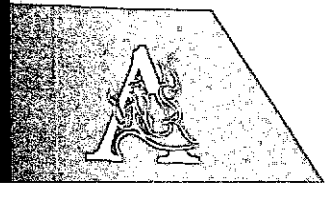
Anno1 - n. 2

COMUNICAZIONE DIGITALE

Periodico semestrale
del Centro Studi Comunicazione Istituzionale
e Innovazione Tecnologica (ComIT)

contributi di
Ilaria Batassa
Mirto Silvio Busico
Eva Carducci
Francesco Di Ciommo
Federica Galuzzo
Paolo Pomati
Alberto Reda
Saverio Rubini
Federica Silvestrini
Elisabetta Zuanelli



COMUNICAZIONE DIGITALE

ANNO I - n. 2

Segreteria di Redazione
ComIT
Piazza della Cancelleria, 85 – 00186 Roma
Tel. +39 06 6839 2146 – fax +39 06 6821 1644
redazione@icomit.it – www.icomit.it

Registrazione
Tribunale di Roma
n. 195 del 12.5.2005

Comunicazione digitale

Periodico semestrale
del Centro Studi Comunicazione Istituzionale
e Innovazione Tecnologica (ComIT)

a cura di

Contributi di
Ilaria Batassa
Mirto Silvio Busico
Eva Carducci
Francesco Di Ciommo
Federica Galuzzo
Paolo Pomati
Alberto Reda
Saverio Rubini
Federica Silvestrini
Elisabetta Zuanelli

www.aracneeditrice.it
info@aracneeditrice.it

via Quarto Negroni, 15
00040 Ariccia (RM)
(06) 93781065

ISBN 978-88-548-8053-5
ISSN 2284-1725

I edizione: dicembre 2014

Indice

MERCATI E TENDENZE

OPINIONI

EVENTI

L'accesso a Internet tra diritto e responsabilità[1]

Francesco Di Ciommo

1. Internet, comunità virtuali e società globale

L'evoluzione delle società tecnologizzate negli ultimi lustri ha subìto una rapidissima, forse imprevista, accelerazione, dipesa *in primis* dalla semplificazione delle modalità di utilizzazione delle risorse informatiche e rafforzata dalla diffusione capillare che la rete Internet e le tecnologie digitali hanno avuto in tutto il mondo progredito[2].

L'avvento della tecnologia digitale – e più ancora di Internet, cioè della piattaforma (o rete) che valorizza al meglio tale tecnologia – in breve tempo ha cambiato il modo in cui l'uomo si relaziona con i prodotti, con le informazioni, con i suoi simili e con se stesso; in definitiva

[1] *Paper* presentato al convegno *Mercati digitali, innovazione tecnologica, sicurezza informatica: la visione nazionale e internazionale. Spunti problematici per il semestre di presidenza europea*, Roma, 10 luglio 2014. Vd. *Editoriale*.

[2] Per gli opportuni approfondimenti circa i temi trattati, oltre agli scritti citati nelle note seguenti, giova rinviare sin d'ora a: F. DI CIOMMO, s.v. "Internet (responsabilità civile)", in *Enciclopedia giuridica Treccani*, Aggiornamento, Roma, 2002; ID., *Evoluzione tecnologica e regole di responsabilità civile*, Edizioni Scientifiche Italiane, Napoli, 2003; ID., "Internet e crisi del diritto privato: globalizzazione, dematerializzazione e anonimato virtuale", in *Rivista critica del diritto privato*, 2003, 21, 1 (2003), pp. 57-116; ID., "La responsabilità civile in Internet: prove tecniche di governo dell'anarchia tecnocratica", in *La Responsabilità Civile*, 6 (2006), pp. 548-563; ID., "Civiltà tecnologica, mercato ed insicurezza", in *Rivista critica del diritto privato*, 28, 4 (2010), pp. 565-596; nonché P. PASSAGLIA, *Diritto di accesso ad Internet e giustizia costituzionale comparata. Una (preliminare) indagine comparata*, disponibile on-line all'indirizzo "http://www.giurcost.org/studi/passaglia.htm"; e T.E. FROSINI, *Il diritto costituzionale di accesso ad Internet*, in *Rivista telematica giuridica dell'Associazione Italiana Costituzionalisti*, disponibile on-line all'indirizzo "file:///C:/Users/Client%205/Downloads/ Frosini.pdf"

essa ha cambiato il modo in cui l'uomo abita la terra, sublimando quel concetto di *ambiente* tecnologico nel quale le dimensioni spaziali e temporali, su cui ragionava Aristotele, semplicemente non esistono più.

Parlare di era digitale – moda oramai invalsa in ogni campo del sapere – serve, dunque, a evidenziare le radicali trasformazioni che hanno, negli ultimi dieci anni, coinvolto il nostro modo di relazionarci con le cose, con gli eventi, con le informazioni e con gli altri. 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). È forse la prima volta nella storia recente dell'umanità che un'innovazione di processo influenza in modo tanto diretto i comportamenti umani al punto 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 a Internet da qualsiasi altro luogo, o sfruttare un servizio prestato *online* da un server fisicamente ubicato ovunque, come se i suoi interlocutori si trovassero, in quel preciso istante, di fronte a lui[3]. 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[4].

[3] 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*, Harvard Business School Press, Boston, 1997, il quale, per inciso, sembra voler evocare G. GILMORE, *The Death of Contract*, State University Press, Columbus, Ohio, 1974 = vers. it. *La morte del contratto*, trad. di

La realità della comunicazione in Internet, tuttavia, a prima vista non distingue il nuovo *medium* dal telefono, dalla televisione o dalla radio, in quanto, per comprendere sino in fondo la portata innovativa del fenomeno in parola, occorre far riferimento ad altre caratteristiche tecniche del *cyberspace*[5]. In particolare, giova evidenziare come attraverso Internet possano essere trasferiti materiali di vario tipo (testi, suoni, disegni, fotografie, filmati, ecc.), circostanza che rende la comunicazione in rete più complessa e completa rispetto a ogni altra forma di comunicazione a distanza sinora conosciuta. Si parla a tal proposito di *multimedialità*. Inoltre in Internet è possibile costruire spazi virtuali (i cosiddetti *siti web*), che offrono servizi o prodotti perennemente a disposizione di utenti che li vogliano visitare con finalità informative, ludiche, commerciali e quant'altro. All'interno del Web l'utente, sfruttando la tecnologie ipertestuale, può muoversi liberamente scegliendo che cosa fare e come farlo, che cosa cercare e attraverso quali traiettorie. Proprio per questo la cosiddetta navigazione in Internet è definita "interattiva": l'utente non subisce, più o meno, passivamente la comunicazione che gli arriva 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.

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.

[4] Circa l'origine del termine "telematica", cfr. G. FROSINI, s.v. "Telematica ed informatica giuridica", in *Enciclopedia del Diritto*, vol. XLIV, Giuffrè, Milano, 1992, pp. 60-82; nonché G. RICHIERI, "Le autostrade dell'informazione. Modelli e problemi", in *Problemi dell'informazione*, 1 (1995), Il Mulino, Bologna, pp. 25-38

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

2. Dalla proprietà all'accesso. Internet come luogo cui accedere

In un fortunato libro del 2000 Jeremy Rifkin ha sottolineato come, nella società attuale, al diritto di proprietà tradizionale si vada sostituendo il cosiddetto *diritto all'accesso*. Rifkin parla di *era dell'accesso*, pensando a un mondo in cui «il fornitore mantiene la proprietà di un bene, che noleggia o affitta o è disposto a cedere in uso temporaneo a fronte del pagamento di una tariffa, di un abbonamento, di una tassa di iscrizione. Lo scambio di proprietà fra compratori e venditori – l'aspetto più importante del moderno sistema di mercato – cede il passo a un accesso temporaneo che viene negoziato tra *client* e *server* operanti in una relazione di rete»[6].

Lo scenario, prospettato dall'autore nordamericano come prossimo a radicarsi in tutte le società evolute, in Internet è già una realtà. Nella più grande rete telematica a oggi operante, infatti – e sebbene ciò, sinora, sia passato, tra i cultori delle diverse branche del sapere, quasi «sotto silenzio»[7] – i rapporti e le dinamiche sociali si sviluppano attraverso la dialettica costante tra due categorie di soggetti: da una parte, coloro che forniscono l'accesso a uno o a più servizi, a una o a più

[6] Il riferimento è a J. RIFKIN, *L'era dell'accesso. La rivoluzione della new economy*, trad. di P. Canton, Mondadori, Milano, 2001 [2000], in part. pagg. 6 e 7. Per avvertire ancora più distintamente la novità del quadro che, in relazione a tali questioni, si va delineando sulle reti telematiche, giova prendere in considerazione il concetto *tradizionale* di bene inteso in senso giuridico e vagliare le forme classiche di appartenenza operanti nel nostro ordinamento. Su entrambe le questioni, si segnala la riflessione pluriennale di O.T. SCOZZAFAVA condotta principalmente attraverso questi studi: *I beni e le forme giuridiche di appartenenza*, Giuffrè, Milano, 1982; s.v. "Oggetto dei diritti", *Enciclopedia Giuridica Treccani*, Roma, 1990, vol. XXI; *Dei beni (art. 810-821)*, Giuffrè, Milano, 1999.

[7] I giuristi non sembrano ancora aver preso piena coscienza dell'importanza che il diritto di accesso va acquisendo nella nostra vita di tutti i giorni. RIFKIN, *L'era dell'accesso*, cit., pp. 154-155, in proposito osserva: «Diversamente da quanto è accaduto con l'avvento della proprietà privata, i cui vantaggi e svantaggi furono oggetto di discussione tra filosofi, economisti e politici al punto da generare un acceso dibattito sociale, l'accesso è penetrato nella società e si è fatto strada fino ai più reconditi recessi della vita pubblica e privata passando quasi completamente sotto silenzio. Il passaggio dalla proprietà all'accesso è un evento impercettibile: la trasformazione, a volte, appare così subdola da essere difficilmente visualizzabile e assolutaz

banche dati, a uno o a più luoghi virtuali; dall'altra, gli utenti che utilizzano tali accessi per sviluppare la propria esperienza esistenziale di rete[8]. Vale, dunque, svolgere un riferimento al concetto di interattività della realtà digitale *online*, così come essa si va sviluppando tramite Internet, ma tale discorso deve essere integrato da una considerazione ulteriore volta a rilevare come, nel rapporto interattivo tra utente e realtà di rete, sia fondamentale il ruolo svolto dagli intermediari. La novità rispetto al passato sta nel fatto che in Internet operano decine di migliaia di intermediari, il che toglie a questi la possibilità di svolgere efficacemente ruoli di controllore o censore.

A ben vedere, la vita dell'uomo postmoderno, ormai anche nella realtà *offline*, relativamente agli aspetti concernenti l'accesso (alle informazioni, ai servizi, al divertimento, ecc.), viene modellata da decisioni che nessuno prende singolarmente e che vengono adottate da milioni di *guardiani*, i quali, a seconda delle proprie competenze e attribuzioni, disegnano i contorni dell'ambiente tecnologico in cui ci muoviamo e ci consegnano gli strumenti di cui possiamo servirci per relazionarci con il mondo e con le cose[9].

In definitiva, la nostra percezione del mondo dipende, oggi che abbiamo per la più parte sostituito la *nostra* esperienza diretta del reale con quella mediata da strumenti tecnologici, da scelte compiute da altri che possono o meno darci un certo strumento o una determinata notizia, in una certa forma, con certe modalità, piuttosto che in altre.

Questo ruolo, in passato, è stato svolto da soggetti istituzionali legati al sistema di governo delle comunità sociali. *Gatekeepers*, per esempio, sono stati i giornalisti, gli editori, in generale le istituzioni

[8] Discorrendo dell'importanza dell'accesso nella vita dell'uomo postmoderno, non dobbiamo esclusivamente pensare all'accesso fisico ad un servizio, bensì anche all'accesso alla conoscenza, all'informazione, al divertimento, ecc.: in breve, all'accesso alle *risorse*. A questo proposito, «è opportuno segnalare, a scanso di equivoci e fraintendimenti, che [quantomeno dal punto di vista terminologico] la fornitura dell'accesso per via telematica alle informazioni computerizzate è cosa diversa dalla fornitura della connessione a un'infrastruttura che consente il collegamento con un *network* di sistemi informativi automatizzati» (così R. PARDOLESI e A. PALMIERI, "Gli 'Access contract': una nuova categoria per il diritto dell'età digitale", in *Rivista di diritto privato*, 7, 2 (2002), pp. 265-286.

[9] Per gli opportuni approfondimenti ed ulteriori spunti di riflessione sul punto, v. A. MANDELLI, *Il mondo in rete*, Egea, Milano, 2001, in part. 191-206.

culturali, politiche e scientifiche, i fornitori di servizi o i produttori di determinati beni e così via. Oggi, al contrario, in Internet chiunque, creando un proprio sito, ovvero sfruttando un sito altrui, può diffondere, nell'intera comunità cibernetica e a livello globale, qualsiasi tipo di informazione; la qual cosa, se, da un lato, sottrae credibilità e forza al singolo dato diffuso in rete, visto che non sempre è possibile controllarne la paternità e la attendibilità, a livello aggregato consente di affermare che, tramite Internet, l'uomo si è definitivamente immerso nel mondo dell'informazione cosiddetta *plurale*[10].

Dal punto di vista tecnico, il pianeta Internet ruota intorno a operatori professionali che acquistano accessi alla rete dalle agenzie competenti e li distribuiscono agli utenti, ovvero che consentono a questi ultimi di accedere *online* a servizi o risorse messi a disposizione nel Web. Queste attività, che potremmo genericamente definire "di portineria", sono svolte dagli *Internet Provider* (i cosiddetti ISP).

Con la generica qualifica di *provider* si fa generalmente riferimento a una pluralità di soggetti che rientrano nella categoria degli operatori che la direttiva 2000/31/Ce definisce «prestatori di servizi della società dell'informazione». Ai fini di questa riflessione, le diverse tipologie di *provider* devono essere tenute ben distinte, in quanto, mentre l'*access provider* fornisce agli utenti la connessione alla rete[11], il *service provider* fornisce servizi ulteriori (caselle *e-mail*, *chatroom*, *forum* telematici, *newsgroup*, motori di ricerca, gestione di banche dati, bacheche elettroniche in cui gli utenti possono pubblicare i propri materiali e quant'altro), e il *content provider* veicola in rete, tramite il suo sito, propri contenuti (notizie di cronaca, ricette di cucina, fotografie d'autore, sentenza della Suprema Corte di Cassazione, racconti, barzellette, ecc.)[12]. L'*host provider*, infine, è un *service provider* che mette a disposizione uno spazio del disco rigido del proprio *server* per "ospitare" i siti creati da utenti che desiderano svolgere il ruolo di *service* o *content provider*, pur non avendo a disposizione le necessarie tecnologie.

È bene chiarire che a queste figure di intermediari si deve aggiungere quella del cosiddetto *maintainer*, che non è un vero e proprio *provider*, in quanto non è un intermediario di Internet, bensì un operatore che interagisce burocraticamente e tecnicamente, per conto di un *provider* che intende "aprire" un sito web, con gli enti preposti alla registrazione dei nomi di dominio.

[10] Per interessanti considerazioni sulla c.d. società dell'informazione "plurale", v. l'agile volumetto di G. DA EMPOLI, *Overdose. La società dell'informazione eccessiva*, Marsilio, Venezia, 2002.

[11] Sulla natura, i problemi giuridici e la disciplina del contratto di accesso, vd. l'ampia riflessione di A. PALMIERI, *I contratti di accesso*, Giuffrè, Milano, 2002. Cfr. anche L. ALBERTINI, "I contratti di accesso ad Internet", in *Giustizia civile*, 2 (1997), pp. 95-116 e partic. 103; nonché, P. LE TOURNEAU, *Théorie et pratique des contracts informatiques*, Dalloz, Paris, 2000, che, in proposito, parla di «fornitura di accesso». In linea di massima, può dirsi che il rapporto tra *access provider* e utente, in mancanza di apposite norme, può essere ricondotto sotto la categoria dell'appalto di servizi, in quanto contiene alcuni elementi tipici dell'appalto (la realizzazione di un servizio a favore dell'utente) e altri della somministrazione (la continuità della prestazione); mentre non può essere ricondotto a questa seconda tipologia contrattuale in quanto, come sottolinea la dottrina maggioritaria, la somministrazione ha per oggetto esclusivamente "cose", e dunque non "servizi". L'art. 1559 c.c., del resto, fa espresso e inequivocabile riferimento a «prestazioni periodiche o continuative di cose». Né sembra possibile il riferimento al contratto d'opera intellettuale (ma, sul punto, cfr. E. MOSCATI, "L'appalto di sistemi e di servizi informatici", in G. ALPA e V. ZENO-ZENCOVICH, *I contratti di informatica. Profili civilistici, tributari e di bilancio*, Giuffrè, Milano, 1987, pp. 227 ss. e partic. 231). Negli Stati Uniti regole *ad hoc* – che, a dire il vero, stanno trovando difficoltà a essere recepite dai singoli stati della confederazione – sono contenute nel recente *Uniform Computer Information Transaction* Act, UCITA, prodotto dalla National Conference of Commissioners of Uniform State Laws. La § 102(a)(1) dell'UCITA definisce l'*access contract* come «a contract to obtain by electronic means access to, or information from, an information processing system of another person, or the equivalent of such access». L'ampia definizione ha consentito ad una parte della dottrina di sostenere che le regole dell'UCITA, dedicate all'*access contract*, siano applicabili a molte operazioni contrattuali aventi per oggetto servizi ulteriori rispetto all'accesso e, in definitiva, a tutti i contratti tra *provider* e utenti. Così, tra gli altri, M. STEWART, "Commercial Access Contracts and the Internet: Does the Uniform Computer Information Transaction Act Clear the Air with Regard to Liabilities when on On-line Access System Fails?", in *Pepperdine Law Review*, 27, 3 (2000), pp. 597-627.

[12] Il rapporto contrattuale tra un *service provider* o un *content provider* e un utente può assumere diverse configurazioni giuridiche. Esso può, per esempio, riguardare l'utilizzazione, da parte dell'utente, di una banca dati, ovvero la fruizione di un servizio di posta elettronica o di un motore di ricerca o di un *newsgroup*, ecc. La qualificazione contrattuale del rapporto e la conseguente disciplina giuridica varieranno a seconda delle circostanze.

Le differenze funzionali ora segnalate si rivelano particolarmente importanti nell'ottica di un corretto inquadramento delle responsabilità degli operatori di Internet, e ciò in quanto – al contrario di quanto la dottrina (non solo) italiana ha fatto in questi anni – occorre riflettere sui criteri di imputazione della responsabilità civile in Internet, distinguendo nettamente gli argomenti a seconda della qualifica assunta, nelle singole fattispecie, dal *provider* eventualmente convenuto per il risarcimento del danno.

A questo proposito, è bene avvertire che la ripartizione sopra proposta raramente è in grado di qualificare a priori e definitivamente il ruolo svolto da un *provider*, visto che spesso accade che le qualifiche si sovrappongano, in quanto un solo operatore può fornire l'accesso, offrire servizi, ospitare siti altrui e veicolare propri contenuti in rete. Ciò significa che l'esatta funzione, svolta dal singolo intermediario in relazione alla fattispecie concreta, andrà indagata caso per caso per verificare l'esatta qualifica che spetta a quel soggetto e il relativo regime di responsabilità.

Altra differenza da non sottovalutare, nell'economia dell'analisi che si va conducendo, è quella tra *provider* che traggono profitti dalla loro attività e *provider* cosiddetti amatoriali o istituzionali. Per *provider* istituzionali si intendono i centri di cultura, le scuole, gli enti pubblici preposti ad attività particolari, che abbiano strutture idonee a fornire il servizio di accesso alla rete; per *provider* amatoriali, singoli o associazioni che, senza alcun fine di lucro, né di ricerca, organizzano modeste strutture in grado di consentire il collegamento e la diffusione di materiali nel ciberspazio. A questi si contrappongono i *provider* professionisti, per lo più società, che curano tale servizio a fini di lucro e che, dunque, si presumono avere un'adeguata organizzazione. In virtù di tale prerogativa, i *provider* professionisti sono considerati, da una parte della dottrina, i soli soggetti in grado di risarcire i danni a terzi causati dagli illeciti compiuti dagli *user*[13]. Ciò in quanto essi assumerebbero tale rischio a fronte di una remunerazione e inoltre potrebbero, considerata l'organizzazione e la struttura di cui normalmente dispongono, apprestare sistemi di controllo sui contenuti che veicolano in rete.

[13] Cfr. B. DONATO, *La responsabilità dell'operatore di sistemi telematici*, in *Il*

Ai *provider* può essere astrattamente imputata una qualche responsabilità, per:

- sospensione o interruzione dei servizi (l'ipotesi riguarda tutte le categorie di *provider* sopra descritte);
- fatto compiuto in rete da soggetti anonimi il cui IP (*Internet protocol*) resta non individuato per colpa del *service provider* gestore del servizio tramite il quale l'illecito è stato realizzato;
- illiceità di propri materiali veicolati in rete dal *content provider*;
- fatto illecito compiuto da utenti che restano anonimi in quanto l'*access provider* non riesce a impedire l'accesso abusivo ovvero a fornire la reale identità dei propri clienti. La disciplina della responsabilità dei *provider* è oggi in Europa contenuta nella direttiva 2000/31/Ce, recepita in Italia con il d.lgs. 70/2003.

3. Il diritto di accesso a Internet

Quello dell'accesso a Internet dei singoli individui, così come delle organizzazioni e delle istituzioni, costituisce oggi uno dei temi giuridici e politici più discussi in tutto il mondo, non solo dai cultori del diritto delle nuove tecnologie.

Con la locuzione *accesso a Internet* si fa riferimento alla possibilità per ogni cittadino – ovvero, in altra accezione, per ogni essere umano o comunque per ogni associazione, società, ente e quant'altro – di accedere alla rete telematica per eccellenza, e così poter esercitare i propri diritti fondamentali ad informarsi, esprimersi, comunicare, sapere, informare e altro. In breve, considerata l'importanza che la grande Rete e, più in generale, la tecnologia digitale, ha assunto nel mondo contemporaneo, può dirsi che il diritto all'accesso alla Rete è oggi considerato uno snodo fondamentale per garantire il pieno sviluppo della personalità umana. Tanto ciò è vero che recentemente l'accesso a In-

ternet è stato configurato alla stregua di un vero e proprio diritto soggettivo in diversi ordinamenti giuridici nazionali[14].

La Finlandia è stato il primo Paese al mondo che ha riconosciuto, per legge, dal 1° luglio 2010, la connessione a Internet in banda larga come vero e proprio diritto di ogni singolo cittadino, con la conseguenza che gli operatori/*provider* presenti nel Paese, in quanto "fornitori di un servizio universale", dovranno mettere a disposizione dei cittadini una connessione in grado di assicurare a ogni abitazione e/o ufficio una velocità di *download* dei dati di almeno un megabit al secondo. A lungo termine, l'obiettivo perseguito dalla riforma in parola è quello di fornire a tutta la popolazione una connessione a 100 Mbps entro il 2015, diffondendo le percentuali di accessibilità anche nelle zone remote, particolarmente influenzate dalle dinamiche del *digital divide*.

In Spagna, in forza dell'approvazione della legge n. 2 del 4 marzo 2011, è stato stabilito che la connessione a banda larga (a una velocità di 1 Mbit al secondo) deve essere garantita a ogni cittadino tramite qualsiasi tecnologia, allo scopo di diffondere in maniera omogenea i servizi telematici su tutto il territorio nazionale. In particolare, l'art. 52 di tale legge inserisce espressamente la banda larga tra gli obblighi del servizio universale, da assicurarsi con l'utilizzo di qualsiasi tecnologia e indipendentemente dalla disponibilità di infrastrutture fisse.

Nel febbraio del 2000 in Estonia il Parlamento ha promulgato la nuova legge sulle telecomunicazioni, qualificando espressamente l'accesso a Internet come servizio universale. L'art. 5, commi 1 e 2 della legge n. 151 del 2010 ricomprende Internet tra i servizi di telecomunicazione, aggiungendo che tali servizi devono essere universalmente disponibili per tutti i cittadini, indipendentemente dalla loro ubicazione geografica, a un prezzo uniforme e accessibile[15].

[14] Nel 2013 anche il Parlamento dell'Unione europea, su iniziativa di un privato, ha cominciato a valutare una richiesta di introduzione di un nuovo art. 3-bis TUE circa il "Diritto di accesso ad Internet nella Società europea dell'Informazione", recante norme volte a garantire il riconoscimento del diritto di accesso a Internet tra i principi fondamentali dell'Ue.

[15] In particolare, grazie a questa importante riforma legislativa, il *Telecommunications Act* del febbraio 2000 ha inserito l'accesso alla rete nel novero degli obblighi di servizio universale, allo scopo di eliminare ogni possibile discriminazione so-

A livello internazionale il Consiglio sui diritti umani delle Nazioni Unite ha diramato, nel 2013, una risoluzione (la A/HCR/20/L.13) che ha considerato espressamente Internet quale diritto fondamentale dell'uomo, ricompreso nell'art. 19 della Dichiarazione universale dei diritti dell'uomo e del cittadino. Nel documento si attribuisce alla rete «una forza nell'accelerazione del progresso verso lo sviluppo nelle sue varie forme» e chiede a tutti di provvedere a realizzare e potenziare le strutture che concretamente possano garantire l'accesso a Internet a tutti i cittadini a parità di condizioni, abbattendo così il *digital divide*.

Sempre l'Onu, nel Rapporto dell'agosto 2011 sulla promozione e la protezione del diritto di opinione ed espressione[16], ha affermato che «gli Stati hanno un obbligo positivo a promuovere o a facilitare il godimento del diritto alla libertà di espressione e dei mezzi di espressione necessari per esercitare questo diritto, compreso Internet», considerando «l'accesso a Internet un mezzo indispensabile per la realizzazione di una serie di diritti umani, combattendo l'ineguaglianza e accelerando lo sviluppo e il progresso dei popoli», con la conseguenza che «l'accesso a Internet è uno degli strumenti più importanti di questo secolo per aumentare la trasparenza, per accedere alle informazioni e per facilitare la partecipazione attiva dei cittadini nella costruzione delle società democratiche».

In Costa Rica, la *Sala Constitucional* (la Corte Costituzionale), con una pronuncia del 30 luglio del 2010 n. 12790, ha affermato che «il ritardo del governo ad aprire il mercato delle comunicazioni alla concorrenza equivale a una violazione delle libertà fondamentali, arrecando un grave pregiudizio alla libertà di scelta dei consumatori e all'eliminazione del *digital divide*». Secondo le argomentazioni della Corte «l'evoluzione negli ultimi venti anni in materia di tecnologia dell'informazione e della comunicazione [...] ha rivoluzionato l'ambiente sociale dell'essere umano [...], con la conseguenza che può affermarsi che questa tecnologia ha avuto un impatto significativo

larmente influenzate dal fenomeno del *digital divide* a causa di problemi nell'accesso alla rete e nell'offerta di ragionevoli tariffe nell'erogazione dei servizi di connessione.

[16] Il rapporto, intitolato *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression* (A/HRC/17/27), è fir-

sul modo nel quale l'essere umano comunica, facilitando la relazione tra persone ed istituzioni a livello mondiale ed eliminando la barriera di spazio e tempo. Ne discende che l'accesso a queste tecnologie si converte in uno strumento primario per agevolare l'esercizio dei diritti fondamentali, come, tra gli altri, la partecipazione democratica (democrazia elettronica) e il controllo dei cittadini, la formazione, la libertà di espressione e di pensiero, l'accesso all'informazione ed ai servizi pubblici online, il diritto a rapportarsi con i pubblici poteri attraverso strumenti elettronici e la trasparenza amministrativa». In questo modo la *Sala Constitucional* ha riconosciuto il ruolo di Internet come strumento fondamentale della comunicazione interpersonale, agevolando il rapporto tra i cittadini privati e i pubblici poteri, mediante il superamento di barriere tecniche che gli strumenti tradizionali non erano in grado di eliminare.

In due Paesi, Grecia ed Ecuador, il diritto di accesso a Internet è stato addirittura inserito espressamente nella carta costituzionale. In particolare, in Grecia, a seguito della revisione del 6 aprile 2001, è stato introdotto nella Costituzione l'art. 5A, comma 2, a tenore del quale «ognuno ha il diritto di partecipare alla Società dell'informazione» e «lo Stato ha l'obbligo di agevolare l'accesso alle informazioni che circolano in forma elettronica, nonché la produzione, lo scambio e la diffusione di queste informazioni».

Più articolata è la disciplina che reca la Costituzione dell'Ecuador del 2008, la quale, all'art. 16, esprime l'esistenza del diritto soggettivo all'accesso alle tecnologie della comunicazione e della informazione[17], e nel successivo art. 17 rafforza tale riconoscimento attraverso la esplicita previsione di impegni che lo Stato si assume per rendere effettivo tale diritto[18].

[17] Questo il testo dell'art. 16: «Todas las personas, en forma individual o colectiva, tienen derecho a: [...] 2. El acceso universal a las tecnologías de información y comunicación. 3. La creación de medios de comunicación social, y al acceso en igualdad de condiciones al uso de las frecuencias del espectro radioeléctrico para la gestión de estaciones de radio y televisión públicas, privadas y comunitarias, y a bandas libres para la explotación de redes inalámbricas».

[18] Questo il testo dell'art. 17: «El Estado fomentará la pluralidad y la diversidad en la comunicación, y al efecto: 1. Garantizará la asignación, a través de métodos

Di sicuro interesse, nell'ambito della presente riflessione, sono anche alcune decisioni di organi di giustizia costituzionale che hanno avuto esplicitamente ad oggetto la collocazione *sub specie juris* del diritto di accesso a Internet[19]. Il riferimento, in particolare, è alla *Décision* n. 2009-580 DC, 10 giugno 2009, resa dal *Conseil constitutionnel* francese[20], e, più di recente, la *sentencia* 30 luglio 2010, n. 12790, del-

dioeléctrico, para la gestión de estaciones de radio y televisión públicas, privadas y comunitarias, así como el acceso a bandas libres para la explotación de redes inalámbricas, y precautelará que en su utilización prevalezca el interés colectivo. 2. Facilitará la creación y el fortalecimiento de medios de comunicación públicos, privados y comunitarios, así como el acceso universal a las tecnologías de información y comunicación en especial para las personas y colectividades que carezcan de dicho acceso o lo tengan de forma limitada. 3. No permitirá el oligopolio o monopolio, directo ni indirecto, de la propiedad de los medios de comunicación y del uso de las frecuencias».

[19] Per un'ampia riflessione in tema di nuove tecnologie e costituzioni, cfr. R. LEENES, B.-J. KOOPS e P. DE HERT (a cura di) *Constitutional Rights and New Technologies. A Comparative* Study, Nationaal Programma Informatietechnologie en Recht, Tilburg Iinstitute for Law, Technology, and Society, The Hague, TMC Asser Press for for ITeR, Cambridge University Press, Cambridge, 2006. Circa le prime considerazioni della Corte europea dei diritti dell'uomo in materia, cfr. T. MURPHY e G. CUINN, "Works in Progress: New Technologies and the European Court of Human Rights", in *Human Rights Law Review*, 10, 4 (2010), pp. 601-638 e partic. 636.

[20] La decisione è consultabile *online* alla pagina http://www.conseil-constitutionnel.fr/conseil-constitutionnel/root/bank/download/cc-2009580dc.pdf; una traduzione in lingua italiana è stata pubblicata da *Il diritto dell'informazione e dell'informatica*, 3 (2009), pp. 524-533 Sulla pronuncia, v. J.-M. BRUGUIÈRE, "Loi «sur la protection de la création sur Internet»: mais à quoi joue le Conseil constitutionnel?", in *Recueil Dalloz*, 2009, pp. 1770 ss.; L. MARINO, "Le droit d'accès à Internet, nouveau droit fondamental", in *Recueil Dalloz*, 2009, pp. 2045 ss.; W. BENESSIANO, "L'inconstitutionnalité, sanction de l'identification d'un pouvoir de répression pénale dévaluć", in *Revue française de droit constitutionnel*, 81 (2010), 168-174.; nella dottrina italiana, vd. G. VOTANO, "Internet fra diritto d'autore e libertà di comunicazione: il modello francese", in *Il diritto dell'informazione e dell'informatica*, 25, 3 (2009), pp. 533-546.; B. CAROTTI, "L'accesso alla rete e la tutela dei diritti fondamentali (Commento a *Conseil Constitutionnel, décision* 10 giugno 2009, n. 2009-580)", in *Giornale di diritto amministrativo*, 6 (2010). pp. 643-649; N. LUCCHI, "La legge «Création et Internet»: le censure del Conseil constitutionnel", in *Quaderni costituzionali*, 2010, pp. 375-378; P. PASSAGLIA, "L'accesso ad Internet è un diritto (il Conseil constitutionnel francese dichiara l'incostituzionalità di parte della c.d. «legge anti file-sharing»)", in *Il Foro italiano*,

la *Sala Constitucional de la Corte Suprema de Justicia* costaricense[21], che – oltretutto – alla prima si richiama esplicitamente, aggiungendovi però ulteriori considerazioni e valutazioni.

Tali ultime pronunce, sebbene rappresentino solo primissimi passi nella direzione della esatta definizione tecnica dei contenuti e del perimetro operativo del diritto di accesso a Internet, appaiono senz'altro in linea con la Dichiarazione di Reykjavik su «una nuova concezione dei *media*» adottata in seno al Consiglio d'Europa[22]. Circostanza questa che evidenza un *trend* evolutivo di particolare rilievo.

Le vicende normative, istituzionali e giurisprudenziali appena richiamate inducono a porsi alcuni interrogativi circa i confini oggettivi del diritto di accesso a Internet e le finalità alle quali tale diritto dovrebbe essere orientato.

4. I confini oggettivi dell'accesso.

Per definire concretamente in che cosa consista l'acceso a Internet, e dunque qual4 sia il perimetro oggettivo del relativo diritto, occorre comprendere che cosa sia effettivamente, sul piano giuridico, la grande rete telematica.

La prima risposta a questa domanda, in ordine di tempo, viene dalla giurisprudenza nordamericana, che, nella ormai celeberrima sentenza sul caso *Reno vs. American Civil Liberties Union*, del 1997[23], ha defi-

[21] In proposito, v., *ex multis*, P. DE HERT e D. KLOZA, "Internet (access) as a new fondamental right. Inflating the current rights framework?", in *European Journal of Law and Technology*, Vol. 3, No. 3, 2012. Cfr. *UN: ARTICLE 19 calls for global access to the Internet*, press release, 21st October 2011, pubblicato alla pagina http://www.article19.org/resources.php/resource/2790/en/un:-article-19-calls-for-global-access-to-the-internet.

[22] La dichiarazione politica è stata redatta in occasione della Prima Conferenza del Consiglio d'Europa dei ministri responsabili dei *media* e dei nuovi servizi di comunicazione, *Une* nouvelle *conception des médias?*, Reykjavik, Islanda, 28-29 maggio 2009, consultabile *online* alla pagina http://www.coe.int/t/dghl/standardsetting/ media/ MCM%282009%29011_fr_fin_web.pdf.

[23] La decisione, del 26 giugno 1997, è consultabile *online* alla pagina [illegible] ed è pubblicata in *Reno* v *American*

nito Internet «un mezzo di comunicazione tra gli uomini di tutto il mondo unico e completamente nuovo», al quale «gli individui possono avere accesso [...] da molte fonti diverse», e precisava che «chiunque abbia accesso ad *Internet* può trarre beneficio da un'ampia varietà di metodi di comunicazione e di recupero di informazioni»[24].

In tale arresto giurisprudenziale si coglie la valorizzazione di un carattere essenziale di *Internet*, e cioè il suo rientrare – indiscutibilmente – nel *genus* dei mezzi di comunicazione, senza poter essere, tuttavia, assimilato ad alcun altro mezzo di comunicazione esistente, visto che Internet non è soltanto un mezzo di comunicazione[25].

the Court, vd. R. TARCHI (a cura di), *Corso di diritto comparato. Casi e materiali*, vol. I, Giuffrè, Milano, 1999, pp. 203 ss. Essa rappresenta il primo intervento della Corte suprema federale relativo ai contenuti presenti su Internet. Nella specie è stata dichiarata l'incostituzionalità di alcune disposizioni del *Communication Decency Act of 1996*, in quanto contrastanti con la *freedom of speech* sancita dal Primo emendamento.

[24] Nella sentenza si legge epressamente che: «The Internet is a unique and wholly new medium of worldwide human communication. [...] Individuals can obtain access to the Internet from many different sources, generally hosts themselves or entities with a host affiliation. [...] Anyone with access to the Internet may take advantage of a wide variety of communication and information retrieval methods. These methods are constantly evolving and difficult to categorize precisely. But, as presently constituted, those most relevant to this case are electronic mail (e-mail), automatic mailing list services ("mail exploders," sometimes referred to as "listservs"), "newsgroups," "chat rooms," and the "World Wide Web." All of these methods can be used to transmit text; most can transmit sound, pictures, and moving video images. Taken together, these tools constitute a unique medium-known to its users as "cyberspace" – located in no particular geographical location but available to anyone, anywhere in the world, with access to the Internet».

[25] Come è noto, in Italia, proprio in ragione di tali criticità, si discute della possibilità di ricondurre il fenomeno Internet nell'alveo dell'art. 15 della Costituzione, piuttosto che nell'alveo dell'art. 21 della stessa, sostanzialmente dibattendosi se la comunicazione in rete sia tutelare attraverso il principio di inviolabilità della libertà e della segretezza della corrispondenza e di ogni altra forma di comunicazione, oppure attraverso il principio di libera manifestazione del pensiero. Sulla configurazione di Internet nell'ordinamento costituzionale italiano, vd. A. CERRI, "Telecomunicazioni e diritti fondamentali", in *Il diritto dell'informazione e dell'informatica*, 6 (1996), pp. 785-808; P. COSTANZO, "Aspetti evolutivi del regime giuridico di Internet", in *Il diritto dell'informazione e dell'informatica*, 6 (1996), pp. 831-846; V. ZENO ZENCOVICH, "Appunti sulla disciplina costituzionale delle telecomunicazioni", in *Il diritto dell'informazione e dell'informatica*, 3 (1996), 393-404 ss.; P. COSTANZO,

La lettura "tecnica" di Internet, che pone al centro, più che la sua efficacia quale veicolo di comunicazione, il suo essere uno strumento utilizzabile a molti fini, trova riscontri in molte altre sentenze successive. A titolo meramente esemplificativo, può richiamarsi la giurisprudenza statunitense ormai ampiamente consolidata, che, sulla scorta della *Declaratory Ruling* emanata nel marzo 2002 dalla *Federal Communications Commission*[26], ha definito la banda larga come un *information service*, negando che fosse un *telecommunications service*, fondamentalmente sull'assunto che «l'accesso a Internet è una capacità di manipolare e immagazzinare informazioni»[27].

Sotto altro profilo, Internet come apparato tecnologico è stato evocato da quelle decisioni che hanno configurato gli strumenti di accesso alla Rete come un mero presupposto per attività poste in essere attraverso l'utilizzo di specifici prodotti *software* (ludici, professionali, informativi e quant'altro). In tal senso, può segnalarsi, tra i più recenti, il caso risolto dalla *Federal Court of Australia*, nel quale si è affermato – diversamente da quanto stabilito in altre pronunce[28] – che la violazione delle leggi sul *copyright* operata attraverso il *download* non giustifica la sospensione dell'accesso a Internet per l'autore delle violazioni, in ragione del fatto che non è tale accesso lo strumento attraverso cui si produce l'infrazione, ma è l'utilizzo – possibile solo per il

"Profili costituzionali delle telecomunicazioni", in F. BONELLI e S. CASSESE (a cura di), *La disciplina giuridica delle telecomunicazioni*, Padova, 1999, pp. 347 ss.; P. COSTANZO, s.v. "Internet (Diritto pubblico)", in *Digesto Quarta Edizione (Discipline pubblicistiche)*, Appendice, Torino, Utet, 2000, pp. 347-371.; A. VALASTRO, *Libertà di comunicazione e nuove tecnologie*, Giuffrè, Milano, 2001; G. CASSANO e A. CONTALDO, *Internet e tutela della libertà di espressione*, Giuffrè, Milano, 2009.

[26] Cfr. FEDERAL COMMUNICATIONS COMMISSION, *Declaratory Ruling and Notice of Proposed Rulemaking*, FCC 02 -77, 14 marzo 2002, consultabile *on line* alla pagina http://hraunfoss.fcc.gov/edocs_public/ attachmatch/FCC-02-77A1.pdf, spec. 34 ss.

[27] In tal senso, vd., in particolare, la decisione della Corte suprema federale sul caso National *Cable & Telecommunications Association et al.* v *Brand X Internet Services et al.*, 545 U.S. 967 (2005), consultabile alla pagina http://www.law.cornell.edu /supct/html/04-277.ZS .html.

[28] Vd., in particolare, le decisioni della stessa *Federal Court* sui casi *Universal Music Australia Pty Ltd* v *Cooper* [2005] FCA 972 e *Universal Music Australia*

tramite della connessione, ma da essa distinto – del *software* particolare, in grado di violare le leggi sul *copyright*[29].

Queste brevi notazioni circa la natura giuridica di Internet risultano di fondamentale importanza per delineare correttamente che cosa si deve intendere per diritto di accesso a Internet. Non già, dunque, diritto ad avere la mera possibilità di comunicare, bensì diritto ad accedere a uno strumento che consente di realizzare molteplici fondamentali interessi tutelati a livello primario nei vari ordinamenti giuridici[30].

In questa prospettiva si fa particolarmente apprezzare la citata *décision* del *Conseil constitutionnel* francese, che costituisce un arresto fondamentale in materia, non solo perché opera una esplicita classificazione dell'accesso a Internet in termini di «diritto», ma soprattutto in quanto essa afferma che il diritto di accesso a Internet va ricondotto sotto la *Déclaration des droits de l'homme et du citoyen* del 1789, cioè sotto il documento più "solenne" tra quelli che compongono il *bloc de constitutionnalité*[31], con ciò ammettendo che non si tratta esclusivamente di diritto a comunicare[32].

[29] Cfr. la sentenza del 4 febbraio 2010 resa dalla *Federal Court of Australia*, sul caso *Roadshow Films Pty Ltd* v *iiNet Limited* (No. 3) [2010] FCA 24, consultabile *on line* alla pagina http://www.austlii.edu.au/au/cases/cth/FCA/2010/24.html, a tenore della quale: «it is obvious that the [...] provision of the Internet was a necessary precondition for the infringements which occurred. However, that does not mean that the provision of the Internet was the 'means' of infringement. The provision of the Internet was just as necessary a precondition to the infringements which occurred [...]»: «the use of the BitTorrent system as a whole was not just a precondition to infringement; it was, in a very real sense, the 'means' by which the applicants' copyright has been infringed. This is the inevitable conclusion one must reach when there is not a scintilla of evidence of infringement occurring other than by the use of the BitTorrent system. Such conclusion is reinforced by the critical fact that there does not appear to be any way to infringe the applicants' copyright from mere use of the Internet. There will always have to be an additional tool employed»; «absent the BitTorrent system, the infringements could not have occurred» (§§ 401-402).

[30] In questi termini senz'altro P. PASSAGLIA, *Diritto di accesso ad Internet e giustizia costituzionale comparata. Una (preliminare) indagine comparata*, cit.

[31] Come noto, la costituzione francese della V Repubblica si compone, oltre che della Carta del 1958, di diversi testi costituzionali che, nel loro complesso, vanno a integrare il parametro di giudizio del *Conseil constitutionnel* (definito, per l'appunto,

5. Pubblico e privato: una differenza significativa in tema di accessibilità

Impedire a qualcuno di accedere a Internet è cosa diversa dall'impedire al medesimo soggetto esclusivamente l'accesso alla rete dal proprio domicilio informatico o comunque da dove egli preferisce. La differenza non è di poco momento, come si coglie indagando le *rationes decidendi* che hanno condotto i giudici costituzionali a pronunciarsi nei due casi sopra citati.

Il *Conseil constitutionnel* era chiamato a giudicare la legittimità di disposizioni legislative che consentivano a una autorità amministrativa di sospendere l'accesso a Internet di un singolo utente allorché il suo *account* fosse stato utilizzato per porre in essere condotte lesive dei diritti di autore[33]. In sede di valutazione della questione, il *Conseil* ha innanzitutto considerato espressamente che «i poteri sanzionatori [...] abilitano la *Commission de protection des droits*, che non ha potere giurisdizionale, a restringere o a impedire l'accesso a Internet a titolari di abbonamento, nonché alle persone che ne beneficiano», e inoltre che «la competenza riconosciuta a questa autorità amministrativa non è limitata a una categoria particolare di persone, ma si estende alla totalità della popolazione», mentre «i suoi poteri possono condurre a limitare l'esercizio, da parte di chiunque, del proprio diritto a esprimersi e a comunicare liberamente, in particolare dal proprio domicilio». Sulla scorta di tali valutazioni il *Conseil* ha ritenuto che, «avuto riguardo alla natura della libertà garantita dall'articolo 11 della Dichiarazione del 1789, il legislatore non poteva, quali che fossero le garanzie che

sai de définition d'après la jurisprudence du Conseil constitutionnel », in *Recueil d'études en hommage à Charles Eisenmann*, Cujas, Paris, 1975, pp. 33 ss. Sul *bloc de constitutionnalité*, per ulteriori riferimenti cfr. P. PASSAGLIA, *La Costituzione dinamica. Quinta Repubblica e tradizione costituzionale francese*, Giappichelli, Torino, 2008, partic. 175 ss.).

[32] Così anche J. HUNTLEY, N. MCKERREL e S. ASHGAR *Universal Service, the Internet and the Access Deficit*, SCRIPTed Vol 1.2 (2004), p 301, consultabile *online* alla pagina Internet "http://www2.law.ed.ac.uk/ahrc/script-ed/issue2/broadband.asp".

[33] Si tratta, in particolare, degli articoli 5 e 11 di quella che sarebbe divenuta la *loi* n. 2009-669 del 12 giugno 2009, *favorisant la diffusion et la protection de la*

connotassero l'irrogazione delle sanzioni, conferire siffatti poteri a una autorità amministrativa allo scopo di proteggere» diritti, quali quello d'autore, la cui tutela non giustifica, evidentemente, il sacrificio imposto al diritto di accedere alla Rete[34].

Questi passaggi della sentenza in parola confermano la strumentalità del diritto di accesso a Internet rispetto alla finalità di garantire la libertà di espressione. Tanto che la determinazione in ordine alla costituzionalità o meno delle disposizioni contestate si basa essenzialmente sull'impossibilità di prescindere *in toto* dal vaglio giurisdizionale al fine di procedere a una compressione della libertà di espressione.

Quanto tali considerazioni incidano in concreto sulla definizione dell'accesso a Internet è più agevolmente individuabile operando un ulteriore richiamo a un caso per molti versi analogo, concluso con una pronuncia piuttosto recente della *High Court* irlandese[35]. Nella specie, si contestava un accordo tra società titolari di *copyright* e un Internet *provider* nel quale veniva previsto che, in determinate circostanze e a determinate condizioni, il *provider* procedesse a interrompere il servizio di accesso a *Internet* offerto a soggetti che avessero commesso infrazioni alle norme poste a tutela del *copyright*.

Il giudice irlandese, pur affermando che «trattasi di una sanzione grave», anzi tanto grave che «qualcuno potrebbe sostenere che è una imposizione concernente una libertà dell'uomo», a differenza del giu-

[34] Così testualmente *Conseil constitutionnel*, *décision* n. 2009-580 DC, del 10 giugno 2009, *considérant* 16: «Les pouvoirs de sanction institués par les dispositions critiquées habilitent la commission de protection des droits, qui n'est pas une juridiction, à restreindre ou à empêcher l'accès à Internet de titulaires d'abonnement ainsi que des personnes qu'ils en font bénéficier; [...] la compétence reconnue à cette autorité administrative n'est pas limitée à une catégorie particulière de personnes mais s'étend à la totalité de la population; [...] que ses pouvoirs peuvent conduire à restreindre l'exercice, par toute personne, de son droit de s'exprimer et de communiquer librement, notamment depuis son domicile; [...] que, dans ces conditions, eu égard à la nature de la liberté garantie par l'article 11 de la Déclaration de 1789, le législateur ne pouvait, quelles que soient les garanties encadrant le prononcé des sanctions, confier de tels pouvoirs à une autorité administrative dans le but de protéger les droits des titulaires du droit d'auteur et de droits voisins».

[35] Il riferimento va alla sentenza sul caso *Emi Records (Ireland) Ltd. et al.* v *Eircom Ltd.*, [2010] IEHC 108, pronunciata il 16 aprile 2010, consultabile *online* alla

dice francese ha evidenziato che «non esiste una libertà di violare la legge», peraltro sottolineando che, «sebbene sia comodo avere un accesso a Internet a casa, molte persone, in Irlanda, debbono soltanto recarsi presso il centro della loro città per ottenere un accesso al costo di circa 1,50 euro all'ora»[36], e ha concluso per la legittimità dell'accordo.

A completare il quadro si pone, poi, la citata sentenza della *Sala Constitucional* costaricense, che ha deciso un *recurso de amparo* nel quale si lamentava la mancata tempestiva attuazione, da parte del Governo, dell'obbligo fissato per legge di rendere concorrenziale il mercato delle telecomunicazioni[37]. Accogliendo il ricorso, la *Sala Constitucional* ha condannato il Governo a porre in essere, entro tre mesi dal deposito della pronuncia, gli atti di propria competenza per rilasciare le concessioni per le bande di frequenza di telefonia cellulare e altre onde. A fondamento della decisione si è posto il principio secondo cui, «nella situazione della società dell'informazione o della conoscenza, si impone ai poteri pubblici, a beneficio degli amministrati, il compito di promuovere e garantire, in forma universale, l'accesso a[lle] nuove tecnologie»[38].

Come è chiaro, l'accesso che è stato preso in considerazione in questo contesto è cosa diversa da quello cui hanno fatto riferimento il *Conseil* francese e/o la *High Court* irlandese. Qui, infatti, non ci si è concentrati sull'atto dell'accedere a Internet, ma sulla possibilità di accedervi, e dunque sulla mera accessibilità.

[36] Così *Emi Records (Ireland) Ltd. et al.* v *Eircom Ltd.*, cit. nel cui par. 9 si legge testualmente: «This is a serious sanction. Some would argue that it is an imposition on human freedom. There is no freedom, however, to break the law. Further, while it is convenient to have Internet access at home, most people in Ireland have only to walk down to their local town centre to gain access for around €1.50 an hour».

[37] Cfr. *Ley General de Telecomunicaciones* n. 8642, del 4 giugno 2008.

[38] Cfr. anche, sul punto, il rapporto della Comisión Interamericana de Derechos Humanos, intitolato *Libertad de expresiÓn e Internet*, licenziato il 31 dicembre 2013, e consultabile alla pagina "http://www. oas.org/es/cidh/expresion/docs/ infor-

6. Il problema dell'anonimato *online*.

Fin qui si è volutamente tralasciato uno degli snodi critici più complessi della riflessione attuale sull'accesso alla Rete, e cioè quello rappresentato dalla possibilità tecnica e/o anche giuridica per gli interessati di accedere a Internet senza essere riconosciuti, o riconoscibili, *online* con le proprie generalità.

Per comprendere la questione occorre svolgere qualche puntualizzazione. Chiunque voglia navigare in Internet deve avere stipulato un apposito contratto con un *access provider*, che gestisce un determinato numero di accessi alla rete per concederli ai propri clienti (*client*). Questi, quando vogliono connettersi, lanciano, mediante segnali elettronici trasportati da linee telefoniche o linee dedicate, tale richiesta al proprio *access provider* che 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 (*userId*) e la *password* che ha ricevuto in forza della stipulazione del contratto di accesso. Il *provider*, da parte sua, a ogni elaboratore connesso alla rete attribuisce un indirizzo, il cosiddetto IP (*Internet protocol*: un numero binario lungo 32 bit, composto da quattro serie di cifre decimali 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 Internet, non lascia traccia del suo nome, né del suo *userId*, ma esclusivamente del suo IP[39].

I problemi pratici nell'individuare i soggetti direttamente responsabili di attività compiute *online* dipendono da alcune complicazioni. Per prima cosa, va detto che soltanto alcuni soggetti, per lo più enti pubblici e privati, dispongono come utenti di un indirizzo fisso, mentre gli Ip per la navigazione (a differenza di quanto avviene per gli IP utili alla creazione un sito nel Web) spesso sono assegnati tempora-

[39] Oltre a seminare il proprio Ip, durante la navigazione in Internet, gli utenti lasciano, spesso inconsapevolmente, nei siti visitati (e non solo) tracce ulteriori del loro passaggio. Ciò accade in quanto, attraverso appositi *software*, molti operatori di Internet,

neamente in quanto vengono, di volta in volta, attribuiti dal *provider* al cliente 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, cosicché, per evitare l'esaurimento degli indirizzi a disposizione, esso, al fine di poter avere più clienti, preferisce attribuire al singolo utente, a ogni richiesta di accesso, uno tra gli IP in quell'istante disponibili. Ciò impedisce all'intermediario 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 tra utente e *access provider* è stipulato senza che vengano accertati i dati anagrafici spesi dal soggetto che aspira a diventare cliente, in quanto il relativo servizio, anche in Italia, dal 1999 viene fornito gratuitamente[40]; per cui l'intermediario fornitore dell'accesso, che punta esclusivamente ad avere il più alto numero di clienti possibile[41], non ha interesse a controllarne l'identità e, dunque, molto spesso ha in archivio contratti contenenti false generalità, sulla base dei quali è impossibile individuare il cliente che si sia reso autore di un illecito.

[40] La Camera di Commercio di Milano ha accertato, per la prima volta in Italia, alcuni usi in voga nella contrattualistica e nelle attività degli Internet *provider* e ne ha ufficialmente approvato l'elenco con la deliberazione n. 258 del 23 luglio 2001, che può leggersi in *Rivista di Diritto privato*, 2002, p. 126.

[41] Il valore degli spazi pubblicitari sui siti Internet è direttamente proporzionale al numero di utenti su cui il singolo sito può contare. Avere un alto numero di clienti porta anche altri vantaggi all'*access provider*. Questi, per esempio, potrà raccogliere più dati relativi alle preferenze manifestate in rete dai naviganti ovvero potrà meglio veicolare propri messaggi e propri contenuti. Significativa, in proposito, appare la decisione dell'Autorità Garante per la Concorrenza e il Mercato del 17 febbraio 2000, n. 8051, in *Il diritto industriale*, 1 (2001), p. 93, con nota di A. LEONE, nella quale è stato considerato ingannevole un messaggio pubblicitario volto a reclamizzare l'offerta di un abbonamento gratuito a Internet in quanto, a fronte del servizio di accesso, in realtà il *provider* si garantiva, mediante contratto, la possibilità di inviare al cliente pubblicità commerciale e di monitorare la navigazione in Internet di quest'ultimo per indagare le preferenze commerciali del navigatore; inoltre l'operatore in questione imponeva al cliente di visualizzare periodicamente, sullo schermo del proprio terminale, un numero minimo di comunicazioni pubblicitarie; e

Ulteriori complicazioni sorgono quando l'utente, per garantirsi l'anonimato in rete, compie la sua navigazione utilizzando *software* o siti appositi (i cosiddetti *anonymizer*), che svolgono una funzione di filtro ed evitano che rimanga traccia dell'IP dello *user* nei registri elettronici (i cosiddetti *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 online*, 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.

7. Gli effetti dell'anonimato sul modo di utilizzare (*rectius* abitare) la Rete.

La comunicazione in Internet, anche tra chi non vuole svelare la propria identità anagrafica, non avviene sempre su base completamente anonima. Gli *user* che desiderano intrattenere rapporti prolungati nel tempo utilizzano una forma di parziale riconoscimento che viene definita «pseudonimato»[42].

Il termine sta a significare che i naviganti, abituali frequentatori di un certo sito o di un certo servizio, si riconoscono vicendevolmente per mezzo di pseudonimi utilizzati per essere individuati e riconosciuti nel ciberspazio. In mancanza di questa forma di riconoscimento, la comunicazione di rete non potrebbe mai dare luogo a relazioni sociali significative in quanto gli utenti dovrebbero, a ogni nuova connessione, ricominciare a qualificarsi, e dovrebbero riprendere a conoscere gli altri senza godere, almeno in prima battuta, di memoria[43].

[42] Cfr. L. PACCAGNELLA, *La comunicazione al computer*, Il Mulino, Bologna, 2000, p. 81; nonché F. RAMPINI, *Una rivoluzione in corso*, Laterza, Roma-Bari, 2000.

[43] La partecipazione al ciberbspazio deve essere continua, anche se non necessariamente frequente, perché l'utente esista in Internet. Essa, inoltre, deve essere asso-

Giova ora soffermarsi sull'anonimato e sullo pseudonimato per indagare gli effetti prodotti sulla personalità del navigatore dalla possibilità di accedere alla rete senza mettere in gioco l'identità anagrafica, bensì assumendo maschere che egli di volta in volta sceglie[44]. Per farlo, occorre subito chiarire che, in rete, l'uomo vive una realtà mediata

altri utenti di ricavare dal nome la storia di quella partecipazione. Queste sono le condizioni per lo sviluppo di quella che è può essere definita la «persona *online*» (cfr. R. MACKINNON, "Searching for the Leviathan in Usenet", in S JONES (a cura di), *Cybersociety. Computer-Madiated Communication and Community*, Sage, Thousand Oaks, Ca., 1995), un «sé *online*» [cfr. J. WALTHER, "Interpersonal Effects in Computer-Mediated Interaction. A Relational Perspective", in *Communication Research*, 19 (1992), pp. 52-90; e ID., "Computer-Mediated Communication: Impersonal, Interpersonal, and Hyperpersonal Interaction", in *Communication research* 23, 1 (1996) pp. 13-43 o, addirittura, un «*cyberself*» (D. WASKUL e M. DOUGLAS, "Cyberself: The Emergence of Self in On-Line Chat", in *The Information Society. An International Journal*, 13, 4 (1997), pp. 375-397]. Per ulteriori considerazioni sul punto, v. N.N.G. ANDRADE, "Right to Personal Identity. The Challenges of Ambient Intelligence and the Need for a New Legal Conceptualization", in: S. GUTWIRTH, Y. POULLET, P. DE HERT *et al.* (a cura di), *Computers, Privacy and Data Protection: an Element of Choice*, Dordrecht *et alib.*, Springer, 2011, p 89..

[44] Il concetto di maschera è tradizionalmente legato a quello di persona. È noto, infatti, come la parola latina *persona* derivi etimologicamente dall'etrusco *phersu*, maschera. Tale circostanza viene comunemente spiegata dai linguisti osservando che le maschere, nelle società antiche, hanno sempre costituito l'interfaccia più significativa tra l'individuo e la società perché proprio attraverso la rappresentazione o la caricatura delle caratteristiche dei consociati più o meno noti si inculcava nella collettività la coscienza sociale, si informava la comunità delle vicende di cronaca, ovvero si propagandavano le idee filosofiche o politiche del tempo (Cfr. M. MAUSS, *Sociologie et anthropologie*, Quadrige, Paris, 1950 = *Teoria generale della magia ed altri saggi*, trad. di F. Zannino, Einaudi, Torino, 1965, secondo il quale il concetto di persona è legato originariamente ai personaggi mitici rappresentati nei rituali attraverso le maschere). Il concetto di persona viene sviluppato dal diritto romano come centro di imputazione di diritti, divieti e doveri. Lo *status* di persona, nel diritto romano, spetta agli uomini liberi, ma non alle donne, agli schiavi e ai figli ancora soggetti alla sfera di controllo del *pater familias*. Il nome, strettamente correlato alla qualifica di persona, indica l'appartenenza a una determinata famiglia, oltre a designare una serie di altre relazioni sociali; in questo senso può dirsi che, nell'esperienza romana più antica, il concetto di persona sia strettamente legato all'uso del nome; mentre è solo con la morale cristiana che la qualifica di persona viene estesa a ogni individuo, indipendentemente dal suo nome e dal suo *status*. Nasce così l'idea che ogni uomo sia una persona. Cfr. PACCAGNELLA, *La comunica-*

che molto spesso ha poco di reale[45]. Lo spazio virtuale rappresenta una sorta di teatro in cui si montano palcoscenici elettronici, per la continua e ripetuta messa in scena di milioni di rappresentazioni individuali o collettive, senza memoria e senza possibilità di distinguere dimensioni spaziali diverse dal presente[46].

Ciò fa sì che l'uomo perda tutti i tradizionali punti di riferimento reali e finisca per subire una vera e propria frammentazione della personalità[47], in quanto egli, nel mondo atomistico, avrà una identità e

[45] È difficile immaginare un esempio di ossimoro più eloquente di quello risultante dalla locuzione "realtà virtuale". Per gli opportuni approfondimenti, si consiglia la lettura di U. FADINI, *Sviluppo tecnologico e identità personale. Linee di antropologia della tecnica*, Dedalo, Bari, 2000. Cfr. anche D. WOLTON, *Internet... et après? Une théorie critique des nouveaux médias*, Flammarion, Parigi, 1999 = *Internet e poi? Teoria critica dei nuovi media*, trad. di C. Marullo Reedtz, Dedalo, Bari, 2001. In proposito, v. anche A.A. MARTINO, "Informatica e diritto farfugliato, imbricato rapporto", in G. ROGNETTA (a cura di), *Informatica giuridica. Nuove tematiche di diritto dell'informatica ed Internet*, Esselibri-Simone, Napoli, 2001, pp. 7-33 e partic. 12, il quale bene evidenzia come: «molte volte si adopera il termine "virtuale" per opposto di "mondo reale", ma non sempre si tiene presente che questo vale per la differenza tra oggetto e rappresentazione, ma la rappresentazione può essere, a sua volta, un altro oggetto, come la fotografia diviene una cosa». Sicché, può dirsi che la realtà virtuale, di cui Internet appare il principale paradigma, è soltanto un'altra realtà rispetto a quella atomistica, e non una "non realtà", o una "realtà in potenza".

[46] M. POSTER, "Virtualità postmoderne", cit., p. 73, in proposito, scrive: «I termini "realtà virtuale" e "tempo reale" dimostrano la capacità, tipica della seconda età dei media, di costituire una cultura di simulazione. La mediazione comunicativa è diventata così intensa che i contenuti della mediazione non possono più nemmeno fingere di rimanere intatti. Sempre più la cultura è simulazione nel senso che i media spesso cambiano le cose con cui vengono in contatto, trasformando l'identità degli originali e dei punti di riferimento. Nella seconda età dei media la realtà diventa multipla».

[47] I sociologi del diritto studiano da anni i problemi del pluralismo comunitario e del pluralismo individualista. Entrambi i fenomeni ora descritti, secondo alcuni, finiscono per incidere sulle relazioni umane isolando sempre di più l'uomo, ovvero falsificando i suoi rapporti sociali e i valori in cui egli pensa di credere. Il giurista nordamericano M. ROSENFELD, *Just Interpretations. Law between Ethics and Politics*, University of California Press, Berkeley, 1998, trad. it. *Interpretazioni. Il diritto fra etica e politica*, Il Mulino, Bologna, 2000, p. 329, sul punto, osserva: «Oltre a esserci una divisione tra il sé e l'altro tra individui, tra individuo e gruppo, e tra gruppi

una percezione di sé e degli altri[48], mentre in rete vivrà in una dimensione in cui tutto e tutti sono solo una proiezione dei suoi desideri, dei suoi gusti, delle sue preferenze e, finanche, delle sue manie[49]. Tutto questo lo espone seriamente al rischio di incorrere in una patologia che gli psicologi e gli psichiatri chiamano: perdita d'identità[50].

all'interno dell'individuo. Inoltre, coerentemente con il pluralismo di fatto, individui e gruppi potrebbero talvolta sposare preferenze valutative contraddittorie, o mancare di una coerente concezione del bene. Per di più, potrebbero trovarsi ad aderire in parte a concezioni differenti del bene, o anche essere inconsapevoli di alcune delle loro fedeltà o preferenze valutative». Cfr. D. MYERS, "«Anonymity is Part of the Magic»: Individual Manipulation of Computer-Mediated Communication Context", *Qualitative Sociology*, 10, 3 (1987), pp. 251-266; S. TURKLE, *Life on the Screen. Identity in the Age of the Internet*, Simon & Schuster, New York, 1995, = *La vita sullo schermo*, a cura di B. Parrella, Apogeo, Milano, 1997; ID., "Multiple Subjectivity and Virtual Community at the End of the Freudian Century", in *Sociological Inquiry*, 67, 1 (1997), pp. 72-84 e S. WILBUR, "An Archaeology of Cyberspaces. Virtuality, Community, Identity", in D. PORTER (a cura di), *Internet Culture*, Routledge, New York-Londra, 1997, pp. 45-55.

[48] Per gli opportuni approfondimenti, v., tra gli altri, P.M. CHURCHLAND, "The Neural Representation of the Social World", in T.W. BYNUM e J.H. MOOR (a cura di), *The Digital Phoenix: How Computers are Changing Philosophy*, Blackwell, Oxford, UK, and Malden, MA, 1998, pp. 153-170 = "La rappresentazione neurale del mondo sociale", in *La fenice digitale. Come i computer stanno cambiando la filosofia*, Apogeo, Milano, 2000, partic. p. 163.

[49] Già Immanuel Kant – come ricorda M. HEIDEGGER quando parla dell'uomo moderno che muove alla conquista del mondo riducendolo ad immagini (M. HEIDEGGER, "Die Zeit des Weltbildes" [1938], in *Holzwege*, Klostermann, Francoforte sul Meno, 1950 = *L'epoca dell'immagine del mondo*, in *Sentieri interrotti*, La Nuova Italia, Firenze, 1968) – precorrendo gli esiti cui sarebbe giunta la scienza moderna in età più avanzata, ebbe a dire che «l'intelletto non attinge le sue leggi (a priori) dalla natura, ma le prescrive a questa» (*Prolegomena zu einer jeden künftigen Metaphysik*, § 36). Secondo il grande filosofo, dunque, l'intelletto umano muove alla creazione della natura, non alla sua scoperta, e dunque la tecnologia crea nuovi ambienti, non li rinviene nella realtà naturale. Tale osservazione sembra trovare conferma nella moderna realtà digitale, la quale si basa su dimensioni sue proprie create dall'uomo, nelle quali lo stesso uomo si trova poi a operare, fare, vivere.

[50] Con la locuzione "perdita di identità" si fa riferimento al concetto "moderno" di identità. Giova, in proposito, citare M POSTER, "Virtualità postmoderne", cit., p. 66, il quale osserva: «Nel XX secolo i media elettronici stanno favorendo una trasformazione dell'identità culturale altrettanto profonda. Il telefono, la radio, il cinema, la televisione, il computer e ora la loro integrazione nella multimedialità riconfigurano le parole, i suoni e le immagini in modo da formare nuove confi-

Ma c'è di più. Se l'individuo, oltre a poter adottare virtualmente mille identità diverse (con il rischio di smarrire la propria), può usare tali identità senza dar conto a nessuno (in questo senso, l'anonimato gioca un ruolo determinante), e così esprimere gusti e preferenze in modo completamente libero da freni inibitori e da ogni forma di etica[51], (egli) non solo esce dalla comunità in cui vive, in quanto non sente più obblighi né vincoli di solidarietà nei confronti degli altri, ma anche esce da se stesso perché non percepisce più le azioni che compie come realmente sue e finisce per imputarle inconsciamente al personaggio di cui, di volta in volta, sceglie di vestire i panni[52].

dell'individualità. Se si può affermare che la società moderna ha prodotto l'ideale di un individuo razionale, autonomo, centrato e stabile (l'uomo ragionevole del diritto, il cittadino della democrazia rappresentativa, l'uomo economico calcolatore del capitalismo, lo studente definito dai suoi voti dell'istruzione pubblica), allora si può anche dire che sta emergendo una società postmoderna che propone forme di identità diverse, o addirittura opposte, a quelle della modernità». Lo stesso A., già qualche anno prima, in *The Mode of Information. Poststructuralism and Social Context*, Blackwell, Oxford, 1990, aveva sottolineato come le comunicazioni elettroniche definiscano il soggetto individuale in modi diversi da quelli delle principali istituzioni moderne, e dunque che «la post-modernità e il modo dell'informazione si esprimono in pratiche di comunicazione che costituiscono i soggetti come instabili, multipli e diffusi».

[51] Tra gli studi più interessanti sull'etica delle nuove tecnologie informatiche, v. T.W. BYNUM, "Etica dell'informazione globale e rivoluzione informatica", in T.W. BYNUM e J.H. MOOR (a cura di), *La fenice digitale...*, cit., p. 301. Uno dei saggi che hanno segnato il passo in materia è di J.H. MOOR, "What Is Computer Ethics?", in T.W. BYNUM (a cura di), *Computer end Ethics*, in *Metaphilosophy*, 16, 4 (1985), pp. 266-275, in cui l'A. scrive: «Un tipico problema di etica informatica sorge perché c'è un vuoto politico su come la tecnologia informatica debba essere usata. I computer ci forniscono nuove possibilità e queste a loro volta ci danno nuove alternative per l'azione. Spesso non esistono politiche di comportamento in queste situazioni, o quelle che esistono sembrano inadeguate. Uno dei compiti centrali per l'etica informatica è quello di determinare cosa si debba fare in questi casi, cioè formulare politiche che possano dirigere la nostra azione». Per una riflessione di tenore giuridico in questo senso paradigmatica, vd. M. GREEN, "Sex on the Internet: A Legal Click or an Illicit Trick?", in *California Western Law Review*, 38 (2002), pp. 527 ss., il quale si chiede se le norme sulla prostituzione possano essere applicate agli spettacoli di carattere sessuale offerti *online* in tempo reale su alcuni siti per adulti.

[52] Cfr. L. GIULIANO, *I padroni della menzogna. Il gioco delle identità e dei mondi virtuali*, Meltemi, Roma, 1997; C. GALIMBERTI e G. RIVA, *La comunicazione virtuale. Dal computer alle reti telematiche: nuove forme di interazione sociale*, Guer-

Stando così le cose, la rete delle reti sembra sul punto di frammentare definitivamente quell'unità del concetto di persona, e di identità, in base alla quale, per secoli, l'uomo ha condotto la sua esistenza e ha intrattenuto le sue relazioni sociali[53]. Già da alcuni anni i sociologi più attenti sottolineano l'idoneità delle nuove tecnologie della comunicazione e dell'informazione a realizzare identità personali multiple o frammentate, e ciò in considerazione della possibilità tecnica, per ogni utente, di costruirsi in rete una o più identità, spendibili a seconda delle circostanze, attraverso la semplice utilizzazione di un *nickname* piuttosto che di un altro[54].

ni, Milano, 1997; nonché E. WYNN e J.E. KATZ, "Hyperbole over Cyberspace: Self-presentation & Social Boundaries in Internet Home Pages and Discorse", *The Information Society*, 13, 4 (1997), pp. 297-328.

[53] Secondo A.C. AMATO MANGIAMELI, *Diritto e cyberspace. Appunti di informatica giuridica e filosofia del diritto*, Giappichelli, Torino, 2000, partic. p. 211, in Internet «l'identità e l'alterità per così dire tradizionali sono messe a dura prova. Pensate a partire da definizioni e determinazioni, inclusioni ed esclusioni, devono ora aprirsi ai nuovi ambiti di interazione, alle inedite cronologie e ai limiti mai tracciati in modo definitivo. [...] Grazie all'interazione a distanza, ci si connette ad altri, scambiando la propria identità, usurpandola, fantasticando su un diverso e *falso io*, oppure mantenendo il *vero io*, del quale però l'altro non può mai essere certo. Comunicazione e condivisione vengono così inseriti in un "gioco dei travestimenti"».

[54] Sul punto, L. PACCAGNELLA, *La comunicazione al computer*, cit., pp. 96-97, scrive: «Gli strumenti per la costruzione della persona *online* possono anche essere usati in modo deliberatamente ingannevole. In questi casi lo scopo non è quello di dare voci a frammenti di se stessi che rimangono inespressi nella vita *offline*, ma è piuttosto quello di far credere di essere qualcosa (o qualcuno) di diverso da ciò che effettivamente si è (o meglio, si pensa di essere)». K. ROBINS, "Cyberspace and the world we live in", in D. BELL e B.M,. KENNEDY (a cura di), *The Cybercultures Reader*, Routledge, Londra-New York, 2000, pp. 77-95 e partic. pp. 80-81, osserva che: nella «realtà accomodante [della rete digitale] il *self* è ricostruito come entità fluida e polimorfa. Le identità possono essere scelte e buttate via quasi a piacere, come in un gioco o in una finzione. [...] Identità nuove, identità mobili, identità esplorative, ma, pare, anche identità banali». Cfr. B. DANET, "Text as Mask: Gender, Play, and Performance on the Internet", in S.G. JONES (a cura di), *Cybersociety 2.0: Revisiting Computer-Mediated Communication and Community*, Sage, Thousand Oaks, Ca., 1998, pp. 129-158; J. O'BRIEN, "Writing in the Body: Gender (Re)Production in Online Interaction", in P. KOLLOCK – M. SMITH (a cura di), *Communities in Cyberspace*, Routledge, London, 1999 pp. 76-104; E. WHITLEY, "Is it Really Possible to Play with Identity in «Cyberspace»? A Review Based on the Sociology of

Basta tutto ciò per ritenere che siano maturi i tempi per sviluppare un nuovo concetto di persona? O ancora, in termini più squisitamente giuridici, è sufficiente osservare questa frammentazione di identità per affermare che il centro di imputazione primario degli interessi tutelati dal diritto, e cioè l'uomo, stia subendo un fenomeno di trasformazione epocale, di vera e propria evoluzione della specie, con tutte le conseguenze che sul piano dell'ordinamento giuridico ne deriverebbero?

Rispondere a queste domande non è agevole. Prendendo in considerazione le teorie sociologiche più moderne, si scopre che il concetto di persona, seppure, per certi versi, tradizionalmente unitario, non è incompatibile con la frammentarietà e pluralità di identità di cui si è detto. Mackinnon, per esempio, afferma che «la persona è un miscuglio complesso di identità (negoziata, ricevuta e coltivata), autorità socialmente legittimata e responsabilità giuridica posizionate in un corpo culturalmente riconosciuto»[55]. Dunque, anche l'uomo dell'era digitale, l'uomo che si relaziona agli altri e alle cose attraverso la rete informatica, può essere considerato persona nel senso tradizionale del termine. Conclusione questa di non poco momento per il giurista, visto che gli consente di mantenere salda l'idea classica di uomo come centro di imputazione degli interessi primari tutelati, nonché centro di imputazione di responsabilità.

Per giungere a tale conclusione, occorre, tuttavia, in via preliminare, verificare la sussistenza, in capo all'utente di Internet, di tutti i requisiti che Mackinnon attribuisce alla persona. Già a una primissima ricognizione, ciò che sembra difettare al navigatore – perché, malgrado la pluralità delle maschere indossate e la frammentarietà della rappresentazione della propria identità, sia considerabile come persona – è l'idea della responsabilità giuridica delle proprie azioni. L'uomo in rete si sente assolutamente libero da vincoli propriamente sociali e

una riflessione meno recente, ma di sorprendente attualità, v. J. MORGAN, C. O'NEILL e R. HARRÈ, *Nicknames, Their Origins and Social Consequences*, Routledge & K. Paul, Londra, 1979.

[55] R. MACKINNON, "Punishing the Persona: Correctional Strategies for the Virtual Offender", in S.G. JONES, *Virtual Culture. Identity & Communication in Cybersociety*, London Thousand Oaks, Ca.-New Delhi, 1997, pp. 206-235.

giuridici[56], in quanto, nascondendosi dietro lo pseudonimo, che cela la sua identità anagrafica, può compiere qualsiasi nefandezza senza poter essere riconosciuto e, in definitiva, senza rispondere delle conseguenze morali e giuridiche delle proprie azioni. Il che rende l'uomo privo del senso di responsabilità che dovrebbe caratterizzare il suo essere in mezzo agli altri in forma associata[57], e dunque mina alla base lo stesso concetto di uomo[58], nonché quello di comunità cibernetica o digitale[59].

Tutto ciò induce ad affermare con forza che occorre recuperare in Internet la logica della responsabilità di ogni singolo utente[60]. Occorre, in altre parole, che l'uomo avverta la sua esperienza di rete come esperienza reale e, dunque, generatrice di onori ed oneri, meriti e sanzioni negative, per farla breve: generatrice di responsabilità[61]. Tornano, così, alla mente considerazioni già svolte in dottrina (non solo da chi scrive[62]) a più riprese, circa la necessità di recuperare, in una società priva di valori condivisi e sopraffatta dalle dimensioni tecnologiche ed economiche, il senso della responsabilità umana[63].

8. Anonimato, *privacy* e problemi di imputazione della responsabilità *online*.

[56] Come osserva K. ROBINS, "Cyberspace and the World...", cit., p. 92, «La perdita di coerenza e di continuità dell'identità è associata alla perdita di controllo sulla realtà. La crisi dell'identità dell'individuo è, allora, più di una crisi personale (cioè psicologica). [...] Questo rilevante cambiamento culturale implica una perdita del significato sociale, e il conseguente svincolarsi dall'impegno morale». Anche C. MONGARDINI, "The Ideology of Postmodernity", in *Theory, Culture & Society*, 9 (1992), pp. 55-65, sostiene che l'uomo in Internet sia privo di morale e privo di etica.

[57] Del resto già I. KANT, *Die Metaphysik der Sitten*, 1797, trad. it. di G. Vidari, *La metafisica dei costumi*, I, *Introduzione alla metafisica dei costumi*, Laterza, Roma-Bari, 1982, IV, 26, definiva la persona come «quel soggetto, le cui azioni sono suscettibili di una imputazione». Per un recente studio italiano che tratta diffusamente l'argomento, v. F. SCIACCA, *Il concetto di persona in Kant. Normatività e politica*, Giuffrè, Milano, 2000.

[58] K.J. GERGEN, *The Saturated Self. Dilemmas of identity in contemporary life*, Basic Books, New York, 1991, p. 7, già più di due lustri fa, osservava come identità, non solo plurime, ma anche frammentate, finiscono per diventare molti sé, e cioè molti sé frammentati; circostanza questa, nella quale «il *Sé autentico* finisce per sparire».

[59] Sulla necessità che, in una comunità umana, ogni consociato abbia un profondo senso di responsabilità nei confronti degli altri, *ex multis*, vd. A. ETZIONI, *The Spirit of Community: Rights, Responsabilities, and the Communitarian Agenda*, Touchstone, New York, 1993.

[60] Alcuni autori, sostenendo che le dichiarazioni effettuate in forma anonima non sono prese in seria considerazione da chi le riceve, affermano che via Internet l'eventuale diffamazione non è idonea a produrre danno e, dunque, non può essere considerato illecito risarcibile. Così I.T. HARDY, "The Proper Legal Regime for 'Cyberspace'", in *University of Pittsburgh Law Review*, 55 (1994), pp. 993-1055 e partic. 1048, e A.W. BRANSCOM, "Anonimity, Autonomy and Accountability: Challenges to the First Amendment in Cyberspace", in *The Yale Law Journal*, 104 (1995), pp. 1639 ss. Per un caso europeo, nel quale la giurisprudenza ha negato *tions des programmes*, v. Trib. Gran. Inst. Parigi, 14 agosto 1996, in *Rev. trim. dir. comm.*, 1997, p. 457.

[61] Tale convinzione è rafforzata da un ammonimento lanciato da A.C. AMATO MANGIAMELI, *Diritto e cyberspace.*, cit., p. 212: «Se l'illusione sarà così potente da non poter distinguere *ciò che è reale* da *ciò che non lo è*, se il gioco diventerà imperioso mescolando sempre più essere ed apparenza, l'identità dipenderà dall'identità virtuale e la comunicazione dalla comunicazione *online*. In altre parole, si corre il rischio che il gioco dei travestimenti finisca per essere giocato e diventi qualcosa di inquietante: una tenebrosa, per niente ludica, comunità di spettri». Particolarmente interessanti si rivelano le considerazioni in proposito svolte da S.E. MILLER, *Civilizing Cyberspace: Policy, Power, and the Information Superhighway*, Addison-Wesley, New York, 1996.

[62] Cfr. in particolare. F. DI CIOMMO, *Evoluzione tecnologica e regole di responsabilità civile*, Edizioni Scientifiche Italiane, Napoli, 2003.

[63] Cfr. C. JEAN e G. TREMONTI, *Guerre stellari. Società ed economia nel cyberspazio*, Franco Angeli, Milano, 2002, pp. 77-79, che scrivono: «nell'economia moderna i servizi ([...] paradigma delle nuove entità immateriali in cui si configura la ricchezza moderna) valgono [...] enormemente più dei beni (entità fisiche). [...] Il mondo dei servizi tende a sottrarsi all'ordine dei principi morali. Infatti, i servizi non sono merce di cui ci si appropria, ma merce che si crea, all'interno di circuiti artificiali esponenziali. [...] In superficie, la libertà sembra dilagare, nella nuova dimensione tridimensionale del Cyberspace, estendendosi in un labirinto sconfinato di dati e segni, di suoni e di musiche, offerti e combinati in un caleidoscopio di volta in volta cangiante. Il mito della libertà sembra davvero realizzarsi, con la trasformazione della libertà di movimento nel suo opposto: nella libertà di non muoversi, di attrarre verso di sé e di manipolare l'universo. Come un nuovo Prometeo, l'uomo di Internet sembra infinitamente potente, libero di ibridare dimensioni eterogenee: reale e vir-

Il problema dell'anonimato in rete, in definitiva, è quello di essere per l'utente strumento che, mentre appare funzionale alla tutela della privacy informatica e di altri diritti della personalità, consente di evitare l'imputazione della paternità, e dunque della relativa responsabilità, rispetto agli atti compiuti *online*[64].

La questione è nota da anni, ma a oggi ancora poco si è fatto per risolverla. In proposito, basta ricordare che nella Raccomandazione europea n. 3/1997, adottata il 3 dicembre 1997 dal "Gruppo per la tutela delle persone fisiche con riguardo al trattamento dei dati personali", il diritto all'anonimato viene definito «essenziale se si vogliono mantenere nel ciberspazio i diritti fondamentali alla riservatezza e alla libertà di espressione», ma allo stesso tempo viene temperato dall'ammissione che «la capacità di partecipare e comunicare in rete senza rivelare la propria identità contrasta con le iniziative che vengono attualmente sviluppate a sostegno di altri settori importanti come la lotta contro il contenuto illegale e nocivo, le frodi finanziarie e il diritto d'autore», per cui si propone che le restrizioni del diritto all'anonimato siano «giustificate, necessarie, proporzionate»[65]. In altre parole, il ragionamento è: non essendo possibile evitare che in Internet vi siano operatori che raccolgono i dati degli *user* e ne abusano, quantomeno bisogna evitare che il profilo dell'utente, ricostruibile attraverso il trattamento di tali dati, sia ricondotto all'identità reale del soggetto interessato[66].

[64] Nella dottrina d'oltreoceano, tra gli altri, v. H. NISSEMBAUM, "The meaning of Anonymity in Information Age", in *Information Society. An International Journal*, 15, 2 (1999), pp. 141-144; C.R. SUNSTEIN, "The first Amendment in Cyberspace", in *Yale Law Review*, 104, 7 (1995), pp. 1757-1804; A.W. BRANSCOMB, "Anonymity, Autonomy and Accountability: Challenges to the First Amendment in Cyberspace", in *Yale Law Review*, 104, 7 (1995), pp. 1639-1679 e partic. 1665.

[65] Nell'Allegato («Linee guida per la protezione delle persone rispetto al trattamento dei dati personali sulle autostrade dell'informazione») alla Raccomandazione n. R. (99) 5 del 23 febbraio 1999, adottata dal Comitato dei Ministri del Consiglio d'Europa e «relativa alla protezione della privacy su Internet», al paragrafo 2.4 si afferma che: «L'anonimato assoluto potrebbe non essere realizzabile a causa di limitazioni di natura giuridica. In questo caso, [...] potreste utilizzare uno pseudonimo in modo che la vostra identità personale sia nota solo al vostro fornitore di servizi della società dell'informazione».

[66] S. RODOTÀ, in proposito, anni fa osservava: «A me serve tutela dell'anonimato, a me serve tutela della riservatezza, della privacy, non per isolarmi, ma per partecipare. Solo se sono certo del mio anonimato potrò partecipare senza timore di essere discriminato o stigmatizzato [...] Ecco allora che la riservatezza non è un problema di silenzio, di isolamento dagli altri, ma è uno strumento di comunicazione» ("Libertà, opportunità, democrazia, informazione", in *Internet e privacy: quali regole?*, Atti del Convegno organizzato dal Garante per la protezione dei dati personali, Roma 8-9 maggio, Suppl. n. 1 al Boll. N. 5, Presidenza del Consiglio dei Ministri, Dipartimento per l'Informazione e l'Editoria, Roma, 1998, pp. 8-18). Lo stesso A., tuttavia, già nel 1997 (*Tecnopolitica. La democrazia e le nuove tecnologie della comunicazione*, Laterza, Roma-Bari, 1997, p. 145) avvertiva i pericoli insiti nel riconoscimento indiscriminato del diritto all'anonimato laddove sottolineava il conflitto tra un interesse all'anonimato (riservatezza attiva) e un interesse a conoscere la reale identità di chi pone in essere comportamenti lesivi della riservatezza altrui (riservatezza passiva). Per un'analoga ricostruzione, vd. E. DAVIO, « Anonymat et autonomie identitaire sur Internet », in E. MONTERO (a cura di), *Droit des technologies de l'information. Regards perspectives*, Cahiers du CRID, 16, Bruylant, Bruxelles, 1999, pp. 295-313; nonché G.M. RICCIO, "Diritto all'anonimato e responsabilità civile del provider", in L. NIVARRA e V. RICCIUTO (a cura di), *Internet e il diritto dei privati. Persona e proprietà intellettuale nelle reti telematiche*, Giappichelli, Torino, 2002, pp. 25-40. Cfr. Ric. IMPERIALI e Ros. IMPERIALI, "La tutela della privacy in Internet: difficoltà di un contemperamento", in *Diritto e pratica delle società*, 6 (2001), pp. 29-30; C. RESTA, "Tutela della privacy in Internet: quali limiti e quali necessità?", in *Impresa*, 2001, pp. 958 ss.

Al contrario, se sul piatto si mettono valutazioni ulteriori, ci si rende conto di come la situazione attuale – in cui l'anonimato, di fatto, viene garantito dalla mancanza di indicazioni legislative contrarie, tanto in Europa quanto negli Stati Uniti – non sia affatto efficiente in termini di equilibrio tra i valori condivisi dalla collettività. Basta osservare quanto il pianeta Internet sia cresciuto negli ultimi anni, per comprendere che una scelta di sostanziale deresponsabilizzazione degli utenti e degli operatori, sino a qualche tempo fa probabilmente giustificata dalle ridotte dimensioni del fenomeno, oggi, anche per le caratteristiche tecniche che la grande rete digitale ha mostrato di avere, non sia più sostenibile. E ciò, tanto alla luce di esigenze di natura giuspubblicistica, e cioè di sicurezza e garanzia dei cittadini, quanto per considerazioni di carattere giusprivatistico, economico ed antropologico.

Lasciare che in rete regni l'anonimato, come più volte sottolineato, in definitiva, vuol dire rendere la realtà digitale un luogo di "non diritto"; e ciò in quanto l'ordinamento giuridico perde, così, il suo riferimento principale, il suo principale centro di imputazione di interessi e

responsabilità: l'uomo. Un ordinamento giuridico, in particolare un ordinamento privatistico, in cui l'individuo non ha più alcuna identità predefinita, è destinato a non essere più applicato e, dunque, a non svolgere più alcun ruolo, né di indirizzo, né di tutela degli interessi condivisi, abbandonando la società a un inevitabile decadimento civile, etico ed economico[67].

In particolare, lasciare che in rete gli utenti e molti operatori continuino ad agire senza che sia possibile, in fase di imputazione delle relative responsabilità, svelare la loro reale identità, significa:

- consentire a chiunque di utilizzare la rete nel più assoluto segreto per compiere qualsiasi illecito, per diffondere messaggi, per organizzare strategie criminose, nonché per aggredire risorse informatiche altrui;

[67] La questione in parola rinvia alla letteratura sociologico-giuridica che si è occupata della cosiddetta "anomia soggettiva" (e cioè della situazione in cui versa il soggetto che non ha interiorizzato le regole sociali e dunque si sente totalmente deresponsabilizzato) e della cosiddetta "anomia sociale" (stato sociale di mancata o insufficiente regolamentazione, giuridica e/o morale, di determinati settori o rapporti della vita collettiva). In proposito, qui giova ricordare che, sebbene il termine compaia già nella teologia inglese del XVII secolo, la prima teoria dell'anomia viene formulata sul finire del XIX secolo per mano del filosofo francese Jean-Marie Guyau, il quale – nella sua opera *Esquisse d'una morale sans obligation ni sanction*, Parigi, 1885, e più ancora nella sua opera più nota, *L'irréligion de l'avenir*, Parigi, 1887 – considera l'anomia morale come l'esito desiderabile della speculazione metafisica nel campo dell'etica. A tale teoria si contrappone Émile Durkheim, che, dopo aver recensito il saggio di Guyau del 1887 [*Guyau. L'irréligion de l'avenir* (rec.), in *Revue Pholosophique*, XXIII, 1887, p. 299], fin dalla sua prima opera (*De la division du travail social*, Parigi, 1983, trad. it. *La divisione del lavoro sociale*, Edizioni di Comunità, Milano, 1977) considera l'anomia una negazione della morale perché capace di inficiare inevitabilmente il sentimento dell'obbligazione, e cioè le basi necessarie di ogni socialità. Lo stesso Durkheim, nell'opera *Le suicide. Étude de sociologie*, Parigi, trad. it. *Il suicidio*, Torino, Utet, 1969, dopo aver stabilito tra anomia soggettiva e sociale un rapporto di reciproca interferenza e condizionamento, giunge ad affermare che le passioni, liberate da ogni freno inibitorio, rimuovono gli obiettivi di promozione sociale assegnati a ciascuno ed espongono quindi l'individuo a una situazione di malessere e di inquietudine. La sociologia moderna si è assestata, seppure con toni diversificati a seconda degli autori, sulla posizione di Durkheim. Per brevi considerazioni in proposito e ulteriori riferimenti bibliografici, v. R. MARRA, s.v. *Anomia*, in *Digesto Italiano, Discipline privatistiche Sez. civile*, Utet, Torino,

- impedire al commercio elettronico di sviluppare pienamente le proprie potenzialità, sino a oggi soffocate proprio dall'incertezza che regna nel mercati telematici, rispetto ai quali, nella stragrande maggioranza dei casi, nessuno può nutrire alcun affidamento circa la reale identità della controparte e, dunque, circa la serietà della altrui dichiarazione negoziale, la solvibilità, la sicurezza dei pagamenti effettuati in rete, ecc.[68];
- permettere che vengano raccolti, trattati e scambiati *online* dati personali altrui senza che alcuno ne risponda;
- favorire il definitivo radicamento della sensazione di deresponsabilizzazione diffusa tra gli utenti, con conseguente accelerazione del processo di perdita o frammentazione dell'identità dei consociati[69].

Tutto ciò non giova allo sviluppo delle tecnologie di rete, né alle comunità umane che alla reti hanno accesso. Del resto, anche la

[68] In proposito, si segnala la riflessione di K.M. REED, "From The Great Firewall of China to the Berlin Firewall: The Cost of Content Regulation on Internet Commerce", in *Transnational Lawyer*, 13, 2 (2000), pp. 451-476, nella quale l'A. si sofferma sull'evoluzione storica della libertà di espressione in Cina e Germania, per poi analizzare gli effetti deprimenti che sullo sviluppo di Internet, e in particolare del commercio elettronico, può sortire la possibilità per gli utenti di svolgere qualsiasi attività, anche illecita, senza subire sanzioni. Cfr. anche A. MANN e B.S. ROBERTS, "CyberLaw: A Brave New World", in *Dickinson Law Review*, 106 (2001), pp. 305-365. In proposito, per una visione del problema parzialmente diversa, vd. D.L. BURK, "Muddy Rules for Cyberspace", in *Cardozo Law Review*, 21, (1999), pp. 168-176. Egli, riflettendo sul DMCA (*Digital Millennium Copyright Act*), sostiene l'efficienza economica di regole che, rispetto alle attività compiute in Internet, non attribuiscano con certezza diritti e tutele. L'A. giustifica la sua posizione osservando che, quando i costi transattivi sono molto alti – è questo il caso del ciberspazio, in cui per ogni diritto negoziabile c'è sempre un numero enorme di potenziali interessati –, regole "fangose" incentivano i soggetti coinvolti a trovare accordi informali, che risultano meno costosi e dunque efficienti. La riflessione di Burk, a ben vedere, è condotta sempre in punta di penna e ciò in quanto lo stesso A. avverte che l'efficienza o meno delle *muddy rules* dipende da molte variabili che andrebbero, di volta in volta, accertate in concreto.

[69] Sulla "libertà virtuale" come "illusione di libertà" ed elemento di reale "trasformazione dell'umano", v. A. PUNZI, *L'ordine giuridico delle macchine. La Mettrie Elvétius D'Holbach, l'uomo macchina verso l'intelligenza collettiva*, Giappi-

Commissione europea, sin dal 1996, riconosce che «Internet does not exist in a legal vacuum»[70]. A ben vedere, anche la direttiva 2000/31/Ce non ignora il problema, visto che ripetutamente nei *considerando* si legge che, per consentire un efficiente sviluppo del commercio elettronico e, più in generale, della società dell'informazione, occorre realizzare un quadro normativo volto a dare certezza agli operatori e agli utenti[71].

9. Il caso Napster: responsabilizzazione degli utenti e sviluppo di Internet.

Un contributo fondamentale, nell'economia della riflessione che stiamo conducendo sugli effetti prodotti dall'accesso anonimo alla Rete attualmente, di fatto, garantito agli utenti di Internet, viene dall'analisi del cosiddetto *caso Napster*.

Come è noto, Napster era un prestatore di servizi di Internet – nato dall'intuizione di un diciannovenne di nome Shawn Fanning – che consentiva ai cibernauti di scaricare gratuitamente in rete, dall'apposito sito web, un programma proprietario, tramite il quale gli utenti mettevano a disposizione di chiunque si servisse dello stesso programma i *file* musicali caricati in formato MP3 sulla memoria fissa del proprio computer[72]. Il servizio in parola, secondo molti, ha rappresentato l'icona della tecnologia cosiddetta *peer-to-peer* (o "P2P") "*file sharing*"; una tecnologia, cioè, che si basa sulla condivisione di *file* tra soggetti che hanno le stesse capacità tecniche di iniziare una sessione di comunicazione (cosiddetta condivisione da pari a pari) e che si candida a diventare la nuova modalità di sfruttamento delle risorse trasferibili e trasmissibili nelle reti digitali e, dunque, in definitiva, il nuovo modello di distribuzione dei prodotti digitalizzati. Tale modello è opposto rispetto a quello tradizionale, fondato, anche in Internet, sulla contrapposizione *client-server*, nel quale il *server* attende le richieste del *client* e le soddisfa. Nel sistema distributivo P2P, le risorse non sono più detenute da *server* centralizzati che le gestiscono, più o meno discrezionalmente, attribuendole solo a determinate condizioni e solo a determinati soggetti; esse infatti sono memorizzate, in maniera diffusa e capillare, sui dischi fissi dei computer degli utenti, i quali le condividono automaticamente senza sostenere i costi che invece il prestatore del relativo servizio dovrebbe sopportare per gestire il *server*[73].

Più in dettaglio, la forza della tecnologia P2P sta nel fatto che un utente interessato a rintracciare in Internet un determinato prodotto lo

[70] Comunicazione [COM(96) 487] del 16 ottobre 1996, della Commissione CE al Parlamento europeo, al Consiglio, al Comitato economico e sociale e al comitato delle regioni, intitolata «Informazioni di contenuto illegale e nocivo su Internet», reperibile all'indirizzo www2.echo.lu/legal/en/internet /content/communic.html.

[71] La direttiva 2000/31/Ce, come si vedrà *infra*, si occupa specificamente, anche se indirettamente, dell'identificabilità degli utenti. Sin d'ora, in proposito, è bene segnalare i considerando n. 40 e 48 della direttiva, sui quali si tornerà tra breve.

[72] La sigla "MP3" indica uno standard di compressione di *file* musicali, elaborato all'interno del *Moving Pictures Experts Group* (MPEG). Il formato MP3consente essenzialmente di ridurre lo spazio di memoria occupato dal *file* musicale e, dunque, ne permette un più facile e veloce trattamento. A esso si è fatto ricorso perché la memorizzazione nel disco rigido del computer di *file* musicali in formato digitale classico – quello supportato dal tradizionale CD musicale – occupa troppo spazio, e

to MP3che in Internet sono nati negli ultimi anni moltissimi siti per la diffusione di brani musicali. Alcuni consentono solo l'ascolto del pezzo (il cosiddetto *streaming*), senza dare la possibilità di scaricarlo e dunque di memorizzarlo sul disco fisso del navigatore (*downloading*).

[73] La Corte Federale Distrettuale degli Stati Uniti, Distretto di New York, nella sentenza 4 maggio 2000, in *Foro italiano*, 2001, IV, 102, con nota di PASCUZZI, si era già occupata di violazione del diritto d'autore tramite *downloading* da Internet di file musicali. Nella circostanza, tuttavia, i brani musicali, in formato MP3, venivano scaricati dagli utenti direttamente dal *server* del sito Internet sul quale essi erano stati precedente memorizzati dai gestori dello stesso (che, infatti, la corte non esita a condannare). In altre parole, le modalità di distribuzione del prodotto editoriale, nella fattispecie presa in considerazione dalla pronuncia in parola, non si distaccavano dal modello classico *client-server*. Per gli opportuni approfondimenti, cfr., tra gli altri, L.A. FLATE "New Technology Clauses Aren't Broad Enough: Why A New Standard of Interpretation Must Be Adopted for Internet Distribution", in *Hastings Communication and Entertainment Law* Journal, 23, (2000), pp. 157-171; D. BALABAN, "The Battle of the Music Industry: the Distribution of Audio and Video Works via Internet, Music and More, in *Fordham Intellectual Property Media & Entertainment Law Journal*, 12, 1 (2001), pp. 235-288; nonché A. COLANGELO, "Copyright Infringement in the Internet Era. The Challenge of MP3s", in *Alberta Law Re-*

cercherà in automatico, mediante l'apposito *software*, presso un determinato numero di altri utenti; se questi non saranno in grado di soddisfare la richiesta, perché sui loro dischi rigidi non esiste quel prodotto, essi stessi invieranno in automatico la stessa richiesta ad altri utenti, fino a quando il materiale ricercato dal primo navigante non verrà rintracciato in uno degli *hard disk* collegati al servizio di condivisione. In questo modo operava Napster, il cui successo fu tale che dal mese di giugno 1999, data di attivazione del servizio, fino al momento della definitiva interruzione dello stesso, occorsa il 26 luglio 2000, il numero degli abbonati raggiunse la cifra record di 20 milioni[74].

Il consenso di pubblico, ottenuto del servizio di condivisione *online* di *file* sonori messo a punto da Napster, spinse 21 *majors* dell'industria discografica mondiale a promuovere collettivamente un'azione legale volta a ottenere l'interruzione dello stesso. Secondo gli attori, Napster, attraverso la sua attività di preparazione dello strumento tecnico e di intermediazione, consentiva la violazione sistematica, da parte degli utenti, dei diritti d'autore sulle opere che questi ultimi si mettevano reciprocamente a disposizione, senza aver avuto alcuna autorizzazione in tal senso, ed era dunque responsabile per *contributory infringment* dei danni causati. Napster, a sua volta, si difendeva osservando preliminarmente che i suoi abbonati, all'atto della registrazione, si impegnavano espressamente a non utilizzare il servizio in modo tale da violare diritti d'autore[75]; e, dunque, sottolineando che il servizio sotto

[74] La vicenda legale di Napster è riassunta efficacemente in P. CERINA, "Il diritto industriale 10 anni dopo. Il punto su... Internet", in *Il diritto industriale*, 10, 4 (2002), pp. 351-369, il quale svolge anche interessanti considerazioni circa il modello distributivo P2P e la tutela della proprietà intellettuale in rete. Sulla tecnologia "*peer-to-peer*" (P2P) e sugli effetti giuseconomici di una sua implementazione, cfr. A.C. YEN, "A Preliminary Economic analysis of Napster: Internet Technology, Copyright Liability, and the Possibility of Cosean Bargaining", in *University of Dayton Law review*, 26 (2001), pp. 248-277; e G. FESSENDEN, "Peer-to-Peer Technology. Analysis of Contributory Infringment and Fair Use", in *IDEA – The Journal of Law and Technology*, 42, 3 (2002), pp. 391-416.

[75] La clausola del contratto recitava testualmente: «Napster will terminate the accounts of users who are repeat infringers of the copyrights, or other intellectual property rights, of others. In addition, Napster reserves the right to terminate the account of a user upon any single infringement of the rights of others in conjunction

accusa si era limitato a creare una comunità di utenti di Internet amanti della musica, senza peraltro permettere che sul proprio *server*, o attraverso quest'ultimo, avvenissero attività illecite[76].

Inoltre, Napster chiedeva che fosse dato risalto al fatto che il servizio di ricerca e scambio di materiale poteva essere usato senza infrangere alcun diritto altrui, e sottolineava come l'utilizzazione illecita fosse soltanto una eventualità, peraltro indipendente dalla volontà del prestatore e sottratta al suo controllo. Ponendo l'accento su tali argomentazioni difensive, Napster richiamava il caso *Sony Betamax*, nel quale la Corte Suprema degli Stati Uniti mandò esente da responsabilità la Sony Corporation per la produzione di videoregistratori che, a detta degli attori – titolari di diritti d'autore su opere televisive – consentivano agli utenti di violare tali diritti[77]. Nella pronuncia che chiuse la vicenda *Sony Betamax*, che rappresenta uno dei *leading case* in materia di *contributory infringment* per violazione del diritto d'autore, la corte aveva affermato che, quando una tecnologia che facilita le copie non autorizzate di opere è comunque capace di significativi utilizzi leciti, la sua fornitura non comporta responsabilità a titolo di *contributory infringment*, anche perché con una inibitoria alla produzione di una tecnologia di tal fatta non si persegue l'interesse pubblico allo sviluppo di nuove tecnologie[78].

[76] Giova precisare che il software utilizzato metteva direttamente in comunicazione il computer dell'utente che cercava determinati brani con quello dell'utente che nel suo *hard disk* deteneva tali brani, senza che i materiali sonori in questione passassero mai per il *server* di Napster.

[77] *Sony Corp. of America v. Universal Studios, Inc.*, 464 *U.S.* 417, 104 *S.Ct.* 774, 78 *L.Ed.2d* 574 (1984). La sentenza emessa della Corte Suprema degli Stati Uniti in data 17 gennaio 1984, che risolse la controversia definitivamente, è riprodotta anche in *Foro italiano*, 1984, IV, 351, con nota di PASCUZZI.

[78] Il contemperamento tra le ragioni degli autori, che vantano il diritto esclusivo di riproduzione e sfruttamento commerciale delle opere, e l'interesse pubblico allo sviluppo delle tecnologie riproduttive è stato perseguito in Italia con la legge 5 febbraio 1992, n. 93, recante «Norme a favore delle imprese fonografiche e compensi per le riproduzioni private senza scopo di lucro», la quale ha stabilito il principio per cui agli autori compete un diritto di credito, verso i produttori e importatori di supporti di registrazione e di apparecchi di registrazione, amministrato da società di gestione dei diritti (come la Siae).

Il 26 luglio 2000 il giudice Marilyn Hall Patel, della Corte Distrettuale del Nothern District della California, dopo aver vagliato in particolare la *section* 512 del *Digital Millenniumm Copyright Act*, sulla base del quale gli attori avevano intentato causa[79], respingeva le argomentazioni difensive di Napster e, accogliendo le pretese attoree, ordinava alla convenuta di cessare entro la mezzanotte del giorno successivo ogni attività che consentisse lo scambio di materiale coperto da diritti d'autore. La pronuncia si fondava sostanzialmente su due affermazioni: la prima, gli utenti, scambiandosi i *file* musicali, violano i diritti d'autore degli attori; la seconda, Napster, poiché fornisce il supporto teologico che consente, o quantomeno facilita, queste contraffazioni, non può godere della esenzione di responsabilità stabilita, in particolari condizioni, per i *service provider* dalla *section* 512 del DMCA, ed è dunque responsabile a titolo di *contributory infringment*[80].

Napster impugnava la decisione presso la Corte d'Appello del non circuito, la quale, prima, in data 28 luglio 2000, accoglieva in via d'urgenza il ricorso per la sospensiva dell'ingiunzione che ordinava la chiusura del servizio e che di lì a qualche ora sarebbe divenuta pienamente operativa; poi, decidendo definitivamente sull'ingiunzione, il 12 febbraio 2001, emanò una pronuncia piuttosto articolata che, malgrado di fatto in parte riformasse la decisione reclamata, sostanzialmente confermava l'analisi svolta dal giudice Patel[81]. Gli argomenti spesi a sostegno della decisione riguardano, in particolare: l'uso "commerciale", quantomeno dal punto di vista del risparmio dei costi, che del servizio facevano gli abbonati di Napster; la non applicabilità del precedente *Sony Betamax*, giustificata dalla circostanza che, mentre i prodotto copiati attraverso un videoregistratore restano nella materiale disponibilità dell'utente, nel caso di Napster il servizio era immediatamente volto a consentire lo scambio dei materiali sonori copiati o da copiare; ed infine, la consapevolezza che, con tutta probabilità, Napster aveva dell'utilizzazione illecita che la stragrande maggioranza dei suoi clienti faceva del servizio. La corte, in parziale riforma dell'ingiunzione, nel rinviare la questione nuovamente alla District Court del Northern District della California, perché decidesse nel merito, affermò l'esigenza di meglio valutare la eventuale *contributory liability* del *provider* Napster, in quanto non si poteva affermare la non applicabilità *tout court* del DMCA alla vicenda in esame, e dunque occorreva verificare la reale possibilità per il gestore del servizio di avere notizia circa l'uso illecito che di quest'ultimo gli utenti facevano, tenendo peraltro in debita considerazione il fatto che la tecnologia utilizzata da Napster non gli consentiva di accedere o controllare i *file* MP3 memorizzati sugli *hard disk* degli abbonati.

La corte distrettuale, accogliendo l'invito del giudice d'appello, nel marzo seguente, emanava una decisione in riforma della precedente inibitoria, con la quale imponeva al prestatore del servizio di bloccare le singole attività nei riguardi delle quali si fossero ricevute formali denunce di violazione del *copyright* entro tre giorni dalla ricezione della notizia, nonché di svolgere un monitoraggio costante del servizio volto a prevenire la realizzazione di attività illecite. Napster, allora, in ottemperanza di tal ultima ingiunzione, sviluppava rapidamente un nuovo *software* finalizzato a impedire agli utenti l'accesso a *file* musicali protetti da diritto d'autore. Senonché il programma non si rivelò realmente efficace, in quanto gli abbonati, modificando i titoli dei brani, lo eludevano facilmente. Ciò portò il giudice Patel – che pure riconosceva a Napster le difficoltà tecniche di effettuare un reale controllo

[79] La pronuncia della Corte Distrettuale del Northern District della California – caso *A&M Records, Inc. v. Napster, Inc.*, 2000 *U.S. Lexis Dist.* 6243, 114 *F. Supp.2d* 896 (N.D. Cal. 2000) – apre la parte dedicata alla *discussion*, chiarendo al §7 che: «Section 512 of the DMCA addresses the liability of online service and Internet access providers for copyright infringements occurring online. Subsection 512(a) exempts qualifying service providers from monetary liability for direct, vicarious, and contributory infringement and limits injunctive relief to the degree specified in subparagraph 512(j)(1)(B). Interpretation of subsection 512(a), or indeed any of the section 512 safe harbors, appears to be an issue of first impression».

[80] Il giudice Patel conclude osservando: «This court has determined above that Napster does not meet the requirements of subsection 512(a) because it does not transmit, route, or provide connections for allegedly infringing material through its system. The court also finds summary adjudication inappropriate due to the existence of genuine issues of material fact about Napster's compliance with subparagraph 512(i)(A), which a service provider must satisfy to enjoy the protection of any

[81] *A&M Records, Inc. v. Napster, Inc.*, 2001 *U.S. App. LEXIS* 1941, 12.02.2001,

– a minacciare nuovamente la chiusura definitiva del servizio, che, del resto, essendo rimasto chiuso per circa tre mesi, dal gennaio al marzo del 2001, aveva perso la maggior parte dei suoi clienti, i quali nel frattempo avevano trovato altri siti analoghi a quello gestito da Napster.

La vicenda, qui riassunta nei suoi tratti essenziali, è sotto diversi aspetti significativa della situazione in cui versa attualmente Internet. In particolare, per quanto di nostro interesse, giova sottolineare come il tenore delle pronunce citate impedisca a qualunque fornitore di prestare un servizio analogo a quello di Napster; e ciò, nonostante il modello distributivo P2P rappresenti una tecnologia in grado di consentire lo sfruttamento più efficiente, e dunque più razionale, delle risorse di rete[82]. Tale modello, infatti, risolve problemi di reperimento delle informazioni su Internet perché supera i motori di ricerca tradizionali, per definizione non in grado di monitorare i materiali memorizzati nei computer degli utenti[83]; inoltre, scardinando le posizioni dominanti dei *gatekeeper* (i soggetti che tradizionalmente detengono e distribuiscono le informazioni al pubblico) garantisce effettivamente a tutti gli

[82] Nello stesso senso si esprime P. CERINA, "Il diritto industriale 10 anni dopo...", cit., p. 361. Così anche V.M. DE SANCTIS, "Internet e il diritto con particolare riferimento al diritto d'autore: un bilancio provvisorio", in *Rivista del diritto commerciale*, 99, 5/8, 1 (2001), pp. 321-355 e partic. p. 332. Per considerazioni più generali sul punto, v. J. WALKER e A. SHARP, "Digital Rights Management", in *Computer Law & Security Report*, 18, 4 (2002), pp. 259-263; nonché T.C. INKEL, "Internet-Based Fans: Why the Entertainment Industries Cannot Depend on Traditional Copyright Protections", in *Pepperdine Law Review*, 28, 4 (2001), pp. 879-913; e H.H. TANAKA, "Post-Napster: Peer-to-Peer File Sharing Systems: Current and Future on Secondary Liability Under Copyright Laws in the United States and Japan", in *Loyola of Los Angeles Entertainment Law Review*, 22 (2001), pp. 37-84. Del resto, un servizio analogo a quello di Napster, prestato da un sito coreano, ha subito lo stesso trattamento giurisprudenziale. Sulla questione, v. K. SOHN, "Soribada, Korea's Napster, Suffers Judicial Blow", in *World eBusiness Law Report*, 4 settembre 2002, 4.

[83] Sui problemi giuridici suscitati dai motori di ricerca tradizionali, in particolare nell'ottica del diritto d'autore, cfr. M. ORLANDI, "Motori di ricerca e diritto d'autore", in *Annali italiani del diritto d'autore*, 1998, pp. 266-281.

utenti la più libera e incondizionata possibilità di scambiare informazioni e prodotti con altri, senza subire censure di alcun tipo[84].

Nell'ottica di uno sfruttamento della rete volto a consentire ai naviganti la massima libertà nel manifestare il proprio pensiero, trovare e scambiare materiali e informazioni, accedere ai contenuti più vari, intraprendere relazioni personali o commerciali, ecc., il modello P2P rappresenta una tappa attualmente obbligata dell'evoluzione di Internet. Ostacolarne la diffusione, come si è fatto nel caso Napster, con evidenti effetti a macchia d'olio su ogni altra tecnologia analoga, vuol dire depotenziare Internet al fine, certamente tutt'altro che trascurabile, di proteggere i diritti d'autore sulle opere digitalizzate.

La soluzione estrema, adottata dai giudici nordamericani nel caso Napster, trova una sua giustificazione nell'anonimato totale di cui gli utenti di Internet possono godere se solo lo desiderano. In altre parole, considerato che i naviganti possono utilizzare qualunque servizio di rete per realizzare fatti illeciti senza essere chiamati a risponderne, le corti hanno ritenuto conveniente vietare la realizzazione di una tecnologia in grado di moltiplicare gli effetti dannosi di questi illeciti, pur considerando che tale tecnologia, in realtà, è in grado di moltiplicare anche gli effetti positivi della comunicazione di rete (o, più tecnicamente, le "esternalità di consumo positive") e va perciò considerata, sostanzialmente, virtuosa[85].

Per impedire (o, quantomeno, contrastare) la violazione *online* di diritti d'autore o di altri diritti, senza, tuttavia, ostacolare l'evoluzione

[84] Nella causa *A&M v. Napster*, addirittura, la società dei medici americani aveva depositato una memoria *amicus curiae* con la quale dichiaravano di voler utilizzare la tecnologia 2P2 per condividere, e dunque scambiarsi, dati scientifici e clinici.

[85] Nell'ambito degli studi condotti in materia di economie dei *network*, si parla di "esternalità di consumo" in riferimento ai casi in cui l'utente è interessato, positivamente o negativamente, alla produzione o al consumo di un altro utente. L'esempio classico è costituito dalla telefonia: più utenti sono collegati alla rete, più aumenta il valore dell'accesso alla stessa, in quanto, più persone sono raggiungibili attraverso quella rete, più cresce l'utilità che il singolo utente trae dall'essere in rete. All'aumentare del numero di utenti, inoltre, cresce in modo molto più che proporzionale l'utilità marginale derivante dall'ingresso nel *network* di un nuovo utente, e ciò in quanto: 4 utenti hanno tra loro 12 relazioni, mentre 6 amici ne hanno 20, 7 ne hanno 42, e così via. Cfr. E. TOMMASINI, "La proprietà intellettuale su Internet tra tutela giuridica e promozione a costo zero", in *Cyberspazio e diritto*, 2 (2002), pp. 203-223.

tecnologica della grande rete, la soluzione che appare di gran lunga preferibile si fonda sull'assunto che chi utilizza una rete di informazione e comunicazione non ha alcun diritto a godere dell'anonimato più completo, così come non ha un tale diritto quando intraprende qualsiasi attività fuori dalla rete[86]. In altre parole, posto che tutti i consociati, almeno negli ordinamenti evoluti, devono sempre essere identificabili, così dovrebbe essere – ma di fatto, a oggi, così non è – anche sulle reti digitali. Nel caso Napster, l'identificabilità degli utenti avrebbe consentito all'industria discografica di colpire i singoli autori degli illeciti senza obbligare il prestatore a sospendere un servizio che in sé si prestava a tante utilizzazioni lecite. Inoltre tale identificabilità appare l'unico espediente tecnico attraverso il quale contrastare giuridicamente l'utilizzazione illecita di servizi distributivi *online* che si basano su un modello P2P non proprietario, nel quale cioè – a differenza di quanto avveniva rispetto a Napster – il *software*, che abilita allo scambio di materiali tra gli utenti, è fornito da un prestatore sul cui sito non si svolge nessuna attività ulteriore rispetto al *downloading* del programma o, addirittura, è venduto *offline* con finalità ricreative, informative, di studio, ricerca e quant'altro. Creare i presupposti perché in rete gli utenti siano identificabili, così come lo sono in ogni altro contesto, si badi bene, significa determinare, peraltro nel modo più semplice e immediato, le condizioni necessarie a rendere operative nella realtà digitale le categorie giuridiche tradizionali.

10. L'identificabilità degli utenti che accedono a Internet finalizzata all'imputazione degli illeciti *online*.

Esiste una strada – sinora, in verità, trascurata sia dai legislatori sia dalla maggior parte degli studiosi[87] – per comporre il conflitto tra i valori e gli interessi coinvolti nella questione dell'anonimato e quelli afferenti ai problemi di imputazione della responsabilità per illeciti commessi *online*. Una strada che, passando per la "identificabilità" di operatori e utenti, consentirebbe, laddove seguita, di ripristinare nelle relazioni di rete, e dunque anche in Internet, alcune delle condizioni essenziali perché l'ordinamento giuridico tradizionale, o meglio la cultura giuridica che da millenni pone l'uomo al centro dell'ordinamento, possa operare[88].

L'opportunità di interpretare la citata direttiva 2000/31/Ce sul cosiddetto "commercio elettronico", e più in generale sulla società dell'informazione, nonché le normative nazionali di attuazione, seguendo la soluzione ermeneutica che qui si propone sembra ricavarsi dall'analisi, in precedenza compiuta, degli obiettivi di politica del diritto perseguiti dalla disciplina di origine comunitaria in esame[89].

[86] Secondo P. CERINA, "Il diritto industriale 10 anni dopo...", cit., p. 361: «l'industria musicale e dell'intrattenimento ha dunque colpito come poteva: non potendo raggiungere gli utenti, si è indirizzato contro l'unico soggetto disponibile, cioè il sito (Napster, appunto)».

[87] Una prima proposta, volta a limitare l'anonimato in Internet, fu formulata da Cyberspace", in *Columbia Law Review*, 96, 6 (1996), pp. 1526-1572. L'autore nordamericano suggerì di garantire ai naviganti una *psuedo-anonymity* piuttosto che una *true anonymity*, attribuendo ad alcuni soggetti il compito di rivelare, in presenza di determinate circostanze, l'identità dei singoli utenti, che durante la navigazione resterebbero, tuttavia, coperti dall'anonimato. Negli Stati Uniti, né il formante giurisprudenziale, né quello legislativo, hanno dimostrato simpatia per le tesi volte a limitare l'anonimato in Internet. Nella dottrina italiana, per una proposta di lettura della Direttiva 2000/31/ce finalizzata ad attribuire agli *access provider* un obbligo di controllo sulle generalità dei propri clienti, v. F. DI CIOMMO, "Internet (responsabilità civile)", cit., pp. 9-11; ID., "La responsabilità civile nell'era di Internet", in G. Ponzanelli, La responsabilità civile. Tredici variazioni sul tema", Cedam, Padova, 2002, pp. 179-226 e partic. pp. 195-196, nota n. 39; e ancora ID., Internet e crisi del diritto privato...", cit. Cfr. Y. POULLET, "Libertés et société de l'information: le droit de participer à la société de l'information et le droit de s'en exclure", in *Revue Ubiquité*, 1, 1998, pp. 21-28; e H. NISSENBAUM, "The Meaning of Anonymity in an Information Age", *The Information Society* 15 (1999), pp. 141-144.

[88] Il giurista, partendo dall'opinione del sociologo, secondo cui «la mancanza della dimensione fisica nel mondo telematico rende impossibile l'applicazione di una serie importante di misure di controllo sociale basate sull'esercizio della forza» (così L. PACCAGNELLA, *La comunicazione al computer*, cit., p. 105), deve muovere alla ricerca di nuove soluzioni che consentano al diritto di trovare applicazione anche a una realtà affatto nuova qual è il pianeta telematico.

[89] Particolarmente importanti si rivelano, a riguardo, le iniziative comunitarie (cfr. la Comunicazione della Commissione del 30 gennaio 2001 [COM(2000)890], intitolata: «Creare una società dell'informazione sicura migliorando la sicurezza del-

Una volta chiarito, infatti, che il legislatore europeo ha voluto realizzare un complesso di principi capace di promuovere il progresso della società dell'informazione, nella consapevolezza che tale progresso è possibile soltanto in presenza di regole giuridiche certe, efficaci ed efficienti, occorre interpretare tali principi cercando di preservare la libertà di prestazione dei servizi della società in parola e la *privacy* di cui l'utente vuole godere in rete, senza, tuttavia, sacrificare l'applicazione del principio di responsabilità giuridica rispetto alle azioni commesse *online*. Il considerando 41 della direttiva, del resto, rappresenta espressione di questa esigenza, laddove esso afferma che: «La direttiva rappresenta un equilibrio tra i vari interessi in gioco [...]».

Come si diceva, la soluzione che qui si propone – per realizzare effettivamente l'equilibrio tra gli interessi in gioco e, dunque, per perseguire nel miglior modo possibile gli obiettivi della direttiva – è rappresentata dalla identificabilità degli utenti della rete. Per realizzare tale identificabilità – che non vuol dire piena e immediata identificazione degli utenti – devono ricavarsi, dal tessuto normativo, obblighi, a carico dei prestatori del servizio di accesso alla rete (nel caso di Internet, gli *access provider*) circa il controllo dell'identità reale dei clienti e il mantenimento dei dati utili a consentire, in ogni momento, l'individuazione dell'autore di un illecito compiuto mediante l'IP gestito dal singolo fornitore di accesso. Attenendosi a quest'obbligo,

volte a istituire una rete di collaborazione a livello europeo per la prevenzione dei crimini informatici. Tali iniziative impongono ai prestatori si servizi della società dell'informazione, e in particolare ai *provider* di Internet, un generale obbligo di conservazione dei dati sul traffico dei propri clienti al fine di favorire i controlli dell'autorità giudiziaria o delle forze di polizia. Sul punto si registra la posizione critica dei c.d. Garanti europei per la *privacy*: v. la Raccomandazione n. 3/99 del 7 settembre 1999 su «La conservazione dei dati sulle comunicazioni da parte dei fornitori dei servizi Internet a fini giudiziaria». A ciò va aggiunto che l'art. 15, par. 1, della direttiva 2002/58/Ce consente agli Stati membri, al fine di prevenire o sanzionare la commissione di reati in rete, «di adottare misure legislative le quali prevedano che i dati siano conservati per un periodo di tempo limitato»; inoltre, l'art. 10 della stessa direttiva ha esplicitamente sancito la derogabilità dei limiti alla conservazione dei dati sull'ubicazione, nonché delle norme sulla identificazione della linea chiamante, in caso di chiamate malintenzionate o inopportune. La recente normativa dimostra la consapevolezza del legislatore europeo circa le ricadute giuridiche ed economiche

ogni prestatore di accesso, quando si presenti l'occasione, sarebbe in grado di rivelare all'autorità giudiziaria, che ne faccia richiesta[90], la reale identità dell'autore dell'illecito, sempre che questi sia un suo cliente; ma, allo stesso tempo, gli altri prestatori e gli altri utenti non potrebbero individuare le generalità del navigante che vuole tutelare il proprio anonimato.

In ogni caso, è bene precisare che la soluzione, qui sostenuta – consistente nel ritenere i prestatori che svolgono il ruolo di *access* o *host provider* obbligati a controllare l'identità dei propri clienti (così come i *service* a conservare, per un congruo periodo di tempo, memoria di ogni attività che gli *user*, coperti dagli IP, compiono nello sfruttamento del servizio) – espone gli utenti della Rete a un rischio non secondario. Infatti, qualora il prestatore di accesso o di ospitalità, che detiene i dati personali dei singoli utenti, li ceda ad altri operatori della Rete, questi ultimi possono violare la *privacy* dei singoli naviganti associando ai dati raccolti *online*, individuati esclusivamente dall'IP, le generalità reali dello *user*.

Il problema in parola, tuttavia, è meno drammatico di come potrebbe sembrare. Con riferimento a Internet, infatti, è dato osservare che le caratteristiche tecniche dei rapporti di Rete fanno sì che l'*access* e l'*host provider* – che dovrebbero essere, a nostro avviso, gli unici a detenere i dati personali reali dei clienti – possono raccogliere le informazioni concernenti la navigazione dei singoli utenti soltanto relativamente al primo sito verso il quale essi muovono dopo essere entrati in Rete. In altre parole, ed esemplificando, se l'utente ha l'accortezza di farsi prestare i servizi ulteriori, rispetto all'accesso, da un soggetto diverso dal suo *access provider*, nessuno – a meno che i prestatori non si scambino ripetutamente i dati dell'utente (ogni volta l'*access provider* dovrebbe dichiarare, ai soggetti interessati, a quale utente, in un determinato momento, è stato attribuito l'IP con il quale la data attività *online* è stata compiuta) – potrà conoscere la reale identità del sogget-

[90] È opportuno che la richiesta all'*access provider*, finalizzata a ottenere le esatte generalità dell'utente, piuttosto che pervenire direttamente dal danneggiato, sia fatta dall'autorità giudiziaria competente su indicazione dell'attore che agisce in giudizio o della forza di pubblica sicurezza che sta svolgendo indagini. Questa soluzione, oltre ad apparire più garantista dal punto di vista della *privacy* degli utenti di Internet,

to di cui spia la corrispondenza elettronica, le preferenze manifestate attraverso le sue passeggiate telematiche, le conversazioni svolte in *chat* e così via.

Del resto, nel nostro ordinamento l'anonimato effettivo non è mai stato considerato un diritto soggettivo dei consociati[91], mentre alcune forme specifiche di anonimato relativo – e la "identificabilità", che qui si propone, si tradurrebbe proprio in un anonimato relativo – sono giustificate in ragione della tutela di interessi ulteriori e primari[92]. Quello all'anonimato, dunque, quando riconosciuto, è un diritto strumentale alla realizzazione di un interesse che l'ordinamento, in determinate circostanze, vuole tutelare. È il caso, per esempio, dell'art. 13, comma 1, lett. c), n. 2, già della legge 675/96 (oggi deve farsi, ovviamente, riferimento al d.lgs. 196/2003) ai sensi del quale «in relazione al trattamento dei dati personali l'interessato ha diritto [...] di ottenere, a cura del titolare o del responsabile, senza ritardo [...] la cancellazione, la trasformazione in forma anonima o il blocco dei dati trattati in violazione della legge, compresi quelli di cui non è necessaria la conservazione in relazione agli scopi per i quali i dati sono stati raccolti o successivamente trattati».

Dunque, anche nella cosiddetta legge sulla *privacy*, il cui scopo precipuo è quello di tutelare la riservatezza delle persone fisiche e giuridiche rispetto al trattamento di dati personali, non c'è una affermazione assoluta del diritto all'anonimato, in quanto quest'ultimo – costituito, nella fattispecie, dalla facoltà di chiedere che il dato assuma

[91] Negli Stati Uniti è la stessa Costituzione che, nel Quarto Emendamento, afferma: «the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized».

[92] Per gli opportuni approfondimenti, tra i non molti autori che si sono dedicati all'argomento, vd. A. CANDIAN, s.v. "Anonimato (diritto all'—)", in *Enciclopedia del diritto*, Treccani, Milano, 1958, II, p. 499-502 e partic. 500; ma anche G. FINOCCHIARO, "Diritto all'anonimato", in F. GALGANO (sotto la direzione di), *Trattato di diritto commerciale e diritto pubblico dell'economia*, Cedam, Padova, 2009, XLVIII, pp. 411 ss.. Per considerazioni recenti sul concetto di anonimato relativo, cfr. M. GAGLIARDI, "La tutela della persona rispetto al trattamento dei dati anonimi tra valenza economica delle informazioni e diritti fondamentali", in G. COMANDÉ (a

forma anonima, e cioè non sia associato alle generalità della persona – è riconosciuto soltanto in presenza di determinati presupposti e a certi fini[93]. Inoltre, a ben vedere, il diritto all'anonimato è volto a tutelare la posizione passiva di un soggetto che, senza nulla aver fatto o aver voluto, scopre i suoi dati inseriti in un archivio e trova, in determinate circostanze, nella resa del dato in forma anonima il modo migliore per tutelare la sua *privacy*; mentre l'anonimato, che finora di fatto si concede agli utenti di Internet che si attrezzano per sfruttare in tal senso le caratteristiche della rete, può essere definito attivo in quanto desoggettivizza le azioni compiute da questi stessi naviganti.

La stessa direttiva 2000/31/Ce consente, del resto, di affermare che nel conflitto tra tutela della *privacy* degli utenti e sicurezza della Rete, il legislatore europeo abbia preferito puntare sulla sicurezza. Infatti, sia nel considerando n. 48, che nell'art. 15, l'articolato di origine comunitaria espressamente – come già detto – prevede che gli stati membri possono stabilire che i prestatori della società dell'informazione siano tenuti a: 1) «informare senza indugio la pubblica autorità competente di presunte attività o informazioni illecite dei destinatari dei loro servizi»; e 2) «a comunicare alle autorità competenti, a loro richiesta, informazioni che consentano l'identificazione dei destinatari dei loro servizi con cui hanno accordi di memorizzazione dei dati»[94]. La stessa giuri-

[93] Cfr., in proposito, anche l'art. 42, comma 1°, della legge 675, il quale, nel sostituire l'art. 10 della legge 1° aprile 1981, n. 121, recante il «Nuovo ordinamento della amministrazione della pubblica sicurezza», ai commi 3 e 5 della nuova disposizione, riconosce, in presenza di determinate condizioni, il diritto per l'interessato di chiedere che il dato assuma forma anonima.

[94] Nella traduzione italiana della direttiva, tra i due obblighi cui gli stati membri possono sottoporre, ai sensi dell'art. 15, gli intermediari, si trova la congiunzione con funzione disgiuntiva "o". A ben vedere, tuttavia, poiché non vi è alcun motivo per reputare che il legislatore comunitario pensasse a tali obblighi in termini di alternatività, è evidente che il testo comunitario va interpretato nel senso che gli stati possono imporre "sia" l'obbligo di "informazione" circa presunte attività illecite compiute dai destinatari dei servizi, "sia" quello di "comunicazione" circa l'identità dei destinatari dei servizi stessi. L'art. 17 del d. lgls. 70/2003 ha inteso in questo senso il principio formulato nell'art. 15 ed ha infatti previsto, al comma due, che gli intermediari debbano sia (lett. a) "informare" l'autorità competente , qualora siano a conoscenza di presunte attività o informazioni illecite riguardanti un loro destinatario del servizio, che (lett. b) fornire senza indugio, su richiesta delle autorità compe-

sprudenza nordamericana, nei casi in cui si è trovata a valutare il comportamento del prestatore di servizi di Rete che comunica, all'autorità competente o direttamente ai presunti danneggiati, dati identificativi dei propri clienti, presunti responsabili dell'illecito, ha ritenuto che in tal caso non vi sia alcuna ipotesi di lesione del diritto alla *privacy*[95].

In conclusione, un diritto del navigatore a mantenere l'anonimato in Internet non esiste. L'anonimato va, dunque, garantito quando e nella misura in cui consente di tutelare la *privacy online* dell'utente; senza, però, che diventi esso stesso un potenziale strumento di aggressione per altri interessi tutelati dall'ordinamento o, addirittura, espediente per sfuggire all'applicazione delle regole giuridiche. La soluzione che qui si propone, e che si è definita "della identificabilità", appare in grado di realizzare un equo bilanciamento tra l'interesse degli utenti a mantenere l'anonimato in Rete e l'interesse della collettività a negare che vi sia una deresponsabilizzazione pressoché assoluta per le attività compiute *online*. È vero, infatti, che l'identificabilità dei navigatori rischia di sacrificare il diritto alla *privacy online*, ma ciò soltanto se non si riuscirà a impedire, attraverso attività di controllo e prevenzione, che i diversi intermediari della Rete e, più in generale, gli operatori che possono raccogliere dati altrui *online*, si facciano cedere dai fornitori di accesso alla Rete i dati personali dei clienti.

11. Accordi di memorizzazione dei dati e responsabilità dei prestatori di servizi di rete.

Quando non sussistono i problemi tecnici di cui si è diffusamente parlato in precedenza, e dunque quando il danneggiato riesce – con la collaborazione del prestatore (*service provider*) che gestisce il servizio attraverso cui si è compiuto l'illecito – a individuare a quale IP sia ricollegabile l'attività dannosa, rimane il problema di risalire, mediante

[95] Cfr., tra le altre, *U.S.C.A. Const. Amend. IV U.S. v. Cox*, 190 *F. Supp. 2d* 330 (N.D. N.Y. 2002); *U.S. v. Hambrick*, 225 *F.3d* 656 (4th Cir. 2000), cert. denied, 121 *S. Ct.* 832, 148 *L.Ed. 2d* 714 (U.S. 2001) ; U.S. v. Hambrick, 55 *F. Supp.* 2d 504 (W.D. Va 1999), aff'd, 225 *F.3d* 656 (4th Cir. 2000), cert. denied, 121 *S. Ct.* 832, 148 *L. Ed. 2d* 714, (U.S. 2001); nonché *U.S. v. Kennedy*, 81 *F. Supp. 2d* 1103 (D.

la collaborazione del fornitore di accesso alla rete da cui risulta gestita la data risorsa, dall'IP all'identità reale dell'autore dell'illecito.

Questa difficoltà può dipendere: 1) dalla falsa identità spesa dal cliente nel contratto con il suo *access provider*; 2) dalla mancata conservazione, da parte di quest'ultimo, dei registri elettronici dai quali risultano le combinazioni di IP e *userId* di volta in volta realizzate; ovvero 3) dal fatto che, mediante quel determinato *Id*, possa aver agito una persona diversa dal titolare formale del contratto di accesso.

Riguardo alle prime due ipotesi, il soggetto su cui sembra il caso di concentrare l'attenzione è il fornitore di accesso alla rete. Se l'uomo – e non solo quello occidentale – è destinato, nell'immediato futuro, a trascorrere una parte sempre maggiore della propria vita in Rete, e se in Rete, così come è in Internet, gli standard tecnici e gli accessi sono gestiti da imprenditori che, per motivi di *marketing*, e cioè al fine di ingrossare le fila dei propri clienti, sono disposti a concedere gratuitamente alcuni servizi, oltre che a garantire a questi ultimi, se del caso, condizioni di favore, quale per esempio la possibilità di accedere a Internet sostanzialmente in forma anonima, al giurista vien fatto di chiedersi se sia possibile, ed efficiente, una soluzione volta a deresponsabilizzare completamente tali soggetti.

La scelta di *marketing* compiuta dai fornitori che offrono gratuitamente l'accesso alla rete ai propri clienti, e quindi non hanno interesse economico a controllarne la reale identità, può dar luogo a ipotesi di responsabilità civile a loro carico quando il danneggiato, proprio per l'inesattezza delle informazioni comunicate dal prestatore che gestisce l'IP con il quale è stato compiuto l'illecito, non riesca a individuare l'identità del danneggiante e dunque a ottenere il relativo risarcimento. Tale convincimento si basa sulle seguenti considerazioni.

I prestatori di accesso a Internet 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 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, i fornitori di accesso continuano a trascurare tale controllo.

Il legislatore comunitario, nella direttiva 2000/31/Ce, si è dimostrato pienamente consapevole dell'importanza del controllo dell'identità degli utenti da parte dei prestatori di servizi della società dell'informazione e 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»[96].

La normativa italiana di recepimento della direttiva sul commercio elettronico ha messo a frutto questa possibilità, e ha stabilito testualmente, all'art. 17, secondo comma, lett. b), che ogni prestatore di servizi della società dell'informazione è comunque tenuto a «fornire senza indugio, a richiesta delle autorità competenti, le informazioni in suo possesso che consentano l'identificazione del destinatario dei suoi servizi con cui ha accordi di memorizzazione dei dati, al fine di individuare e prevenire attività illecite»[97].

Tale norma rappresenta uno snodo fondamentale della riflessione che si va conducendo. Non vi è dubbio, infatti, che oggi in Italia, in

[96] Già dal tenore dell'art. 15 della direttiva, S. SICA, *op. ult. cit.*, p. 230, ricava l'impressione che: «Detta ultima disposizione è di peculiare rilievo rispetto alla *vexata quaestio* del diritto all'anonimato in Internet. Si è, infatti, giustamente notato che, *a contrario*, si ricava un generale obbligo di identificazione a carico dell'intermediario, che, se non assolto, deve allocare nella sua sfera la responsabilità per gli illeciti attuati da soggetti non identificabili». Così, se consentito, anche F. DI CIOMMO, *Internet (responsabilità civile)*, cit.; ID., *La responsabilità civile nell'era di Internet*, cit., partic. pp. 195-196, nota n. 39; e ancora ID., *Internet e crisi del diritto privato...*, cit., p. 133; nonché G. RICCIO, "Diritto all'anonimato e responsabilità civile del *provider*", cit., pp. 36-38

[97] In proposito, vale la pena di ricordare che in seguito all'entrata in vigore della direttiva 2000/31/Ce, già il legislatore francese, con la *loi* 719-2000, ha espressamente posto in capo all'*access* e all'*host provider* l'obbligo di 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 septembre 1986 relative a la liberté de communication: dernier épisode ed

forza del principio appena enunciato, ogni prestatore, che abbia accordi di memorizzazione dei dati con i suoi clienti, sia tenuto a comunicare, su richiesta dell'autorità giudiziaria competente (ma, si badi bene, non anche su richiesta di privati), i dati identificativi di cui l'intermediario sia in possesso.

12. Principio solidaristico, correttezza e responsabilità degli *access provider* per mancata identificazione degli utenti

Le disposizioni di cui all'art. 15 della direttiva 2000/31/Ce e all'art. 17 della normativa italiana di recepimento lasciano aperti due problemi non secondari. Il primo riguarda la possibilità che lo stesso dovere di conservazione e comunicazione dei dati identificativi dei clienti gravi, oltre che sugli intermediari che hanno con gli utenti accordi di memorizzazione dei dati, anche su prestatori che non abbiano tali accordi. Il secondo concerne l'esistenza (o meno) di un dovere generale in capo al prestatore – accessorio a quelli di conservazione e comunicazione dei dati identificativi dei clienti – avente come contenuto il controllo dell'esattezza di tali dati.

Per risolvere la prima delle due questioni, occorre innanzitutto chiarire quali sono i casi in cui i prestatori di servizi della società dell'informazione non concludono con i propri clienti accordi di memorizzazione. Ciò accade quando l'intermediario si limita a fornire l'accesso ad Internet (*access provider*) o a un determinato servizio (*service provider*) senza impegnarsi a memorizzare alcunché per conto del cliente. A ben vedere, tuttavia, anche in queste circostanze, l'esigenza di assicurare la cooperazione di tali soggetti, per conoscere le generalità dell'utente che commette un illecito *online* utilizzando un certo IP, non viene meno. Infatti, il danneggiato, per individuare l'identità dell'autore dell'illecito, avrà sempre bisogno della collaborazione attiva del prestatore del servizio di accesso per associare a quell'IP i dati identificativi del cliente che utilizzava tale risorsa di accesso alla rete al momento del compimento del fatto dannoso.

Tanto l'art. 15 della direttiva, quanto l'art. 17, comma 2, lett. b) del decreto italiano di recepimento fanno gravare un dovere di fornire

senza indugio, a richiesta dell'autorità competente, le informazioni in [loro] possesso che consentano l'identificazione del destinatario dei suoi servizi» sui tutti i prestatori di servizi della società dell'informazione, ma solo rispetto ai clienti con cui essi hanno accordi di memorizzazione. La scelta di politica del diritto effettuata dal legislatore comunitario sembra volta a non penalizzare – rispetto ai concorrenti extraeuropei – gli intermediari ubicati nel vecchio continente che si limitano a fornire soltanto servizi di connessione alla rete, ovvero a determinate risorse informatiche, senza mettere direttamente a disposizione dell'utente proprie risorse su cui memorizzare i materiali dei clienti. Le ragioni a fondamento di questa soluzione sono comprensibili. Chi fornisce esclusivamente l'accesso alla risorsa, senza consentire al cliente di pubblicare in rete i propri materiali, si sottrae a qualunque tipo di discorso volto a valorizzare la sua eventuale cooperazione (anche attraverso la semplice omissione) nell'attività illecita dell'utente. Mentre, al contrario, gli intermediari che vogliono fornire il servizio di memorizzazione dei materiali (di qualunque tipo) scaricati in rete dagli utenti, proprio perché tecnicamente coinvolti nell'attività di immissione in rete di tali materiali, devono assumersi l'onere di conservare i dati identificativi dei clienti al fine di comunicarli, all'occorrenza, alle autorità competenti.

Le (pur, in astratto, condivisibili) ragioni giustificatrici della soluzione normativa in esame non sono sufficienti a garantirne la concreta efficienza. Infatti, se pensiamo ad Internet, appare evidente come per l'utente che voglia compiere illeciti *online* sia sin troppo facile (e anche conveniente economicamente[98]) concludere contratti di accesso alla rete, o a una determinata risorsa telematica, con un operatore (che, a una prima lettura della direttiva, sembrerebbe essere) non tenuto a conservare i suoi dati identificativi, per poi collegarsi a siti gestiti da operatori extraeuropei al fine, ad esempio, di gestire il proprio *box e-*

[98] Le spese di collegamento a Internet, per l'utente, si calcolano in ragione del tempo di connessione (anche se molti contratti di accesso, oggi, consentono di pagare un canone periodico prescindendo dai tempi di connessione) e, soprattutto, della lontananza geografica dall'*access provider*. Sicché, scegliere un *access provider* ex-

mail (tramite cui intende compiere illeciti) o, più in generale, per immettere in rete i propri materiali lesivi di diritti altrui.

La circostanza appena segnalata mette in evidenza il rischio connaturato alla scelta compiuta a livello comunitario e induce a pensare che, in definitiva, essa sia destinata a risultare inefficiente nell'ottica della individuazione della identità degli autori di fatti illeciti compiuti *online* e, dunque, della responsabilizzazione degli utenti delle reti telematiche. Meglio, allora, sarebbe stato optare per la via intrapresa dal legislatore francese a due mesi dall'entrata in vigore della direttiva, con la *loi* 2000/719, che, come anticipato, impone a tutti i fornitori di accesso (*access provider*) e di ospitalità (*host provider*) l'individuazione dei propri utenti e la conservazione dei relativi dati identificativi. È proprio su tali intermediari, la cui localizzazione geografica non è irrilevante per gli utenti, che sembra opportuno far gravare l'onere di conservare i dati identificativi dei clienti, piuttosto che, in generale, su tutti i prestatori di servizi ma solo in presenza di contratti di memorizzazione.

Appare dunque utile provare a verificare se, in assenza di un espresso divieto, da parte della direttiva, di ampliare il dovere di conservazione e comunicazione dei dati, sia possibile giungere ad affermare, a livello ermeneutico, che esso grava anche sui prestatori di accesso e memorizzazione che non hanno accordi di memorizzazione con i propri clienti. L'obiettivo ora segnalato non sembra difficile da perseguire se solo si considera che molti intermediari operanti in rete, e in particolare tutti i soggetti che forniscono agli utenti l'accesso alla rete Internet, svolgono attività caratterizzate da imprenditorialità o, quantomeno, professionalità. Quanto dire che, nei loro confronti, risulta pienamente operativa la clausola generale che impone la prestazione diligente di ogni attività che possa avere conseguenze nei confronti dei terzi, nella particolare accezione della diligenza, o correttezza, professionale. Interpretando tale clausola alla luce del principio costituzionale di solidarietà, e ribadendo la gravità dei danni che i consociati possono subire quando non si riesca a individuare l'identità dell'autore di un illecito commesso *online*, si può affermare che qualunque prestatore che fornisce il servizio di accesso alla rete, ovvero quello di ospitalità sul proprio *server* di siti altrui, sebbene non abbia accordi di memorizzazione con i clienti, non può evitare di chiedere le generalità di

questi ultimi, conservare i relativi dati e, all'occorrenza, metterli a disposizione delle autorità competenti.

Anche senza far riferimento alla categoria degli obblighi di protezione nei confronti dei terzi[99], e soprattutto senza attribuire al principio di solidarietà il ruolo di fonte di un generico dovere di attivarsi nell'interesse altrui[100], pare di tutta evidenza che le accortezze appena

[99] Sulla questione, tra gli altri, v. C. CASTRONOVO, s.v. "Obblighi di protezione", in *Enciclopedia giuridica*, Treccani, Roma, 1990, XXI; e G. MASTRANDEA, *L'obbligo di protezione nel trasporto aereo di persone*, Cedam, Padova, 1994; nonché G. DE FAZIO, "Art. 2087 c.c.: obblighi di protezione e responsabilità di impresa (nota a Cass. 20 aprile 1998, n. 4012)", in *Responsabilità civile*, 1999, p. 449; D. COLASANTI, "Note in tema di obblighi di protezione (nota a Pret. Perugia, 26 ottobre 1996)", in *Rassegna giuridica umbra*, 1997, p. 121; e D. SANTINI, "Brevissime note in materia di responsabilità per fatto degli ausiliari e c.d. obblighi di protezione – Condizioni di applicabilità dell'art. 1228 c.c. (nota ad App. Genova, 31 dicembre 1994)", in *Diritto marittimo*, 98 (1996), pp. 400-402.

[100] L'esistenza di una responsabilità a carico di chi, potendo intervenire ad evitare un danno a terzi mediante un'azione positiva, non rischiosa né impegnativa, ometta di prestare l'attività in fatto occorrente, è argomento discusso nella dottrina giuridica italiana. Per l'affermazione di tale responsabilità, cfr. P. GALLO, *Introduzione al diritto comparato. II. Istituti giuridici*, Giappichelli, Torino, 1998, p. 297; P. TRIMARCHI, s.v. "Illecito (dir. priv.)", in *Enciclopedia del diritto*, Treccani, Milano, 1970, XX, pp. 90 ss., in particolare p. 100; P. D'AMICO, *Il soccorso privato*, Edizioni Scientifiche Italiane, Napoli, 1981; e G. ALPA, *Il problema della atipicità dell'illecito*, Jovene, Napoli, 1979, in partic. pp. 142 e ss. e 176. Rispetto al problema in esame, L. BIGLIAZZI GERI, U. BRECCI, F.D. BUSNELLI e U. NATOLI, *Diritto civile. 3. Obbligazioni e contratti*, Giappichelli, Torino, 1989, p. 705, sostengono la possibilità di individuare un giusto contemperamento tra libertà individuale e solidarietà sociale distinguendo «tra comportamenti omissivi che rientrano nell'esercizio della libertà di astensione e comportamenti omissivi che, in quanto contrassegnati da malafede o almeno da colpa grave, ne superano i limiti colorando conseguentemente di ingiustizia i danni provocati». Analoga appare la posizione di A.L. CHECCHINI, *Rapporti non vincolanti e regola di correttezza*, Cedam, Padova, 1977, partic. pp. 337-342, il quale individua, come sotteso all'art. 2043, «un principio inderogabile dettato in primo luogo dall'interesse della collettività, in base al quale il fatto di arrecare danno consapevolmente, ed a maggior ragione intenzionalmente, costituisce di per sé un illecito». Recentemente il tema è stato indagato criticamente da F. GIGLIOTTI, "Solidarietà e responsabilità tra libertà di astensione e (pretesi) comportamenti abusivi. Riflessioni a margine dell'omissione dolosa", in *Diritto & Formazione*, 3 (2003), pp. 351-360, il quale conclude la sua riflessione affermando che: «un dovere generale di intervenire per evitare che altri subisca un danno non è desumibi-

segnalate rientrano nell'ambito di un diligente svolgimento della attività professionale dei prestatori di servizi della società dell'informazione, e dunque devono essere tenute in debita considerazione nell'ambito del giudizio relativo all'eventuale applicazione dell'art. 2043 a carico dei medesimi[101].

Questi ultimi, qualora, nell'esercizio della propria attività, pongano in essere comportamenti poco diligenti, così cagionando danni a terzi, risponderanno delle relative conseguenze dannose a titolo di responsabilità diretta e non vicaria. Essi, in altre parole, non risponderanno del danno cagionato dal fatto dell'utente rimasto anonimo, ma della loro condotta colposamente omissiva, che determina un evento diverso da quello prodotto dal fatto dell'utente. Quest'ultimo, infatti, avrà leso un certo diritto soggettivo del danneggiato o, comunque, un suo interesse giuridicamente tutelato, mentre l'omissione del prestatore è dannosa soltanto nella misura in cui impedisce di individuare l'autore dell'illecito; sicché essa cagiona un evento che – sebbene dal punto di vista della quantificazione del danno appaia del tutto simile a quello

ogni volta e *per il solo fatto* che, per le circostanze del caso concreto, il soggetto che si imbatte nella situazione (per altri) potenzialmente dannosa risulti l'unico in grado di attivarsi per evitare l'evento dannoso». Lo stesso A. applica di tale conclusione in un altro suo recente saggio intitolato "Illeciti da informazione e responsabilità omissiva", in *Rivista di diritto civile*, 6 (2002), I, pp. 911-938.

[101] Il ricorso all'art. 1176 c.c., e dunque al criterio di diligenza, per valutare la responsabilità colposa anche in ambito aquiliano è ormai diffuso in giurisprudenza. Cfr. A. PALAZZO, "Responsabilità, doveri di protezione e di tutela della persona", in *Vita notarile*, 1999, pag. 14; M. LOBUONO, *La responsabilità degli intermediari finanziari*, Edizioni Scientifiche Italiane, Napoli, 1999; L. NIVARRA, "La responsabilità civile dei professionisti (medici, avvocati, notai): il punto sulla giurisprudenza", in *Europa e diritto privato*, 2000, pp. 513 ss. Chiarificatore, in proposito, risulta il pensiero di A. RAVAZZONI, s.v. "Diligenza", in *Enciclopedia giuridica*, Treccani, Roma, 1988, VII, pp. 1, secondo il quale: «La c.d. responsabilità extracontrattuale e, nell'ambito di questa, la formulazione del concetto di colpa (il riferimento alla "negligenza, imprudenza, imperizia") non può prescindere da un richiamo, sia pure in senso negativo, alla nozione di diligenza». Per ulteriori approfondimenti in questa direzione, tra gli altri, v. M. BUSSANI, *La colpa soggettiva. Modelli di valutazione della condotta nella responsabilità extracontrattuale*, Cedam, Padova, 1991; e L. CORSARO, "Colpa e responsabilità civile: l'evoluzione del sistema italiano", in *Rassegna di diritto civile*, 2000, p. 270.

prodotto dall'illecito dell'utente, perché da questo, sotto tale profilo, dipende *in toto* – in realtà è affatto diverso ed autonomo[102].

13. La responsabilità dei prestatori di servizi di rete per mancato accertamento della reale identità dei clienti, tra correttezza e codici di condotta

Chiarito che un dovere di conservazione e comunicazione dei dati identificativi dei clienti grava, oltre che sugli intermediari che hanno con gli utenti accordi di memorizzazione dei dati, anche su prestatori che non abbiano tali accordi, occorre ora prendere in considerazione il secondo dubbio innanzi prospettato, per sciogliere il quale giova partire dalla lettura del già citato considerando n. 48 della direttiva, a tenore del quale quest'ultima «non pregiudica la possibilità per gli Stati membri di chiedere ai prestatori di servizi che detengono informazioni fornite dai destinatari del loro servizio, di adempiere al dovere di diligenza che è ragionevole attendersi da loro ed è previsto dal diritto nazionale, al fine di individuare e prevenire alcuni tipi di attività illecite»; e del considerando n. 40, il quale prevede che: «Le disposizioni della presente direttiva sulla responsabilità non dovrebbero impedire ai vari interessati di sviluppare e usare effettivamente sistemi tecnici di protezione e di identificazione, nonché strumenti tecnici di sorveglianza resi possibili dalla tecnologia digitale, entro i limiti fissati dalle direttive 95/46/Ce e 97/66/Ce».

Alla luce dei principi espressi dalla direttiva europea e dell'art. 17 del decreto di attuazione, nel nostro ordinamento, il punto è se, in assenza di un'apposita previsione legislativa, la clausola generale di correttezza o diligenza – ricavabile, in ambito extracontrattuale, dall'art. 2043 – possa essere sufficiente a fondare un giudizio di responsabilità, a carico di un prestatore di servizi della società dell'informazione, per l'omesso accertamento della correttezza dei dati identificativi dei propri clienti che abbia

[102] Ci sono buone ragioni per dubitare, dunque, che si possa parlare, in tal caso, di responsabilità concorrente del *provider* circa il danno provocato dall'illecito dell'utente rimasto anonimo. Per un recente studio sul concorso di colpa nell'ambito aquiliano, cfr. F. PARISI e G. FREZZA, "Rischio e causalità nel concorso di colpa", in

causato ad un terzo il danno derivante dall'impossibilità di rintracciare l'autore del fatto illecito e, dunque, di ottenere il relativo risarcimento.

Ammessa l'applicazione dell'art. 2043 nel senso ora chiarito, il prestatore non verrebbe condannato per concorso nell'illecito del danneggiante, bensì – come è nel caso di mancata conservazione o comunicazione alle autorità competenti dei dati riguardanti l'identità dei propri clienti – per un fatto autonomo e per un evento diverso dal fatto illecito dell'utente.

Non si tratta, dunque, di imporre al prestatore una responsabilità oggettiva o semioggettiva per illeciti realizzati dai suoi clienti. Tale tipologia di responsabilità, infatti, come spiegato nei precedenti paragrafi, nel caso di specie, non avendo l'attività svolta dagli operatori di rete caratteristiche proprie del prodotto, bensì del servizio, con tutta probabilità non sortirebbe effetti positivi in termini di deterrenza e, dunque, prevenzione dei danni e sarebbe, anzi, «in grado di provocare patologie di *overdeterrence*»[103]. E, del resto, la direttiva europea, negli articoli 12-15, vuole proprio evitare l'applicazione ai prestatori di regimi di responsabilità oggettiva; ma non anche sottrarre totalmente gli stessi alle regole di responsabilità civile.

Tornando alla domanda concernente la possibilità di fondare un giudizio di responsabilità dei prestatori, per mancato controllo dell'identità dei propri clienti, sulla clausola di correttezza (o diligenza) ricavabile dall'art. 2043, bisogna considerare, in aggiunta a quanto già evidenziato, che proprio il codice di autoregolamentazione e di deontologia dell'ANFoV (un'associazione che riunisce i maggiori *provider* italiani di Internet), adottato il 1° gennaio 1998, prevede, al 1° comma dell'art. 6, dedicato alla «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 più persona giuridiche, di documentazione idonea a comprovare il potere di rappresentanza»; ed all'art. 11, dedicato all'"Anonimato", che: «L'accesso di un utente o

[103] Così G. PONZANELLI, "Verso un diritto uniforme per la responsabilità degli internet service providers?", in *Danno e responsabilità*., 1 (2002), p. 5. Nello stesso senso, W.M. MELONE, Contributory Liability for Access Providers: Solving theConundrum Digitalization Has Placed on Copyright Laws, *Federal Communication Law Journal*, 49 (1997), pp. 491-507 e partic. 501.

di un abbonato al sistema o al servizio è consentito previa identificazione iniziale dello stesso ed archiviazione e custodia dei 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 non ha un valore giuridico vincolante, ma può certamente essere utilizzato dall'interprete per riempire di contenuti la clausola generale di correttezza (o diligenza, professionale) nel momento in cui si debba vagliare la liceità del comportamento assunto dal prestatore di servizi di rete nel singolo in caso concreto.

Inoltre, al fine di comprovare ulteriormente la bontà della tesi ermeneutica qui sostenuta, vale la pena di riflettere su una precisa circostanza testuale del più volte citato art. 17, secondo comma, lett. b), il quale – riproducendo letteralmente l'analogo passo dell'art. 15 della direttiva – obbliga ogni intermediario a fornire alle autorità competenti, non semplicemente i dati identificativi dei clienti, bensì «le informazioni in suo possesso "che consentano" l'identificazione del destinatario».

Il dato testuale in questo caso non è trascurabile e appare anzi risolutivo della questione ermeneutica in esame. Infatti, se il prestatore non si attiverà in modo tale da controllare la affidabilità dei dati identificativi spesi dai propri clienti, rispettando la clausola di correttezza, e cioè dandosi da fare nei limiti delle sue possibilità, egli non sarà certo in grado di fornire, all'autorità giudiziaria che ne faccia richiesta, informazioni "che consentano l'identificazione" del destinatario del servizio.

In ragione delle considerazioni sin qui esposte, sembra lecito ritenere che il fornitore di accesso alla rete, ai sensi dell'art 2043, sia tenuto – così come i prestatori di servizi che forniscono ospitalità stabile ai materiali degli utenti pubblicati in rete – non solo a conservare i dati tecnici in suo possesso, quantomeno per il periodo sufficiente a fornire all'autorità giudiziaria le informazioni necessarie a individuare il danneggiante, ma anche ad accertare l'identità dei clienti con cui si concludono contratti di accesso o di memorizzazione, e ciò al fine di controllare la veridicità dei dati identificativi raccolti[104]. Tale obbligo, considerato che Internet è uno strumento dalle potenzialità dannose enormi e che

[104] *Contra* Trib. Grand Instance di Parigi, 22 maggio 2000, in *La Gazette du Palais*, 25 giugno 2000, jur., 41; e Court d'Appel di Versailles, 8 giugno 2000, in *Juris-*

i prestatori che forniscono attività di accesso o *hosting* sono, per lo più, società che svolgono tale attività a fini di lucro, scaturisce direttamente dall'applicazione della regola di diligenza che presidia i rapporti tra privati nel nostro ordinamento giuridico[105].

Quest'ultima osservazione consente di concludere che l'art. 2043 deve senz'altro trovare applicazione agli intermediari della rete, che, pur essendo tenuti a conservare i dati identificativi dei propri clienti, non controllano la veridicità di tali dati. Pensandola diversamente, infatti, si finirebbe, tra l'altro, per utilizzare in modo quanto meno inefficiente le regole di responsabilità civile che, per definizione, sono chiamate a svolgere un ruolo importante (anche) per favorire lo sviluppo di Internet e, più in generale, dell'economia telematica[106].

[105] Del resto, come evidenziato dalla letteratura specialistica, «essere *gatekeepers* [e non c'è dubbio che dal punto di vista tecnico e commerciale i *provider* lo siano] significa controllare la porzione strategica di un canale – nel quale fluiscono indifferentemente beni, notizie, persone – in modo da poter decidere se qualcosa che sta scorrendo vi possa essere ammessa o meno» (E. KATZ e P.F. LAZARSFELD, *Personal Influence: The Part Played by People in the Flow of Mass Communication*, Transaction Publishers, Glencoe, 1995, p. 211). Sicché, non sembra eccessivo chiedere ai *provider*, non di controllare i contenuti veicolati in rete e selezionarli, bensì esclusivamente di controllare i dati identificativi dei propri clienti e di tenere memoria, per un congruo lasso di tempo, di ogni informazione in proprio possesso.

[106] G. CALABRESI, *Costo degli incidenti e responsabilità civile*, Milano, Giuffrè, 1975, p. 57, in relazione alle funzioni delle regole di responsabilità civile, osserva che: «la responsabilità civile, come ogni altra branca del diritto, può essere usata per assolvere una enorme varietà di funzioni. In passato si sono così affermati certi sistemi di responsabilità civile perché in realtà servivano a sostenere industrie in via di sviluppo, in un periodo in cui ciò era probabilmente necessario. In altri momenti la responsabilità civile è stata usata come strumento di perequazione delle ricchezze, o come mezzo per affrontare i problemi della depressione e della disoccupazione. [...] Riguardo a queste funzioni e ad altre simili, ho la sensazione che potremmo raggiungere risultati migliori se attaccassimo il problema specifico direttamente, anziché attraverso la responsabilità civile. Se si ritiene che il sovvenzionamento alle industrie in via di sviluppo sia necessario, è meglio dirlo apertamente, indicando chiaramente chi deve subirne gli oneri, piuttosto che servirsi di un sistema che rimuove il costo dei sinistri, in tutto o in parte, dalle attività che li causano, e cela il sovvenzionamento, facendone ricadere i relativi costi su gruppi indefiniti o privi di peso politico adeguato».