SABRINA MAGNI
MARCO SAVERIO SPOLIDORO

LA RESPONSABILITÀ DEGLI OPERATORI IN INTERNET: PROFILI INTERNI E INTERNAZIONALI

1. Struttura della relazione.

È opportuno, anzitutto, illustrare il programma della nostra relazione, cioè spiegare come abbiamo deciso di organizzare l'esposizione del tema che ci è stato affidato.

Preliminare ci è sembrata una ricognizione dei comportamenti e delle fattispecie da cui potrebbe derivare una responsabilità *civile* dei vari soggetti che, a diverso titolo, partecipano ad INTERNET. Per ragioni intuibili di semplicità e chiarezza abbiamo ritenuto più conveniente adottare una prospettiva di « diritto italiano »: questa scelta infatti ci consente di avvicinarci all'oggetto della nostra indagine partendo dai concetti che sono (o dovrebbero esserci) più famigliari.

Data la natura « delocalizzata » ed « aterritoriale » di INTERNET, una prospettiva di diritto interno non è tuttavia esaustiva. Essa deve dunque essere completata da una considerazione approfondita dei problemi internazionalprivatistici posti da una realtà, come quella di INTERNET, che aspira ad abolire le distanze del mondo reale e addirittura a sostituire al mondo reale un mondo virtuale che non conosce frontiere.

Nella trattazione si è scelto di limitare l'esame alla disciplina ed ai problemi di diritto privato, trascurando i profili — peraltro assai rilevanti — di diritto penale e di diritto pubblico.

* Relazione predisposta per la giornata di studio su « Gli aspetti giuridici di INTERNET » organizzata dalla Direzione Legale IBM SEMEA S.p.A. e tenutosi a Milano il 27 novembre 1996.

2. Programma di indagine — Profili interni.

Nella prima parte della relazione forniremo dunque un primo quadro di riferimento, segnalando altresì alcuni problemi concreti, in parte già emersi nella pratica.

Senza con ciò accampare ambizioni sistematiche, ma solamente per comodità di esposizione, proponiamo di suddividere il tema in tre sezioni, delle quali (come si vedrà) due saranno trattate in modo alquanto rapido e quindi relativamente superficiale, mentre la terza richiederà qualche maggiore sviluppo.

Abbiamo pensato di dare alle tre sezioni della prima parte di relazione dei titoli che potessero in qualche modo imprimersi nella memoria: *a*) gli illeciti *di* INTERNET; *b*) gli illeciti *contro* INTERNET; *c*) gli illeciti *per mezzo* di INTERNET.

Precisiamo subito che con questi titoli vogliamo soltanto aiutarci ad organizzare un discorso abbastanza complicato ed aggiungiamo che ci rendiamo conto che essi sono per più versi imprecisi e in una certa misura fuorvianti. Fatta questa doverosa premessa, procediamo con ordine.

3. Illeciti di internet.

Parlando di « illeciti di INTERNET » intendiamo riferirci agli illeciti che potrebbero esser commessi dai soggetti che, a vario titolo, regolano l'accesso alla rete, ne definiscono i protocolli ed attribuiscono gli indirizzi IP.

In questo contesto vengono in considerazione i comportamenti abusivi eventualmente tenuti dai gestori di INTERNET i quali, per esempio, promuovano o non promuovano a *standard* del sistema determinate tecnologie di comunicazione sulla rete; oppure che rifiutino o limitino l'assegnazione di numeri o di indirizzi IP o di nomi a dominio ai *providers*.

Sempre in questo contesto può porsi il problema degli eventuali abusi dei *providers* ai danni degli utilizzatori: abusi che possono tipicamente esprimersi in comportamenti di fissazione di prezzi eccessivamente elevati o di discriminazione. Si pensi alla notizia, recentemente pubblicata dalla stampa americana (e dal sito *Cyberlex* nell'*Update 8/96*), della transazione di una controversia *antitrust* nella quale si accusava America Online di scarsa trasparenza nella comunicazione delle sue tariffe.

Anche nei rapporti fra *providers* e gestori di servizi di interconnettività tra reti possono verificarsi rifiuti di accesso o di connettività oppure imposizioni di condizioni contrattuali non eque.

Rispetto alle ipotesi fin qui formulate, il criterio di valutazione giuridica è costituito dal diritto *antitrust* e dalle norme che reprimono il fenomeno della concorrenza sleale.

Ciò che qui interessa sottolineare è che il riferimento a questi due nuclei normativi non consente di qualificare automaticamente

come illecito qualunque comportamento che, astrattamente considerato, sembrerebbe discriminatorio, predatorio o scorretto.

Ad esempio, il *provider* che praticasse condizioni inique o rifiutasse i propri servizi di connettività a determinate categorie di utilizzatori non violerebbe di per sé il diritto *antitrust*, se non fosse dimostrato che egli dispone di una posizione dominante sul mercato considerato o se, nella situazione concreta, non fosse ravvisabile l'esecuzione di un accordo restrittivo della concorrenza o di una pratica concordata. In teoria sembrerebbe più facile ipotizzare che poteri monopolistici spettino agli organismi che gestiscono il sistema di INTERNET nel suo complesso: organismi che, pertanto, potrebbero trovarsi nelle condizioni di abusare di siffatti poteri. Si pensi a ISOC, IAB, IETF, IANA, ecc.. Anche in questa prospettiva un rilevante ostacolo all'applicazione delle norme *antitrust* potrebbe tuttavia essere costituito dall'estrema fluidità ed evanescenza della struttura di INTERNET, ma soprattutto dall'assenza di criteri sicuri di imputazione dell'attività di INTERNET ai diversi soggetti che, su base volontaristica, danno vita al sistema.

Allo stesso modo, se non è impossibile, è piuttosto difficile immaginare una concreta applicazione del divieto di concorrenza sleale, giacché tale divieto presuppone che tra autore e vittima dell'illecito sussista un rapporto di concorrenza. Tuttavia, come è facile constatare tornando agli esempi formulati poc'anzi, non sempre questo rapporto ricorre, anche restando all'interno della sola categoria dei *providers* e dei gestori delle reti.

Ad ogni modo ci si può chiedere infine se, fra i soggetti di INTERNET, abbia preso corpo un gruppo di regole di correttezza, che funzionerebbe come una specie di « etica del sistema » o di « Netiquette » suscettibile in qualche modo di esser richiamata come specificazione del generale dovere di buona fede e come criterio di « ingiustizia » dei danni eventualmente arrecati ad altri operatori della rete. Ma qui si entra veramente nel regno del diritto « virtuale » e conviene pertanto arrestarsi.

4. Illeciti contro internet.

Con la rubrica « Illeciti contro INTERNET » ci riferiamo essenzialmente ad attività di utilizzatori i quali danneggino la rete ed i suoi operatori con comportamenti devianti.

Stiamo pensando ovviamente alla diffusione su INTERNET di *viruses* o di c.d. *worms*, cioè di *viruses* che non causano danni permanenti, ma provocano comunque una serie di inconvenienti per altri utenti della rete.

Basterà ricordare, al riguardo, il caso di Robert Tappan Morris, uno studente della Cornell University condannato nel 1991 in America per aver infettato con un *worm* 6.000 *computers* mentre tentava un esperimento malriuscito di dimostrare l'assoluta inaffidabilità dei sistemi adottati per impedire l'accesso non autorizzato ad INTERNET.

Alla stessa stregua occorre considerare lo *hacking*, cioè l'accesso non autorizzato alla memoria di un calcolatore, eventualmente allo scopo di commettere ulteriori violazioni, e la manipolazione non autorizzata dei dati contenuti nella memoria del *computer* (anche per inserirvi un *virus*). Anche in questo caso può essere interessante un esempio: il *New York Times* del 18 agosto 1996 (a p. 18) riferisce che uno *hacker* è riuscito a penetrare nel sito INTERNET dello *US Department of Justice*, sostituendo e spostando dati, nonché inserendovi oscenità e frasi di dileggio all'indirizzo del governo degli Stati Uniti.

Qui l'ordinamento reagisce con sanzioni penalistiche, il che si spiega abbastanza ovviamente con l'esigenza di reprimere in modo efficace comportamenti assai insidiosi, i cui responsabili — fra l'altro — possono essere scoperti (a prezzo comunque di sforzi non trascurabili) solo con i mezzi offerti dall'istruzione penale. Si pensi ad esempio che Robert Morris fu scoperto solo perché, essendogli sfuggita di mano la diffusione del suo *worm*, si confidò con un amico, la cui testimonianza fu decisiva per la sua condanna.

Ciò che tuttavia interessa al cultore del diritto privato, in questo discorso, non è tanto il fatto che il responsabile di uno dei reati previsti nella L. 23 Dicembre 1993, n. 547, sia anche tenuto al risarcimento del danno.

C'è infatti un aspetto più sottile e, forse, più inquietante. Pensiamo infatti ai principi generali in tema di responsabilità aquiliana: l'art. 2043 c.c. ci dice che chiunque abbia cagionato (o abbia concorso a cagionare) un danno con dolo o con colpa è tenuto a risarcire il danno.

Se basta la colpa, si potrà forse pensare che la diffusione di un *virus*, o di un *worm*, possa comportare la sanzione civilistica del risarcimento a carico di chi — pur senza volerlo — vi abbia negligentemente contribuito. Ricordo al riguardo che lo *standard* di diligenza varia a seconda dei tempi, dei luoghi e delle circostanze; e segnalo inoltre che almeno alcuni giuristi stranieri hanno avanzato l'idea che l'utilizzatore eticamente corretto di INTERNET avrebbe il dovere, prima di (re)immettere in rete i messaggi ricevuti o i dati elaborati con il proprio *computer*, di utilizzare i normali programmi di « disinfezione » dai *viruses* o almeno di porre in opera le stesse procedure di sicurezza da lui normalmente seguite nel *downloading* da INTERNET.

Poniamo poi, per ipotesi, che la diffusione del *virus* o del *worm* sia opera di un dipendente di un'impresa, che ha utilizzato una postazione del datore di lavoro, collegato ad INTERNET. Si può prospettare che in queste circostanze ricorra una responsabilità oggettiva del datore di lavoro, ai sensi dell'art. 2049 c.c.. Ed anche se si esclude l'applicazione di questa norma, ci si può chiedere se non sia negligente l'impresa che non adotta le misure necessarie per impedire o almeno per contrastare la diffusione di *viruses* o altri comportamenti dannosi del proprio personale.

5. Illeciti per mezzo di INTERNET: fattispecie.

E veniamo così alla categoria degli illeciti che si realizzano « per mezzo di INTERNET ».

Si tratta ovviamente di una categoria in cui confluiscono fattispecie molto diverse fra loro, perché eterogenei sono i diritti che l'utilizzatore di INTERNET può violare servendosi della rete e perché varie sono le modalità mediante le quali queste violazioni possono aver luogo.

Pur rendendoci conto dei difetti di una trattazione casistica, crediamo inevitabile — al momento attuale — procedere con l'analisi di singole ipotesi e situazioni di interesse più immediato.

A questa analisi, che prenderà in esame i diritti che possono essere violati per mezzo di INTERNET (o più precisasmente alcuni di questi diritti) faremo seguire alcune considerazioni sulle responsabilità civili che derivano dalla violazione di tali diritti e sul modo in cui dette responsabilità si distribuiscono fra i diversi soggetti coinvolti.

A. *INTERNET e marchi.* — Come ogni strumento di comunicazione, INTERNET può essere utilizzato dagli imprenditori per rivolgere al pubblico offerte commerciali.

Quando queste offerte siano contrassegnate da marchi o da altri segni distintivi confondibili con i segni registrati da terzi o comunque a loro spettanti, si può prospettare una contraffazione di marchio. Un buon esempio per illustrare questo tipo di violazione — peraltro non difficile da ricondurre a norme che ci sono familiari — può essere offerto da una recentissima decisione del 19 Giugno 1996 con la quale la *U.S. District Court — Southern District* di New York ha ordinato — in sede cautelare — che la rivista italiana per adulti « Playmen » adottasse misure idonee a rendere inaccessibile il suo sito INTERNET ad utenti USA, perché l'offerta dei suoi servizi a tali utenti costituirebbe violazione di una precedente inibitoria rivolta agli editori di tale rivista a tutela del marchio « Playboy ».

« Playboy », inoltre, è stato al centro di un'altra vertenza giudiziaria nella quale George Frena è stato riconosciuto responsabile (fra l'altro) di contraffazione di marchio per aver organizzato un *Bulletin Board System* (BBS) che distribuiva copie non autorizzate delle fotografie pubblicate da « Playboy », nelle quali comparivano i marchi registrati « PLAYBOY » e « PLAYMATE » (*Playboy Enter. Inc v. Frena*, 839 F. Supp. 1552 (M.D. Fla. 1993)).

Altro caso simile, in cui il convenuto era una società dal poco rassicurante nome di MAPHIA, è quello dell'organizzazione di un BBS, attraverso il quale gli utilizzatori abbonati venivano incoraggiati a fornire al *server* ed a copiare dal server programmi di videogiochi che, fra l'altro, pervenivano con il marchio origi-

nale del legittimo proprietario del programma (*Sega Enter. Ltd. v. MAPHIA*, 857 F. Supp. 679 (N.D. Col. 1994)).

Il caso più interessante e, se si vuole, più nuovo è però un altro: è noto che i nomi a dominio sono scelti in modo tale da facilitarne l'identificazione con il rispettivo assegnatario. In pratica il nome a dominio coincide spesso con il « cuore » dei segni distintivi dell'assegnatario: e su questo punto le regole di *naming* vigenti, anche in Italia, sono molto chiare nel raccomandare di attenersi, per quanto possibile, a questa prassi.

Le autorità che attribuiscono i nomi a dominio (*Registration Authorities* - RA) non possono tuttavia assumersi il compito (che è poi un onere ed un rischio) di verificare in tutti i casi loro sottoposti che questa raccomandazione venga rispettata e che non insorgano pericoli di confusione. È vero infatti che nelle regole oggi vigenti in Italia si dice che « il nome richiesto per la registrazione di una entità non deve essere fuorviante, né indurre casi di possibili ambiguità » e che la autorità può « segnalare i possibili casi di contrasto con questo principio », attivando delle procedure di comunicazione alle parti. È altresì vero che le regole italiane prevedono procedure di contestazione e la creazione di una sorta di *panel* di arbitri, cui le eventuali controversie possono essere sottoposte in base ad una procedura alquanto informale.

Ma è anche vero che si dichiara espressamente che « non rientra nei compiti della RA Italiana la discussione e/o la risoluzione di eventuali dispute sull'uso di nomi simili ... tra entità differenti. La RA Italiana si limiterà a segnalare le possibili ambiguità alle parti interessate ». La stessa politica di *laissez faire* è in sostanza seguita dalle autorità americane, che sembrano preoccupate (soprattutto) di non essere coinvolte nelle liti delle parti.

Orbene, ciò premesso, è accaduto in America che un giornalista, di nome Josh Quittner, sia riuscito a farsi attribuire il nome a dominio « mcdonalds.com », ed abbia poi iniziato una campagna di stampa, un po' satirica e un po' seria, sui pericoli che la McDonald's Corp. avrebbe potuto correre se lui, Quittner, avesse assunto un atteggiamento ricattatorio. La cosa si è poi conclusa con un accordo, in base al quale la McDonald's Corp. si è impegnata a versare un contributo ad una scuola di New York per consentirle di accedere a INTERNET e Quittner ha rinunciato al suo nome a dominio.

In questo caso si è trattato di un dispetto. In altri casi il c.d. « *domain grabbing* » può costituire l'arma di una vera e propria aggressione commerciale. Nel caso *Kaplan v. Princeton Review* (che non è stato oggetto di una decisione giudiziale, ma di una procedura arbitrale, su cui v. A. BRUNEL, ***Trademark Protection for Internet Domain Names***, **in *International Business Laywer*, 1996, 174) Princeton Review aveva assunto, come nome a dominio, quello del suo rivale Stanley H. Kaplan Educational Centers Ltd. Nel proprio sito, così contrassegnato, Princeton Review met-**

teva a disposizione una comparazione fra i propri servizi e quelli di Kaplan: comparazione ovviamente congegnata in modo tale da far risaltare l'inferiorità dei secondi. Immaginiamoci lo sconcerto dei naviganti di INTERNET che, credendo di giungere nel « porto » di Kaplan, vi ritrovano un'impietosa autocritica e un'ammissione della propria inferiorità rispetto al più temibile concorrente. È ovvio che in questo caso, accanto ad un profilo confusorio, vi è anche un aspetto di scorrettezza commerciale che rileva, anche autonomamente dall'eventuale contraffazione del marchio, nella prospettiva del divieto della concorrenza sleale.

In altre ipotesi, infine, la somiglianza dei *domain names* deriva dalla somiglianza dei nomi legittimamente usati dai soggetti interessati: ed il conflitto sorge e si ingrandisce sia perché i *domain names* non possono riflettere esattamente le denominazioni di cui costituiscono abbreviazioni, sia perché denominazioni uguali o molto simili, fra le quali (a causa dei diversi contesti in cui sono utilizzate) normalmente non sorgono conflitti o confusioni, possono venire in collisione quando si tratti di conquistare uno spazio su INTERNET.

L'emergere di questi problemi ha suscitato un dibattito acceso. Da un lato ci si è chiesti se le autorità che presiedono alla attribuzione dei nomi a dominio dovrebbero adottare nuove politiche o prassi di registrazione, introducendo controlli anche sulla legittimazione del richiedente ad appropriarsi di un certo nome. D'altra parte si prospetta l'opportunità che dette autorità rivedano la regola per cui, salvo ipotesi eccezionali, a ciascuna entità non può essere attribuito più di un nome a dominio (« una entità, un dominio ») salvo ipotesi eccezionali) per consentire al titolare di più marchi o di marchi particolarmente rinomati di occupare il maggior spazio possibile « attorno » ai loro segni distintivi.

A questi suggerimenti è tuttavia possibile obiettare che mai nessuna autorità potrà svolgere efficacemente i controlli richiesti per evitare conflitti e soprattutto per risolverli quando sorgessero: insomma non possono essere attribuite alle autorità di attribuzione dei *domain names* competenze che spettano al potere giudiziario. Tali controlli risulterebbero poi illusori se si considera la dimensione planetaria di INTERNET, che renderebbe puramente velleitaria l'aspirazione ad una verifica preventiva della legittimità della richiesta di assegnazione del nome.

Quanto poi alla registrazione di *domain names* « protettivi », che alcuni suggeriscono, anch'essa può rivelarsi illusoria, quando soprattutto si consideri che confusioni volontarie o involontarie possono verificarsi anche rispetto agli *usernames* (che non sono registrati) o dalla loro combinazione con i *Full Qualified Domain Names* (FQDN). Ma soprattutto la rottura della regola « *una entità un dominio* » è contraddittoria con la politica di INTERNET, che è quella di non restringere l'accesso al sistema, ma di am-

pliarlo quanto più è possibile: e si badi che consentire una pluralità di registrazioni può anche prestarsi a comportamenti devianti (registrazioni a fini di prenotazione, o di speculazione, ecc.).

Più in generale occorre chiedersi — e di fatto ci si è chiesti negli ambienti più qualificati — se davvero i *domain names* possano essere considerati segni distintivi e possano quindi venire in considerazione come marchi, o se invece non siano da avvicinare in qualche modo a segni d'incerta natura (forse prevalentemente descrittivi) come gli indirizzi postali o i numeri del telefono: segni cioè che non appartengono agli utilizzatori (che infatti non possono disporne per trarne profitto), ma che certamente li identificano o concorrono ad identificarli.

In sintesi diremo che l'analogia con gli indirizzi ed i numeri di telefono, proposta anche da una Corte americana, ci convince solo in parte. Riconosciamo tuttavia che, come il numero di telefono può — in certe circostanze — acquistare un *secondary meaning* e divenire un segno distintivo atipico dell'impresa, altrettanto può dirsi per il *domain name*; d'altra parte non crediamo che ci possa esser dubbio sul fatto che, nel contesto dell'uso concreto o in relazione all'affinità dei servizi o dei prodotti offerti attraverso INTERNET o (ancora) con riguardo alla eventuale celebrità di determinati segni distintivi, il *domain name* adottato da Tizio possa generare confusione con o arrecare pregiudizio a oppure sfruttare senza giustificato motivo, il prestigio del marchio di Caio. In questi casi — ricorrendo i presupposti della tutela dei marchi o il rapporto di concorrenza — sarà giustificata una azione di contraffazione o di concorrenza sleale.

B. *INTERNET e diritti della personalità*. — Il materiale raccolto in questo sottotitolo è, anch'esso, eterogeneo.

Sta di fatto che INTERNET è un mezzo di comunicazione dalle potenzialità diffusive impressionanti, capaci di moltiplicare vertiginosamente gli effetti di un'eventuale aggressione alla personalità altrui o ai singoli aspetti della medesima (i c.d. diritti della personalità).

La materia che ci interessa si colloca poi all'incrocio di una serie di rami dell'ordinamento giuridico: anche a trascurare del tutto il profilo internazionalistico, di cui ci occuperemo più avanti, accanto agli aspetti civilistici si pongono quelli di tutela costituzionale della libertà di espressione, quelli penalistici di tutela dell'onore, del decoro e della *privacy*, quelli pubblicistici della corretta identificazione degli individui, delle associazioni, delle imprese, ecc.

Un ulteriore fattore di complicazione è dato dalla stessa natura « anarchica » di INTERNET, che è rispecchiata (ovviamente non sempre) da un comportamento « anarcoide » degli utilizzatori, quasi che l'ingresso nel nuovo mondo virtuale giustifichi una temporanea sospensione della legge o dei freni inibitori. Non è infre-

quente, insomma, che in INTERNET si incontrino messaggi scurrili, oscenità, satire più o meno pesanti, pornografia ed offerte « illecite ». Addirittura i « giri di frase » più comuni nel gergo di INTERNET denotano una certa volgarità di atteggiamento, che si spiega almeno in parte con la frequente metafora di INTERNET come « nuovo *wild west* ».

Alcune violazioni della riservatezza, e quindi della personalità, di terzi possono consistere in comportamenti cui ho già accennato in precedenza: si pensi allo *hacking* — cioè in particolare all'accesso non autorizzato ai dati personali di un certo individuo contenuti in una banca dati, o alla loro alterazione.

Si pensi inoltre al fatto che alcune fattispecie, in sé non preoccupanti, possono con INTERNET assumere un rilievo quantitativo tale da suscitare interrogativi serissimi con riferimento alla tutela della *privacy*. Un bollettino di informazioni giuridiche relative ad INTERNET ha recentemente dato notizie di un caso abbastanza interessante, nel quale un esperto di *computers*, che aveva « messo in rete » il registro automobilistico dell'Oregon (liberamente consultabile da chiunque), ha dovuto chiudere il suo sito per non subire azioni giudiziali minacciate nei suoi confronti da centinaia di automobilisti inferociti (*Cyberlex - Update 9/96*).

Larga attenzione hanno avuto alcuni casi nei quali la diffusione su INTERNET di notizie tali da violare la *privacy* di determinate persone è stata addotta come pretesto per bloccare le iniziative cautelari di tali persone. In questi casi la presenza sulla scena di INTERNET non sposta i termini sostanziali della questione, ma quelli processuali. Per rendere più concreto il discorso con un esempio, si può citare il caso del libro « *Le grand sécret* » in cui il Dott. Gubler, medico del presidente francese Mitterand, narra i particolari della malattia che lo condusse a morte: ai famigliari che chiedevano un provvedimento d'urgenza di inibizione della ulteriore diffusione del libro, l'editore aveva replicato che non sussisteva il pericolo attuale di un danno irreparabile dato che, nelle more del procedimento, un terzo aveva diffuso su INTERNET il contenuto integrale del libro, con la conseguenza che il pregiudizio si era ormai interamente verificato. La Corte di Appello di Parigi (I^{e} Chambre) ha respinto l'eccezione il 13 Marzo 1996: ma la questione ovviamente resta aperta, dato che ormai chiunque può avere accesso al libro via INTERNET nei siti non francesi in cui è stato « caricato » (v. la notizia pubblicata in *CTRL*, 1996, n. 3, T-72).

Vi sono poi i casi, per cui la sanzione penale (per quanto magari praticamente poco efficace) è l'unica ad avere una sperabile efficacia dissuasiva, nei quali vi sia intercettazione, modificazione o alterazione dei dati, informazioni, messaggi che viaggiano su INTERNET. La violazione dei diritti della personalità delle vittime di queste attività è, in queste ipotesi, solo una delle possibili conseguenze della criminalità informatica: conseguenze che, peraltro,

più tipicamente assumeranno dimensioni patrimoniali assai rilevanti nel successivo utilizzo, da parte del delinquente informatico, dei dati carpiti o manipolati. Si pensi, anche qui soltanto a titolo esemplificativo, al furto di *passwords*, di codici di accesso, di numeri di carte di credito o di carte di debito (tipo BANCOMAT) e perfino di numeri di telefoni cellulari.

L'altra faccia della medaglia è la diffusione di *software* e di *hardware* di crittografia, delle c.d. *key encriptions* che, quando rispondono a certi requisiti e sono gestite con attenzione, garantiscono una assoluta sicurezza dei dati e un'altrettanto assoluta riservatezza dei messaggi. In un panorama pieno di luci e di ombre queste caratteristiche sono però anche fonte di pericoli: la sicurezza degli onesti può coincidere con l'impunità dei delinquenti.

Si spiega così che il Governo degli Stati Uniti d'America, per ragioni di sicurezza, abbia posto limiti assai restrittivi all'esportazione della tecnologia della *key enscription*; e si spiegano anche i tentativi, come quello della *clipper chip proposal*, di allestire forme di controllo pubblico dei messaggi crittati o di « tatuaggio » delle comunicazioni immesse in rete. Tentativi ai quali, peraltro, si sono vigorosamente opposti (per ora con successo) i paladini delle libertà civili e della tutela della sfera privata dalle intromissioni dello Stato.

Il caso però più eclatante, e che ha attirato numerosi commenti, è quello della diffamazione diretta, attraverso la diffusione di notizie maliziose (o talvolta addirittura del tutto false) tali da gettare il discredito su l'una o l'altra persona. Si pensi ad esempio all'inserimento di un messaggio screditante nel circuito di un BBS, o nelle bacheche elettroniche del tipo USENET, o in pubblicazioni in rete di bollettini, quotidiani, settimanali, ecc.. Qui si apre un capitolo veramente importante sulle responsabilità ascrivibili ai vari soggetti coinvolti, alla possibilità di instaurare analogie con la responsabilità del direttore di un periodico o dell'editore: ma di tutto questo, secondo il programma che ci siamo dati, si dovrà trattare più avanti.

Basterà per il momento ricordare il (del resto ormai celebre) caso *Stratton Oakmont v. Prodigy Services Co.* del Marzo-Maggio 1995, in cui un giudice della *Supreme Court of New York, Nassau County*, ha stabilito che il gestore di una bacheca elettronica può essere ritenuto responsabile dei danni causati dall'inserimento, fra i messaggi del « giro », di un comunicato gravemente lesivo dell'immagine di un intermediario in valori mobiliari.

Ma soprattutto occorre mettere sul tavolo fin da adesso (e con riserva di tornare più tardi sull'argomento) la questione della « anonimità »-« non identificabilità concreta » degli autori dei messaggi diffamatori o delle altre violazioni cui abbiamo appena accennato. Si pensi all'ipotesi in cui un *service provider* offra ai suoi *subscribers* — come servizio — quello di renderli anonimi. A parte le questioni penalistiche che si potrebbero porre, quale

può essere in questi casi la conseguenza civilistica? Si penserà ad un'assunzione di responsabilità del *service provider* su base volontaria oppure si dovrà provare una colpevole assenza di controllo sul contenuto dei messaggi anonimi? È ipotizzabile, inoltre, che vi sia un obbligo per il *provider* di detenere un *record* degli utenti, di organizzare i propri servizi in modo di evitare che vi siano scambi di persona o lacune, di controllare accessi ed informazioni in modo da evitare inquinamenti ed irruzioni di *hackers*? E quali sarebbero le sanzioni civilistiche in mancanza di adempimento di questi presunti obblighi?

Su questo tema torneremo — come già detto — nell'ultima sezione della prima parte del lavoro.

C. *INTERNET e diritto d'autore*. — Il presupposto tecnico dei problemi di cui ora passiamo ad occuparci è costituito dalla possibilità di riprodurre opere protette in forma « digitale », cioè in forma leggibile da parte del *computer*, e di trasmetterle via INTERNET da un capo all'altro dell'orbe terracqueo.

Ponendoci in primo luogo dal punto di vista del diritto morale di autore, occorre ricordare che una delle caratteristiche più appariscenti di taluni servizi offerti su INTERNET è data dalla c.d. *interattività*, cioè dalla possibilità che l'utente ha di interagire con i dati (e quindi con le opere dell'ingegno) cui accede attraverso la rete, talvolta arricchendole di contenuti, talvolta distorcendole, ridicolizzandole, distruggendole, inserendole in contesti estranei a quelli in cui vennero concepite. Si pensi alla creazione di opere multimediali che, al di là di profili squisitamente patrimoniali, possono incidere pesantemente nella sfera dei diritti morali: per fare un'ipotesi immediatamente comprensibile, basterà formulare l'esempio che un brano musicale che sia opera di un musicista religioso e timorato sia usato come sottofondo di una rappresentazione cinematografica di un festino a luci rosse.

Altro profilo rilevante in chiave di diritto morale d'autore è quello della « qualità » della copia. E questa « qualità » non va ridotta al mero profilo della corrispondenza della riproduzione all'originale, giacché anche una copia perfetta può interferire con un legittimo interesse morale dell'autore.

Rispetto a questo gruppo di problemi si pone allora la necessità di precisare quali siano i (nuovi) confini del diritto morale di autore; entro quali limiti si può ipotizzare un consenso alla manipolazione della propria opera (eventualmente desumibile dal solo fatto di averla resa disponibile su INTERNET); come sia possibile conciliare l'eventualità di un simile consenso con l'inalienabilità del diritto morale di autore; come si riescano a conciliare le regole sul diritto di inedito con un eventuale riconoscimento all'autore di un diritto morale ed opporsi alla sua diffusione su INTERNET. E si potrebbe proseguire.

Spostiamoci ora di prospettiva e poniamoci dal punto di vista dei diritti patrimoniali. Marco Ricolfi ha giustamente messo in luce (in una brillante relazione di prossima pubblicazione in *AIDA*, 1996) che il diritto d'autore italiano ed europeo ha dimostrato una notevole capacità nell'adattare la definizione delle attività riservate all'autore (ed al cessionario dei diritti) nella prospettiva delle nuove tecnologie. Disponiamo ora di una definizione del diritto esclusivo di distribuzione dell'opera (art. 17 l. dir. aut., riformato nel 1994) che prescinde dall'intento di lucro del distributore e ricomprende ogni possibile forma di messa a disposizione del pubblico delle opere protette. Disponiamo ora di una norma che, almeno per il *software* (ma forse per tutte le opere protette, o almeno per quelle « digitalizzate »), attrae nell'ambito del diritto esclusivo di riproduzione, oltre che la vera e propria duplicazione in copie materiali o relativamente stabili, anche le copie realizzate transitoriamente nella memoria del *computer*.

Per illustrare questi concetti basterà ricordare alcuni casi tratti dall'esperienza americana:

a) in *Playboy Enter. Inc. v. Frena*, 839 F. Supp. 1552 (M.D. Fla. 1993) George Frena, un operatore di un BBS, è stato giudicato colpevole di violazione del *copyright* di Playboy su alcune fotografie per adulti caricate sul *server* del BBS da alcuni sottoscrittori e scaricate da altri sottoscrittori sui propri terminali;

b) in *Sega Enterprises Ltd. v. MAPHIA*, 857 F. Supp. 679 (N.D. cal. 1994), MAPHIA vendeva strumenti adatti a copiare i *videogames* di Sega ed incoraggiava gli abbonati al proprio BBS a caricare sul *server* del BBS e scaricare detti videogiochi nei loro *computers*;

c) in *Religious Technology Center v. Netcom — Online Communication Services, Inc.* -, No. C-95-20091 (N.D. Cal. Nov. 21, 1995) la diffusione su un BBS di stralci di opere del fondatore di Scientology, Ron Lafayette Hubbard, è stata ritenuta una violazione del diritto d'autore.

Quest'ultima decisione è importante anche perché prende in considerazione un profilo di grande rilievo (peraltro già presente nel caso *Playboy v. Frena*) e cioè quello della possibile violazione del *copyright* da parte di qualunque soggetto il cui *computer* abbia — anche al di fuori della sua sfera di controllo — registrato per quanto transitoriamente l'opera protetta. Nel caso specifico l'immissore in rete degli stralci delle opere di Hubbard era un ex-seguage di *Scientology*, tale Dennis Erlich, che era abbonato di un BBS gestito da un certo Thomas Klemesrud, il cui accesso a INTERNET era assicurato da Netcom. Scientology sosteneva che Netcom avesse violato il *copyright* sulle opere di Hubbard perché, per almeno 11 giorni, gli stralci delle opere di Hubbard immessi in rete da Erlich tramite Klemesrud erano restati nella memoria del *server* di Netcom. Ponendosi in contrasto con le conclusioni del *Final Report of the Working Group on Intellectual*

Property Rights americano, il giudice ha ritenuto improprio nella fattispecie prospettare una violazione diretta del copyright da parte di Netcom (come invece suggeriva la attrice) perché (salva l'ipotesi di riconoscere nelle circostanze un *contributory infringement*) ciò finirebbe per postulare arbitrariamente una « *liability for every single Usenet server in the worldwide link of computers transmitting Erlich's message to every other computer* ».

Giusta o sbagliata che sia la decisione appena ricordata nella prospettiva europea, accettabile o inaccettabile l'argomentazione che la sorregge, il nocciolo della questione resta la definizione di « riproduzione » dell'opera ed il rapporto che, almeno nella nostra legge, si deve instaurare fra l'art. 13 e l'art. 64-bis l. dir. aut. per stabilire se l'illiceità della riproduzione temporanea sia, nel nostro ordinamento, la regola oppure l'eccezione.

Ma non basta. Si è detto infatti che l'ambito del diritto di esclusiva riconosciuto all'autore riguardo alla distribuzione dell'opera protetta è stato considerevolmente ampliato, in Italia, a partire dal 1994. Cosa si deve intendere, tuttavia, per « distribuzione »? Più precisamente occorre stabilire se si possa parlare di distribuzione in relazione ad ipotesi in cui il preteso responsabile della violazione non trasmette alcun dato, ma sia l'utilizzatore che acceda alla memoria che contiene le informazioni desiderate, magari attraverso una serie di collegamenti indiretti o ipertestuali. E che dire poi dei casi in cui il collegamento, anziché richiedere un intervento umano, è predisposto automaticamente dalla macchina? Che, infine, si dovrebbe pensare del *browsing*, che produce una visualizzazione temporanea sulla RAM del contenuto di un sito?

Qui il discorso si interseca con il tema, anch'esso molto delicato e complesso, delle c.d. utilizzazioni libere, cioè di quegli atti materialmente ricompresi nell'ambito astratto dell'esclusiva, che il legislatore tradizionalmente sottrae al monopolio dell'autore in vista di superiori interessi. Come acutamente ha rilevato Marco Ricolfi (nell'articolo già ricordato in precedenza), al dinamismo del legislatore nel ridisegnare il contenuto dei diritti di esclusiva degli autori, ha fatto tuttavia riscontro una quasi assoluta inerzia nell'intervenire sulle utilizzazioni libere: ed anzi, per le banche dati « elettroniche », va segnalato che l'attuazione della Direttiva CEE del 1996 determinerà una sostanziale abolizione dello stesso concetto di « utilizzazione libera ». Ricolfi vede in ciò un disegno del legislatore, che vuole o vorrebbe un rafforzamento dei diritti di esclusiva, e prenderebbe atto dell'impossibilità di estendere allo sfruttamento in rete i principi già seguiti in passato per risolvere i problemi delle copie private con la conversione del diritto di autore in un tributo sulla vendita degli apparati di riproduzione. D'altro lato la discussione ferve in tutto il mondo sulla questione se veramente sia possibile conservare un diritto d'autore classico sulle opere trasmesse via INTERNET (il che richiede-

rebbe una sorta di « tatuaggio » delle opere, o di « *digital plate* », tale da consentire l'identificazione dell'utente, dell'opera riprodotta, del numero di accessi per ogni utente e dei tempi di accesso) oppure sull'opportunità di passare ad un nuovo sistema di remunerazione del lavoro creativo, magari basato su licenze obbligatorie.

6. Illeciti per mezzo di INTERNET: responsabilità.

Si può ora passare alla trattazione dell'ultimo argomento della prima parte di relazione: quello che attiene ai criteri di attribuzione della responsabilità, quando si sia verificata una violazione dei diritti di terzi « per mezzo di INTERNET ».

Dobbiamo precisare che, parlando di responsabilità, non intendiamo riferirci soltanto all'aspetto risarcitorio, ma anche ad altri aspetti, e segnatamente al profilo inibitorio, reintegratorio, ecc. In termini forse più semplici, la questione non è soltanto: « chi risponde dei danni »? ma anche: « chi è il potenziale legittimato passivo, rispetto alle azioni del titolare del diritto che risulti leso da attività realizzate su INTERNET, se dette azioni sono rivolte ad ottenere la cessazione della lesione o la rimozione degli effetti della stessa o degli strumenti attraverso i quali essa viene perpetrata »?

Il tema è all'ordine del giorno negli Stati Uniti d'America ed investe interessi — anche economici — di non trascurabile rilievo, poiché (intuitivamente) l'affermazione della responsabilità dei *service providers*, per attività compiute dagli *users* o dai BBS e dai relativi abbonati che ne sfruttino la connettività, ha ricadute importanti sul modo di organizzare, di offrire e distribuire i servizi, nonché sul relativo costo. Allo stesso modo ci si deve interrogare sull'applicabilità nella fattispecie di norme che prevedono, con criteri di imputazione più o meno obiettivi, la responsabilità indiretta per fatto altrui (si pensi all'art. 2049 c.c., ma anche all'ipotesi della violazione compiuta materialmente da un minorenne che, per collegarsi ad INTERNET, usa il *computer* della scuola oppure quello di casa).

Un elemento di ulteriore complicazione è costituito dal fatto che alcune delle violazioni più frequentemente riscontrabili nel mondo di INTERNET sono violazioni che incidono su diritti di proprietà intellettuali. Entra pertanto in gioco la definizione del contenuto del diritto di esclusiva; definizione che attrae nel campo del divieto una serie di condotte che, giudicate secondo il metro del monopolio garantito al titolare dell'esclusiva, sono senz'altro lesive, ma che, giudicate invece nella prospettiva « classica » del dolo e della colpa, appaiono o potrebbero apparire del tutto innocenti. Insomma può succedere che, a mia totale insaputa e perfino contro la mia volontà, mi accada di riprodurre nella memoria del

mio *computer* dei materiali, cui ho avuto accesso per mezzo di INTERNET, che sono tutelati da un *copyright* o da un analogo diritto. E può succedere, inoltre, che io partecipi — senza volerlo o senza avere una reale possibilità di rendermene conto — alla propagazione di un illecito originariamente commesso da altri.

Come dicevo, negli Stati Uniti d'America si è già formata una casistica giurisprudenziale. Passiamola in rassegna.

A. *Esempi.* — I) Nel caso *Cubby Inc. v. CompuServe*, 776 F. Supp. 135, 140 (S.D.N.Y. 1991) l'attore aveva convenuto in giudizio il gestore di un *host* ed il *service provider*, CompuServe, in relazione ad una pretesa diffamazione che avrebbe avuto luogo in uno *special-interest forum* denominato « Rumorville ». Accogliendo la richiesta di CompuServe di pronunciare un *summary judgment* a suo favore, il giudice ha ritenuto che la situazione di CompuServe non fosse paragonabile a quella di un editore (che è legalmente tenuto al controllo dei materiali pubblicati), quanto piuttosto a quella di un libraio, cui sarebbe irragionevole imporre l'onere di esaminare il contenuto di ogni singolo libro che entra nel suo negozio (per informazioni più dettagliate su questo caso v. S. DOOLEY, *Defamation on the Internet*, *CTLR*, 1995, 191).

II) Nella causa *Auvil v. CBS '60 Minutes'*, 800 F. Supp. 928 (1992), i concetti implicitamente contenuti nel caso « Cubby » sono stati rielaborati nel senso di precisare che non sarebbe sufficiente una teorica possibilità di controllare i contenuti di ciascuna « pubblicazione » in INTERNET da parte del *service provider*, perché divenga ipotizzabile una responsabilità di quest'ultimo. Il giudice di questa causa ha però lasciato intendere che il *service provider* potrebbe essere ritenuto responsabile se ne fosse dimostrata la malafede o la colpa grave.

III) Molto scalpore ha suscitato il caso *Stratton Oakmont Inc. v. Prodigy Services Co.* n. 31063/94 (Supreme Court of New York, Nassau County), 10 Marzo 1995, nel quale una società di intermediazione in valori mobiliari ha convenuto in giudizio il gestore di una bacheca elettronica, denominata « Money Talk », nella quale venivano pubblicate notizie diffamatorie relative all'attività della società attrice. Nell'affermare la responsabilità del convenuto, il giudice ha ritenuto che il caso si distinguesse dal precedente « Cubby », perché Prodigy di fatto avrebbe esercitato veri e propri poteri « editoriali ». Era in effetti risultato che Prodigy aveva adottato delle *content guidelines*, in base alle quali sarebbe stato possibile eliminare i materiali offensivi del sito; inoltre era applicato un *automatic software screening* per la ricerca e l'eliminazione delle parole oscene ed offensive; e Prodigy aveva personale interno ed esterno (*Board Leaders*) specificamente incaricato di sorvegliare sull'applicazione delle *guidelines*. Al contrario il giudice non ha ritenuto rilevante la prova, offerta dal convenuto,

della variazione delle politiche di controllo seguite da Prodigy, a causa della loro eccessiva onerosità, in particolare perché a tale supposta variazione non era stata data sufficiente o adeguata diffusione tra il pubblico. Paradossalmente questa decisione, che ha subito critiche anche troppo severe, ha spinto alcuni commentatori americani a suggerire ai *service providers* di non controllare il contenuto degli *incoming messages* e di dare la massima pubblicità possibile a questa determinazione. Malgrado che le parti avessero raggiunto un accordo transattivo, il giudice del caso Stratton Oakmont Inc. v. Prodyges Services Co. ha rifiutato di revocare il suo provvedimento (cfr. NY Supreme Court, Nassau County, December 11, 1995, *CTLR*, 1996, T-50).

IV) Nel caso *Playboy Enter. Inc. v. Frena*, già citato, l'operatore di un BBS è stato ritenuto responsabile di contraffazione del diritto di *copyright* spettante a Playboy su certe fotografie (nonché del diritto sul marchio 'PLAYBOY' che compariva a contraddistinguere quelle fotografie) in relazione ad un caso in cui l'inserimento di dette foto nel BBS era opera degli abbonati ed in cui il convenuto aveva offerto di provare *a*) che l'inserimento era avvenuto contro la sua volontà; *b*) che le foto incriminate erano state immediatamente eliminate non appena erano state scoperte.

V) In *Sega Enterprises Ltd. v. MAPHIA*, anch'esso già citato, MAPHIA vendeva degli strumenti utilizzabili per copiare i *videogames* di Sega; inoltre offriva l'accesso ad un BBS per il cui tramite gli abbonati venivano indotti a caricare e scaricare i videogames in questione. In questo caso, il giudizio sommario della Corte adita è stato nel senso che poteva in effetti sussistere una responsabilità dell'operatore per *contributory infringement*.

VI) Un caso interessante è anche quello, penalistico, di uno studente del MIT che, sfruttando la connettività dell'Istituto aveva organizzato un circuito amatoriale per il baratto di *software* basato sull'utilizzazione dell'anonimato garantito dalla disponibilità di taluni *host* finlandesi (*United States v. Lamacchia*, F. Supp. 535, B.D. Ma. 1994).

VII) In *Religious Technology Center v. Netcom — Online Communications Service, Inc.*, anch'esso citato in precedenza, si discuteva se il semplice caricamento di materiale coperto dal *copyright* nella memoria di un host del *service provider*, anche al di fuori di una diretta responsabilità di quest'ultimo o di un suo concorso, potesse violare il *copyright*. I giudici hanno riconosciuto che il diritto d'autore « *is a strict liability statute* », ma hanno aggiunto che « *there should still be some element of volition or causation which is lacking where a defendant's system is merely used to create a copy by a third party* ». Questo elemento mancherebbe se il *computer* del *service provider* è stato usato solamente come mezzo. D'altro lato i giudici hanno ritenuto che sarebbe configurabile un concorso del *service provider* nella illecita attività dei *subscribers*, se venga dimostrato un colpevole ritardo del *provider*

nell'eliminare il materiale contestato dopo aver ricevuto una *notice of infringement* del soggetto leso. Ed anche quando non fosse configurabile un concorso (o *contributory infringement*) potrebbe venire in considerazione la dottrina della *vicarious liability*, in base alla quale risponde della violazione chi, avendo il diritto e la capacità concreta di controllare le azioni del soggetto direttamente responsabile della violazione, omette di impedirne il verificarsi, traendone al contempo profitto.

VIII) Infine vale la pena di menzionare una controversia, risolta in via stragiudiziale, nella quale Knowledge Net Inc. aveva citato in giudizio i registranti del nome a dominio « Knowledgenet.com » e l'autorità di registrazione statunitense (come concorrente nella violazione) perché ciò avrebbe costituito una contraffazione di marchio. La controversia è importante perché, per diretta conseguenza del suo insorgere, le regole di attribuzione dei nomi a dominio americane sono state modificate, prevedendo che, in caso di contestazione, il registrante debba dare la prova (entro un breve termine) di disporre di una registrazione di marchio tale da giustificare la sua pretesa ad un determinato nome a dominio, a lui attribuito. Soddisfatto questo onere di prova, la cancellazione del nome a dominio potrebbe avvenire solo su conforme ordine di un giudice o di un collegio arbitrale.

IX) Nell'ambito della *vicarious liability*, cui già si è accennato, si discute negli Stati Uniti delle interrelazioni fra le possibili attività illecite messe in opera per mezzo di INTERNET e le regole che fanno risalire al datore di lavoro le responsabilità per gli atti illeciti ascrivibili ai, e/o commessi dai, lavoratori dipendenti. Anche in questo caso si tratta di un tema al quale abbiamo già fatto un cenno e che meritava di essere ripreso anche in questa sede.

B. *Considerazioni critiche*. — L'ormai ricca esperienza giurisprudenziale americana cui ho appena fatto riferimento può essere almeno parzialmente tradotta in categorie giuridiche italiane.

Anche da noi si può infatti prospettare una responsabilità dei datori di lavoro per i fatti dei dipendenti, o dei genitori, per gli illeciti commessi via INTERNET. Alla stessa stregua ci si può porre il problema se il *service provider* debba esercitare un qualunque controllo sui contenuti degli innumerevoli messaggi che, per suo tramite, possono avere una dimensione planetaria oppure se un simile onere valga soltanto quando vi sia una specifica « assunzione di rischio » da parte del *provider* stesso, come nel caso Prodigy.

Ammesso poi che questa, che abbiamo chiamato « assunzione di rischio » sia veramente necessaria, ci si deve domandare in che cosa concretamente essa debba o possa consistere. Ad esempio il fatto che il *provider* controlli il contenuto di ciò che contribuisce a diffondere è assunzione del rischio? O non lo è, piuttosto, il fatto di astenersi da ogni sorveglianza? Basta, per escludere la respon-

sabilità del *provider*, che egli pubblicizzi dei *disclaimers*? E si potrebbe continuare.

Certamente si può tentare di rispondere a questi interrogativi sulla base del diritto positivo. Ad esempio, qualcuno potrebbe dire che, anche rispetto agli illeciti commessi per mezzo di INTERNET, si applicano norme come l'art. 2049 c.c. o l'art. 57 c.p.. Ma la domanda che occorrerebbe porsi subito dopo, in una prospettiva seria di politica del diritto, è per esempio se il datore di lavoro possa veramente accollarsi la responsabilità di qualunque illecito commesso, via INTERNET, da un suo dipendente, le cui conseguenze planetarie sono evidentemente spropositate, ogni volta che l'espletamento delle mansioni abbia fornito « l'occasione necessaria » per il compimento della violazione, senza che sia possibile addurre a giustificazione, per esempio, l'esistenza di procedure interne di controllo, la pubblicazione di direttive interne, o altre simili « scusanti ».

Allo stesso modo dovrebbero essere rimesse in discussione le definizioni legislative, giurisprudenziali e dottrinali delle attività riservate al titolare dei diritti d'autore o di altri diritti di proprietà intellettuale o industriale, nonché le presunzioni di colpa che (ai fini del risarcimento dei danni e della pubblicazione della sentenza) vengono tradizionalmente riconnesse alle fattispecie in cui obiettivamente sussistano una condotta o uno stato di fatto contrari al diritto di privativa.

Sono queste, direi, le sfide che attendono i legislatori ed i giuristi che in futuro si cimenteranno con la disciplina delle responsabilità nel mondo di INTERNET.

7. Profili internazionali.

Vogliamo illustrarvi, nella seconda parte di relazione, quanto sia falso l'assunto in base al quale gli operatori di INTERNET si troverebbero in una specie di spazio anarchico in cui non esistono leggi ed in cui non vi è tutela per i « deboli », né sanzione per i « prepotenti ».

Al contrario scopriremo come, attraverso l'applicazione delle norme del diritto internazionale privato e processuale (ed in particolare delle norme di cui alla legge 218/95 che ha riformato la materia in Italia), un medesimo comportamento illecito posto in essere in INTERNET possa essere regolato, tutelato o sanzionato da più ordinamenti ugualmente applicabili e sottoposto alla giurisdizione di più giudici ugualmente competenti. Si potrebe quindi affermare che vi è più un eccesso che un difetto di leggi, con tutti gli inconvenienti che ciò comporta.

La relazione si limiterà all'analisi della legge applicabile e del foro competente relativamente alla categoria degli illeciti di natura extracontrattuale, in quanto la materia contrattuale sarà oggetto nella relazione del Prof. Vincenzo Franceschelli.

Conclude la relazione con alcune proposte avanzate dagli studiosi o dagli stessi soggetti che operano in INTERNET, volte alla ricerca di una disciplina specifica ed il più possibile uniforme di alcuni aspetti del fenomeno.

8. Legge applicabile.

Nell'ambito dei contatti che si creano quotidianamente tra i « naviganti » in INTERNET o al difuori da qualsiasi tipo di relazione, può accadere che si creino conflitti tra interessi o diritti contrastanti e che il comportamento di un soggetto cagioni ad altri un danno ingiusto.

Proprio la natura capillare di INTERNET e la diffusione globale di qualunque informazione che vi sia immessa amplificano enormemente le conseguenze di un eventuale comportamento illecito, ponendo all'interprete il difficile compito di individuare quale (o quali) legge/i possano venire invocate dal soggetto che ha subito dei danni in conseguenza del suddetto comportamento.

Il primo problema che si pone all'interprete per la determinazione della legge applicabile è, evidentemente, l'identificazione della norma di conflitto di riferimento.

In pratica, dato un determinato diritto ed individuata la legge che lo disciplina, quale sarà la legge applicabile alla sua violazione?

La stessa *lex substantiae* ovvero una legge che venga determinata in base ad un unico criterio di collegamento valido per tutti i comportamenti illeciti?

Il problema è stato affrontato in relazione alla violazione dei diritti di proprietà intellettuale, che sembrano essere i diritti più facilmente soggetti a violazione per mezzo di INTERNET.

La legge 218/95 disciplina espressamente, all'art. 54, i diritti sui beni immateriali, disponendo l'applicabilità della legge dello Stato di utilizzazione .

Alcuni autori hanno ritenuto che all'art. 54 si dovesse fare riferimento per disciplinare ogni aspetto della tutela del diritto di proprietà intellettuale, ivi inclusa la responsabilità per la sua violazione.

Altri autori, ed è forse l'opinione più convincente, hanno invece affermato che il criterio introdotto dalla Riforma non fa altro che ribadire il principio, largamente affermato, della territorialità dei diritti di proprietà intellettuale e cioé la loro rilevanza unicamente nel paese in cui ne viene invocata la tutela.

Questo comporta che, nel caso di richiesta di risarcimento di danni conseguenti a violazioni di diritti di proprietà intellettuale, la legge applicabile ex art. 54 determinerà l'esistenza del diritto oggetto della violazione, le cui conseguenze saranno poi regolate dalla legge competente in materia di illecito ai sensi dell'art. 62 della legge 218/95: quest'ultimo, come vedremo, concede alla

parte danneggiata e quindi considerata più debole o quantomeno maggiormente meritevole di protezione, una maggiore flessibilità ed indirettamente una maggiore tutela.

Cosa succederà quindi nel caso che, attraverso l'utilizzazione fattane in INTERNET, un soggetto italiano subisca una violazione di un proprio diritto di proprietà intellettuale, tutelato appunto in Italia in quanto tale?

Il soggetto italiano leso, partendo dal presupposto che il suo diritto esiste (art. 54) ne invocherà la tutela ed il risarcimento dei danni subiti e, se si segue l'opinione per noi preferibile, sceglierà uno dei criteri di collegamento indicati nell'art. 62.

Per quanto riguarda la violazione di altri diritti, in alcuni casi è la legge stessa a suggerirci quale è la norma di conflitto applicabile: ad esempio, l'art. 24 della legge 218/95 dispone che le conseguenze della violazione dei diritti della personalità sono regolate dall'art. 62 della stessa legge. Quindi per riprendere il caso già descritto in precedenza che vede quali protagonisti gli eredi del Presidente Mitterand in occasione della diffusione dell'opera « *Le Grand Sécret* », il fatto che l'opera sia poi stata immessa in INTERNET non solo non preclude l'emissione del provvedimento cautelare in Francia, ma non escluderebbe neppure la possibilità per gli eredi di iniziare un procedimento davanti ad un giudice italiano ed ottenere il risarcimento del danno subito in Italia in seguito alla trasmissione ed all'eventuale *downloading* del libro nel nostro Paese.

In generale, l'art. 62 si applicherà ad ogni responsabilità derivante da illeciti di più varia natura che possano verificarsi attraverso l'utilizzo di INTERNET ed ampiamente descritti nel paragrafo « Illeciti per mezzo di INTERNET » della prima parte della relazione.

Nella annosa controversia tra sostenitori della « teoria dell'azione » e sostenitori della « teoria dell'evento » l'art. 62 prende posizione a favore di quest'ultima, disponendo che la responsabilità per fatto illecito è regolata dalla legge dello Stato in cui si è verificato l'evento.

La qualificazione adottata introduce una nuova rigidità per il giudice obbligandolo ad individuare il luogo dell'illecito come il luogo dell'evento; essa ha inoltre delle rilevanti conseguenze, a *fortiori* se pensiamo ad INTERNET, in quanto ad una azione unica (es. immissione di un messaggio o *uploading*) possono corrispondere una pluralità di eventi dannosi localizzati in paesi diversi. Il margine di discrezionalità che è stato tolto al giudice viene conferito, dall'art. 62 secondo comma, al danneggiato, il quale ha ora la facoltà di chiedere, in alternativa alla legge del luogo dell'evento, l'applicazione della legge del luogo in cui si è verificato il fatto che ha causato il danno. Questa facoltà attribuita al danneggiato introduce, in un certo senso, il principio della autonomia privata anche nella materia extracontrattuale.

Quindi, proviamo ad immaginare, ad esempio, il caso di un tipico illecito che può verificarsi in INTERNET: l'immissione illecita in INTERNET da parte di un soggetto francese, attraverso l'utilizzazione del sito di un *provider* tedesco, dell'opera di un autore italiano che venga poi copiata, scaricandola sul proprio terminale, da diversi operatori collegati al medesimo sito e che si trovano nei più svariati paesi.

L'autore dovrà in primo luogo decidere quale sia il soggetto che intende perseguire, se colui che ha immesso illecitamente la sua opera, se conosciuto, ovvero il *provider* responsabile del sito, o ancora ciascuno dei soggetti che ha copiato l'opera.

In tutti i casi verificatisi negli Stati Uniti l'autore ha preferito citare in giudizio il *provider* in quanto soggetto sempre conosciuto e, probabilmente, economicamente più stabile.

Ora, presumendo che l'autore inizi la causa in Italia, la legge che sarà applicata all'illecito commesso ed al conseguente risarcimento dei danni subiti dall'autore potrà essere, a scelta dell'autore stesso, scelta che egli farà in base a valutazioni di opportunità, la legge francese (se è conosciuto colui che ha immesso l'opera) o quella tedesca (legge in cui si trova il *provider*), intese come leggi dei paesi in cui si è verificato il fatto che ha causato il danno, ovvero la legge di ciascuno dei paesi in cui l'autore sostiene di aver subito il danno, ad esempio, la legge italiana, qualora egli ritenesse di aver subito in Italia un pregiudizio economico.

9. Foro competente.

La tendenza sopra esposta in materia di legge applicabile rispecchia una tendenza già consolidata in materia di giurisdizione.

L'art. 5.3 della Convenzione di Bruxelles, richiamata dall'art. 3.2 della legge 218/95, prevede che il giudice competente a conoscere dei delitti e quasi-delitti sia — in alternativa al giudice del domicilio del convenuto — il giudice del luogo in cui il fatto dannoso è avvenuto. La norma è stata ed è interpretata « in modo da attribuire all'attore una facoltà di scelta, quanto al proporre la domanda nel luogo ove si è manifestato il danno, ovvero nel luogo dell'evento generatore di tale danno. ».

Questa è l'interpretazione dell'art. 5.3 fornita dalla Corte di Giustizia in un noto caso del 1976 che riguardava danni derivanti dall'inquinamento transfrontaliero delle acque del Reno.

Recentemente, il 7 marzo 1995 nella decisione del caso « *Shevill* », la Corte ha confermato questa interpretazione anche con riferimento ad un illecito commesso a mezzo stampa.

È molto interessante il principio affermato in questa sentenza, in base al quale, una volta attribuita competenza al foro del luogo di pubblicazione (nel caso di INTERNET si potrebbe leggere di *uploading*), o, in alternativa, ai giudici degli stati in cui c'è stata

la diffusione (o *downloading*), al primo giudice è attribuita competenza a conoscere dell'insieme del danno subito dalla vittima, mentre i singoli giudici nazionali sono competenti a conoscere della sola porzione di danno subito all'interno del loro territorio.

È evidente l'analogia che esiste tra l'illecito commesso attraverso mezzi di comunicazione più noti e quello commesso attraverso INTERNET. Una importante conseguenza che li caratterizza è che il danno può essere subito dallo stesso soggetto in più luoghi. In base al principio espresso nel caso « *Shevill* », ciascun giudice adito avrà visibilità e competenza a conoscere della sola porzione di danno relativo al proprio paese.

Il principio, seppure con qualche differenza, è stato applicato nella decisione del caso « *Playmen* » da parte della *U.S. District Court Southern District di New York* del giugno 1996. La Corte, dopo aver ribadito l'applicabilità del suo provvedimento cautelare anche alla distribuzione e trasmissione via INTERNET, ha riconosciuto di non avere giurisdizione per condannare la società convenuta alla chiusura del proprio sito localizzato in Italia, ma ha comunque condannato la stessa a rifiutare qualsiasi richiesta di abbonamento proveniente da utenti residenti negli Stati Uniti ed a versare all'attrice le somme percepite fino ad allora per abbonamenti forniti a soggetti residenti negli Stati Uniti (« *While this Court has neither the jurisdiction nor the desire to prohibit the creation of INTERNET sites around the globe, it may prohibit access to those sites in this country* »).

La soluzione semplificatrice adottata dalla Corte di Giustizia, ed in certo senso,dalla Corte newyorkese, sembra scontrarsi con l'esigenza, più volte espressa dalla stessa Corte comunitaria, di impedire il frazionamento delle competenze giurisdizionali, con un conseguente aumento del rischio di *forum shopping* su scala mondiale.

10. Inconvenienti e tentativi di armonizzazione.

L'analisi sopra esposta dimostra come l'applicazione delle norme di conflitto poste dalla legge 218/95 e dalle Convenzioni internazionali ivi richiamate comporti inevitabilmente alcuni inconvenienti.

In primo luogo può accadere, come abbiamo visto, che le norme di più ordinamenti di paesi diversi siano simultaneamente applicabili ad una medesima fattispecie e che la decisione sia rimessa alla volontà di una parte che potrà evidentemente esercitarla a sua discrezione ed in qualsiasi momento, anche in sede processuale.

Può inoltre accadere che un medesimo comportamento leda più individui; ciò significa che ciascuno di essi potrà autonomamente decidere a quale legge sottoporre lo stesso illecito?

Parrebbe di sì, con la inevitabile conseguenza di creare una sorta di « *depeçage* » della fattispecie.

Ad esempio, se qualcuno immette un messaggio in INTERNET dal quale risulti che « tutti i Signori Smith sono dei mascalzoni », ogni signor Smith avrà subito un potenziale danno e potrà scegliere di agire nel proprio paese ed in base alla propria legge per il risarcimento del danno subito.

Tutto ciò rappresenta una fonte di significativa incertezza del regime internazionalprivatistico e, conseguentemente, di imprevedibilità della disciplina applicabile.

Gli stessi inconvenienti possono verificarsi in sede giurisdizionale.

Non può non rilevarsi come il frazionamento della competenza tra i giudici dei diversi luoghi in cui il messaggio in INTERNET si è manifestato ed ha provocato danni, può causare oltre che una molteplicità di giudicati anche una contradditorietà degli stessi.

Può darsi infatti che la parte danneggiata introduca, contemporaneamente, la domanda di risarcimento dei danni presso i tribunali di ciascuno degli Stati in cui sostiene di avere subito un danno. In questo caso, secondo l'interpretazione data dalla Corte di Giustizia, ciascun giudice adito potrà pronunciarsi sulla parte del danno subito nel proprio paese.

Le diverse quantificazioni del danno non sarebbero, a giudizio della Corte, tra di loro inconciliabili.

Ma cosa accadrebbe se uno dei giudici investiti si pronunciasse per l'insussistenza del danno?

Ad esempio, sempre nel caso « Playmen » sopra citato, nel 1981 il giudice italiano si era pronunciato nel senso di escludere la violazione del marchio in quanto marchio debole ed aveva rigettato la domanda dell'attrice, con la conseguenza che la società convenuta ha continuato, sino ad oggi, a pubblicare e distribuire la propria rivista in Italia.

Non è stata la nascita di INTERNET ad aver generato questi problemi per gli internazionalprivatisti. La diffusione di informazioni tramite i mezzi di comunicazione più comuni, così come le trasmissioni via satellite possono presentare i medesimi inconvenienti. Ciò che caratterizza INTERNET è, ancora una volta, il suo carattere globale, l'immediata interazione tra un numero indefinito di utenti e quindi l'imprevedibilità delle dimensioni che ciascun fenomeno può assumere. Non dimentichiamo infine che il numero dei soggetti che possono « fare comunicazione » attraverso i *media* più noti è limitato, e comunque essi sono sempre identificabili. Per contro, i soggetti che possono trasmettere informazioni sulla Rete delle reti sono potenzialmente illimitati e difficilmente controllabili a livello centralizzato.

Alcuni suggerimenti avanzati dalla dottrina o dagli stessi soggetti che operano in INTERNET per cercare di superare le diffi-

coltà poste dalla potenziale applicabilità di un numero indefinito di leggi e dalla potenziale competenza di un numero indefinito di giudici, possono così brevemente riassumersi:

A) Una fantasiosa proposta è quella di chi ha suggerito di considerare INTERNET un unico spazio virtuale senza confini territoriali e quindi senza alcun potenziale conflitto di leggi. In questo *cyberspace* esisterebbero fonti consuetudinarie quali una sorta di « *lex mercatoria* » degli operatori di INTERNET che dovrebbe venire applicata da « Corti virtuali » nelle quali siederebbero « magistrati virtuali » con il potere di condannare la parte soccombente sino ad una « morte virtuale » consitente in pratica in una espulsione di diritto dal *cyberspace*.

Una soluzione così singolare è evidentemente irrealizzabile e dimentica che, per quanto INTERNET possa essere considerato uno spazio virtuale, in esso agiscono soggetti reali i cui comportamenti producono effetti nel mondo reale.

Inoltre la sanzione potrebbe essere risibile rispetto al danno provocato ove non fosse possibile accertarsi su scala mondiale che il danneggiante non ottenga, immediatamente dopo la decisione, un nuovo accesso ad INTERNET in altri paesi.

B) Una soluzione per regolamentare la materia della responsabilità degli operatori in INTERNET potrebbe essere il tentativo di regolamentare la limitazione e l'esclusione della responsabilità attraverso una disciplina dei cd. *disclaimers*.

Il *disclaimer* è una dichiarazione inserita solitamente nella *home page* da parte del *provider* nella quale si ammoniscono gli utenti circa i contenuti del sito e si dettano alcune regole al fine di ridurre od escludere del tutto la responsabilità del *provider* nei confronti di chi, nonostante il *disclaimer*, abbia deciso di navigare in quel sito.

Un esempio di *disclaimer* è quello utilizzato da Penthouse che nella sua *home page* dichiara che i contenuti del sito sono vietati ai minori di 21 anni e ne proibisce inoltre la visione a soggetti che appartengono a quei paesi (indicati in una lista a parte) che non permettono la pubblicazione di riviste per soli adulti.

Nel noto caso « *Playmen* » è la stessa corte americana che ha condannato la società convenuta, tra l'altro, ad inserire un *disclaimer* con il quale si informassero i « naviganti » che si sarebbe negato l'accesso a qualsiasi utente proveniente dagli Stati Uniti.

È molto discutibile quale sia il valore giuridico dei *disclaimers*, soprattutto ove non sia dimostrabile che il *disclaimer* è stato accettato o perlomeno conosciuto dall'utente.

Teniamo presente che le pagine di un sito possono essere raggiunte anche evitando di passare dalla *home page* e che quindi se il *provider* non avrà avuto l'accortezza di inserire il *disclaimer* in ogni pagina, la conoscibilità ed accettazione dello stesso non può che essere esclusa.

Inoltre la lingua utilizzata può comportare ulteriori problemi: un *disclaimer* in inglese difficilmente sarà ritenuto efficace in Cina.

Ecco perché un codice di norme uniformi per l'utilizzo dei *disclaimer* oltre a sviscerare tutte le problematiche giuridiche connesse a tale utilizzo potrebbe ingenerare negli operatori una sorta di prassi accettata e seguita a livello internazionale.

C) Un importante esempio di regolamentazione centralizzata è quella che è stata realizzata con riferimento ad un settore specifico come quello della politica di assegnazione dei cosiddetti *domain names* o nomi a dominio da organizzazioni indipendenti aventi funzioni e poteri specifici.

In Italia ad esempio la Naming Authority Italiana (ITA.PE) ha stabilito un regolamento e delle procedure operative su cui si basa il lavoro della Registration Authority Italiana, istitutita presso l'Istituto CNUCE del CNR, che è preposta alla assegnazione dei nomi a dominio ed alla gestione del relativo Registro (RNA - Registro dei Nomi Assegnati).

Nel Regolamento stesso, che deve essere accettato dal soggetto che richiede l'assegnazione del nome a dominio tramite la sottoscrizione della cosiddetta « Lettera di assunzione di responsabilità », è prevista una procedura per la risoluzione di eventuali contestazioni sollevate da qualsiasi soggetto interessato tramite il semplice invio di una lettera alla Registration Authority.

Nel caso in cui le parti non trovino un'accordo sulla controversia, la Registration Authority può proporre un « comitato di arbitrazione (!) » per risolvere rapidamente la questione. Ovviamente l'assoggettamento alla decisione del comitato di arbitrazione è condizionato all'accettazione di entrambe le parti che comunque « possono in ogni caso procedere con i mezzi che riterranno opportuni per dirimere la questione » (art D.4).

Qualora invece le parti accettino l'arbitrato nella forma proposta e disciplinata dal regolamento della Registration Authority, esse saranno soggette alle norme del regolamento stesso che, in modo un poco sommario, determinano la composizione del collegio ed il procedimento di quello che sarà, a tutti gli effetti, un arbitrato irrituale.

D) Infine, una soluzione auspicata da più autori, anche se limitatamente alla materia del diritto d'autore, per superare l'inadeguatezza delle norme esistenti e cercare di regolare in modo specifico il fenomeno INTERNET, è quella della stipulazione di accordi a valenza internazionale.

Le proposte riguardano la stipulazione di convenzioni che uniformino la materia sia dal punto di vista delle norme materiali che da quello delle norme di conflitto.

Fondamentale è una convenzione internazionale di diritto materiale che disciplini in modo uniforme l'esistenza, i contenuti, la titolarità, la violazione e le eventuali licenze del diritto d'autore re-

lativamente ad INTERNET; solo successivamente si potrebbe cercare un criterio di collegamento unico, previsto nella stessa convenzione ovvero in una convenzione specifica, che si adatti ad essere utilizzato a livello internazionale.

Alcuni studi realizzati negli Stati Uniti, anche sulla base di decisioni rese dalla corti americane, hanno portato ad identificare i seguenti criteri come « candidati » al ruolo di norma di conflitto uniforme:

— la legge del luogo di immissione;
— la legge del paese di origine dell'opera;
— la *lex fori*.

Nessuno dei tre criteri sopra indicati è stato però ritenuto soddisfacente.

La legge del luogo di immissione (legge dell'*uploading*), mutua un principio espresso in alcune decisioni delle Corti americane ed, in Europa, dalla Direttiva 93/83/CEE del 27 settembre 1993 sul coordinamento di alcune norme in materia di diritto d'autore e diritti connessi applicabili alla radiodiffusione via satellite ed alla ritrasmissione via cavo.

Per quanto rispondente ad esigenze di semplicità ed uniformità, questa soluzione rischierebbe di essere strumentalizzata a scapito degli autori in quanto sarebbe sufficiente, per il *provider* in mala fede, tasferirsi in un paese in cui la protezione del diritto d'autore è scarsa o inesistente e trasmettere da qui i propri servizi, per aggirare le norme a tutela dell'autore.

La legge del paese di origine dell'opera non è stato ritenuto un criterio soddisfacente in quanto non porterebbe alla applicazione delle norme di un solo ordinamento. Il criterio, introdotto dall'art. 5.4 della Convenzione di Berna si riferisce al Paese di origine quale paese di prima pubblicazione dell'opera o paese di nazionalità dell'autore.

La conseguenza potrebbe essere che il giudice, pur applicando una unica norma di conflitto, si veda obbligato ad applicare diversi ordinamenti nazionali.

Infine, il criterio della *lex fori*, strettamente collegato al principio di territorialità, pur presentando due innegabili vantaggi: una unica legge applicabile; una legge conosciuta dal giudice, potrebbe essere strumentalizzato, questa volta dall'autore danneggiato, il quale potrebbe ricercare un ordinamento a lui particolarmente favorevole e qui iniziare una causa anche in assenza di qualsiasi reale collegamento tra il giudice investito della causa e l'oggetto della controversia.

Ecco perché la conclusione a cui sono giunti tutti gli studiosi che hanno affrontato l'impresa di ricercare una unica norma di conflitto applicabile alla violazione dei diritti di proprietà intellettuale in INTERNET, è che quella norma non esiste, ma che piuttosto è suggeribile combinare più criteri di collegamento tra loro complementari o alternativi.

Ad esempio, è stato proposto di applicare a tutta la materia del diritto d'autore la legge del paese del foro purché sussita almeno un'altro dei seguenti criteri riferibili al paese del foro:

1) si tratti del paese nel quale si è verificato il fatto che ha causato il danno (inteso come paese di prima trasmissione dell'opera); ovvero

2) si tratti del paese del domicilio, residenza o nazionalità del convenuto; ovvero

3) si tratti del paese in cui il convenuto abbia una sede della propria attività.

Secondo un'altra parte della dottrina la legge dell'*uploading* dovrebbe essere la legge regolatrice delle conseguenze della violazione dei diritti di proprietà intellettuale, purché questa possa essere esclusa nel caso in cui, nell'ordinamento richiamato, non esista una disciplina che sia sufficientemente protettiva per l'autore.

Il giudice si troverebbe così a dover affrontare una analisi concreta di diritto materiale, in principio applicando la legge dell'*uploading* eventualmente integrandola con disposizioni più favorevoli all'autore che potrebbero essere contenute in una convenzione internazionale di diritto materiale, o nella legge del luogo in cui si è verificato l'effetto della violazione.

In conclusione, per quanto, come abbiamo dimostrato, le norme di diritto internazionale privato e processuale esistenti possano e debbano essere utilizzate ed applicate dall'interprete a fattispecie che si realizzano in INTERNET adattando i principi espressi da quelle norme alle peculiarità del fenomeno, l'esigenza di un Cyber-code, come è stato definito, è sentita ormai a livello mondiale.

Lo spunto per la creazione di un corpo di norme uniformi non dovrebbe, a mio avviso, prescindere da una analisi di principi che già esistono e sono applicati ad INTERNET.

Si tratta dei principi contenuti nelle numerose decisioni giurisprudenziali statunitensi che l'operatore europeo non può ignorare nell'analisi delle fattispecie verificatesi nel proprio paese, neppure quando affermano, come nella recente sentenza della Corte Federale d'Appello di Philadelphia che ha stabilito la non applicabilità della « Legge per la Decenza nelle Telecomunicazioni » ad INTERNET, che la forza di INTERNET sta proprio nel caos che lo caratterizza.

NOTA BIBLIOGRAFICA.

STEFANIA BARIATTI, ***Internet e il diritto internazionale privato: aspetti relativi alla disciplina del diritto di autore***, **relazione al convegno di Pavia del 4-5 Ottobre 1996, di prossima pubblicazione in *AIDA*, 1996**

ANDRÉ BRUNEL, *Trademark Protection for Internet Domain Names*, in *IBL*, 1996, 174 ss.

PAOLO CERINA, *Satellite ed Internet: superamento del principio di territorialità*, in *Il dir. ind.*, 1996, 511 ss.

FRED CHILTON-SIMON CANT, *Privacy and the Internet*, in *IBL*, 1996, 162 ss.

FRED CHILTON-EMMA MOLONEY, *Regulation on the Internet*, in *IBL*, 1996, 172 ss.

COMMISSIONE EUROPEA, *Comunicazione al Parlamento Europeo, al Consiglio, al Comitato Economico e Sociale, al Comitato delle Regioni su «Informazioni di contenuto illegale e nocivo su Internet»*, del 16 Ottobre 1996, COM (96) 487.

LARS DAVIES, *The Internet and the Elephant*, in *IBL*, 1996, 151 ss.

BARBARA DONATO, *La responsabilità dell'operatore di sistemi telematici*, in questa *Rivista*, 1996, 135 ss.

STEPHEN DOOLEY, *Defamation on the Internet*, in *CTRL*, 1995, 191

IRIS FEROSIE, *Don't Shoot the Messenger: Protecting Free Speech on Editorially Controlled Bulletin Board Services by Applying «Sullivan» Malice*, in *John Marshall Journal of Computer & Information Law*, 1994, 347 ss.

MIKE GODWIN, *Internet Libel: Is the Provider Responsible?*, <mnemonic@eff.org>

ROSARIO IMPERIALI d'AFFLITTO, *Il diritto alle prese con la società dell'informazione*, relazione al Convegno di Milano del 27 Novembre 1996.

CHRISTOPHER KUNER, *Legal Aspects of Encryption in the Internet*, in *IBL*, 1996, 186 ss.

ANTONIO A. MARTINO, *Validità legale internazionale dei contratti di acquisto di beni e servizi tramite Internet*, relazione al Convegno di Milano del 15-16 Maggio 1996 «Conference on Electronic Commerce» sotto gli auspici AIS-Artificial Intelligence Software.

DIANA J.P. MCKANZIE, *Commerce on the Net: Surfing Through Cyberspace Without Getting Wet*, in *John Marshall Journal of Computer & Information Law*, 1996, 247 ss.

CHRISTOFER MILLARD-ROBERT CAROLINA, *A European Perspective*, in *John Mar-shall Journal of Computer & Information Law*, 1996, 269 ss.

KEN MOON, *How important are Internet Domain Names to Trade Mark Owners?*, in *CTRL*, 1996, 79 ss.

RAYMOND T. NIMMER, *Electronic Contracting: Legal Issues*, in *John Marshall Journal of Computer & Information Law*, 1996, 211 ss.

R. CLIFFORD POTTER, *Cyber Age and Internet Ethics*, in *IBL*, 1996, 162 ss.

PHILLIP E. REIMAN, *Cryptography and the First Amendment: The Right to Be Unheard*, in *John Marshall Journal of Computer & Information Law*, 1996, 325 ss.

MARCO RICOLFI, *Internet e le libere utilizzazioni*, relazione al Convegno di Pavia del 4-5 Ottobre 1996, di prossima pubblicazione in *AIDA*, 1996

HAMISH R. SANDISON, *International Legal Problems of the Electronic Commerce on the Internet*, relazione al Convegno di Milano del 15-16 Maggio 1996 «Conference on Electronic Commerce» sotto gli auspici di AIS - Artificial Intelligence Software.

DAVIDE SARTI, *I soggetti di Internet*, relazione al Convegno di Pavia del 4-5 Ottobre 1996, di prossima pubblicazione in *AIDA*, 1996

GRAHAM J.H. SMITH et al., *Internet Law and Regulation*, FT Law & Tax, London, repr. 1996

VICTOR TIMON, *The Internet: Some Important Legal Issues*, in *CTRL*, 1995, 35 ss.

LUCA TREVISAN, *L'impatto di Internet e delle altre reti sul regime giuridico dell'opera multimediale*, relazione inedita.