SERGIO SEMINARA

LA RESPONSABILITÀ PENALE DEGLI OPERATORI SU INTERNET

SOMMARIO: 1. La legge contro la pornografia minorile come il più recente esempio dell'incompetenza del legislatore. — 2. Il vigente sistema penale e Internet. — 3. Estensione analogica ad Internet della disciplina degli altri *mass media*? — 4. I codici di autoregolamentazione. — 5. La prevenzione dei reati su Internet. — 6. Un modello di disciplina: la legge tedesca 22 luglio 1997. — 7. Gli effetti della ricezione nell'ordinamento italiano della disciplina tedesca. — 8. Tutela dei dati personali e strategie di controllo per la prevenzione dei reati su Internet. — 9. Armonizzazione internazionale del diritto penale e transnazionalità di Internet.

1. LA LEGGE CONTRO LA PORNOGRAFIA MINORILE COME IL PIÙ RECENTE ESEMPIO DELL'INCOMPETENZA DEL LEGISLATORE.

La legge 3 agosto 1998, n. 269, contenente « Norme contro lo sfruttamento della prostituzione, della pornografia, del turismo sessuale in danno di minori, quale nuova forma di riduzione in schiavitù », prevede l'introduzione di numerose nuove fattispecie criminose, destinate a trovare inserimento nel codice penale dopo l'art. 600, sulla « Riduzione in schiavitù ».

Tra l'altro, il nuovo art. 600-*ter* cod. pen., ai commi 3 e 4, stabilisce la reclusione a 1 a 5 anni e la multa da 5 a 100 milioni di lire per chiunque, « con qualsiasi mezzo, anche per via telematica, distribuisce, divulga o pubblicizza il materiale pornografico di cui al primo comma (cioè derivante dallo sfruttamento di minori infradiciottenni, *n.d.s.*), ovvero distribuisce o divulga notizie o informazioni finalizzate all'adescamento o allo sfruttamento sessuale di minori degli anni diciotto » e la reclusione fino a 3 anni o la multa da 3 a 10 milioni di lire nei confronti di chi « consapevolmente cede ad altri, anche a titolo gratuito, materiale pornografico prodotto mediante lo sfruttamento sessuale dei minori degli anni diciotto »; mentre il nuovo art. 604 cod. pen. afferma che « le disposizioni di questa sezione, nonché quelle previste dagli articoli 609-*bis*, 609-*ter*, 609-*quater* e 609-*quinquies*, si applicano altresì quando il fatto è commesso all'estero da cittadino italiano, ovvero in danno di cittadino italiano, ovvero da cittadino straniero in concorso con cittadino italiano. In quest'ultima ipotesi il cittadino

straniero è punibile quando si tratta di delitto per il quale è prevista la pena della reclusione non inferiore nel massimo a cinque anni e quando vi è stata richiesta del Ministro di grazia e giustizia ».

Non è necessario, in questa sede, soffermarci sulla drammatica realtà dello sfruttamento sessuale di minori dalla quale trae origine la disciplina in questione, né appare opportuno indugiare sulla problematicità della fattispecie volta ad incriminare il mero possesso di materiale pornografico da parte di chi non sia concorso nella sua realizzazione. Ai nostri fini, risulta invece di estremo interesse la previsione delle condotte di distribuzione, divulgazione e pubblicizzazione « anche per via telematica », la quale sta a dimostrare univocamente il riconoscimento legislativo di Internet come un possibile strumento di realizzazione del reato.

Questo intento di criminalizzare la diffusione in rete di materiale pornografico è verosimilmente ravvisabile nei numerosi disegni di legge presentati alla Camera dei deputati e poi confluiti nel testo approvato dal Senato: nel progetto n. 263 presentato dall'on. Rizza, il cui art. 1 punisce con la reclusione da 6 a 12 anni e la multa da 30 a 300 milioni di lire « chiunque produce, diffonde, mette in commercio ovvero detiene materiale pornografico concernente minori degli anni diciotto »; nel progetto n. 2265 presentato dall'on. Aprea, ove il comma 3 dell'art. 1 prevede la reclusione da 12 a 24 anni e la multa da 100 a 600 milioni di lire per la produzione, la diffusione o il commercio di materiale pornografico finalizzati a indurre, avviare, favorire o sfruttare la prostituzione di infradiciottenni (?); nel progetto n. 2930 presentato dall'on. Marras, che all'art. 1 sanziona con la reclusione da 6 a 12 anni e la multa da 50 a 300 milioni di lire « chiunque produca, diffonda, metta in commercio ovvero detenga fotografie, film, video e materiali pornografici che abbiano come protagonisti minori di anni diciotto ». Per certo, l'obiettivo di reprimere le condotte realizzate via Internet emerge invece con chiarezza nel progetto n. 2931 presentato dall'on. Signorini, il cui art. 1 stabilisce la reclusione da 6 mesi a 6 anni per « chiunque detenga, commerci, divulghi o scambi immagini o testi a sfondo sessuale che abbiano ad oggetto minori di anni quattordici ». La relazione di presentazione a tale progetto, dopo avere sottolineato l'esigenza di « andare a colpire tutti i comportamenti del pedofilo che sono caratteristici della sua abbietta perversione, come la ricerca di materiale fotografico o filmato, il porsi in contatto con altri deviati o con organizzazioni criminali che favoriscono lo sfruttamento sessuale dei minori e l'adescamento », rileva infatti, senza infingimenti o circonlocuzioni, « la totale assenza di una normativa che reprima l'attività dei pedofili sulla rete Internet, che qui ha trovato un mezzo tecnologico su cui scambiare informazioni ed immagini attraverso siti non riconducibili a soggetti direttamente identificabili ».

Questa esplicitazione della volontà legislativa di estendere le incriminazioni alle condotte di distribuzione e divulgazione di immagini, testi o filmati a contenuto pornografico realizzate su Internet si espone a due ordini di censure. Per un verso, essa appare ridondante, non sussistendo alcun dubbio che una diffusione può svolgersi in rete come pure attraverso la posta o i tradizionali *mass media*; onde la precisazione in esame si presta ad essere percepita come il frutto di una visione 'demonizzatrice' di Internet, qui presentato come uno strumento di comunicazione altamente criminogeno, specie nei suoi effetti di perversione dei costumi sessuali. Per altro verso, essa rivela una profonda incomprensione del fenomeno che si vorrebbe regolare, poiché — anche senza soffermarci sulle pene accessorie della chiusura degli esercizi « la cui attività risulti finalizzata » ai delitti in questione e della confisca (vd. art. 600-*septies* cod. pen.), che non si comprende in quale senso e in quale misura possano trovare applicazione nella complessa realtà che prende il nome di Internet —, la tipizzazione di condotte come 'distribuire', 'divulgare', 'pubblicizzare', 'cedere', 'procurarsi' o 'disporre' risulta in grado di aprire enormi incertezze rispetto alle varietà dei ruoli e delle categorie dei soggetti operanti sulla rete.

Non è chiaro, infatti, se come responsabili della distribuzione, divulgazione, pubblicizzazione o cessione a terzi debbano intendersi esclusivamente gli autori materiali della immissione in rete dei dati illeciti (c.d. *content providers* o produttori di contenuti sotto forma di testi, immagini o suoni) ovvero anche i proprietari di infrastrutture di telecomunicazione (c.d. *network providers*), i fornitori di accessi (c.d. *access providers*, i quali offrono l'accesso in rete e la facoltà di utilizzare funzioni come il Web e l'*e-mail*) ed i fornitori di servizi (c.d. *service providers*, i quali si rivolgono all'utente finale consentendogli il collegamento ad Internet e a suoi ulteriori servizi come ad esempio i *news-servers*)[1].

Come vedremo, ad una così ampia e indiscriminata punibilità si oppongono insuperabili argomenti. Appare però estremamente deprecabile che un testo di legge, specificamente concepito per sanzionare anche le condotte realizzate per via telematica, manifesti un atteggiamento di totale indifferenza rispetto al tema — oggi ve-

[1] Per un'articolata analisi delle tipologie di servizi offerte dai *providers*, D. SARTI, *I soggetti di Internet*, in *AIDA* 1996, 27 ss. Rispetto alle osservazioni appena svolte nel testo, si omette qui di prendere in considerazione l'art. 600-*quater* cod. pen. e il connesso problema concernente l'assimilazione alle condotte di 'procurarsi' e 'disporre' del fatto di coloro che si limitano a scaricare sul proprio computer il materiale pornografico: nel silenzio della norma, risulta ardua l'equiparazione della detenzione al mero consumo personale; oltretutto, rispetto a questa interpretazione più ampia, insorgono gravi dubbi sotto il profilo della effettività della sanzione minacciata (cfr. C.E. PALIERO, *Il principio di effettività nel diritto penale*, in *Riv. it. dir. proc. pen.* 1990, 471 ss.).

ramente cruciale — della individuazione (e differenziazione) delle responsabilità di coloro che agiscono in rete.

Allo scopo di colmare questa lacuna, a dire il vero, il 4 aprile 1997 era già stata presentata alla Camera dei deputati, ad iniziativa dell'on. Stagno d'Alcontres, la proposta di legge n. 3530 (« Disciplina delle reti telematiche ad accesso variabile in connessione sovranazionale »), costituita da tre articoli ambiziosamente destinati a scolpire diritti e doveri dei soggetti attivi su Internet. Per quanto rileva in questa sede, il comma 2 dell'art. 2 perentoriamente stabiliva che, « qualora per commettere i reati di cui all'articolo 266 del codice di procedura penale sono utilizzate le reti telematiche di cui all'art. 1 (cioè « site sul territorio dello Stato, in connessione ad accesso variabile a livello sovranazionale con altre reti telematiche », *n.d.s.*), le pene previste per tali reati sono raddoppiate »: prescrizione, questa, che non solo nel suo richiamo ad un'elencazione di delitti operata al ben diverso fine di disciplinare l'intercettazione di telecomunicazioni non si avvedeva della necessità di distinguere tra illeciti commessi via Internet e illeciti la cui esecuzione sia preparata o concordata attraverso Internet, ma inoltre appariva incomprensibile quanto al presunto maggior disvalore derivante dall'utilizzo della rete. Ulteriormente, il comma successivo stabiliva che « il titolare ed il responsabile delle reti telematiche di cui all'articolo 1 non sono responsabili per quanto da altri comunicato attraverso le reti da essi gestite o ivi immesso, salvo l'obbligo di denunziare ad autorità dotata di potere di polizia giudiziaria ogni e qualsiasi violazione di cui essi siano venuti a conoscenza perpetrata in danno o per mezzo delle reti da essi gestite »: senza indugiare qui sulla singolarità di un dovere di denuncia posto a carico di imprenditori privati (v. sul punto *postea*, § 4), neppure accompagnato da un termine per l'adempimento, l'assenza di una sanzione stava a significare che un siffatto obbligo sia già sancito e punito dall'ordinamento (ciò che certamente non è) ovvero che la sua inosservanza avrebbe determinato una responsabilità concorsuale (successiva alla commissione del fatto!) per l'omittente.

Come si vede, simili tentativi di legiferazione valgono a rendere apprezzabile l'inerzia del Parlamento. Nondimeno, occorre riconoscere che l'incertezza giuridica che oggi grava sui soggetti che agiscono in Internet rende necessaria l'introduzione di una regolamentazione.

2. Il vigente sistema penale e Internet.

Tale situazione di incertezza rappresenta peraltro una caratteristica dell'attuale sistema sanzionatorio penale.

Così, per restare al tema della pornografia, l'art. 528 cod. pen. punisce con la reclusione da 3 mesi a 3 anni e la multa non infe-

riore a lire 200.000 « chiunque, allo scopo di farne commercio o distribuzione ovvero di esporli pubblicamente, fabbrica, introduce nel territorio dello Stato, acquista, detiene, esporta, ovvero mette in circolazione scritti, disegni, immagini od altri oggetti osceni di qualsiasi specie » o, ancora, li distribuisce o espone pubblicamente. Dinanzi ad una così ampia formulazione, come si vede, non è possibile stabilire, sul piano della tipicità, se la responsabilità si estende fino a raggiungere i *providers* o se, invece, essa si limita agli autori materiali dell'immissione in rete dei dati illeciti[2].

Un'analoga formulazione onnicomprensiva — incentrata sul fatto di riprodurre, diffondere, distribuire, detenere a scopo commerciale ecc. — si rinviene negli artt. 171 ss. l. 22 aprile 1941, n. 633, in materia di violazione dei diritti di autore, che rappresenta peraltro uno dei terreni più fertili per la commissione di reati attraverso Internet[3]. E parimenti ampie — e quindi in grado di prestarsi ad un'incriminazione a tappeto — risultano le fattispecie normative concernenti altri illeciti realizzabili in rete, come la diffamazione (art. 595 cod. pen.), la rivelazione di segreti (artt. 261, 326, 617-*quater*, comma 2, 618, 621 ss. cod. pen.), la diffusione di codici di accesso a sistemi informatici o di programmi diretti a danneggiarli (artt. 615-*quater* e *quinquies* cod. pen.), l'istigazione e la propaganda contrarie all'ordine pubblico (artt. 266, 272, 302 s., 414 s. cod. pen.) ecc.

A complicare ulteriormente la situazione intervengono poi le norme sulla partecipazione criminosa: a quali condizioni può ritenersi che il *provider* sia concorso nell'altrui illecito? È necessaria

[2] Merita peraltro di essere sottolineata, rispetto all'art. 528 cod. pen., la sua inapplicabilità ai soggetti operanti all'estero che, servendosi di *servers* parimenti siti all'estero, immettono in rete materiali pornografici, non configurandosi in questa ipotesi una condotta di introduzione nel territorio dello Stato (la quale suppone oggetti dotati di consistenza tangibile) né potendosi considerare commesso in Italia il fatto della messa in circolazione: cfr. S. SEMINARA, *La pirateria su Internet e il diritto penale*, in *Riv. trim. dir. pen. econ.* 1997, 106 ss. Sotto tale profilo, emerge però l'inadeguatezza anche della previsione del nuovo art. 604 cod. pen., che — limitatamente alle incriminazioni di maggiore gravità — avrebbe potuto essere sostituita (come avvenuto ad esempio in Germania, attraverso la modifica del § 6 StGB) dall'inserimento delle relative fattispecie nell'elenco contenuto dall'art. 7 cod. pen., che stabilisce l'applicabilità della legge italiana per specifici reati commessi all'estero.

[3] Anche limitando l'attenzione alle più diffuse forme di pirateria, sulla base di recenti indagini i danni arrecati ai produttori di *software* ammontano a circa seicento miliardi di lire per il solo mercato italiano, mentre quelli cagionati ai diritti degli artisti e delle case discografiche sono stimati in due miliardi di dollari per il mercato mondiale; ovviamente, si tratta di una valutazione approssimativa, in quanto ogni utente di Internet è un pirata potenziale. La richiesta di un inasprimento delle pene, proveniente dal mondo dell'industria, ha già trovato un riconoscimento nel « *No electronic theft act* », firmato dal Presidente degli USA il 17 dicembre 1997, che stabilisce la pena della reclusione fino a sei anni nei confronti di chi traffica via Internet opere il cui valore commerciale è non inferiore a mille dollari.

a questo proposito l'effettiva conoscenza dell'intenzione o della condotta dell'autore del reato o è sufficiente un dolo eventuale? Oppure è ravvisabile, a carico del *provider*, un obbligo giuridico di impedire l'evento?

Come si vede, la tranquillante e ricorrente affermazione secondo cui ciò che è illegale *off-line* lo è anche *on-line* — onde un reato non cessa di essere tale se commesso su Internet e dunque la rete delle reti non è uno spazio libero dal diritto — risulta provvista di una portata esplicativa assai modesta: anche senza indugiare sulla difficoltà di individuare la giurisdizione nazionale competente ad agire[4], quell'affermazione concerne infatti esclusivamente la punibilità del c.d. produttore di contenuti, mentre tace del tutto rispetto alla posizione degli altri soggetti operanti su Internet.

Le riflessioni che seguono sono destinate ad approfondire i profili della responsabilità penale degli *access-* e *service providers*, la cui vaghezza e aleatorietà sembrano costituire una caratteristica del sistema normativo.

3. Estensione analogica ad Internet della disciplina penale degli altri *mass media*?

I criteri di individuazione della responsabilità dei *providers* possono essere teoricamente ricondotti allo schema dell'autoria, a quello della responsabilità concorsuale o a quello dell'omissione di controlli finalizzati all'impedimento di eventi illeciti.

L'inquadramento della figura del *provider* come autore del reato di divulgazione in rete di contenuti illeciti si limita a situazioni marginali, ove a tale soggetto sia attribuibile la paternità dei dati in questione o almeno la loro riconducibilità, qualora egli agisca come moderatore di un *newsgroup* o di una *mailing-list* e quindi provveda al controllo dei messaggi pervenuti e decida in ordine alla successiva disponibilità di essi per gli utenti del servizio. L'utilizzazione dello schema della responsabilità concorsuale risulta invece consentita nelle ipotesi in cui sia dimostrabile che il *provider* abbia consapevolmente fornito l'accesso a dati illeciti da altri immessi in rete; situazione anche questa in grado di assumere una valenza assai limitata, a causa della difficoltà sia di provare il dolo del *provider* in riferimento ad un reato non ancora verificatosi, sia di derivare la sua responsabilità dalla consa-

[4] Cfr., nella prospettiva civilistica, C. De Martini, *Telematica e diritti della persona*, in questa *Rivista* 1996, 858 s. e 861 s.; S. Magni-M.S. Spolidoro, *La responsabilità degli operatori in Internet: profili interni e internazionali*, *ivi* 1997, 78 ss. Nella prospettiva penalistica, S. Seminara, *op. cit.*, 102 ss.

pevolezza sopravvenuta in ordine ad un reato già perfezionatosi nei suoi elementi essenziali[5].

Riservandoci di tornare più avanti sui problemi appena evidenziati, appare comunque chiaro che la ridotta capacità operativa dei due criteri ora esaminati potrebbe indurre verso la costruzione di una responsabilità colposa del *provider* conseguente alla violazione di un obbligo giuridico di impedire eventi illeciti, similmente a quanto già dispone l'art. 57 cod. pen. per il direttore o vicedirettore responsabile in tema di stampa periodica rispetto ai reati commessi con il mezzo della pubblicazione.

Ora, è vero che taluni recenti interventi giurisprudenziali hanno esteso ai giornali c.d. telematici la disciplina amministrativa della stampa o hanno affermato una equiparazione tra gli organi di stampa e i siti Internet[6]. Tuttavia, il tentativo di estendere analogicamente la normativa penale vigente in tema di stampa è destinato inesorabilmente a infrangersi sul principio di legalità, giacché l'art. 1, l. 8 febbraio 1948, n. 47, tassativamente stabilisce che « sono considerate stampe o stampati, ai fini di questa legge, tutte le riproduzioni tipografiche o comunque ottenute con mezzi meccanici o fisico-chimici, in qualsiasi modo destinate alla pubblicazione »[7].

Nel prosieguo di queste riflessioni, avremo modo di constatare anche l'inammissibilità pratica di un obbligo di controllo a carico del *provider* sui contenuti immessi dall'esterno sul *server* da lui gestito e, dunque, l'impossibilità teorica di costruire una sua responsabilità a titolo di colpa. Per il momento, è comunque importante sottolineare come un siffatto onere di controllo non trovi alcun fondamento sul piano del diritto positivo.

4. I CODICI DI AUTOREGOLAMENTAZIONE.

In linea generale, i codici deontologici adempiono alla finalità di prevedere sanzioni disciplinari rispetto a fatti non costituenti reato e lesivi della onorabilità della categoria dalla quale essi sono emanati. Accanto a questa funzione complementare ad un'eterodisciplina vigente e cogente, l'esperienza tuttavia dimostra come tali codici a volte sono emanati in una situazione di vuoto normativo, allo scopo di rendere superfluo l'intervento del legislatore ovvero di for-

[5] Relativamente alle considerazioni ora svolte, v. ancora S. SEMINARA, *op. cit.*, 96 ss.

[6] V. Trib. Roma, 6 novembre 1997 e Trib. Napoli, 8 agosto 1997, entrambi in questa *Rivista*, rispettivamente 1998, 75 e 1997, 970.

[7] Sotto questo profilo (e su quello, affine, della responsabilità per i reati commessi con il mezzo della radio e della televisione, di cui all'art. 30 l. 6 agosto 1990, n. 223) sia consentito ancora un rinvio a S. SEMINARA, *op. cit.*, 91 ss.; conf., anche sul versante della disciplina amministrativa e civilistica della legge sulla stampa, V. ZENO-ZENCOVICH, *La pretesa estensione alla telematica del regime della stampa: note critiche*, in questa *Rivista* 1998, 19 ss.

nirgli criteri orientativi da subito destinati a valere nei confronti degli associati. Quest'ultimo caso ricorre nel tema che ci occupa.

Mai prima d'ora come nel settore in esame si è verosimilmente registrata, a tutti i livelli, una convergenza di vedute in ordine alla necessità di un'autoregolamentazione. Così, sul piano comunitario, la risoluzione 17 febbraio 1997 del Consiglio UE relativa alle informazioni di contenuto illegale e nocivo invita gli Stati membri « ad incoraggiare ed agevolare sistemi di autoregolamentazione, che includano organismi rappresentativi dei fornitori e degli utenti dei servizi su Internet »; nello stesso senso si sono tra le altre espresse, in ordine cronologico, la Proposta di decisione del Consiglio UE 27 novembre 1997 di adozione di un piano pluriennale d'azione comunitaria per promuovere l'uso sicuro di Internet, la Dichiarazione finale 8 luglio 1997 della Conferenza ministeriale europea di Bonn sui mezzi di comunicazione globale, la relazione 21 novembre 1996 del Comitato dei Rappresentanti permanenti presso il Consiglio UE, la comunicazione 16 ottobre 1996 della Commissione sulle informazioni di contenuto illegale e nocivo su Internet, la risoluzione 25 settembre 1995 dell'Assemblea parlamentare del Consiglio d'Europa sulla democrazia informatica.

Alla base di questo orientamento sta la consapevolezza — per usare le parole contenute nella relazione 19 marzo 1997 alla Proposta di risoluzione redatta dalla Commissione per le libertà pubbliche e gli affari interni costituita presso il Parlamento europeo — « che una impostazione esclusivamente repressiva delle reti informatiche, di cui Internet è soltanto la prefigurazione, nuocerebbe in larga misura al contributo positivo di queste ultime allo sviluppo delle nostre società, ma che nel contempo sono necessarie forme efficienti di autoregolamentazione ». Ciò che a ben vedere porta con sé il riconoscimento, per un verso, della inadeguatezza degli assetti giuridici vigenti a comprendere la realtà rappresentata dalla rete delle reti, per altro verso della necessità di impostare la nuova disciplina attraverso una comune riflessione su base internazionale che possa fungere da piattaforma per una successiva armonizzazione degli ordinamenti nazionali.

Per quanto riguarda l'Italia, il modello di riferimento è costituito dalla bozza di « Codice di autoregolamentazione per i servizi Internet », redatto da un gruppo di lavoro composto da esperti dell'Associazione Italiana Internet Provider (AIIP), dell'Associazione Nazionale Editoria Elettronica (ANEE), di Telecom Italia e di Olivetti, diffuso il 22 maggio 1997 a seguito di un incontro svoltosi presso il Ministero delle Poste e telecomunicazioni. Nella sua versione aggiornata al 10 giugno 1997[8], il § 4b così enuncia i

[8] Il testo del codice è accessibile, tra gli altri, in *http://www.aiip.it/codice.htm* (consultazione effettuata il 15 luglio 1998).

« principi generali di responsabilità »: « 1. Il fornitore di contenuti è responsabile delle informazioni che mette a disposizione del pubblico. (...) 3. Nessun altro soggetto di Internet può essere ritenuto responsabile, salvo che sia dimostrata la sua partecipazione attiva. Per partecipazione attiva si intende qualsiasi partecipazione diretta all'elaborazione di un contenuto. 4. La fornitura di prestazioni tecniche senza conoscenza del contenuto non può (fare, *n.d.s.*) presumere la responsabilità dell'attore che ha fornito tali prestazioni ». Inoltre, il § 6.1. aggiunge — in tema di « obblighi relativi alla tutela della dignità umana, dei minori e dell'ordine pubblico » — che « qualunque soggetto di Internet venga direttamente a conoscenza dell'esistenza di contenuti accessibili al pubblico di carattere illecito, provvede ad informare direttamente l'autorità giudiziaria ».

Come si vede, i punti qualificanti della disciplina ora riferita stanno nella esclusione della responsabilità del *provider* rispetto ai contenuti a lui non direttamente riconducibili e nel suo contestuale obbligo di dare comunicazione all'autorità giudiziaria dei dati illeciti, accessibili al pubblico, di cui sia venuto a conoscenza. Senza indugiare sul margine di genericità derivante dall'assunzione — caratteristica dei codici deontologici — di un indistinto concetto di responsabilità (e anche scontando l'atteggiamento di autotutela corporativa che solitamente ispira la redazione di tali codici), entrambi i profili appena evidenziati si espongono però a motivate censure.

E invero, il requisito della « partecipazione diretta all'elaborazione di un contenuto », come presupposto esclusivo della responsabilità del *provider*, appare eccessivamente restrittivo, giacché ingiustificatamente esclude tutte le ipotesi in cui tale soggetto, nell'esercizio dei suoi poteri di controllo e di vigilanza, abbia reso accessibili al pubblico determinati contenuti nella consapevolezza della loro natura illecita. Come si è osservato in precedenza, infatti, il moderatore di un *newsgroup* o di una *mailing-list* che provvede al controllo dei testi pervenuti e decide in ordine alla loro successiva disponibilità per gli utenti del servizio è da considerarsi come l'autore della diffusione e a nulla rileva l'assenza di un suo personale contributo nella fase della elaborazione.

Per contro, una pericolosa dilatazione della responsabilità può derivare dalla imposizione di un dovere di denuncia all'autorità giudiziaria, che il nostro codice penale attualmente prevede in via generale solo nei confronti dei pubblici ufficiali e degli incaricati di un pubblico servizio per i fatti appresi nell'esercizio o a causa delle funzioni (artt. 361 e 362) e, rispetto ai cittadini, limitatamente ai delitti contro la personalità dello Stato puniti con la pena dell'ergastolo (art. 364). In conseguenza di un siffatto obbligo di collaborazione con gli organi inquirenti, la figura del *provider* viene infatti sganciata dalla sua connotazione privatistica di imprenditore e risulta proiettata in un ambito pubblicistico certa-

mente produttivo di ambiguità e potenzialmente foriero di ulteriori vincoli tendenti a trasformarlo in una sorta di garante dei contenuti accessibili sul proprio *server*.

Infine, desta perplessità l'omessa previsione, a carico del *provider*, dell'obbligo di rimuovere i materiali illeciti di cui abbia conoscenza. Per quanto tale soggetto possa essere assimilato ad un qualsiasi vettore di informazioni provenienti da terzi, la valenza neutrale della sua condotta svanisce infatti quando egli coscientemente contribuisce alla diffusione di contenuti antigiuridici immessi sul proprio *server*; né un siffatto obbligo risulta desumibile dall'ultimo capoverso del § 4b — secondo cui la responsabilità di chi fornisce prestazioni tecniche è subordinata alla conoscenza dei contenuti —, poiché la medesima norma ulteriormente vincola la punibilità alla diretta partecipazione all'elaborazione del materiale[9].

Alla luce delle critiche ora esposte, il « Codice di autoregolamentazione per i servizi Internet » non appare in grado di ispirare il legislatore nazionale. Ancor più risalta poi l'inadeguatezza di questa bozza di disciplina ove si consideri che, sul piano comunitario, la citata Dichiarazione finale 8 luglio 1997 della Conferenza ministeriale europea di Bonn, riconoscendo « la necessità di fare chiara distinzione tra la responsabilità di chi produce e mette in circolazione i contenuti e quella degli intermediari », ammette la possibilità di rendere i *providers* destinatari di limitati doveri di intervento[10]. E, nella medesima prospettiva, la già citata Proposta

---

[9] Tale obbligo non è previsto neppure dal « Codice di deontologia e di buona condotta per i servizi telematici » redatto dall'Associazione Nazionale Fornitori di Videoaudioinformazione (ANFoV) ed entrato in vigore il 1º gennaio 1998 (il testo è riportato in O. TORRANI-S. PARISE, *Internet e diritto*, Milano, 1998, 2ª ed., p. 163 ss.), che in generale non un cenno dedica alla responsabilità del *provider*, prevedendo a suo carico esclusivamente obblighi di informativa nei confronti degli abbonati rispetto ai contenuti illegali e nocivi (art. 13). Assai più articolata si presenta invece la « Carta delle garanzie di Internet », compilata dal gruppo di studio della rivista InterLex, che nella bozza divulgata il 29 aprile 1998 (sul sito *http://www.interlex.com/testi/carta41.htm*, consultato il 15 luglio 1998) così afferma all'art. 10: « 1. I fornitori di accesso o di contenuti rimuovono dai propri sistemi, non appena ne vengano a conoscenza, i contenuti palesemente e inequivocabilmente illeciti o offensivi, informando, ove possibile, il responsabile dell'immissione. (...) 3. I fornitori di accesso o di contenuti informano l'attività giudiziaria nei casi in cui vengano a conoscenza di contenuti palesemente e inequivocabilmente illeciti immessi nei propri sistemi »; in conformità a quanto osservato nel testo, l'art. 9 inoltre dispone: « 1. I fornitori di accesso non sono responsabili dei contenuti provenienti dall'esterno dei propri siti o *immessi direttamente* dagli utenti e non sono tenuti a impedirne la visibilità, tranne che in osservanza di un provvedimento motivato dell'autorità giudiziaria e fatte salve le disposizioni dell'art. 10 ».

[10] La Dichiarazione così osserva sul punto in questione: « I Ministri sottolineano che le regole sulla responsabilità riguardo ai contenuti debbano essere basate su un insieme di regole comuni tali da assicurare un campo di azione comune e omogeneo. Perciò gli intermediari come gli operatori di rete e i *providers* non sono, in generale, responsabili dei contenuti. Tale principio dovrebbe essere applicato in modo tale che gli intermediari come gli operatori di rete e i *providers* non siano soggetti a regole irragionevoli, sproporzio-

di risoluzione, redatta dalla Commissione per le libertà pubbliche e gli affari interni costituita presso il Parlamento europeo, al punto 35 suggerisce che « i fornitori di accesso e di servizi siano obbligati a rispettare le seguenti norme minime: assumere la piena responsabilità, compresa quella penale, per i contenuti che essi stessi mettono a disposizione; rispondere dei contenuti passibili di pena offerti da servizi esterni se i singoli contenuti concreti sono loro noti e se è loro ragionevolmente e tecnicamente possibile impedirne l'utilizzo (...) ».

Riservandoci di tornare successivamente sui contenuti della prescrizione appena citata, possiamo per il momento limitarci a constatare l'insufficienza del modello italiano di autoregolamentazione e la sua significativa divergenza rispetto alla proposta comunitaria. Tali elementi, insieme ai limiti insiti nella natura inevitabilmente volontaristica dell'adesione al codice deontologico — dalla quale consegue la debole efficacia generalpreventiva delle già miti sanzioni minacciate[11], la cui inflizione viene paralizzata dalla contraria volontà del destinatario —, depongono in favore di una soluzione su base legislativa.

5. La prevenzione dei reati su Internet.

Prima di passare all'esame dei possibili contenuti di una disciplina normativa, è opportuno accertare le strategie utilizzabili per la prevenzione dei reati commessi in rete, al fine di verificare se — oltre l'evidente responsabilità dell'autore materiale — sia possibile costruire, e in quali termini, una responsabilità del *provider*.

A tale scopo, si è già rilevato come sia pacifica la punibilità del *provider* laddove egli assume il ruolo di diretto produttore dell'informazione ovvero svolge il compito di controllare o rivedere il materiale da pubblicare nella BBS o nel *newsgroup* o nel forum

nate o discriminatorie. In ogni caso, il terzo che opera il servizio di *hosting* di tali contenuti non dovrebbe esercitare un ruolo di controllo sui contenuti che non ha ragione di ritenere illegali. Si dovrebbe tenere conto di quanto tali intermediari abbiano ragionevole motivo di conoscere e ragionevole possibilità di controllare i contenuti ».

[11] Il § 13 del *Codice di autoregolamentazione* prevede che, in presenza di un'infrazione, il Giurì emetta un provvedimento di diffida, con l'invito a conformarsi entro due giorni e, in caso di inosservanza della diffida, un formale ammonimento da pubblicarsi sul sito relativo all'organismo di autoregolamentazione Internet, con un sollecito ad adempiere. In aggiunta a queste previsioni, la « Carta delle garanzie » consente al Giurì, nelle ipotesi di particolare gravità, di comminare sanzioni pecuniarie fino ad un massimo di cinque milioni di lire, da destinare ad un fondo o ente per la ricerca nel settore del diritto dell'informazione; mentre il « Codice di deontologia e di buona condotta », per i casi di inottemperanza o di maggiore gravità, prevede l'applicazione di una censura, di una « sanzione amministrativa pecuniaria » (?) da uno a sei milioni di lire, l'espulsione dall'associazione e la pubblicazione del provvedimento a spese del fornitore.

di discussione, decidendo in ordine alla sua accessibilità da parte degli utenti del servizio. Il problema, come è ovvio, concerne però le ipotesi in cui manca qualsiasi partecipazione attiva da parte del *provider* rispetto ai dati illeciti immessi sul suo *server*.

Il primo dato che si impone con evidenza concerne l'inesigibilità di un effettivo controllo, almeno da parte dei fornitori di maggiori dimensioni, sui dati immessi nel *server*, a causa non solo della loro immensa quantità ma anche della loro continua mutevolezza; nel caso specifico dell'*e-mail*, neppure si trascuri che i messaggi vengono trattenuti solo temporaneamente dal *server* (specie quelli in uscita) e che una loro cognizione o soppressione integrerebbe l'art. 616 cod. pen., in tema di violazione della corrispondenza telematica[12].

Né, al fine di aggirare tali difficoltà, è possibile fare affidamento sulla installazione di filtri destinati a reagire a determinate parole chiave, in modo da scollegare automaticamente l'utente o sopprimere al passaggio i dati ritenuti indesiderabili. A questo proposito, la Relazione sulla comunicazione della già citata Commissione sulle informazioni di contenuto illegale e nocivo su Internet osserva che « queste soluzioni, oltre alla loro macchinosità tecnica, presentano problemi diversi, ad esempio di tipo semantico. Il fornitore *America Online* ha tentato, nel 1995, di intercettare i messaggi con alcune parole di carattere sessuale, tra cui la parola 'seno'; così facendo ha bloccato un foro destinato a consigliare le donne vittime di cancro al seno... ». A ciò è da aggiungere che, comunque, tali filtri non funzionano se i materiali vengono criptati, compressi o trasmessi in linguaggio diverso dall'ASCII o, laddove il filtro sia reso noto agli utenti, questi sostituiscono le parole-chiave con numeri o altri termini. Breve: mentre i controlli di tipo manuale sono impraticabili a causa dell'insostenibile

[12] Sul punto, P. Costanzo, *Aspetti evolutivi del regime giuridico di Internet*, in questa *Rivista* 1996, 839; B. Donato, *La responsabilità dell'operatore di sistemi telematici*, *ibid.*, 146 ss.; U. Sieber, *Responsabilità penali per la circolazione di dati nelle reti internazionali di computer* (trad. a cura di M. Sforzi), in *Riv. trim. dir. pen. econ.* 1997, 750 s.; l'ipotizzabilità di un generale obbligo di controllo è invece prospettata da C. De Martini, *op. cit.*, 864. In relazione a quanto osservato nel testo, si consideri anche l'art. 13, d.p.r. 10 novembre 1997, n. 513 (« Regolamento recante criteri e modalità per la formazione, l'archiviazione e la trasmissione di documenti con strumenti informatici e telematici, a norma dell'art. 15, comma 2, della legge 15 marzo 1997, n. 59 »). Nelle more della pubblicazione, grazie alla cortesia del prof. Zeno-Zencovich sono venuto a conoscenza di due arresti giurisprudenziali di segno opposto: nel primo (Trib. Roma, ord. 4 luglio 1998 Banca del Salento c. Pantheon s.r.l.) si esclude la legittimazione passiva del *provider* in quanto egli ''si limita a mettere a disposizione'' degli utenti lo spazio 'virtuale' dell'area di discussione e nel caso di specie, trattandosi di un *newsgroup* non moderato, non ha alcun potere di controllo e vigilanza sugli interventi che vi vengono inseriti'', con il secondo (P.M. Pret. Vicenza, ord. 23 giugno 1998) si dispone invece il sequestro preventivo ''di tutte le attrezzature usate per diffondere sul sito web il messaggio diffamatorio'', cioè l'intero *server* gestito dal *provider*, al fine di impedire l'ulteriore diffusione di un messaggio immesso in uno spazio web.

dispendio di mezzi e di energie richiesto, quelli di tipo automatico si rivelano di scarsa utilità[13].

Qualora tuttavia, di propria iniziativa o a seguito di segnalazione da parte degli utenti o dell'autorità giudiziaria, il *provider* venga a conoscenza di materiali illeciti immessi sul proprio *server*, un suo intervento non incontra ostacoli tecnici. Così, nel settore dei *newsgroups* è possibile la cancellazione del singolo testo o anche dell'intero *newsgroup*, che in questa ipotesi viene eliminato dal *server* in modo da non consentire più l'accesso agli utenti. Analogamente vale per le pagine Web, ove possono eliminarsi (o chiudersi temporaneamente) singole pagine o l'intera offerta del *content provider*, per l'*FTP server* e per l'*e-mail*.

Il problema, però, è che il buon esito di tale intervento viene vanificato dal fatto che gli utenti possono agevolmente accedere ai medesimi contenuti attraverso differenti siti Web, un altro FTP *server*, le linee telefoniche o la comunicazione satellitare mediante antenne paraboliche; oppure — considerando che, attraverso un programma automatico di sincronizzazione (c.d. *store and forward principle*), i dati memorizzati da ciascun *news server* sono contemporaneamente trasmessi agli altri *news servers* che ospitano il medesimo *newsgroup* — gli utenti possono avvalersi di un qualsiasi *News-Reader-Programm* o di un comune *browser* per collegarsi ad un *news-server* diverso da quello del loro *provider*, ove rinvenire *newsgroups* non contenuti nel *server* locale o da questo eliminati. Né è possibile ipotizzare per l'*access provider* l'obbligo di escludere l'accesso dei suoi clienti ai materiali illeciti attraverso un intervento sull'indirizzo IP del *server* sul quale i dati sono disponibili, poiché tale misura non solo comporterebbe la chiusura (totale o parziale) di ogni comunicazione e scambio di materiali tra gli altri utenti collegati al medesimo indirizzo, ma oltretutto potrebbe essere facilmente aggirata da un semplice mutamento di indirizzo da parte del gestore del *news server* interessato ovvero da un suo ricorso ad un servizio anonimo su Internet o ad un *Proxy-cache-server* di altro *provider*[14].

---

[13] In ordine alle conseguenze derivanti dall'imposizione di oneri di controllo sui *providers*, cfr. inoltre le meditate riflessioni del giudice Dalzell contenute nella sentenza 11 giugno 1996 della *District Court for the Eastern District of Pennsylvania* (v. *postea*, § 9), in questa *Rivista* 1996, 634 s. (trad. a cura di V. Zeno-Zencovich). Le osservazioni svolte nel testo valgono, ovviamente, solo in riferimento alla posizione dei *providers* e non mirano certo a negare la rilevanza di tali procedure di filtraggio e la loro utilità per gli utenti. Ancora di recente, la citata Risoluzione del Consiglio UE 17 febbraio 1997 invita gli Stati membri ad « incoraggiare la messa a disposizione degli utenti di meccanismi di filtraggio e promuovere la creazione di sistemi di classificazione, ad esempio la PICS lanciata dal consorzio internazionale *World-Wide-Web* con il sostegno della Comunità » (o anche, può aggiungersi, il *Cyber Patrol*, il *Netnanny*, il *Surfwatch* ecc.). Nello stesso senso si esprimono, tra le altre, la Proposta di decisione del Consiglio UE 27 novembre 1997 e la Dichiarazione finale 8 luglio 1997 della Conferenza ministeriale di Bonn.

[14] Con particolare dovizia di informazioni tecniche, v. U. SIEBER, *Kontrollmö-*

D'altra parte, una volta scartata la possibilità di un controllo individuale degli attuali 60 milioni di utenti di Internet rispetto alle innumerevoli vie di accesso in rete a loro disposizione, neppure risulta realizzabile (anche senza considerare l'inammissibile compressione della libertà di manifestazione e di comunicazione del pensiero, garantita dalla Costituzione e dalla Convenzione europea di salvaguardia dei diritti dell'uomo) la « compartimentazione » di una massa di utenti di un sistema chiuso di rete (ad esempio, un servizio *on-line* o un'intera nazione) agendo sul suo punto di collegamento alla rete mondiale, giacché tale soluzione non solo presuppone che tale collegamento si realizzi attraverso un *Proxy-cache-server* — i cui contenuti verrebbero così sottoposti a controllo al fine di selezionare i dati da rendere accessibili — ma in ogni caso, come dimostra l'esperienza cinese, risulta aggirabile dalle possibilità di collegamento telefonico o satellitare esistenti su scala mondiale. A quanto precede va aggiunto che, a fronte dell'enorme massa di dati continuamente modificabili immessi in rete, un controllo preventivo in tempo reale risulta impossibile, mentre uno fondato su parole chiave si esporrebbe alle obiezioni prima avanzate[15].

In conclusione: come è attualmente impraticabile un sistematico ed effettivo controllo per l'individuazione su scala mondiale dei contenuti illeciti accessibili in rete, così è impossibile una definitiva chiusura dell'accesso a contenuti già individuati come illeciti. Onde un *provider* può tecnicamente rendere più difficile, ma non può impedire — a causa del procedimento di *routing* prima riferito — che i suoi clienti possano comunque accedere ai dati da lui censurati: le misure di controllo e di intervento realizzabili rivestono dunque — come si esprime la Relazione prima citata sulla comunicazione della Commissione sulle informazioni di contenuto illegale e nocivo su Internet — una « portata simbolica ».

L'esperienza pratica conferma le conclusioni ora raggiunge. In particolare, le iniziative adottate in Germania dalla polizia e dalla Procura della Repubblica contro la CompuServe Deutschland GmbH (alla quale fu consegnata nel novembre 1995 una lista di 282 *newsgroups* contenenti materiali pornografici illeciti, che venne inoltrata alla casa-madre statunitense CompuServe Inc. provocando la chiusura di quei *newsgroups*), contro le pagine Web di Ernst Zündel che dal Canada divulgavano teorie neonaziste, contro l'indirizzo di rete « xs4all » ove attraverso un *provider* olandese si diffondevano messaggi integranti le fattispecie di istigazione all'odio sociale e apologia di reati, sono servite solo ad accre-

---

glichkeiten zur Verhinderung rechtswidriger Inhalte in Computernetzen, in *Computer and Recht* 1997, 596 s. e 656 ss.

[15] Cfr. U. Sieber, *op. ult. cit.*, 659 s.

scere la pubblicità dei rispettivi contenuti, rimasti accessibili su numerosi altri *servers*: con il risultato che l'adozione di tali misure si è rivelato al contempo inefficace come censura e valida come ulteriore propaganda dei materiali ritenuti illeciti[16].

6. UN MODELLO DI DISCIPLINA: LA LEGGE TEDESCA 22 LUGLIO 1997.

Nel panorama europeo, la Germania rappresenta l'unica nazione che ad oggi si sia dotata di una compiuta normativa espressamente concernente la responsabilità degli operatori su Internet[17].

L'art. 5 della l. 22 luglio 1997 sui servizi di informazione e di comunicazione (*IuKDG*) dispone infatti: « 1. I fornitori di servizi sono responsabili secondo le leggi generali dei propri materiali da essi resi disponibili. 2. I fornitori di servizi sono responsabili dei materiali altrui da essi resi disponibili solo se hanno conoscenza dei loro contenuti e sia tecnicamente possibile ed esigibile impedirne la disponibilità. 3. I fornitori di servizi non sono responsabili dei materiali altrui ai quali essi hanno fornito solo l'accesso. Un'automatica e di breve durata ritenzione di materiali altrui, conseguente alla richiesta di utenti, va intesa come fornitura di accesso. 4. Qualora, nel rispetto della riservatezza delle comunicazioni a distanza di cui al § 85 della legge sulle telecomunicazioni, il fornitore di servizi acquisisce conoscenza di contenuti illeciti e una chiusura sia tecnicamente possibile ed esigibile, rimangono salvi, secondo le leggi generali, gli obblighi di impedimento della disponibilità di tali materiali »[18].

---

[16] Così ancora U. SIEBER, *op. ult. cit.*, 582 e 665.

[17] In relazione all'ordinamento francese, l'art. 15 della *Loi de réglementation des télécommunications* 26 luglio 1996, n. 96-659, inserito come art. 43-1 nella legge 30 settembre 1986, n. 86-1067, dispone: « Ogni soggetto la cui attività consiste nell'offerta di servizi di connessione a uno o più servizi di connessione audiovisiva menzionati nel comma 1 dell'art. 43, è tenuto a proporre ai clienti un mezzo tecnico che consenta loro di limitare l'accesso a determinati servizi o di selezionarli ». Il medesimo art. 15 ulteriormente prevedeva un art. 43-2, che affidava al *Comité supérieur de la télématique* i compiti di elaborare raccomandazioni finalizzate all'osservanza delle regole deontologiche in materia di servizi di connessione audiovisiva e di vigilare sul loro adempimento, nonché un art. 43-3, che escludeva la responsabilità penale dei fornitori di servizi che si fossero conformati alle prescrizioni dell'art. 43-1 e ai pareri del *Comité*, pubblicati sul *Journal officiel de la République française*, concernenti i servizi ritenuti lesivi delle raccomandazioni, salvo i casi di personale esecuzione del reato o di dolosa partecipazione; entrambe le norme sono state però dichiarate illegittime con sentenza 23 luglio 1996, n. 96-378 DC, del *Conseil Constitutionnel* (il cui testo può leggersi in *http://www.jura.uni-sb.de/france/constit/1996/96378dc.htm*, consultato il 15 luglio 1998). Sul punto, v. L. THOUMYRE, *Abuses in the Cyberspace*, 1996, in *http://www.argia.fr/lij/telechargement/file1.doc*, p. 62 ss. (consultato il 15 luglio 1998) e, più in generale, V. SÉDALLIAN, *Le contrôle du flux des informations. La responsabilité des acteurs dans le flux des informations*, 1997, in *http://www.argia.fr/lij/livre/respact.html*, p. 7 ss. (consultato il 15 luglio 1998).

[18] Per una generale esposizione dei contenuti della legge, S. ENGEL-FLECHSIG, F.A. MAENNEL, A. TETTENBORN, *Das neue*

Come si vede, tale disciplina recepisce il punto 35 della già citata Proposta di risoluzione redatta dalla Commissione per le libertà pubbliche e gli affari interni costituita presso il Parlamento europeo, assumendo come base di partenza l'insussistenza di un generale obbligo di controllo del *provider* e l'assenza di responsabilità di colui che si limita a fornire infrastrutture per il collegamento ad Internet — qui correttamente equiparato a qualsiasi altro servizio di telecomunicazione —[19] o un *hosting*, senza interferire sui contenuti veicolati attraverso la rete. Per quanto più specificamente riguarda la prospettiva penalistica, la norma pone una duplice distinzione riferita per un verso alla disponibilità o indisponibilità dei materiali, per altro verso alla loro proprietà o altruità.

In ordine alla prima distinzione, il requisito della disponibilità funge da presupposto della responsabilità del *provider* rispetto ai materiali propri nonché del suo obbligo di attivazione nei confronti dei materiali altrui: ove è chiaro che, nel primo caso, la disponibilità corrisponde alla mera accessibilità da parte degli utenti, mentre nel secondo caso si caratterizza pure come « signoria » sui contenuti memorizzati nel proprio *server* per un tempo apprezzabile (ciò che, alla luce della precisazione operata dal comma 3, non ricorre per i *Proxy-Cache servers*, ove si realizza una ritenzione automatica e di breve durata conseguente ad un richiamo effettuato dagli utenti).

La distinzione tra materiali propri e altrui vale invece a definire i contenuti dei precetti penalmente rilevanti. In particolare, la nozione di proprietà — che ovviamente rinvia allo schema dell'auto-

---

Informations- und Kommunicationsdienste-Gesetz, in *Neue Juristische Wochenschrift* 1997, 2981 ss.; v. anche F.A. KOCH, *Zivilrechtliche Anbieterhaftung für Inhalte in Kommunikationsnetzen*, in *Computer und Recht* 1997, 193 ss. Per quanto concerne specificamente il § 5.2, è interessante notare come la sua formulazione richiami assai da vicino la prima « raccomandazione » contenuta nel *Bericht einer interdepartementalen Arbeitsgruppe zu strafrechtlichen, datenschutzrechtlichen und urheberrechtlichen Fragen rund um Internet*, divulgato il 30 maggio 1996 dal Ministero della Giustizia svizzero: « Il *provider* che ha conoscenza certa di contenuti illeciti immessi in rete, specie se penalmente rilevanti, deve senza indugio adottare le misure tecnicamente possibili ed esigibili per chiudere l'accesso ad essi » (il testo del *Bericht* è riportato in *http://www.admin.ch/ejpd/d/bj/internet/inbearbd/htm*, consultato il 15 luglio 1998).

[19] Risale al 17 febbraio 1995 la sentenza di condanna emessa dal *Bundesgericht* svizzero nei confronti del direttore generale del *Post-, Telefon- und Telegraphendienst*, il quale — avendo concesso all'agenzia Telekiosk un'autorizzazione per l'esercizio di conversazioni telefoniche a distanza, su cui si erano inserite talune *sex lines* — aveva respinto l'intimazione della Procura cantonale di adottare iniziative volte a impedire la prosecuzione del fatto, adducendo la necessità di una sentenza esecutiva di condanna nei confronti dei responsabili; donde la contestazione nei suoi confronti di concorso nel reato di divulgazione di materiale pornografico a minori di 16 anni, *ex* art. 197.1 cod. pen. svizzero (v. SEMINARA, *op. cit.*, 102, nota 69). Sul piano dogmatico, il problema qui consiste nello stabilire se la condotta autonomamente punibile dei gestori delle *sex lines* interrompeva il nesso di imputazione nei confronti del fornitore di infrastrutture alla luce del c.d. divieto di regresso e in forza del carattere neutrale della prestazione da lui resa (cfr. sul punto anche U. SIEBER, *Responsabilità penali*, cit., 1207).

ria per i reati in concreto configurabili — va intesa nel senso di diretta riconducibilità al *provider* (che può essere pure il titolare di una *homepage*), il quale si presenta come l'autore del materiale — anche in quanto se ne sia appropriato, non indicandone la paternità — ovvero, laddove eserciti un controllo preventivo di congruità e/o di liceità sui materiali da rendere accessibili, come responsabile della loro immissione in rete[20]. Una siffatta situazione, almeno in linea generale, non sembra peraltro ravvisabile rispetto ai *links* di rinvio, dovendosi escludere che il mero collegamento ipertestuale valga ad attribuire la proprietà del relativo materiale; in tal caso, soccorre comunque il richiamo alle « leggi generali », che qui va riferito all'applicabilità delle norme sulla partecipazione criminosa[21].

La responsabilità per i materiali altrui risulta invece subordinata, anzitutto, alla conoscenza del contenuto illecito, che correttamente la dottrina tedesca — al fine di evitare l'ingresso del dolo eventuale, che sarebbe causa di illimitati ampliamenti degli spazi di punibilità — interpreta come dato effettivo e non semplicemente potenziale[22]. I criteri della possibilità tecnica e della esigibilità presentano, dal canto loro, un grado di profonda interrelazione.

Il parametro della esigibilità — che nel suo simmetrico concetto di inesigibilità, intesa come causa sovralegale di esclusione della colpevolezza, viene respinto dalla prevalente dottrina italiana e risulta oggi in crisi anche nella dottrina e giurisprudenza tedesche[23] — si fonda in generale su un bilanciamento degli interessi in conflitto, arricchito da una valutazione sulle concrete possibilità di tutela del bene in pericolo in rapporto alla idoneità e congruità del mezzo prescelto per il conseguimento del fine. In riferimento al tema che ci occupa, la contrapposizione tra le libertà di manifestazione del pensiero e di iniziativa economica (del *provider*, degli utenti o dei titolari di una pagina Web) e gli interessi collettivi of-

[20] Tra gli altri, conf. C. PELZ, *Die strafrechtliche Verantwortlichkeit von Internet-Providern*, sub II.1.a-b, in *http://www.anwaltsforum.de/gebiete/straf/pelz/strafrecht.htm* (sito gestito dalla *Deutscher Anwaltsverein*, consultato il 15 luglio 1998).

[21] Tale problema risulta estremamente controverso tra i primi commentatori della normativa tedesca: nel senso che un'appropriazione di contenuti possa verificarsi anche mediante un *link* di rinvio, C. PELZ, *op. cit.*, sub II.1.b; diff., configurando il § 5.1 o il § 5.3 *IuKDG* a seconda che il *link* si inserisca in un contesto tale che possa ritenersi la sua incorporazione nell'offerta del *provider* ovvero si presenti solo come una « via breve » di collegamento, S. ENGEL-FLECHSIG, F.A. MAENNEL, A. TETTENBORN, *op. cit.*, 2985; *contra*, proponendo la soluzione adottata nel testo, S. ERNST, *Rechtliche Fragen bei der Verwendung von Hyperlinks im Internet*, in *Neue Juristische Wochenschrift - CoR* 1997, 228; nel senso di richiamare il § 5.4 *IuKDG*, F.A. KOCH, *Neue Rechtsprobleme der Internet-Nutzung*, *ivi* 1998, 48.

[22] Conf. S. ENGEL-FLECHSIG, F.A. MAENNEL, A. TETTENBORN, *op. cit.*, 2985; U. SIEBER, *Kontrollmöglichkeiten*, cit., 655.

[23] Per tutti, G. FIANDACA-E. MUSCO, *Diritto penale, pt. gen.*, Bologna, 1995, 3ª ed., p. 363 ss.; H.-H. JESCHECK-T. WEIGEND, *Lehrbuch des Strafrechts, A.T.*, Berlin, 1996, 5ª ed., p. 503 s. Ampiamente, v. pure G. FORNASARI, *Il principio di inesigibilità nel diritto penale*, Padova, 1990, *passim*.

fesi dalla pornografia, dalla violazione dei diritti di autore ecc. sembra tuttavia in grado di risolversi in un irrigidimento del problema all'interno dell'astratta alternativa tra i vantaggi e i pregiudizi derivanti dalla previsione di interventi repressivi a carattere inevitabilmente censorio. Sotto il profilo in esame, la nozione di esigibilità rileva dunque nella più specifica accezione — già suggerita dalla citata Proposta di risoluzione del Parlamento europeo — di ragionevolezza o proporzionalità della condotta imposta all'agente per la tutela del bene in pericolo: ciò che rinvia anche all'ulteriore parametro della possibilità tecnica[24].

Per l'illustrazione del concetto di possibilità tecnica — che si presta così ad essere valorizzato come un limite interno del criterio dell'esigibilità — valgono le considerazioni espresse in precedenza, dalle quali deriva che il *provider* può cancellare i dati illeciti dal proprio *server*, ma non è in condizione di precluderne l'accessibilità su altri *servers*. Né in ogni caso appare ipotizzabile un obbligo di chiudere l'intera connessione alla rete agendo sull'indirizzo IP, giacché una siffatta misura, coinvolgendo i diritti di terzi estranei senza escludere del tutto l'accesso ai materiali illeciti, risulta in ogni caso priva del requisito della proporzionalità.

Nei confronti del *provider* sussiste dunque il dovere — esigibile e tecnicamente possibile — di sopprimere i materiali illegali contenuti nel *server* da lui gestito e dei quali egli in qualsiasi modo abbia acquisito conoscenza. Il riconoscimento che un tale intervento vale al più a contrastare la diffusione dei contenuti illeciti, ma si rivela inefficace per una completa tutela dei beni aggredibili in rete, rappresenta solo il frutto di una corretta valutazione dell'attuale realtà di Internet[25].

Questa impostazione, conforme ai criteri enunciati già in sede comunitaria, va condivisa. Sul piano della tecnica legislativa, essa infatti si limita ad esprimere regole generali, in grado di consentire il loro costante adeguamento all'evoluzione tecnologica e, quindi, al continuo mutamento delle « possibilità tecniche » di sop-

---

[24] Cfr. sul punto U. SIEBER, *Kontrollmöglichkeiten*, *cit.*, 585 ss. Per inciso, si noti che il criterio della proporzionalità — ampiamente elaborato nella giurisprudenza della Corte di Giustizia europea ed espressamente accolto dall'art. 3b del Trattato istitutivo della Comunità europea — trova già un diffuso riconoscimento all'interno degli ordinamenti nazionali degli Stati della Comunità. Per quanto riguarda l'Italia, vd. ad esempio l'art. 10, comma 4, l. 31 dicembre 1996, n. 675, sulla tutela dei dati personali, che esclude l'onere dell'informativa all'interessato « quando essa comporta un impiego di mezzi che il Garante dichiari manifestamente sproporzionati rispetto al diritto tutelato, ovvero si rivela, a giudizio del Garante, impossibile ».

[25] Per analoghe conclusioni, S. ENGEL-FLECHSIG, F.A. MAENNEL, A. TETTENBORN, *op. cit.*, 2985; U. SIEBER, ***op. ult. cit.*, 657. Il citato *Bericht* divulgato dal Ministero della Giustizia svizzero osserva sul punto che la soppressione dei materiali illeciti consente al *provider* di escludere la sua responsabilità e inoltre, « per quanto non efficace in assoluto, rende tuttavia sensibilmente più difficile l'accesso e così limita la diffusione e la disponibilità dei contenuti penalmente rilevanti ».**

pressione dei contenuti illeciti; al contempo, essa contiene chiari parametri orientativi nei confronti del giudice, manifestando una valenza indubbiamente superiore di quella ascrivibile a qualsiasi codice deontologico.

Sul piano dei contenuti, inoltre, la soluzione in esame risulta apprezzabile in quanto — correttamente assumendo l'utilità sociale di Internet (con le connesse aperture verso la categoria del rischio consentito) e la conseguente necessità di un suo bilanciamento rispetto agli interessi potenzialmente offendibili[26] — evita il ricorso a schemi presuntivi e ad irreali oneri di controllo, incentrando il rimprovero sulla condotta effettivamente tenuta dal *provider* nel caso di materiali propri e sulla sua volontaria omissione di intervento nel caso di materiali altrui.

7. Gli effetti della ricezione nell'ordinamento italiano della disciplina tedesca.

Come risulta chiaro dalla sua formulazione — e come viene pure evidenziato dai commentatori —, il § 5 *IuKDG* possiede una valenza non costitutiva, ma semplicemente dichiarativa della responsabilità del *provider* alla stregua del diritto tedesco vigente, presentandosi così come un'interpretazione autentica fornita dal legislatore allo scopo di evitare incertezze e contrasti giurisprudenziali. Tale valutazione ha recentemente trovato un'autorevole conferma in un decreto di archiviazione emesso il 13 febbraio 1998 dalla Procura generale presso la Corte di Cassazione tedesca, relativamente ad un procedimento penale che vedeva numerosi *providers* come imputati di agevolazione in istigazione e apologia di reati, e i cui passaggi argomentativi essenziali possono così sintetizzarsi.

Anzitutto, il decreto rileva che a carico di un *access provider* è configurabile, in linea generale, una posizione di garanzia derivante non da una precedente attività antigiuridica (« la condotta del *provider* consistente nell'apertura di accessi ad Internet per gli utenti non è antigiuridica in sé ma anzi, alla luce delle esigenze dell'attuale società dell'informazione e in particolare anche della scienza, risulta socialmente diffusa e auspicata ») ma da un onere di controllo sulla fonte del pericolo: « nel momento in cui i *providers* consentono l'accesso alla rete, essi devono essere considerati come destinatari di determinati ''doveri per la sicurezza del traffico'' ». Alla luce dei generali principi penalistici — prosegue il de-

[26] Nel senso di sottolineare l'ambiguità della categoria del rischio consentito v. però G. Fiandaca-E. Musco, *op. cit.*, p. 497 ss.; M. Romano, *Commentario sistematico del codice penale*, Milano, 1995, I, 2ª ed., *sub* art. 43, 80.

creto —, un concreto obbligo di agire è però ipotizzabile solo quando l'agente sia consapevole delle circostanze che determinano l'insorgenza di tale obbligo ed egli abbia la possibilità di impedire la verificazione dell'evento attraverso una condotta esigibile: così, mentre un generale dovere di controllo non risulterebbe né possibile né esigibile, l'obbligo di impedire l'accesso ai materiali illeciti sussiste quando il *provider* abbia conoscenza che determinati contenuti punibili sono disponibili in rete. Rispetto a tale soluzione — conclude il provvedimento in esame — la promulgazione della legge 22 luglio 1997 « non ha mutato nulla »[27].

Ora, può dubitarsi che l'introduzione in Italia di una disciplina conforme al modello tedesco assolverebbe alla medesima funzione dichiarativa.

E invero, se nessuna perplessità insorge sulla punibilità del *provider* per i materiali propri da lui resi disponibili, altrettanto non può ritenersi nell'ipotesi di materiali altrui, ove la costruzione di una posizione di garanzia in grado di integrare un obbligo giuridico di impedire l'evento *ex* art. 40 cpv. cod. pen. incontra una serie di difficoltà. Anzitutto, l'operatività della norma appena citata risulta espressamente limitata a fattispecie incriminatrici strutturate in senso causale, laddove la divulgazione, diffusione ecc. si presentano come mere condotte[28]. Inoltre, integrando (almeno nella maggior parte) tali condotte altrettanti reati a consumazione istantanea, il riconoscimento di un obbligo giuridico di intervento a carico del *provider* verrebbe ulteriormente complicato dal fatto che, nella impossibilità di esercitare una vigilanza preventiva sui materiali immessi sul *server* da lui gestito, egli verrebbe reso destinatario di un dovere finalizzato non ad « impedire un evento », nella specie costituito dall'altrui condotta già verificatasi, ma solo ad attenuarne gli effetti[29]. Ancora, una parte della

---

[27] Il testo del decreto è riportato, a cura della *Internet-Zeitschrift für Rechtsinformatik*, in *http://www.jura.uni-sb.de/jurpc/rechtspr/19980017.htm* (consultato il 15 luglio 1998). Anche alla luce di tale provvedimento risulta incomprensibile la sentenza emessa dall'*Amtsgericht* di Monaco di Baviera il 28 maggio 1998, che (nonostante la richiesta di assoluzione del Pubblico Ministero!) ha condannato a due anni di reclusione e 100.000 marchi di multa il responsabile *pro-tempore* della CompuServe Deutschland GmbH per concorso nella diffusione di materiale pornografico. La sentenza — che ha suscitato accese critiche non solo nei settori più direttamente interessati ma anche a livello politico — è stata pubblicata nelle more della stampa di questo articolo, su *Multimedia und Recht* 1998, 429 ss., con una nota critica di U. SIEBER (che, nella vicenda processuale in oggetto, componeva il collegio di difese dell'imputato...).

[28] Per tutti, A. PAGLIARO, *Principi di diritto penale, pt. gen.*, Milano, 1996, 5ª ed., p. 371.

[29] Sul punto, v. Cass. 22 settembre 1994, Di Giovanni, in *Cass. pen.*, 1996, 79: « In materia di concorso di persone nel reato, la condotta consistente nel non impedire l'evento che si ha l'obbligo giuridico di impedire deve essere accompagnata dal dolo che caratterizza il concorso stesso, da ravvisarsi nella coscienza e volontà di concorrere con altri nella realizzazione di un reato comune, evidentemente prima della sua realizzazione ».

nostra dottrina ammette la configurabilità di posizioni di controllo solo in riferimento alla tutela di beni primari come la vita o l'incolumità fisica[30], ciò che ovviamente non ricorre per i delitti commissibili via Internet. Infine, per quanto specificamente concerne la configurabilità di posizioni di controllo relative all'altrui agire illecito, una diffusa opinione richiede alternativamente che il terzo (per minorità, malattia mentale o altra causa) non sia in grado di governare responsabilmente il proprio operato ovvero esista un potere giuridico di impedire la commissione di reati da parte di terzi[31], certamente insussistente rispetto al tema che ci occupa.

Come si vede, dunque, l'atteggiamento della dottrina italiana rispetto alla costruzione di posizioni di garanzia appare notevolmente più restrittivo di quello rinvenibile nella dottrina tedesca[32]. E a riprova di tale maggiore cautela può anche utilizzarsi il rilievo che la configurazione di una posizione di controllo del direttore di stampa periodica risulta in Italia solitamente impostata entro i limiti della responsabilità colposa espressamente sancita dall'art. 57 cod. pen., mentre la responsabilità dolosa per omesso controllo del concessionario di impianti di radiodiffusione e televisione viene delimitata ai reati di spettacoli osceni e di diffamazione aggravata, previsti dall'art. 30, commi 1 e 4, l. 6 agosto 1990, n. 223[33].

E non basta, poiché ulteriori difficoltà si presentano in ordine ai presupposti della responsabilità concorsuale del *provider*. Una volta ammesso che i reati (di condotta) fondati su verbi modali come diffondere, divulgare ecc. si consumano nel momento in cui i contenuti illeciti sono resi accessibili da parte del loro autore[34], una partecipazione del *provider* non può ravvisarsi né

[30] Così G. FIANDACA-E. MUSCO, *op. cit.*, p. 537 s.; *contra*, però, M. ROMANO, *op. cit.*, *sub* art. 40, 69.

[31] In questo senso, tra gli altri, G. FIANDACA-E. MUSCO, *op. cit.*, p. 556. La giurisprudenza solitamente accoglie la teoria giuridico-formale, secondo cui gli obblighi giuridici di impedire l'evento trovano i propri referenti « in una norma di legge o di regolamento e persino in una disposizione negoziale in forza della quale al soggetto si impone l'obbligo di attivarsi » (così Cass. 12 luglio 1994, Di Martino, in *Cass. pen.*, 1996, 80); applicazioni di questo principio sono ad esempio le sentenze che desumono dall'art. 2392 c.c. il concorso omissivo dell'amministratore di società in bancarotta fraudolenta (da ult., Cass. 27 maggio 1996, Perelli, in *Cass. pen.*, 1997, 2232) e dall'art. 1759 c.c. il concorso omissivo del mediatore nella truffa (Cass. 23 giugno 1989, Della Torre, in *Riv. pen.*, 1991, 224).

[32] A questo proposito, è sufficiente un rinvio alle soluzioni adottate, in tema di posizioni di controllo rispetto alle condotte di terzi, da H.-H. JESCHECK-T. WEIGEND, *op. cit.*, p. 627 s. e W. STREE, in A. SCHÖNKE-H. SCHRÖDER, *Strafgesetzbuch Kommentar*, München, 1997, 25ª ed., § 13 Rn. 51 ss.

[33] Per tutti, v. L. FIORAVANTI, *Statuti penali dell'attività televisiva*, Milano, 1995, p. 271 ss.; T. PADOVANI, in *Il sistema radiotelevisivo pubblico e privato*, a cura di E. Roppo e R. Zaccaria, Milano, 1991, p. 505 ss.

[34] A questo proposito, non sembra possa attribuirsi rilievo alla pur contestata distinzione tra perfezione e consumazione del reato (accolta, tra gli altri, da F. MANTOVANI, *Diritto penale, pt. gen.*, Padova, 1992, p. 427 e A. PAGLIARO, *op. cit.*, pp. 502 e 504; *contra*, per tutti, G. FIANDACA-E. MUSCO, *op. cit.*, p. 405 nota 1), poiché il ripetuto passaggio del testo attraverso al-

nel successivo mantenimento della disponibilità in rete di quei contenuti, né nella loro omessa cancellazione, in entrambi i casi trattandosi di condotte susseguenti la già avvenuta realizzazione del reato. Per quanto ovviamente qui si tratta di problemi che rinviano alla formulazione e all'interpretazione delle singole fattispecie incriminatrici, in linea generale sembra doversi ammettere che, nel nostro sistema, un concorso del *provider* nella diffusione di materiali illeciti da terzi direttamente immessi sul *server* da lui gestito risulta attualmente ammissibile solo qualora egli abbia una previa consapevolezza dell'altrui intenzione di commettere uno specifico reato e dolosamente intenda agevolarne la realizzazione, ciò che ad esempio ricorre nel caso di offerte di materiali a contenuto tematico altamente specifico e immediatamente riconoscibile nel suo carattere antigiuridico[35].

Alla luce delle conclusioni ora raggiunte, la ricezione nel nostro ordinamento della soluzione suggerita a livello comunitario e già adottata in Germania non assumerebbe una valenza meramente dichiarativa di principi generali già vigenti, risolvendosi al contrario nella previsione, nei confronti del *provider*, di un obbligo di soppressione — oggi inesistente — dei contenuti illeciti immessi da terzi sul *server* da lui gestito. L'introduzione di questa forma autonoma di responsabilità si accosterebbe così alle ipotesi di partecipazione criminosa punibile negli ambiti prima evidenziati e si porrebbe come un limite espresso rispetto ad ulteriori (ma non ragionevoli) doveri di attivazione.

Rispetto alla dibattuta alternativa tra legge e autoregolamentazione, il modello di disciplina in esame rappresenta a nostro avviso una adeguata conciliazione tra le opposte esigenze di garantire la libertà di comunicazione e manifestazione del pensiero su Internet e di apprestare una valida tutela ai beni aggredibili in rete.

8. Tutela dei dati personali e strategie di controllo per la prevenzione dei reati su Internet.

La globalità e l'interconnessione dei servizi e delle infrastrutture in rete impongono un approccio in grado di valorizzare e contemperare tutte le esigenze di tutela emergenti nei diversi settori. Come di recente ribadito anche da Rodotà, si tratta di « trovare quindi non solo regole specifiche per ciascuno di questi spazi,

---

tri *servers* o altri computer, come conseguenza della sua immissione in rete, si presenta come l'automatico svolgimento di un'azione di diffusione o distribuzione già conclusasi, sottratto alla signoria del soggetto agente.

[35] Cfr. S. Seminara, *op. cit.*, 101 s. e 107 ss.

ma regole di compatibilità, che impediscano ad esempio alla dinamica economica — che prende sempre più forza nella rete — di oscurare, non voglio dire di cancellare, le potenzialità di Internet come grande spazio pubblico di confronto e di discussione. (...) Dunque si tratta di tenere insieme le diverse questioni e di connetterle »[36].

In riferimento al nostro problema, le conclusioni precedentemente raggiunte in ordine all'impossibilità di costruire una responsabilità del *provider* come garante della liceità dei contenuti da lui resi accessibili al pubblico inducono a riflettere sul rapporto che intercorre tra il diritto dell'utente all'anonimato e il dovere del *provider* di apprestare i mezzi per l'individuazione degli autori di illeciti in rete.

A questo proposito, la contrapposizione tra i sostenitori di una regolazione a tappeto e di una *deregulation* integrale viene arricchita — e forse disvelata nelle sue più recondite motivazioni — dal contrasto tra quanti propongono la creazione di una chiave di accesso universale ai messaggi crittografati trasmessi in rete e quanti negano la sua ammissibilità alla luce del diritto individuale alla riservatezza[37]. Su un piano generale, può comunque ritenersi che, soprattutto in Europa, oggi prevale una soluzione fondata su una disciplina rispettosa dei diritti fondamentali ma non appiattita sul convincimento che le reti possano essere governate solo dalle logiche di mercato[38].

---

[36] Così S. RODOTÀ, *Libertà, opportunità, democrazia, informazione*, relazione presentata al convegno *Internet e privacy. Quali regole?* (Roma, 8 maggio 1998), il cui testo, non rivisto dall'A., è pubblicato in *http://www.privacy.it/garanterelrod.html* (consultazione effettuata il 15 luglio 1998).

[37] Il 27 marzo 1997, l'OCSE ha bocciato la proposta statunitense (sostenuta dalla Gran Bretagna e dalla Francia) di creare una chiave di accesso universale, in grado di decodificare tutti i messaggi trasmessi via Internet, allo scopo — si affermava nella proposta — di consentire a tutti gli organi investigativi del mondo di decifrare le comunicazioni in codice delle quali si ritiene che la criminalità organizzata e quella terroristica fanno ampio uso. Dinanzi all'alternativa tra diritto alla riservatezza ed esigenze di natura investigativa, i 29 Paesi aderenti all'OCSE hanno dunque rinviato a ciascun Stato membro il diritto di regolare discrezionalmente la materia delle comunicazioni in codice. La situazione, in effetti, è oggi estremamente confusa, poiché Gran Bretagna e Francia regolano in senso assai restrittivo l'uso privato di comunicazioni in codice, mentre nel resto d'Europa prevale un orientamento volto ad attribuire preminenza al diritto di riservatezza dei cittadini e delle imprese. Non esente da contraddizioni, infine, è la posizione degli USA, che permettono l'uso di sistemi di trasmissione in codice solo all'interno dei confini nazionali, rigorosamente vietando l'esportazione di tali tecnologie.

[38] Ne è significativa conferma la direttiva n. 97/66/CE sul trattamento dei dati personali e sulla tutela della vita privata nel settore delle telecomunicazioni, che i paesi UE devono recepire entro il 24 ottobre 1998 [ma v. già gli artt. 6(1)(c) e 7 della direttiva 95/46/CE e la raccomandazione del Consiglio d'Europa 7 febbraio 1995, n. R 95.4, sulla protezione dei dati personali nel settore dei servizi di telecomunicazioni]. In Italia, ove già l'art. 1, lett. *n*), legge delega 676/96 affidava al Governo il compito di sottoporre la comunicazione in rete ai vincoli della *privacy*, tale disciplina è stata introdotta con il d.lgs. 13 maggio 1998, n. 171 (v. la nota successiva).

Questo orientamento trova per un verso espressione nella garanzia apprestata alla riservatezza delle informazioni concernenti il « cittadino elettronico », anche sotto il profilo della conoscenza che altri possano avere dei siti da lui consultati, indipendentemente dal loro oggetto[39]; e, per altro verso, nelle misure — progettate e adottate — per l'individuazione degli autori di reati commessi in rete.

Fermando l'attenzione su quest'ultimo profilo, la più volte citata Proposta di risoluzione del Parlamento europeo, espressamente sottolineando l'utilità dell'anonimato su Internet, specie negli Stati in cui vigono regimi autoritari e repressivi, prospetta l'obbligo di identificazione degli utenti della rete. « Una simile situazione — si osserva — è conforme al principio democratico secondo il quale gli individui, pur restando liberi di esprimere i loro pareri, devono tuttavia essere tenuti responsabili dei loro atti. In questa prospettiva, il principio dell'identificazione legale (« reperibilità legale ») dovrebbe quindi essere incorporato nei codici di condotta nazionali ed europei. Qualora esistano tuttavia motivi legittimi perché un utente desideri rimanere anonimo (timori di rappresaglie per opinioni espresse o mancanza di fiducia per quanto riguarda l'utilizzazione che potrebbe essere fatta dal destinatario delle sue coordinate personali), bisognerebbe consentirgli di fare ricorso ad uno pseudonimo identificabile ».

---

[39] L'art. 2, commi 1 e 3, d.lgs. n. 171/1998 rispettivamente prescrive ad ogni « fornitore di un servizio di telecomunicazioni accessibile al pubblico » l'adozione delle misure tecniche e organizzative di cui all'art. 15, comma 1, l. n. 675/1996 per la salvaguardia della sicurezza del servizio e dei dati personali e la comunicazione agli abbonati della sussistenza di particolari rischi di violazione della sicurezza della rete. L'art. 4 ulteriormente stabilisce che i dati personali relativi al traffico possono essere sottoposti a trattamento solo da parte del fornitore del servizio, o da un suo incaricato, esclusivamente per finalità di fatturazione o di pagamento e sino alla fine del periodo (quinquennale) « durante il quale può essere legalmente contestata la fattura o preteso il pagamento ». Per quanto invece concerne la tecnica dello *spamming* (dall'inglese spalmare) — cioè l'invio di messaggi pubblicitari in posta elettronica a una moltitudine di sconosciuti —, l'art. 10 d.lgs. n. 171/1998 subordina al consenso espresso dell'abbonato « l'uso di un sistema automatizzato di chiamata senza intervento di un operatore o del telefax per scopi di invio di materiale pubblicitario o di vendita diretta, ovvero per il compimento di ricerche di mercato o di comunicazione commerciale interattiva », prevedendo per il caso di inosservanza le sanzioni di cui all'art. 35 l. 676/1995. Ma v. anche l'art. 26 del Regolamento di servizio concernente le norme e le condizioni di abbonamento al servizio telefonico, pubblicato con il d.m. 8 maggio 1997, n. 197: « 1. L'abbonato non può servirsi del proprio impianto per effettuare comunicazioni che arrechino molestia o che violino le leggi vigenti. 2. L'abbonato non può utilizzare il servizio in modo da creare turbativa ad altri abbonati. 3. L'abbonato si impegna a non consentire ad altri di utilizzare il suo telefono per telefonate moleste. 4. Il gestore ha la facoltà di sospendere immediatamente il servizio senza preavviso qualora l'abbonato ne faccia l'uso improprio indicato nei casi precedenti dandone, se del caso, idonea comunicazione alle autorità competenti ». Rispetto a quanto osservato nel testo in ordine alla garanzia di riservatezza delle informazioni concernenti il ''cittadino elettronico'', i più gravi timori sono però ingenerati dall'art. 14, l. 3 agosto 1998, n. 269, in tema di ''attività di contrasto'' verso i delitti di sfruttamento sessuale dei minori.

Tali principi — recepiti dal « Codice di autoregolamentazione per i servizi Internet », il cui § 4a dispone che « tutti i soggetti di Internet devono essere identificabili. Qualsiasi soggetto di Internet, una volta identificato, ha diritto a mantenere l'anonimato nell'utilizzo della rete al fine della tutela della propria sfera privata »[40] — hanno trovato un ulteriore sviluppo nella Raccomandazione n. 3/1997 adottata il 3 dicembre 1997 dal « Gruppo per la tutela delle persone fisiche con riguardo al trattamento dei dati personali », istituito dalla direttiva 95/46/CE del 24 ottobre 1995.

Anche qui la definizione del diritto all'anonimato come « essenziale se si vogliono mantenere nel ciberspazio i diritti fondamentali alla riservatezza e alla libertà di espressione » viene temperata 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 o le violazioni al diritto d'autore ». Tuttavia, la composizione di tale contrasto avviene all'insegna del « principio di proporzionalità come criterio fondamentale per valutare la conformità di eventuali misure restrittive applicate ai diritti fondamentali garantiti dalla Convenzione » europea di salvaguardia dei diritti dell'uomo, così esprimendo nel modo più chiaro il rapporto tra regola generale ed eccezione intercorrente tra il diritto all'anonimato e le sue limitazioni, che — così come per ogni altro strumento di comunicazione — devono risultare « debitamente giustificate, necessarie e proporzionate ».

In particolare, ad avviso dei redattori della Raccomandazione, il parallelismo istituito rispetto agli altri mezzi di comunicazione implica che i servizi anonimi di ritrasmissione di posta elettronica e gli accessi anonimi alla rete devono essere salvaguardati al pari dei servizi postali e telefonici, che consentono ancora maggiori possibilità di riservatezza; che la navigazione passiva, come pure l'acquisto di beni e servizi su Internet, devono svolgersi nel pieno anonimato allo stesso modo in cui, nel mondo non virtuale, è possibile girare per librerie o negozi senza dichiarare le proprie generalità; che i possibili abusi consentiti dalla partecipazione a *new-*

[40] Il § 5 ribadisce: « I soggetti devono consentire l'acquisizione dei propri dati personali a chi fornisca loro accesso e/o *hosting*. I fornitori di detti servizi sono tenuti a registrare i dati per renderli disponibili all'autorità giudiziaria nei termini previsti dalla legge. Una volta identificato, l'utente può chiedere al suo fornitore di accesso e *hosting* di avere un identificativo diverso dal suo nome (pseudonimo) con cui operare in rete (anonimato protetto) »; sugli obblighi dei fornitori relativi al trattamento dei dati, v. il § 7b. Analogamente dispongono la « Carta delle garanzie di Internet » (artt. 5 e 9) e il « Codice di deontologia e di buona condotta per i servizi telematici » (artt. 6 e 11).

sgroups o a *chat rooms* non legittimano in assoluto sistemi di identificazione obbligatori, che alla luce del criterio di proporzione possono essere sostituiti da strumenti più adeguati di controllo e moderazione del contenuto.

Questa chiara presa di posizione sui contenuti della tutela apprestata in sede comunitaria al diritto alla riservatezza, qui inteso come libertà di espressione del pensiero e della manifestazione della personalità, vale anzitutto a confermare la correttezza della disciplina adottata dal legislatore tedesco, la quale — come si è visto — evita di imporre al *provider* obblighi sproporzionati e soprattutto destinati a risolversi in gravose restrizioni apportate alla libertà di comunicazione su Internet.

Inoltre, essa ha il merito di focalizzare i contenuti delle misure adottabili per la prevenzione e la repressione dei reati commessi in rete alla luce della loro natura « debitamente giustificata, necessaria e proporzionata ». Senza qui soffermarci sui sistemi di filtraggio utilizzabili dai fruitori dei servizi[41], nell'attuale stadio dell'evoluzione tecnologica tali misure sembrano individuabili, da un lato, nell'obbligo per i *providers* di accertare l'identità degli utenti[42], dall'altro nella costituzione — già auspicata dalla citata Proposta di decisione 27 novembre 1997 del Consiglio relativa all'adozione di un Piano pluriennale d'azione comunitaria — di una rete europea di *hot-lines* che consentano agli utenti di segnalare i materiali illeciti da essi rinvenuti e così rendere consapevoli i *providers* dei contenuti immessi sui propri *servers* attivando il conseguente obbligo di soppressione.

È evidente che nessuna delle due misure sia in grado di svolgere un ruolo decisivo al fine di assicurare l'effettività dell'apparato sanzionatorio: non la prima, a causa della possibilità di ottenere l'accesso a Internet attraverso false generalità o alterando il proprio indirizzo elettronico o ricorrendo ai c.d. *anonymous remailings* ovvero — eventualmente utilizzando una *password* altrui — servendosi di computer siti all'interno di strutture pubbliche o private (Università, imprese, comunità, *computer coffee shops* ecc.), rispetto ai quali l'identificazione dell'autore del materiale

---

[41] L'art. 3 della Proposta, in particolare, prevede la promozione di sistemi di autodisciplina e di controllo dei contenuti da parte dell'industria, lo sviluppo di sistemi di filtraggio e valutazione da porre a disposizione degli utenti, la diffusione tra questi ultimi dell'informazione sui servizi offerti dall'industria, il sostenimento ad attività di concertazione sul piano giuridico e di cooperazione internazionale.

[42] Già prima dell'emanazione del d.lgs. 171/1998 era comunque prassi diffusa tra i *providers* la tenuta di un registro elettronico (c.d. *Log*) che, con procedure automatiche, consente di monitorare la durata degli accessi al servizio di connessione in rete e di memorizzare i siti raggiunti o visitati. Tale registrazione, oltre che per scopi tecnici di controllo sull'efficienza del sistema, serve anche a tutelare il fornitore sul piano contrattuale (al fine di dimostrare la durata degli accessi e la correttezza degli importi addebitati) che extracontrattuale (ad esempio, laddove intervenga una richiesta dell'autorità giudiziaria per verificare la commissione di illeciti da parte dell'utente).

si arresta all'individuazione del punto di partenza del messaggio[43]; non la seconda, il cui funzionamento presuppone non solo l'esistenza di organizzazioni preposte alla sistematica ricerca dei contenuti illeciti immessi in rete ma anche una cooperazione internazionale talmente diffusa da consentire l'integrale soppressione di tali materiali da tutti i *servers* accessibili dagli utenti.

La consapevolezza della limitata efficacia delle misure attualmente disponibili per la prevenzione dei reati su Internet non deve però indurre verso la ricerca di soluzioni alternative, inevitabilmente destinate a risolversi nella costituzione di obblighi penali di controllo a carico dei *providers*. Parafrasando una ricorrente affermazione e considerando l'attuale realtà normativa concernente gli altri più tradizionali strumenti di comunicazione, può affermarsi che ciò che non viene sottoposto ad oneri di controllo *off-line* non deve esserlo neppure *on-line*.

9. Armonizzazione internazionale del diritto penale e transnazionalità di Internet.

Il primo tentativo, su scala mondiale, di introdurre sanzioni nell'ambiente (fino ad allora) totalmente deregolamentato di Internet risale al 1º febbraio 1996, cioè all'emanazione negli Stati Uniti del *Telecommunications Act*. Tale statuto, che pur esordiva enunciando gli obiettivi di ridurre la regolamentazione e incoraggiare « il rapido sviluppo delle nuove tecnologie di telecomunicazione », si componeva di sette titoli, di cui il quinto (noto come *Communications Decency Act*) conteneva due precetti penali — il primo [47 U.S.C.A. § 223 (a) (Supp. 1997)] che proibiva la cosciente trasmissione di messaggi osceni o indecenti ad ogni destinatario minore di 18 anni, l'altro [§ 223 (d)] che vietava il consapevole invio o esposizione di messaggi manifestamente offensivi con modalità tali da renderli disponibili a persone minori di 18 anni — presidiati dalla pena, alternativa o congiunta, della multa o della reclusione non superiore a due anni.

Queste norme diedero vita ad asprissime polemiche, che il 12 giugno 1996 sfociarono in una decisione — presa all'unanimità, seppure ciascuno dei tre giudici scrisse un'opinione separata[44] — della *District Court for the Eastern District of Pennsylvania*, che decretò la temporanea sospensione del CDA. In particolare, la presidente Sloviter, pur riconoscendo l'interesse cogente ad una disciplina in materia, affermava che la legge « copre un am-

[43] V. sul punto O. Torrani-S. Parise, *op. cit.*, p. 124 ss.

[44] La sentenza è riportata in questa *Rivista*, 1996, 604 ss., con un commento di V. Zeno-Zencovich.

bito più esteso del necessario e spegne le comunicazioni tra gli adulti » e che i termini « manifestamente offensivo » e « indecente » risultano « intrinsecamente indeterminati ». Il giudice Buckwalter rilevava la medesima indeterminatezza, ravvisandovi una violazione del primo e quinto emendamento. Il giudice Dalzell sottolineava invece che le peculiarità della comunicazione su Internet impediscono al Parlamento di regolare il contenuto delle espressioni su tale *medium*.

La decisione, appellata dal Governo, è stata confermata dalla Corte Suprema con sentenza 26 giugno 1997 resa all'unanimità, seppure con un'opinione di due giudici in parte concorrente e in parte dissenziente dall'opinione manifestata dagli altri sette[45].

Nell'opinione della maggioranza, stesa dal giudice Stevens, si afferma « che il CDA manca della precisione richiesta dal primo emendamento quando una legge regola la libertà di parola. Negando ai minori l'accesso ad espressioni potenzialmente dannose, il CDA effettivamente sopprime un'ampia quantità di espressioni che gli adulti hanno il diritto costituzionale di ricevere e di inviare. Questa compressione della libertà di comunicazione fra adulti è inammissibile laddove esistano soluzioni alternative meno restrittive altrettanto idonee nel conseguimento degli scopi perseguiti dalla legge » (sul punto, si rileva — come già aveva fatto la *District Court* — che un metodo ragionevolmente accettabile è offerto dai *software* che impediscono ai minori l'accesso a determinati contenuti). « Dato il tipo di potenziale *audience* per la maggior parte dei messaggi — prosegue la decisione —, nell'assenza di un praticabile sistema di verificazione dell'età, ch li invia dovrebbe ritenersi responsabile se consapevole che uno o più minori saranno in grado di vederli. La conoscenza che, ad esempio, uno o più componenti di un *chat group* di cento persone sia un minore — onde sarebbe illecito inviare un messaggio indecente al gruppo — costituirebbe sicuramente un limite alla comunicazione tra adulti ». Per quanto infine concerne l'obiezione del Governo, secondo cui l'incontrollata disponibilità su Internet di contenuti indecenti e manifestamente offensivi sta allontanando innumerevoli cittadini

[45] Deve peraltro aggiungersi che, nell'immediata vigilia di tale sentenza, il presidente Clinton aveva manifestato la volontà di non insistere sui contenuti della legge contestata, ammettendo che « per le sue caratteristiche intrinseche, e soprattutto per non bloccarne le potenzialità, Internet non può essere soggetto a vincoli di censura di tipo normativo » e proponendo che « i compiti di vigilanza siano affidati alle famiglie, che già oggi hanno a disposizione tecnologie che consentono di limitare il flusso di informazioni a cui si può accedere con il personal computer domestico » (così il documento redatto dal consigliere del presidente Ira Magaziner: v. A. PLATEROTI, *La Casa bianca non censura Internet*, in *Il Sole-24 ore*, 17 giugno 1997, n. 165, 11, ove si riferisce che l'atteggiamento del presidente si spiega alla luce della volontà di non compromettere i rapporti con il mondo delle telecomunicazioni e il futuro del commercio *on-line*, che la stessa Casa bianca si era impegnata a promuovere).

dal *medium* a causa del rischio di trovarsi esposti essi stessi o i loro figli a materiale dannoso, così si conclude: « Noi troviamo tale argomentazione assolutamente non persuasiva. La vistosa espansione di questo nuovo mercato delle idee contraddice il suo contenuto fattuale. È dimostrato che la crescita di Internet è stata e continua ad essere fenomenale. E la nostra tradizione, in assenza di evidenza del contrario, ci induce a presumere che la disciplina governativa sul contenuto dell'espressione è idonea più a interferire con il libero scambio delle idee che a incentivarlo. L'interesse a promuovere la libertà di espressione in una società democratica prevale su ogni teorico ma indimostrato beneficio di una censura »[46].

È da notare tuttavia che la sentenza non ha modificato la legge contro il materiale « osceno » (che si distingue da quello indecente in base al linguaggio e alle immagini usate), sicché la pedofilia su Internet risulta oggi ammessa solo se debitamente mascherata, ma non se esplicita. Ed è proprio su questa base che si svolge l'opinione — in parte concorrente e in parte dissenziente — del giudice O'Connor, condivisa dal Presidente Rehnquist, secondo cui il CDA va considerato come qualcosa di più di un tentativo del Congresso per creare « *adult zones* » su Internet, legittimo nel suo scopo di tutelare i minori ma incostituzionale nella parte — e solo in essa — in cui indebitamente restringe l'accesso degli adulti al materiale. Ciò significa che, laddove tale restrizione non sia indebita, la legge risulta conforme al primo emendamento; tuttavia — prosegue l'opinione —, poiché gli utenti possono trasmettere e ricevere messaggi senza rivelare la loro identità o età, non è attualmente possibile escludere taluno dall'accesso a determinati messaggi in base alla sua identità. Vero è pure, però, che il ciberspazio differisce dal mondo fisico anche sotto un altro fondamentale profilo: la sua malleabilità, che consente di costruire barriere e di usarle per selezionare l'identità, ciò che a sua volta permette di costruire *zoning laws*. Questa possibilità di trasformazione del ciberspazio non è solo teorica, come dimostra la creazione della tecnologia *gateway* che richiede all'utente di fornire informazioni sulla propria persona prima di ottenere l'accesso; ovvero i *software* che i genitori utilizzano per limitare l'accesso dei figli in rete. La trasformazione non è però ancora completa, non essendosi estesa a tutti i servizi Web e non essendo obbligatoria. Donde la conclusione che, pur concordandosi con la Corte sulla necessità

[46] *Supreme Court of the United States*, 26 giugno 1997, no. 96-511 (Janet Reno, Attorney general of the United States, et al., appellants v. American Civil Liberties Union et al.), in *http://supct.law.cornell.edu/supct/html/96-511.ZO.html* (consultazione effettuata il 15 luglio 1998) la cui traduzione, a cura di V. Zeno-Zencovich, è in questa *Rivista* 1998, 64 ss.

di valutare la costituzionalità del CDA rispetto all'attuale situazione di Internet e di ravvisarvi una violazione del primo emendamento rispetto al diritto di espressione degli adulti, rimangono estranee le ipotesi in cui coloro che iniziano la comunicazione sanno che tutti i destinatari sono minori, sicché l'incostituzionalità del CDA andrebbe affermata solo rispetto alle comunicazioni cui partecipa più di un adulto, ritenendone al contrario la legittimità rispetto alle comunicazioni tra un adulto e uno o più minori.

La decisione della Corte Suprema, tanto nell'opinione di maggioranza che in quella di minoranza, poggia all'evidenza su basi sensibilmente diverse da quelle che trovano attualmente riconoscimento in Europa, ove anche a livello comunitario la libertà di manifestazione e comunicazione del pensiero viene invece ritenuta comprimibile attraverso l'obbligo, per i *providers*, di cancellare i materiali illeciti immessi sui loro *servers*. Né questo contrasto si presta ad una delimitazione territoriale, poiché la ritenuta inapplicabilità negli Stati Uniti di normative dirette a limitare il c.d. *free speech*, insieme alle caratteristiche tecnologiche della rete, consente di collocare in quel paese qualsiasi sito dai contenuti potenzialmente illeciti e così renderlo protetto dal primo emendamento della Costituzione americana.

Come si vede, dunque, se il riconoscimento dell'impossibilità di costruire una generale responsabilità dei *providers* in ordine ai contenuti illeciti immessi attraverso i servizi da essi forniti rinvia all'esigenza di affinare le possibilità tecniche di identificazione e persecuzione degli autori dei reati commessi in rete, a sua volta il conseguimento di questo obiettivo postula la necessità di individuare a livello internazionale un comune minimo denominatore di illiceità rispetto a specifici fatti, in modo da consentire la loro repressione ovunque essi siano realizzati. Ma — è appena il caso di rilevarlo — solo nel regno dell'utopia la globalità di Internet oggi può trovare corrispondenza nella globalità di un diritto « comune ».