. 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. R. PARDOLESI-A. RENDA, *Appunti di un viaggio nel capitalismo digitale: reti e retaggi culturali nel diritto antitrust*, in N. LIPARI-I. MUSU (a cura di), *La concorrenza tra economia e diritto*, Bari, 2000, 147; T.L. YARBROUGH, *Connecting the World: The Development of the Global Infromation Infrastructure*, 53 *Federal Commission Law Journal* 315 (2001); H.H. PERRITT, Jr., *Law and Information Superhighway*, II ed., Gaithersburg-New York, 2001.

proietta l'individuo in un vero e proprio spazio di nuova concezione, nel quale i confini nazionali – come meglio si vedrà nei paragrafi n. 3 e 4 – non hanno più alcun rilievo, quale legislatore nazionale o sovranazionale ha l'autorità e gli strumenti tecnici per disciplinare il nuovo fenomeno, considerato che questo è, per sua stessa natura, globale ([18])?

Nel tentativo di rispondere ai quesiti ora formulati, basta notare come tutti gli organi di governo di Internet attualmente operativi – che peraltro svolgono sostanzialmente funzioni tecniche – abbiano natura privata e siano direttamente riconducibili agli Stati Uniti, per avvertire subito quale sia il più grande problema politico e giuridico di Internet: la mancanza di rappresentatività, di legittimazione e di democrazia in chi lo dirige ([19]). Per affrontare al meglio la questione in parola, che si palesa cruciale anche nell'ottica di un delineamento dei futuri assetti giuridici di Internet, occorre svolgere un'ulteriore considerazione: ogni cambiamento dei protocolli tecnologici della rete può avvenire al di fuori di procedure formalizzate ed è in grado di produrre effetti di più forte impatto rispetto alla modifica delle regole giuridiche ([20]).

([18]) P. STANZIONE, *Commercio elettronico, contratto ed altre categorie civilistiche*, in *Dir. inf. e inform.*, 2001, 652, osserva che «[...] per la natura stessa del commercio elettronico [...] mai come in questo settore è insufficiente il ricorso alla sola normativa nazionale; laddove proprio la globalizzazione del mercato dei servizi e delle informazioni travalica lo spazio giuridico di un dato ordinamento e impone la ricerca delle norme applicabili».

([19]) Cfr. N. WEINSTOCK, *Cyberspace Self-Governance: A Skeptical View from Liberal Democratic Theory*, 88 *Calif. L. Rev.*, 395 (2000); J. WEIBERG, *ICANN and the Problem of legitimacy*, 50 *Duke L.J.* 187 (2000).

([20]) L'osservazione di L. LESSING, *Code and Other Laws of Cyberspace*, New York, 1999, 160, mette in evidenza come, mentre i legislatori municipali e, più in generale, gli ordinamenti giuridici nazionali, tardano ad attivarsi per intervenire in maniera decisa ed efficiente a regolare Internet, questo – incurante del sostanziale vuoto normativo che lo circonda – continui la sua espansione e la sua evoluzione. La situazione, così come ora descritta, riporta alla mente le parole con cui René Daumal ne *Le Mont Analogue* (Parigi, 1952; versione italiana a cura di C. Rugafiori per la collana "gli Adelphi", Milano, 1991, 139) ammonisce, nel linguaggio metaforico e simbolico che caratterizza il suo romanzo, circa i pericoli in cui incorre chi procede senza curarsi del suo procedere: «Tieni l'occhio fisso sulla via della cima, ma non dimenticare di guardare ai tuoi piedi. L'ultimo passo dipende dal primo. Non credere d'essere arrivato solo perché scorgi la cima.

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 ([21]); dall'altra quelli che invece sostengono la necessità di interventi statali ([22]), o quantomeno di una regolamentazione mista, in parte lasciata al mercato e in parte realizzata dagli Stati nazionali ([23]). 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 ([24]). Giova, in proposito, evidenziare come la direttiva europea 2000/31/CE – relativa a taluni aspetti giuridici della società dell'informazione ([25]), su cui più volte si tornerà nel corso della presente riflessione – agli artt. 16 e 17 faccia carico agli Stati di incoraggiare l'elaborazione di codici di autocondotta, peraltro senza chiarire il valore giuridico da riconoscere a tali codici, e raccomandi di non ostacolare il

---

Sorveglia i tuoi piedi, assicura il tuo prossimo passo, ma che questo non ti distragga dal fine *più alto*. Il primo passo dipende dall'ultimo».

([21]) Così A. LANIN, *Who controls the Internet? States' Rights and the Reawakening of the Dormant Commerce Clause*, 73 *South Calif. L. Rev.* 1423 (2000).

([22]) Così M.A. LEMLEY, *The Law and Economics of Internet Norms*, 73 *Chicago-Kent Law Review* 1257 (1998), il quale contesta l'efficienza in termini economici di un'autoregolamentazione di Internet; nonché J.L. GOLDSMITH, *Against Cyberanarchy*, 65 *UCLR* 1199 (1998); e A.L. SHAPIRO, *The Disappearence of Cyberspace and the Rise of Code*, 8 *Seton Hall Constitutional Law Journal* 703 (1998).

([23]) In questo senso, tra gli altri, LESSING, cit., *passim*; e R.E. LITAN, *Law and Policy in the Age of the. Internet*, 50 *Duke L.J.* 187 (2000). V. VIGORITI, *E-Commerce e tutela giurisdizionale*, in *Dir. inf. e inform.*, 2001, 669 afferma che «I problemi che in concreto si pongono vanno ovviamente risolti nell'immediatezza, e risolti con gli strumenti disponibili, da adeguare peraltro, nei limiti strutturali degli stessi, ai bisogni da soddisfare. E questo in attesa di adeguare *ex novo* le categorie, i principi, i concetti necessari alla regolamentazione dei fenomeni sostanziali. [...] Senza improbabili estremizzazioni, tipo l'evocazione di una non molto meglio precisata *lex electronica*, ma in attesa di supporti più solidi, qui fortemente necessari se si vuole utilizzare l'apparato concettuale esistente».

([24]) Cfr. J.H. SOMMER, *Against Cyberlaw*, 15 *Berkeley Technology Law Journal* 1145 (2000).

([25]) La direttiva 31/2000/CE del Parlamento europeo e del Consiglio, datata 8 giugno 2000, «relativa a taluni aspetti dei servizi della società dell'informazione, in particolare il commercio elettronico, nel mercato interno (Direttiva sul commercio elettronico)», pubblicata in *G.U.C.E.*, 17 luglio 2000, L 178/1, in Italia è ad oggi ancora inattuata.

ricorso a forme stragiudiziali di composizione delle controversie (c.d. *Alternative Dispute Resolution*, ADR) ([26]).

Al centro del dibattito dottrinale appena riassunto, un altro argomento di discussione concerne l'efficienza delle c.d. regole giuridiche di Internet. Questi i termini della questione: tra coloro i quali ritengono che un intervento legislativo eteronomo sia in ogni caso necessario, i più sostengono l'opportunità di un coordinamento tra il maggior numero possibile di legislatori nazionali, o addirittura la necessità di norme uniformi destinate a regolare il fenomeno Internet, mentre altri ritengono che sia sufficiente individuare a priori criteri precisi ed oggettivi di selezione delle norme statali di volta in volta applicabili e riconoscere maggior potere all'autonomia privata nella scelta della legge applicabile e della giurisdizione ([27]).

2. Internet e responsabilità civile

«Le c.d. autostrade telematiche 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 ([28]), dunque, che risultano maggiormente visibili quei

([26]) Sulle ADR v. M. Pierani, *La crisi del diritto internazionale privato ed i sistemi alternativi di risoluzione delle controversie on-line*, in V. Franceschelli (a cura di), *Commercio elettronico*, Milano, 2001, 591.

([27]) Tra i sostenitori di questa seconda tesi, v. L.E. Ribstein-B.H. Kobayashi, *State Regulation of Electronic Commerce*, saggio pubblicato nel 2002, dalla *George Mason University School of Law*, tra i *Law and Economics Working Paper Series*, sul sito Internet «http://papers.ssrn.com/abstract=294466», nel quale si sostiene che «regulation of electronic commerce by individual states has several advantages over federal or uniform state laws and that the problems of state regulation have been exagerated. First, state regulation provides variety, evolution and competition that is especially well suited to the dynamic nature of electronic commerce. Second, courts can minimize jurisdictional overlaps by enforcing choice-of-law and choice-of-forum contracts. Third, markets alleviate concerns that enforcing contractual choice would lead to a "race-to-the-bottom" in state Internet regulation».

([28]) Nella maggior parte degli studi sull'incrocio tra Internet e responsabilità civile

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» ([29]).

Malgrado vi siano studiosi che sostengono si possa perseguire questo risultato anche soltanto attraverso sapienti operazioni ermeneutiche compiute sui principi giuridici esistenti, basta fare un semplice inventario delle problematiche emerse negli ultimi anni nel campo della responsabilità extracontrattuale e ricollegabili ad Internet, per capire che una soluzione di tal fatta è ottimistica al punto da poter essere considerata semplicistica. Autorevole dottrina italiana, infatti, già 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» ([30]).

è stato analizzato, in particolare, il ruolo dei *provider*. Così, tra gli altri, B. DONATO, *La responsabilità dell'operatore di sistemi telematici*, in *Dir. inf. e inform.*, 1996, 135; M. FRANZONI, *La responsabilità del provider*, in *Annali it. Dir. autore*, 1997, 250; S. MAGNI-M.S. SPOLIDORO, *La responsabilità degli operatori in Internet: profili interni e internazionali*, in *Dir. inf. e inform.*, 1997, 61; O. TROIANO, *Gli illeciti attraverso Internet: problemi di imputazione e responsabilità*, in *Annali it. Dir. autore*, 1998, 405; L. BUGIOLACCHI, *Principi e questioni aperte in materia di responsabilità extracontrattuale dell'Internet provider. Una sintesi di diritto comparato*, in *Dir. inf. e inform.*, 2000, 829; M.P. GOLDSTEIN, *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); G.M. RICCIO, *Profili di responsabilità civile dell'*Internet Provider, Salerno, 2000; P. SAMMARCO, *Assegnazione dei nomi a dominio su Internet, interferenze con il marchio, domain grabbing e responsabilità del Provider*, in *Dir. inf. e inform.*, 2000, 82; A.C. YEN, *Internet Service Provider Liability for Subscriber Copyright Infringement, Enterprise Liability, and First Amendment*, 88 *The Georgetown Law Journal* 1833 (2000).

([29]) Così F. DI CIOMMO, *Profili di responsabilità del commercio elettronico*, in E.M. TRIPODI-F. SANTORO-S. MISSINEO, *Manuale di commercio elettronico*, Milano, 2000, 486, a cui, se consentito, si rinvia per ulteriori considerazioni sul punto. Cfr. STANZIONE, cit., 661, secondo il quale: «La responsabilità è il nodo cruciale per ogni tematica giuridicamente rilevante: lo è a maggior ragione per il commercio elettronico».

([30]) Così F.D. BUSNELLI, *Introduzione*, in G. ALPA (a cura di), *Computers e responsabilità civile*, Milano, 1985.

Al fine mettere in luce l'imbarazzo avvertito dall'operatore giuridico italiano che oggi si trova a dover trattare questioni pratiche riconducibili alla grande rete senza avere gli strumenti normativi adatti allo scopo, e con il proposito di offrire (se possibile) soluzioni ermeneutiche in grado, allo stato attuale, di tappare le falle che, sempre più numerose, si aprono nell'ordinamento giuridico a causa dell'evoluzione e della diffusione delle nuove tecnologie della comunicazione ([31]), nei paragrafi che seguono vengono affrontati alcuni dei tanti problemi giuridici sollevati da Internet nel campo della responsabilità aquiliana ([32]). Più in particolare: nei paragrafi n. 3 e 4 vengono affrontate questioni di carattere generale afferenti alle ricadute giuridiche della delocalizzazione delle attività svolte in rete e dell'anonimia che quest'ultima, in qualche modo, garantisce agli utenti; nei paragrafi che seguono, invece, si tenta di dare un quadro sintetico, ma tendenzialmente completo, del regime giuridico dei fatti illeciti più ricorrenti in Internet.

3. La difficile individuazione di chi commette fatti illeciti via Internet

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 nella quale la globalizzazione dei mercati, la multimedialità dell'informazione (giornalistica, culturale, ricreativa, personale o commerciale che sia) e l'abbatti-

([31]) A. Gentili, *L'inefficacia del contratto telematico*, in *Riv. dir. civ.*, 2000, I, 748, riflettendo sull'opportunità di affrontare, in tema di commercio elettronico, domande che possono apparire "premature", osserva come «poiché frattanto che si cerca è comunque necessario operare, si sente la necessità di una "morale provvisoria" *affin que je ne demeurasse point irresolu en mes actions, pendant que la raison m'obligeroit de l'estre en mes jugemens*».

([32]) In proposito, oltre alle opere citate nella nota n. 28, v. V. Zeno-Zencovich, *I rapporti fra responsabilità civile e responsabilità penale nelle comunicazioni su Internet*, in *Dir. inf. e inform.*, 1999, 1049; F. Olivier-E. Barbry, *La responsabilité sur internet*, in *JCP*, 2000, 1739; S. Peron, *Responsabilità extracontrattuale: problematiche giuridiche connesse all'utilizzo della rete Internet*, in *Resp. civ. prev.*, 2000, 822.

mento 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)» ([33]). 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. 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 ([34]).

L'irrilevanza dei confini geografici fa il paio con altre due caratteristiche della comunicazione via Internet: la "delocalizzazione" e la "dematerializzazione". 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» ([35]). La qual cosa significa, per il giurista, che l'individuazio-

([33]) Così già F. Di Ciommo, *Dispute sui «domain names», fatti illeciti compiuti via Internet ed inadeguatezza del criterio del «locus commissi delicti»*, in *Foro it.*, 2001, I, 2033.

([34]) Cfr. G. Alpa, *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.

([35]) Così P. Mathias, *La Cité Internet*, Parigi, 1997, in P. Mathias-G. Pacifici-P. Pozzi-P. Sacco, *La Polis Internet*, Milano, 2000, 27.

ne – 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.

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 dell'internazionalizzazione – delle attività compiute su Internet, parla di "*glocalization*", termine derivato dalla fusione delle parole *globalization* e *localization* ([36]).

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 efficacemente ha notato che 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» ([37]). Se è vero che l'utente, come appena

([36]) Il neologismo è stato coniato da E. SOJA, *Afterword*, 48 *Stanf. Law Rev.* 1427, 1996. Sul punto, cfr. B. GROSSFELD, *Global accounting: Where Internet Meets Geography*, 48 *AJCL* 261 (2000). In Germania considerazioni in proposito sono svolte, tra gli altri, da C. MÜLLER-HENGSTENBERG, *Nationale und internationale Rechtsprobleme in Internet*, in *NJW*, 1996, 1777; e A.F. KOCH, *Internet-Recht*, Munchen, 1998, in particolare 28.

([37]) V. in proposito le considerazione svolte da L. LESSING, *The Zones of Cyberspace*, 48 *Stanford Law Review* 1403, 1996.

ricordato, occupa un luogo fisico mentre *naviga in rete* (espressione convenzionale usata per indicare l'attività dell'utente 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 tecnologie fisicamente ubicate 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.

Inoltre, ed indipendentemente dall'ultimo problema a cui si è fatto cenno, occorre sottolineare come le difficoltà tecniche di rintracciare il luogo fisico dal quale l'autore del fatto illecito ha operato siano 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, seppure brevemente, 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 (cd. *client*). Questi, quando vogliono connettersi, lanciano, mediante segnali elettronici trasportati da linee telefoniche, tale richiesta al proprio *access provider* che, sempre servendosi delle linee telefoniche, fa, per tutto il corso della navigazione, da tramite tra essi e la rete. Il cliente, prima di ogni connessione, per farsi riconoscere dall'*access provider* digita il proprio nome di identificazione (c.d. *user Id*) e la *password* che ha ricevuto in forza della stipulazione del contratto di accesso. Il *provider*, da parte sua, ad ogni elaboratore connesso alla rete attribuisce un indirizzo, c.d. Ip (*Internet protocol*: composto da quattro serie di cifre, di quattro numeri ciascuna, tra loro divise da tre punti), che consente all'utente di navigare e, in teoria, dovrebbe permettere di individuare la paternità di tutti i segnali lanciati in rete e dunque di tutte le attività in essa realizzate dal singolo utente. Ciò in quanto, lo *user*, muovendosi tra le pagine In-

ternet, non lascia traccia del suo nome, né del suo *user Id*, bensì del suo Ip.

I problemi pratici dipendono da alcune complicazioni. 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, dal 1999, 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, 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 ([38]).

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 ([39]), il problema dell'indi-

([38]) In proposito, giova, tuttavia, ricordare che la Direttiva 2000/31/CE, cit., al considerando n. 19 afferma che «[...] il luogo di stabilimento, per le società che forniscono servizi tramite Internet, non è 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». Tale precisazione consente di ritenere che, qualora un gestore europeo di un qualunque sito Internet sia qualificabile, ai sensi dell'art. 2 della direttiva, lett. a) e b), come «prestatore di servizi della società dell'informazione», non potrà sottrarsi così facilmente all'applicazione della legge dello stato in cui esso svolge con prevalenza la sua attività economica, in quanto a nulla gli varrà ubicare all'estero la propria tecnologia di supporto del sito.

([39]) La mancanza di attendibilità dei dati in possesso degli *access provider* italiani dipende dal fatto che essi, dal 1999 – e quindi da quando decisero per motivi di *marketing* di offrire l'accesso ad Internet gratuito – consentono la stipulazione dei relativi contratti direttamente *on-line*, senza controllare l'identità reale del cliente. Chi scrive pensa che questo atteggiamento degli *access provider* italiani possa dar luogo ad ipotesi di responsabilità civile a loro carico quando il danneggiato, proprio per l'inesattezza delle informazioni comunicate dall'*access provider*, gestore dell'Ip con il quale è stato compiuto l'illecito, non riesca ad individuare l'identità del danneggiante e dunque ad

viduazione dell'autore del fatto illecito e quello della sua localizza-

ottenere il risarcimento che gli spetterebbe. Tale convincimento si basa sulle seguenti considerazioni. Gli *access provider* oggi consentono ai propri clienti, per meri motivi di strategia commerciale, di compiere in rete ogni tipo di attività garantendo loro, sostanzialmente, l'anonimato assoluto e dunque l'immunità. Così facendo, essi dimostrano di non farsi carico della circostanza per cui proprio dalla loro diligenza nel controllare gli accessi alla rete dipende la sicurezza in Internet e la responsabilizzazione degli utenti. In altre parole, in assenza di un loro controllo sull'identità degli *user* titolari di un contratto di accesso, la rete diventa realmente un *far west* dove ognuno è libero di far ciò che vuole senza rispondere delle proprie malefatte, e tuttavia gli *access provider* di tale controllo non si curano. Il legislatore comunitario, nella direttiva 31/2000, cit., si è dimostrato pienamente consapevole dell'importanza del controllo dell'identità degli utenti da parte dei *provider* ed infatti al comma 2 dell'art. 15, rubricato «Assenza dell'obbligo di sorveglianza», si legge «Gli Stati membri possono stabilire che i prestatori di servizi della società dell'informazione siano tenuti a [...] comunicare alle autorità competenti, a loro richiesta, informazioni che consentano l'identificazione dei destinatari dei loro servizi con cui hanno accordi di memorizzazione». Sembrerebbe, dunque, che della raccolta di tali informazioni l'attività degli *access provider* non possa prescindere.

Nel nostro ordinamento, il punto – anche alla luce di quanto affermato nel considerando n. 48 della direttiva – è se, in assenza di un'apposita previsione legislativa (in Italia la direttiva non è stata ancora attuata), la clausola generale di correttezza – ricavabile dall'art. 2043 (cfr., a ultimo, F. Di Ciommo, *Dovere di correttezza in ambito extracontrattuale*, in *Danno e resp.*, 2001, 1183) – possa essere sufficiente a fondare un giudizio di responsabilità, a carico di un *access provider*, per l'omesso accertamento dell'identità dei propri clienti che abbia causato ad un terzo il danno derivante dall'impossibilità di rintracciare l'autore del fatto illecito e dunque di ottenere il relativo risarcimento. In altre parole, il *provider* non verrebbe condannato per concorso con il danneggiante, bensì per un fatto autonomo e per un evento diverso dal fatto illecito. Non si tratta, dunque, nemmeno di imporre al *provider* una responsabilità oggettiva per gli illeciti realizzati dai suoi clienti; questa infatti, nel caso di specie, non avendo l'attività svolta dai *provider* caratteristiche proprie del prodotto, bensì del servizio, «non funziona perché è in grado di provocare patologie di *overdeterrence*» (così G. Ponzanelli, *Verso un diritto uniforme per la responsabilità degli internet service providers?*, in *Danno e resp.*, 2002, 5). Per l'espresso divieto di applicare ai *provider* regimi di responsabilità oggettiva, v. articoli da 12 a 15 della direttiva sul commercio elettronico.

Tornando alla domanda sopra formulata, bisogna considerare, in aggiunta a quanto già evidenziato, che proprio il codice di autoregolamentazione e di deontologia dell'ANFoV, adottato il 1° gennaio 1998, prevede al 1° comma dell'art. 6, rubricato «Responsabilità dei fornitori di accesso e di servizi», che «I fornitori di accesso e di servizi: A) accertano l'identità degli utenti e degli abbonati richiedendo l'esibizione o la produzione di copia di un documento personale, ovvero, nel caso di persone giuridiche, di documentazione idonea a comprovare il potere di rappresentanza», ed all'art. 11, rubricato "Anonimato", che «L'accesso di un utente o di un abbonato al sistema o al servizio è consentito previa identificazione iniziale dello stesso ed archiviazione e custodia dei

zione 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 l'Ip del danneggiante con la collaborazione del *service provider* che gestisce la pagina o il servizio tramite il quale il fatto illecito è stato commesso. 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 pro-*

---

relativi dai a cura del fornitore. I dati sono conservati in modo da permettere l'identificazione dei soggetti ai quali i dati si riferiscono [...]». Tale codice di autoregolamentazione non ha un valore giuridico vincolante, ma può certamente essere utilizzato dall'interprete per riempire di contenuti la clausola generale di correttezza nel momento in cui si debba vagliare la liceità del comportamento assunto dal *provider* nel singolo caso concreto. Per ulteriori considerazioni sul punto, sia consentito rinviare a DI CIOMMO, *Internet (responsabilità civile)*, cit. In tema di correttezza dei *provider*, v. da ultimo PONZANELLI, *Verso un diritto uniforme?* cit.

Val la pena, infine, notare che, in seguito all'entrata in vigore della direttiva in parola, il legislatore francese, con la *loi* 1° agosto 2000, n. 719, pubblicata in *Journal Officiel*, 2 agosto 2000, 11903, ha introdotto il capitolo VI nel titolo II della *loi* 30 settembre 1986, n. 1067, che adesso 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., sul punto, J.E. SCHOETTL, *La nouvelle modification del aloi 30 semptembre 1986 relative a la liberté de communication: dernier épisode ed date d'un feuilleton constitutionelle*, in *Petites affiches*, 31 luglio 2000, 12. È vero che l'identificazione in parola rischia di sacrificare il diritto alla *privacy on-line* degli utenti, ma ciò soltanto se non si riuscirà ad impedire che i diversi *provider* trattino e si scambino illecitamente i dati personali dei propri clienti.

vider – 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 ([40]). 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 ([41]). 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.

([40]) Ciò sempre che il *provider* in questione non svolga altrove la sua prevalente attività economica, visto che in tal caso, come già detto (v. la precedente nota n. 38), ai sensi del considerando 19 della direttiva 2000/31/CE, diverrebbe irrilevante il luogo in cui sono ubicate le tecnologie da lui utilizzate.

([41]) Cfr. sul punto C. PARODI-A. CALICE, *Responsabilità penali e Internet*, Milano, 2001, 13-35.

4. L'INADEGUATEZZA DEL CRITERIO DEL *LOCUS COMMISSI DELICTI* PER RISOLVERE QUESTIONI DI LEGGE APPLICABILE, GIURISDIZIONE E COMPETENZA TERRITORIALE

La difficoltà tecnica di individuare e localizzare chi abbia commesso un fatto illecito servendosi di Internet, considerata la vocazione sovranazionale del mezzo di comunicazione prescelto, crea questioni di diritto internazionale privato e di competenza territoriale di non poco momento ([42]).

Prendendo come riferimento la legge 31 maggio1995, n. 218, e dunque adottando una prospettiva tipicamente italiana, 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 la legge nazionale applicabile si individua in base al criterio del *locus commissi delicti*, 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 settembre 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

([42]) Diffusamente su tali problematiche, U. DRAETTA, *Internet e commercio elettronico nel diritto internazionale dei privati*, Milano, 2001.

tramite il quale l'illecito è stato realizzato. In tal caso, infatti, viene in soccorso del danneggiato il considerando 19 della citata direttiva 2000/31/CE, 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». Principio, questo, che tuttavia 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 prestatori di servizi della società dell'informazione. La direttiva, peraltro, al considerando 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 ragiona circa il luogo in cui «si è verificato l'evento», qualora si prenda come luogo di riferimento 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 egli dovrà sperare nella collaborazione dei *provider* coinvolti nella vicenda. 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, questa, ostacolata dal carattere essenzialmente immateriale del ciberspazio.

A questo punto, giova richiamare il combinato disposto degli artt. 56, della legge 21 giugno 1942, n. 929 (c.d. legge marchi), e 3, 1° comma, della già citata legge 218/95, 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 ([43]). 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 ([44]), strizzando l'occhio all'autoregolamentazione, 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 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 dell'*uploading* dei dati che hanno causato il danno ([45]).

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 relazio-

([43]) Per una recente affermazione della giurisdizione italiana in applicazione dell'art. 56 della legge marchi, v. Trib. Roma, ordinanza 9 marzo 2000, in *Foro it.*, 2000, I, 2334, con nota di G. PASCUZZI.

([44]) Cfr. T. BALLARINO, *Internet nel mondo della legge*, Padova, 1998, in particolare 224.

([45]) Sul punto, v. C. GIURDANELLA, *Problemi di giurisdizione*, in G. CASSANO (a cura di), *Internet. Nuovi problemi e questioni controverse*, Milano, 2001, 373. Cfr. il regolamento CE n. 44/2001 (in *G.U.C.E.*, 16 gennaio 2001, L 12), concernente la competenza giurisdizionale, il riconoscimento e l'esecuzione delle decisioni in materia civile e commerciale.

ne alle prime, il d. lgsl. 22 maggio 1999, n. 185 – 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 giudice del luogo di residenza o di domicilio del consumatore, se ubicati nel territorio dello Stato» ([46]). 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 a fissare – in ambito contrattuale e per fattispecie sottoposte alla legge di Stati facenti parte dell'Unione Europea – alcuni necessari punti fermi ([47]).

Svolta questa breve precisazione relativa ai contratti, è evidente come i maggiori dubbi sulla competenza territoriale dell'autorità giudiziaria per attività compiute in rete ruotino attorno ad ipotesi di fatto illecito. 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

---

([46]) Per gli opportuni approfondimenti sulla questione specifica, tra gli altri, v. G. DE MARZO, *I contratti a distanza*, Milano, 1999, 67; nonché F. DANOVI, *Il foro del consumatore nei contratti a distanza*, in *Riv. dir. proc.*, 2000, 430.

([47]) Sul punto, cfr. S. GIOVA, *La conclusione del contratto via Internet*, Napoli, 2000, 92-96.

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 e chi ritiene il contrario ([48]), 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 ([49]).

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, 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 ([50]), 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 ([51]).

La problematica in esame si palesa ancora più complessa se solo

([48]) Tra le sentenze che esprimono il primo indirizzo, v. Cass. 5 giugno 1991, n. 6381, in *Foro it.*, 1992, I, 436. Tra quelle che, invece, accolgono il secondo orientamento, v. Cass. 29 marzo 1995, n. 3733, in *Foro it.*, Rep. 1995, voce cit., n. 8.

([49]) Cfr. C. MANDRIOLI, *Diritto processuale civile*, XIII ed., vol. I, Torino, 2000, 109.

([50]) Così Trib. Lecce, sentenza 24 febbraio 2001, e Trib. Verona, ordinanza 18 dicembre 2000, entrambe in *Foro it.*, 2001, I, 2032, con nota di F. DI CIOMMO, cit.

([51]) Così v. Trib. Cagliari, ordinanza 28 febbraio 2000, in *Nuova giur. civ.*, 2000, I, 535.

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 duplice 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 ([52]). Tale precisazione consente di ritenere che, nel caso di specie, ogni tribunale italiano sia 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 *on-line* 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» ([53]).

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, tuttavia, 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 ([54]).

([52]) Per l'affermazione di questo principio, v. Cass. 28 ottobre 1997, n. 10582, in *Riv. dir. ind.*, 1998, II, 273.

([53]) Così già in DI CIOMMO, *Dispute sui «domain names», fatti illeciti compiuti via Internet ed inadeguatezza del criterio del «locus commissi delicti»*, cit., 2041.

([54]) Tale soluzione è stata adottata, da ultimo, da Trib. Napoli, sezione di Pozzuoli, ordinanza 14 giugno 2000, in *Dir. inf. e inform.*, 2001, 231, con nota di P. SAMMARCO.

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» ([55]). 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 ([56]). 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'interpreta-

([55]) Così N. NEGROPONTE, *Being Digital*, Knopf, 1995, 211.

([56]) Per una soluzione giurisprudenziale che sembra accarezzare tale prospettiva, v. Trib. Messina, 6 novembre 2000, in *Foro it.*, 2001, I, 2032, con nota di DI CIOMMO, cit.

zione 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, della legge 6 agosto 1990, n. 223 – 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.

5.1. *Le fattispecie di responsabilità civile più diffuse in Internet: la diffamazione* on-line

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 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 diffusio-

ne») 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, 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 ([57]). 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*, il diritto internazionale privato e il foro territorialmente competente (v. *supra*) – saranno efficacemente risolte mediante l'applicazione dalle comuni regole di responsabilità civile ([58]).

([57]) La giurisprudenza in proposito è già assai vasta. Tra le altre v. Trib. Teramo, 11 dicembre 1997, in *Dir. inf. e inform.*, 1998, 370, con nota di P. Costanzo, e in *Riv. dir. priv.*, 1998, 637, con nota di M. De Mari; Tribunal de Grand Istance di Parigi, 9 giugno 1998, in *Expertise*, 1998, n. 216, 319; Trib. Roma, 4 luglio 1998, in *Dir. inf. e inform.*, 1998, 807, con nota di P. Costanzo, e in *Nuova giur. civ.*, 1999, I, 399, con nota di M. Luzza; App. Parigi, 10 febbraio 1999, in *Dir. inf. e inform.*, 1999, 926, con nota di G.M. Riccio, e in *Danno e resp.*, 1999, 754, con nota di F. Di Ciommo; Tribunal de Grande Instance di Nanterre, 8 dicembre 1999, in *Dir. inf. e inform.*, 2000, 307, con nota di G.M. Riccio; Trib. Oristano, 25 maggio 2000, in *Dir. inf. e inform.*, 2000, 652, con nota di P. Costanzo; Trib. Lecce, 24 febbraio 2001, in *Foro it.*, 2001, I, 2031, con nota di Di Ciommo, cit., e in *Dir. inf. e inform.*, 2001, 721, con nota di G. Cassano e G. Sisto.

([58]) Cfr. Cass., sez. V penale, 17 novembre 2000, in *Dir. inf. e inform.*, 2001, 21. Nella dottrina nordamericana, tra le riflessioni più aggiornate e lucide, si segnalano AA.VV., *Recent Developmnentsin Media Law and Defamation Torts*, 36 *Tort & Insurance Law Journal* 431, 2001; L.B. Lidsky, *Silencing John Doe: Defamation and Discourse in Cyberspace*, 49 *Duke Law Journal* 855 (2000). Tra gli scritti italiani, v. R. Natoli, *La tutela dell'onore e della reputazione in Internet: il caso della diffamazione anonima*, in

5.2. (continua) *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; 4) data e ora correnti; 5) i *file* scaricati dal sito, il tempo impiegato per completare il *download* (scaricamento) e le componenti *software* e *hardware* utilizzate; 6) il sito da cui l'utente proviene e cioè l'ultimo sito visitato; 7) tutte le immagini che sono state automaticamente scaricate con la pagina; 8) ogni ulteriore attività compiuta dal navigante su quel sito; 9) 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 ([59]). 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* ([60]). E ciò, mentre lo sprovveduto ed ignaro *user*, 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 ([61]).

Ulteriori motivi di preoccupazione, sollevati dalla dottrina americana che si occupa della *privacy* in Internet ([62]), sono rappresentati

---

Europa e dir. priv., 2000, 441; G.M. Riccio, *La responsabilità del provider nell'esperienza francese: il caso Halliday*, in *Dir. inf. e inform.*, 1999, 929; F. Di Ciommo, Internet, *diritti della personalità e responsabilità aquiliana del* provider, in *Danno e resp.*, 1999, 754. Per considerazioni di carattere penalistico, v. C. Parodi, *I reati di ingiuria e diffamazione a mezzo Internet*, in *Dir. pen. e proc.*, 2000, 882.

([59]) Cfr. M. Danda, *Online senza paura*, Milano, 2001, 155.

([60]) Per gli opportuni approfondimenti, v., tra gli altri, G. Maccaboni, *La profilazione dell'utente telematico fra tecniche pubblicitarie* online *e tutela della privacy*, in *Dir. inf. e inform.*, 2001, 425.

([61]) Cfr. E. Giannantonio, *Introduzione all'informatica giuridica*, Milano, 1984, 215; nonché S. Rodotà, *Tecnologie e diritti*, Bologna, 1995.

([62]) Per considerazioni di ampio respiro sul punto, v. N. Lugaresi, *Internet, Privacy e pubblici poteri negli Stati Uniti*, Milano, 2000; cfr. anche E.J. Jennings, *Carnivore: US Government Surveillance of Internet Transmission*, in V. Franceschelli (a cura di), *Commercio elettronico*, cit., 463.

dal numero seriale (*Processor Serial Number*, PSN) che dal 1999 contraddistingue ogni computer dotato di un microprocessore Intel Pentium III ([63]), e dalla scarsa segretezza della posta elettronica ([64]). 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 nell'occasione precedente ([65]).

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 ([66]). 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 ([67]). È allo stesso modo

([63]) Sul punto, v. G.M. DERY-J.R. FOX, *Chipping Away at the Boundaries of Provacy: Intel's Pentium III Processor Serial Number and the Erosion of Fourth Amendment Privacy Expectations*, 17 *Georgia State University Law Review* 331 (2000).

([64]) In proposito, v. Tar Lazio, 15 novembre 2001, n. 9425, in *Italia Oggi*, 27 dicembre 2001, 28.

([65]) Per gli opportuni approfondimenti, tra le riflessioni più aggiornate si segnala quella di V. CARIDI, *La tutela dei dati personali in Internet: la questione dei* logs *e dei* cookies *alla luce delle dinamiche economiche dei dati personali*, in *Dir. inf. e inform.*, 2001, 763.

([66]) Dal punto di vista espositivo, efficace appare la ricostruzione di G. TASSONI, *Il trattamento dei dati personali nel commercio elettronico*, in FRANCESCHELLI (a cura di), *Commercio elettronico*, cit., 455, la quale individua quattro diverse categorie di operazioni di trattamento di dati personali: 1) gestione degli archivi da parte degli Internet *provider*; 2) raccolta dei c.d. *transactional data* (che ricostruiscono le connessioni telematiche di ciascun utente, nonché la durata e la frequenza di tali connessioni); 3) raccolta dei dati riguardanti un singolo individuo attraverso l'uso dei motori di ricerca messi a disposizione in rete per rintracciare materiali pubblicati in Internet; 4) ricostruzione, mediante programmi di monitoraggio, di tutti gli spostamenti effettuati da un singolo utente in rete.

([67]) Cfr. Giudice di Pace di Roma, 29 marzo 1997, in *Contratti*, 1997, 608, con nota di R. CROCITTO.

chiaro, però, che – al di là di ogni, pur rilevante, questione relativa ai problemi di diritto internazionale privato – 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 ([68]). 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 ([69]).

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 novembre 1997, n. 513, 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 dicembre 2000, n. 445, «Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa») ([70]) quanto a proposito degli

([68]) In tema, v. J. BERMANN-D. MULLIGAN, *Privacy in the Digital Age: Work in Progress (the Internet and the Law)*, 23 *Nova Law Review* 551 (1999); e E.S. KOSTER, *Zero privacy: personal data on the Internet*, 12 *The computer Lawyer* 10 (1999).

([69]) Cfr. S. VILIANI, *Strategie contrattuali del consenso al trattamento dei dati personali*, in *Riv. crit. dir. priv.*, 1999, 159; e R. CLARIZIA, *Contratto informativo per l'oggetto e per il mezzo*, in *Enc. dir.*, Aggiornamento II, Milano, 1998, 245.

Sulle modalità con cui deve essere raccolto il consenso dell'utente al trattamento dei propri dati si è espresso anche il Garante per la protezione dei dati personali, il quale, in un provvedimento del 13 gennaio 2000 (pubblicato in *Cittadini e società dell'informazione*, Bollettino del garante, n. 11-12, 2000, 52), emesso in risposta ad un quesito, ha precisato che bisogna rispettare a volontà dei cittadini e dei consumatori di accettare la cessione di dati identificativi o attinenti a gusti, preferenze o interessi per ottenere gratuitamente determinati servizi, ma ciò soltanto se gli interessati vengono messi in grado di esprimere la proprie scelte sull'uso dei dati che li riguardano in maniera consapevole e libera.

([70]) Il d.P.R. 513/97 fu pubblicato in *G.U.*, 13 marzo 1998, n. 60; il d.P.R. 445/2000 è pubblicato in *G.U.*, 20 febbraio 2001, n. 42.

obblighi delle autorità di certificazione (art. 9, 2° comma, lett. f, d.P.R. 513/97, cit.; ora art. 28(R), 2° comma, lett. f, d.P.R. 445/2000, cit.) ([71]). Tali richiami paiono, in verità, superflui atteso che l'art. 1 della legge n. 675 del 31 dicembre 1996, c.d. legge sulla *privacy*, manifesta chiaramente la volontà di tutelare ogni trattamento di dati personali, effettuato con qualsiasi mezzo e da chiunque ([72]), nel territorio dello Stato ([73]).

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 persona-

([71]) In proposito, appare utile segnalare che il 12 novembre 2001 il Parlamento europeo ha approvato a larga maggioranza in prima lettura la proposta di direttiva sulla *privacy* nelle telecomunicazioni elettroniche nell'ambito dello sviluppo del mercato interno (COM, 2000, 385, pubblicata in *G.U.C.E.*, 19 dicembre 2000, L 365).

([72]) Il legislatore italiano, con la legge n. 676 del 1996, coeva della più nota 675/96, c.d. legge sulla *privacy*, conferì al Governo, tra le altre, un'apposita delega (contenuta nell'art 1, lettera n) per l'emanazione di decreti legislativi concernenti «modalità applicative della legislazione in materia di protezione dei dati personali ai servizi di comunicazione e di informazione offerti per via telematica, individuando i titolari di trattamento di dati inerenti ai servizi accessibili al pubblico e la corrispondenza privata nonché i compiti del gestore anche in rapporto alla connessioni con resti sviluppate su base internazionale». La delega, oramai decaduta, è rimasta inattuata, cosicché oggi in Italia registriamo ancora la mancanza di norme specifiche che tutelino la *privacy* in Internet.

([73]) Tra i molti scritti in tema di applicazione della legge a tutela dei dati personali e tecnologie informatiche, si segnalano G. COMANDÉ, *Privacy informatica: prospettive e problemi*, in *Danno e resp.*, 1997, 140; G. BUTTARELLI, *Banche dati e tutela della riservatezza*, Milano, 1997; M. MAGLIO, *Le misure di sicurezza nei sistemi informativi: Il punto di vista di un giurista alla luce della legge sui dati personali*, in *Inf. e dir.*, 1998, I, 7; A. CONIO, *La privacy naviga su Internet*, in *Riv. polizia loc.*, 1998, 545; V. FRANCHESCELLI (a cura di), *La tutela della privacy informatica*, Milano, 1998; V. GRIPPO, *Analisi dei dati personali presenti su Internet. La legge 675/96 e le reti telematiche*, in *Riv. crit. dir. priv.*, 1998, 639; E. GIANNANTONIO, *Responsabilità civile e trattamento dei dati personali*, in *Dir. inf. e inform.*, 1999, 1035; E. TOSI, *Prime osservazioni sull'applicabilità della disciplina generale sulla tutela dei dati personali a internet e al commercio elettronico*, in *Dir. inf. e inform.*, 1999, 591; G. CIACCI, *Internet e diritto alla riservatezza*, in *Riv. trim. dir. e prov. civ.*, 1999, 233; D. MEMMO, *La privacy informatica: linee di un percorso normativo*, in *Contratto e impr.*, 2000, 1213.

li. 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».

5.3. (continua) *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 ([74]), si deve far riferimento all'art. 1, 1° comma, lett. b, d.P.R. 513/97 cit., nonché agli artt. 1(R), lett. n, 23(R) e 24(R), d.P.R. 445/2000 ([75]). L'ultimo intervento legislativo in materia, in Italia, è costituito dal d. lgsl. 23 gennaio 2002, n. 10, recante norme di «attuazione della direttiva 1999/93/CE relativa ad un quadro comunitario per le firme elettroniche» ([76]). La recente normativa, di derivazione comunitaria, si esprime in termini di «firma elettronica» e «firma elettronica avanzata»; in questa seconda categoria va sicuramente ricondotta la firma digitale, che rappresenta la tecnologia

([74]) Per gli opportuni approfondimenti, v., tra gli altri, i lavori monografici di G. CIACCI, *La firma digitale*, Milano, 1999; G. ROGNETTA, *La firma digitale e il documento informatico*, Napoli, 1999; F. SORRENTINO, *Firma digitale e firma elettronica: stato attuale e prospettive di riforma*, Milano, 2000; R. ZAGAMI, *Firma digitale e sicurezza giuridica*, Padova, 2000.

([75]) Il d.P.R. n. 445, approvato il 28 dicembre 2000, rappresenta il Testo Unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa. Per la pubblicazione in *G.U.*, cfr. la nota n. 70.

([76]) Il d. lgsl. n. 10/2002 è pubblicato in *G.U.* n. 39 del 15 febbraio 2002.

scelta dal legislatore italiano sin dal 1997, sebbene ad oggi non ancora a regime, per attribuire certezza circa la paternità e l'originalità dei documenti elettronici ([77]).

I certificatori abilitati ad operare in tutta Europa a seguito della direttiva ora citata sono – così come acclarato dall'art. 2, lett. b) del d. lgsl. n. 10/1999 – i soggetti «che prestano servizi di certificazione delle firme elettroniche o che forniscono altri servizi connessi alle firme elettroniche». Tra questi, vi sono alcuni operatori, dotati di particolari requisiti di ordine tecnico, nonché di solidità finanziaria e di onorabilità, che possono essere accreditati (in Italia l'accreditamento è concesso dal Dipartimento per l'innovazione e le tecnologie presso la Presidenza del Consiglio dei Ministri), ad emettere certificati qualificati idonei a consentire un più semplice e sicuro affidamento da parte degli utenti circa la paternità dell'atto e la corretta identità del soggetto autore dell'atto stesso. I certificatori di firma digitale, a cui la normativa italiana preesistente al d. lgsl. 10/2002 fa esclusivo riferimento, sono certamente da inquadrare tra questi soggetti accreditati che rilasciano certificati qualificati ([78]). Essi conservano e gestiscono i registri di chiavi pubbliche, garantendo, tra l'altro: la corri-

([77]) L'art. 6 del d. lgsl. 10/2002 fa chiarezza sul diverso valore del documento informatico, del documento siglato con firma elettronica e di quello siglato con firma digitale o con un'altra firma avanzata, sostituendo integralmente l'art. 10 del d.P.R. 28 dicembre 2000, n. 445, ora rubricato «Forma ed efficacia del documento informatico», e dunque disponendo che:

«1 - Il documento informatico ha l'efficacia probatoria prevista dall'art. 2712 del codice civile, riguardo ai fatti e alle cose rappresentate.

2 - Il documento informatico, sottoscritto con firma elettronica, soddisfa il requisito legale della forma scritta. Sul piano probatorio il documento stesso è liberamente valutabile, tenuto conto delle sue caratteristiche oggettive di qualità e sicurezza. Esso inoltre soddisfa l'obbligo previsto dagli articoli 2214 e seguenti del codice civile e da ogni altra analoga disposizione legislativa o regolamentare.

3 - Il documento informatico, quando è sottoscritto con firma digitale o con altro tipo di firma elettronica avanzata, e la firma si basa su di un certificato qualificato ed è generata mediante un dispositivo per la creazione di una firma sicura, fa inoltre piena prova, fino a querela di falso, della provenienza delle dichiarazioni da chi l'ha sottoscritto.».

([78]) Circa il valore giuridico di un documento elettronico sottoscritto con firma digitale e dunque certificata da un soggetto qualificato e accreditato, v. la nota precedente.

spondenza 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 febbraio 1999, nonché artt. 22(R), lett. f, e 28(R), 2° comma, d.P.R. 445/2000, cit.). 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. 445/2000, cit.); tale attività, come già accennato, è peraltro sottoposta alla citata legge 675/96.

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 cui è tenuto, sono per lui fonte di responsabilità extracontrattuale ([79]). A tal proposito, occorre precisare che, quando il certificatore cagioni un danno violando direttamente obblighi di legge – e cioè non riuscendo a garantire l'affidamento dei terzi così come richiesto, da ultimo, dall'art. 7 del d. lgsl 10/2002 – per il danneggiato non è necessario dimostrarne la colpa, poiché tale condotta costituisce di per sé valido titolo di imputazione della responsabilità ai sensi degli artt. 28(R) e 28-*bis*(L) del d.P.R. 45/2000. E ciò, malgrado la direttiva del 13 dicembre 1999 n. 1999/93/CE ([80]), nella sua versione originale all'art. 6, e nella sua attuazione italiana all'art. 7, consenta al certificatore di liberarsi da responsabilità dimostrando di non aver agito senza colpa ed inoltre permetta allo stesso di inserire nel certificato qualificato i limiti di utilizzazione dello stesso.

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,

([79]) Le prime considerazioni in proposito si devono a M. GRANIERI, *La responsabilità del certificatore nella disciplina della firma digitale*, in *Danno e resp.*, 1998, 513.

([80]) La direttiva è pubblicata in *G.U.C.E.*, 19 gennaio 2000, L 13.

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 citato d.p.c.m. dell'8 febbraio 1999). 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 ([81]).

5.4. (continua) *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 ([82]). Gli strumenti ad oggi utilizzabili possono, per comodità espositiva, essere classificati in tre categorie: 1) trasferimento elettronico di fondi mediante documento informatico siglato con fir-

([81]) Cfr. U. ROMANO, *Firma digitale*, in *Dig. civ.*, Aggiornamento, Torino, 2000, 392-393. Sul diverso tema della efficacia probatoria del documento elettronico, v. M. DE CATA, *Il documento elettronico e la firma digitale*, e S. MINOTTO, *Il documento elettronico nel processo civile*, entrambi in FRANCESCHELLI (a cura di), *Commercio elettronico*, cit., rispettivamente 359 e 415.

([82]) Tra gli scritti più esaurienti in materia di mezzi di pagamento del commercio elettronico, v. G. FINOCCHIARO, *Il problema dei mezzi di pagamento*, in E. TOSI (a cura di), *I Problemi Giuridici di Internet*, I ed., Milano, 1999, 105; C. ROTUNNO, *Gli strumenti di pagamento*, in TRIPODI-SANTORO-MISSINEO (a cura di), *Manuale di commercio elettronico*, cit., 449; L.M. DE GRAZIA-M. TAGLIAFERRI, *I mezzi di pagamento*, in CASSANO (a cura di), *Internet. Nuovi problemi e questioni controverse*, cit., 129; G. STUMPO, *Il quadro tecnico e normativo di riferimento degli strumenti di pagamento* on-line, in *Dir. comm. int.*, 2001, 685.

ma digitale (art. 14, d.P.R. 513/87, cit.); 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 moneta elettronica, ai sensi dell'art. 1, 3° comma, lett. b, della direttiva 2000/46/CE del 18 settembre 2000 ([83]) – 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 *on-line* verifica i codici criptati della moneta spesa dal consumatore e certifica la bontà del pagamento al venditore, 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.

([83]) La direttiva è pubblicata in *G.U.C.E.*, L 275, del 27 ottobre 2000.

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. lgsl. n. 185/99, cit., 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, del decreto legge 3 maggio 1991, n. 143, convertito con modificazioni dalla legge 5 luglio 1991, n. 197), ma avrà, poi, in presenza di determinate circostanze, il diritto di addebitare tali somme al fornitore. 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.

5.5. (continua) *La tutela in rete della proprietà intellettuale, industriale e dei segni distintivi dell'impresa: in particolare, il* cybersquatting *(o* domain name 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 ed inoltre non si svolge in luoghi fisici), sia per la carenza di norme adatte a disciplinare fenomeni di recente fioritura (ma in proposito cfr. la legge 18 agosto 2000, n. 248, recante nuove norme di tutela del diritto d'autore ([84]); nonché la direttiva 2001/29/CE del 22 maggio 2001, sull'armonizzazione di taluni aspetti del diritto d'autore e dei diritti connessi nella società dell'informazione ([85]); per la legislazione statunitense, v. il *Digital Millennium Copyright Act* del 1998, 17 *United State Code*

([84]) La legge 248/2000 è pubblicata in *G.U.*, 4 settembre 2000, n. 206.
([85]) La direttiva 2001/29/CE è pubblicata in *G.U.C.E.*, L 167, del 22 giugno 2001.

§§ 1201-1205), risulta operazione semplice violare, tanto la proprietà intellettuale su brani musicali ([86]), testi scritti, opere letterarie, immagini, software ([87]), opere multimediali ([88]), e banche dati ([89]), quanto la proprietà industriale e gli altrui segni distintivi ([90]). 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 nota. Sembra opportuno, invece, nell'economia della presente riflessione, svolgere alcune brevi considerazioni sulla vicenda giuridica dei c.d. nomi di dominio (*domain name*), questione che ha dimostrato di poter avere notevoli ricadute sugli assetti presenti e futuri del web ([91]).

([86]) Cfr. B.D. JOLISH, *Scuttling the music pirate: protecting recordings in the age of the Internet*, 17 *Enterteinment & Sports Lawyer* 9 (1999); L. PICKERING-M.F. PAEZ, *Music on the Internet: how to minimize liability risks while benefitting from the music on the Internet*, 55 *Business Law Journal* 409 (1999); nonché G. PASCUZZI, *Opere musicali su Internet: il formato MP3*, in *Foro it.*, 2001, IV, 102.

([87]) Tra le ultime opere monografiche dedicate alla problematica della tutela del software, v. L. CHIMIENTI, *La tutela del software nel diritto d'autore*, II ed., Milano, 2000; e G. DE SANTIS, *La tutela giuridica del software tra brevetto e diritto d'autore*, Milano, 2000.

([88]) In tema, v. L. NIVARRA, *Le opere multimediali*, in *Annali it. dir. autore*, 1996, 131.

([89]) Per gli opportuni approfondimenti sulla protezione delle banche di dati, v. L. MANSAWI, *La protezione dei data base in Internet*, in *Annali it. dir. autore*, 1996, 149; e F. AUTELITANO, *La rilevanza delle banche dati nel sistema di «ciberlaw»*, in *Contratti*, 1999, 930. Tra gli studi di carattere generale sul problema della tutela della proprietà intellettuale in Internet, si segnalano quelli di P. SPADA, *La proprietà intellettuale nelle reti telematiche*, in *Riv. dir. civ.*, 1998, I, 635; A. MASSIMINI, *Cyberdiritto d'autore. Il diritto d'autore nell'era di Internet*, Napoli, 1999; S. STABILE, *Internet e diritto d'autore: il cyberspace e la mondializzazione delle opere*, in *Il dir. industriale*, 1999, 87. Tra le riflessioni più interessanti condotte negli Stati Uniti sul tema in parola, v. D.M. CENDALI-C.E. FORSSANDER-R.J. TURIELLO, Jr., *An overview of intellectual property issues relating to the Internet*, 32 *Intellectual Property Law Review* 503 (2000); M. KANE, *Copyright and the Internet: the balance between protection and encouragement*, 22 *Jefferson Law Review* 183 (2000); M. RICOLFI, *A copyright for cyberspace? The european dilemmas*, in *Annali it. Dir. autore*, 2000, 443; A.C. YEN, *Internet Service Provider Liability for Subscriber Copyright Infringement, Enterprise Liability, and First Amendment*, 88 *The Georgetown Law Journal* 1833 (2000).

([90]) Cfr. A. PALAZZOLO-E.M. TRIPODI, *Privative industriali, nomi di dominio, concorrenza, pubblicità* on line, in TRIPODI-SANTORO-MISSINEO (a cura di), cit., 321; C. FIMIANI, *Marchi e nome a dominio*, in *Il dir. industriale*, 2000, 343.

([91]) Per gli opportuni approfondimenti sulle problematiche giuridiche sollevate

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 ([92]). 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 ([93]). 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 ([94]). Questa pratica di accaparramento è definita *cybersquatting* o *domain grabbing* ([95]).

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 esclu-

---

dai nomi a dominio, tra le opere più complete si segnalano A. AMBROSINI, *La tutela del nome di dominio*, Napoli, 2000; G. ZICCARDI-P. VITIELLO, *La tutela giuridica del nome di dominio*, Modena, 2000; P. VARÌ, *La natura giuridica dei nomi a dominio*, Padova, 2001. Per un'aggiornata rassegna della giurisprudenza, v. C. GALLI, *I domain names nella giurisprudenza* Milano, 2001.

([92]) È nel 1984 che 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 Names*), in quanto questi, essendo costituiti da gruppi di lettere, acronimi, nomi o parole di senso compiuto, risultano di più semplice digitazione e più facile memorizzazione per gli utenti che muovano alla ricerca di un sito o di una pagina web. Cfr. COSTANZO, P., *Internet (diritto pubblico)*, in *Dig. Pubbl.*, Aggiornamento, Torino, 2000, 354.

([93]) Per gli opportuni approfondimenti, v. G. PASCUZZI, *Internet*, cit.

([94]) Per un tentativo italiano di regolamentare la materia, v. il disegno di l. "AS n. 4594" presentato nella XIII Legislatura. Sulla questione, v. R. SCIAUDONE, *Il disegno di legge sulla regolamentazione dei nomi a dominio su Internet*, in *Giust. civ.*, 2000, 493.

([95]) Per un tentativo di distinzione, v. G. CASSANO, *Cybersquatting*, in *Dir. inf. e inform.*, 2001, 83.

sivamente le regole tecniche di *naming* ([96]). 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 ([97]).

5.6. (continua) *Il* deep- *e il* 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 di-

([96]) Così Trib. Firenze, sez. dist. di Empoli, ordinanza 23 novembre 2000, in *Disciplina comm.*, 2001, 280; Trib. Firenze, ordinanza 29 giugno 2000, in *Dir. inf. e inform.*, 2000, 675, con nota di P. SAMMARCO; cfr. Trib. Bari, 24 luglio 1996, in *Foro it.*, 1997, I, 2316, con nota di F. COSENTINO.

([97]) Cfr. P. SAMMARCO, *Assegnazione dei nomi a dominio su Internet, interferenze con il marchio,* domain grabbing *e responsabilità del provider*, in *Dir. inf. e inform.*, 2000, 82.

stinguere 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 accedere ai materiali di proprio interesse tramite quest'ultimo piuttosto che dal 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 soltanto in alcuni casi e per analogia ([98]).

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, sviamento o sottrazione di clientela. Tuttavia, anche in questo caso, 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, in presenza di determinate condizioni, 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

([98]) Cfr. E.Tosi, *Le responsabilità civili*, in Tosi (a cura di), cit., 272; J.A. Tonnodonato, *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).

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*).

5.7. (continua) *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 ([99]).

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 – violi 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., ed eventualmente le norme a tutela del diritto d'autore e delle banche dati.

([99]) Questa, del resto, è stata la conclusione a cui, nel primo caso giurisprudenziale italiano, è giunto il Trib. Genova, nell'ordinanza 22 dicembre 2000, in *Dir. inf. e inform.*, 2001, 529. In materia si annoverano oggi pronunce più recenti, v. Trib. Monza, ordinanza 14 maggio 2001, in *Corriere giur.*, 2001, 1625, con commento di S. MEANI.

5.8. (continua) *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 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 *on-line* 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), 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 ([100]).

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. lgsl. 25 gennaio 1992, n. 74, che vieta la pubblicità nascosta ([101]). 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-na-

([100]) Sul punto, cfr. A.S. CHINNOCK, *Meta Tags: Another Whittle from the Stick of Trademark Protection?*, 32 *University of California, Davis* 255 (1998).

([101]) V. L. PEYRON, *I «metatags» di Internet come nuovo mezzo di contraffazione del marchio e di pubblicità nascosta: un caso statunitense*, in *Giur. it.*, 1998, 739.

vigatore. 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 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 ([102]). 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 ([103]).

Il primo caso giurisprudenziale italiano, che ha visto condannare l'utilizzatore dei *meta-tag* per concorrenza sleale, può individuarsi nella sentenza del Tribunale di Roma, 18 gennaio 2001 ([104]). Su un'analoga questione qualche giorno dopo si è pronunciato anche il Tribunale di Rovereto, 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» ([105]).

([102]) Cfr. T.F. PRESSON-J.R. BARNEY, *Trademarks as Metatags: Infringement of Fair Use*, 26 *AIPLA Quarterly Journal* 147 (1998); T. MONAGAN, *Can an Invisible Word Create Confusion? The Need for Clarity in the Law of Trademark Infringement through Internet Metatags*, 62 *Ohio St. L. J.* 973 (2001).

([103]) Per gli opportuni approfondimenti, v. C.D. GALBRAITH, *Electronic Billboards along the Information Superhighway: Liability under the Lanham Act for Using Trademarks to Key Internet Banner ADS*, 41 *Boston College Law Review*, 847 (2000); E. TOSI, *Nomi di dominio e tutela dei segni distintivi in Internet tra "domain grabbing", "linking" e "meta-tag"*, *in Riv. dir. ind.*, 2000, II. 168; J.R. WARNER, *Trademark Infringement Online: Appropriate Federal Relief from the Illicit Use of Trademarked Material in Web Site Meta Tags*, 22 *Thomas Jefferson Law Review* 133 (2000).

([104]) La sentenza è pubblicata in *Corr. giur.*, 2001, 1087, con nota di G. CASSANO, e in *Dir. inf. e inform.*, 2001, 551, con nota di P. SAMMARCO. Cfr. la recente ordinanza dell'8 febbraio 2002 con cui il Trib. di Milano ha inibito l'utilizzazione come metatag di una "denominazione corrispondente a marchio comunitario appartenente ad altra società concorrente". Detta ordinanza, emessa in applicazione dell'art. 2598 n. 3 c.c., è pubblicata in *Guida al dir.*, 2002, n. 12, 40, con commento di E. SACCHETTINI.

([105]) Trib. Rovereto, sentenza 2 febbraio 2001, in *Giur. merito*, 2001, II, 405.

5.9. (continua) *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 una parte della dottrina in nome della libertà di espressione e della libertà di iniziativa economica ([106]). 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 ([107]).

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).

([106]) Cfr. S.M. GRAYDON, *Much Ado About Spam: Unsolicited Advertising, the Internet, and You*, 32 *St. Mary's Law Journal* 77, 2000.

([107]) S. NESPOR-A.L. DE CESARIS, *Internet e la legge*, II ed., Milano, 2001, 315.

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. lgsl. 13 maggio 1998, n. 171 ([108]) – 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. lgsl. 185/99, cit.). Del resto, già l'art. 13, lett. e, della legge 675/96, 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) ([109]), le quali, nella versione 2001, al punto 8 vietano l'invio, tramite posta elettronica, di messaggi pubblicitari o comunicazioni non sollecitati ([110]).

([108]) Il d. lgsl. 171/98 è pubblicato in *G.U.*, 3 giugno 1998, n. 127.

([109]) Le regole di Netiquette più aggiornate possono leggersi *on-line* all'indirizzo Internet «ftp://ftp.nic.it/rcf/ rcf1855.txt».

([110]) Per l'illiceità di qualsiasi invio generalizzato di e-mail, v. la decisione adottata in Italia dal Garante per la protezione dei dati personali in data 11 gennaio 2001 e pubblicata, tra l'altro, in *Dir. inf. e inform.*, 2001, 2.