IUS DICERE IN A GLOBALIZED WORLD

VOLUME ONE

Edited by
Chiara Antonia d'Alessandro
Claudia Marchese

Studies in Law and Social Sciences **3**

Studies in Law & Social Sciences

3

IUS DICERE IN A GLOBALIZED WORLD

A COMPARATIVE OVERVIEW

VOLUME ONE

Edited by

CHIARA ANTONIA D'ALESSANDRO

CLAUDIA MARCHESE

Roma TrE-Press

2018

Questo volume è stato realizzato con il contributo finanziario del Dipartimento di Giurisprudenza dell'Università degli studi Roma Tre e della Associazione Italiana di Diritto Comparato

Coordinamento editoriale:
Gruppo di Lavoro *Roma TrE-Press*

Elaborazione grafica della copertina: Mosquito mosquitoroma.it

Impaginazione: Colitti-Roma colitti.it

Edizioni: Roma TrE-Press ©
Roma, marzo 2018
ISBN: 978-88-94885-96-5

http://romatrepress.uniroma3.it

Università degli Studi Roma Tre – Dipartimento di Giurisprudenza

Studies in Law & Social Sciences

La collana *Studies in Law and Social Sciences* intercetta nuove frontiere nello studio del diritto italiano, del diritto di matrice europea e poi del diritto comparato e transnazionale. In questa prospettiva, ospita lavori che propongono una nuova lettura delle fonti del diritto, dei fenomeni giuridici, dei rapporti fra diritto e società, osservati sia con i tradizionali strumenti ermeneutici e sistematici del giurista, sia attraverso il prisma conoscitivo delle scienze sociali. La collana, aperta a lavori redatti anche in lingue straniere, è pubblicata su una piattaforma editoriale digitale *open access*.

The Roma TrE-Press Studies in Law and Social Sciences Series *sets itself at the crossroads of research in Italian and European law, and of comparative and transnational legal studies. It publishes groundbreaking work on legal issues, on sources of law and on the interactions between law and society. This perspective is pursued not only by using traditional tools of legal scholarship, but also through the application of the "Law and…" methodology. The series publishes studies in Italian and foreign languages and is hosted on an open access digital platform.*

Indice

Volume I

PROCESSO CIVILE, CLASS ACTION, ADR

NOVA REMEDIA DEL POTERE GIURISDIZIONALE

Enrico Maestri[*/**]

Giurisdizione e rete: effettività versus *legalità?*

Sommario: 1. Introduzione - 2. *Lex* informatica e sovranità digitali - 3. Modalità di regolazione della Rete - 4. *Lex* informatica e fonti del diritto - 5. Delocalizzazione e multi-giurisdizionalità del cyberspazio - 6. *Internet* e *soft law* - 7. Conclusione.

1. *Introduzione*

Uno dei vantaggi di Internet rispetto ad altri sistemi di comunicazione è certamente quello di consentire l'accesso all'uso di contenuti e di servizi digitali ad uno spettro di utenti pressoché universale: in un certo senso, una persona può essere ovunque nel mondo; per la creazione di rapporti intersoggettivi a carattere economico, politico e giuridico la distanza spaziale e i confini nazionali sono irrilevanti. Questa facilità di comunicazione solleva, però, una questione giuridica fondamentale: quando una persona naviga su un sito web o permette l'accesso al proprio server principale da ogni punto del globo, a quale regime giuridico fa riferimento? Al fine di decidere quale Stato e quali leggi governano le controversie che sorgono in Internet, con il sistema attuale, un tribunale deve prima decidere "dove" la condotta digitale si è concretizzata e "quando" si può dire che essa sia giuridicamente rilevante all'interno di uno Stato.

Questa visione *border-centric* della legislazione e della giurisdizione rischia di determinare la soccombenza del principio di legalità (il diritto come *Rule of law*) a favore del principio di effettività (il diritto come *Problem solving*). In tal senso le tutele apprestate dalle giurisdizioni nazionali e sovranazionali rischiano di affievolirsi per difetto di sovranità, diventando tutele dimezzate a causa del continuo mutamento delle norme tecniche di

[*] Un grazie particolare alla dottoressa Silvia Lucchiari, preziosa collaboratrice, per aver letto l'elaborato, aiutandomi a sviluppare meglio le idee portanti del lavoro.

[**] Professore associato di Filosofia del diritto presso l'Università di Ferrara. Attualmente titolare delle cattedre di Teoria generale del diritto (sede di Ferrara) e di Metodologia e logica giuridica (Polo di Rovigo).

soft law che regolano il *cyberspazio*[1].

Nei paragrafi che seguono si intende approfondire e discutere la seguente tesi generale: la *Lex informatica* è un'espressione che si riferisce alle scelte tecniche che impongono dei comportamenti agli utenti del web. Nel caso delle tecnologie informatiche, la relazione tra attori, azioni e diritto si dispiegherebbe attraverso logiche *bottom-up*: leggerezza dei vincoli, legami orizzontali tra le persone. La dislocazione spaziale non territoriale della comunicazione digitale trasforma la società in un modello organizzativo che presenta la forma di una rete globale, alla cui *governance* provvedono soprattutto forme regolative aventi natura giuridica di *soft law*.

In contrapposizione con questa potenzialità inclusiva, aperta e interattiva della rete Internet, emerge l'altra faccia dell'era dell'informazione caratterizzata da una lotta per il dominio della Rete, attuata attraverso la gestione e il controllo di Internet da parte di una "*corporate governance multi-stakeholder*", diretta da un *network* delle multinazionali della comunicazione informatica e telematica. La Rete diventa a un tempo centralizzata e decentrata, si adatta e si ripolarizza in una variazione infinita, eludendo il territorio, strutturando confinamenti immateriali dello "spazio globale". L'espressione *Code is law* (sinonimica a *Lex informatica*) dimostra come le architetture tecnologiche di Internet contengano codici e linguaggi normativi di auto-organizzazione che stabiliscono e controllano *ex ante* le regole per l'accesso e per l'uso delle informazioni disponibili in Rete. Nel caso della *Lex informatica*, il quadro normativo consiste nelle architetture tecnologiche e negli standard di rete; la giurisdizione è rappresentata dal *network* e dalle informazioni filtrate, regolate dai codici informatici, da una rete spaziale che travalica i confini territoriali e giurisdizionali degli Stati, essendo in grado di far compiere agli utenti determinate operazioni e pratiche reali che si usano in Rete.

2. Lex *informatica e sovranità digitali*

Il *code*[2]*,* ossia il software e l'hardware che costituiscono il cyberspazio, impone un assetto normativo sul comportamento individuale e collettivo

[1] J.R. Reidenberg, *Technology and Internet Jurisdiction*, in *University of Pennsylvania Law Review*, n. 153/2004, pp. 1951-1974.

[2] Per *code* (o *Lex informatica*) s'intende l'insieme dei protocolli informatici, del software, dell'hardware, degli algoritmi e del codice binario con cui i programmatori informatici strutturano ed architettano la Rete, stabilendo i vari modi d'uso delle tecnologie informatiche.

nel web.

Con ciò non si nega la funzione regolativa del diritto sul cyberspazio; si pensi ad esempio alle sanzioni previste dalle leggi sul *copyright*, sul diritto contrattuale, sulla diffamazione e sull'oscenità.

Pur tuttavia, è ormai inimmaginabile basare la gestione del web sulla continua evoluzione di paletti normativi preposti a ratificare e a *gregariare* l'implementazione e la diffusione di nuove tecnologie digitali. Internet rappresenta un universo di flussi e di attriti privo di qualsivoglia *governance* estranei ai propri utenti: basti pensare che, allo stato attuale, circa 30 *corporations* controllano il 90 per cento del traffico mondiale della rete. Gli *Internet Service Provider* (ISP), vera e propria spina dorsale della rete, preferiscono l'autogestione e l'autoregolamentazione a qualsiasi forma statale e sovranazionale di controllo giuridico[3].

Gli Stati, nel tentativo di riaffermare la propria sovranità digitale, cercano di monitorare, filtrare o proteggere i flussi digitali, ma i dati di Internet «sono replicabili all'infinito ed esistono in molteplici luoghi allo stesso tempo. Essi possono essere reindirizzati o inoltrati illegalmente a determinati destinatari, mentre i riceventi hanno la possibilità di eluderli, come pure di accedervi»[4].

Sulla base di tali premesse e in contrapposizione al riduzionismo normativistico, i cui sostenitori ritengono che il diritto continui a disciplinare compiutamente le attività digitale di ogni utente, si intende difendere la tesi che il *code* supplisce alle carenze endogene del diritto.

Lo sviluppo della Rete, d'altro canto, non è stato accompagnato da un *enforcement* giurisdizionale adeguato alla tutela dei nuovi diritti informatici; pur tuttavia le capacità tecnologiche e la progettazione dei sistemi informatici impongono *ex ante* regole sanzionatorie ai partecipanti.

L'assenza di frontiere fisiche nel cyberspazio determina il venir meno della territorialità, carattere intrinseco di un ordinamento giuridico, sicché appare impossibile delimitare l'ambito di operatività delle norme statali.

Facendo leva sull'ingannevole e fuorviante metafora del cyberspazio come luogo (*cyberspace as place*), i tribunali applicano alle e-mail e all'accesso ai siti web la dottrina dell'illecita turbativa del possesso di cose, da un lato ignorando che nessuno "entra" in un sito web[5] e dall'altro veicolando l'idea, errata e assurda al contempo, che Internet sia un luogo in cui viaggiare. In

[3] P. Khanna, *Connectography. Le mappe del futuro ordine mondiale*, Roma, 2016, p. 451.
[4] Ivi, p. 453.
[5] In tal senso, nella casistica giurisprudenziale, si vedano, ad esempio, *eBay, Inc. v. Bidder'sEdge, Inc.*, 100 F. Supp. 2d 1058 (N.D. Cal. 200); *Register.com, Inc. v. Verio, Inc.* 126 F. Suppl. 2d 238 (S.D.N.Y. 2000); *American Online v. National Health Care Discount, Inc.*, 174 F. Supp. 2d 890 (N.D. Iowa 2001).

realtà, nessuno si trova *nel* cyberspazio. Internet è un *non-luogo* logico e concettuale; più semplicemente è un protocollo, ossia una parte di codice che consente agli utenti di trasmettere dati fra computer tramite i network comunicativi esistenti[6].

La *Lex informatica* permette sia di stabilire norme specifiche per i flussi di informazioni veicolati sulla Rete sia di imporre politiche generali dei flussi e di automazione delle informazioni digitali. Attraverso le architetture tecnologiche (si pensi ai protocolli PICS[7]) la *Lex informatica* può vietare alcune azioni sulla Rete (come l'accesso) e imporre alcuni flussi informazionali (come il conferimento obbligatorio di dati di *routing* per l'invio dei messaggi elettronici).

Con riguardo alle modalità di affermazione dei linguaggi sociali e giuridici orizzontali della Rete, l'intromissione delle nuove tecnologie e il loro rapporto con l'adesione alla Rete, oltre a causare una separazione dal contesto geografico, fanno apparentemente emergere due traiettorie contrastanti.

Da un lato, Internet è uno spazio che stimola una forte spinta alla libertà e alla conoscenza, rivelando una capacità *dialettica* di squarciare i tradizionali spazi geopolitici territoriali che produce "cunei" di nuovi linguaggi e di nuove interazioni[8].

Dall'altro lato, in contrapposizione con questa potenzialità *comprendente*, la Rete, dominata da attori privati della globalizzazione tecnologica e della competizione economica[9], produce una "nebulosa normativa" implementata da un'architettura tecnologica stratificata (TCP/IP, DNS, PICS) di filtraggio, etichettatura e valutazione dei contenuti web[10]. Da questo punto di vista l'espressione "*Code is law*"[11], coniata da Lawrence Lessig, designa architetture tecnologiche di Internet già contenenti codici e linguaggi normativi di auto-organizzazione in grado di stabilire e controllare le regole per l'accesso e per l'uso delle informazioni disponibili in Rete[12]. Il

[6] M.A. Lemley, *Place and Cyberspace*, in *California Law Review*, n. 91/2003, p. 523.

[7] PICS – acronimo di *Platform for Internet Content Selection* – denota un codice che permette di filtrare, valutare e bloccare interi pacchetti di contenuti in Internet, associando etichette valutative (*rating*) alle pagine web e al contenuto delle pagine in base ad una determinata classificazione.

[8] P. Moro, *Topica digitale e ricerca del diritto. Metodologia e informatica giuridica nell'era dell'infosourcing*, Torino, 2015, pp. 6-8.

[9] E. Mostacci, A. Somma, *Il caso Uber. La sharing economy nel confronto tra common law e civil law*, Milano, 2016, p. 219.

[10] L.B. Solum, M. Chung, *The Layers Principle: Internet Architecture and the Law*, in *Notre Dame Law Review*, 3, 2004, pp. 815-948.

[11] L. Lessig, *Code and Other Laws of Cyberspace*, New York, 1999, pp. 3-9.

[12] C. Formenti, *Aporie del cosmopolitismo digitale*, in L. Tundo Ferente (a cura di),

web produce svariati strumenti di controllo atti a regolamentare l'azione dei soggetti e a limitarne le libertà: la registrazione degli utenti, le *password* di accesso, l'autenticazione, i *cookies*, i filtri sui contenuti, la tracciabilità degli indirizzi IP[13]. I movimenti di mercato hanno acquisito il monopolio nella produzione dei dispositivi di controllo del web, un tempo appartenente al potere statale, proprio perché si è realizzato che le tecnologie in grado di potenziare l'efficienza commerciale si attagliano maggiormente alla regolamentazione dei flussi[14].

3. *Modalità di regolazione della Rete*

Nonostante risulti difficile individuare un corretto inquadramento della natura giuridica del cyberspazio, secondo i sostenitori dell'approccio "normocentrico"[15] il diritto continua a disciplinare compiutamente le attività digitali di ogni cybernauta. Internet rinvia all'immagine di uno spazio virtuale, in cui la difficoltà risiede tanto nel definire le relazioni tra spazio reale e virtuale tanto nello stabilire come predisporre un diritto della Rete; esso, infatti, non può essere ancorato a uno spazio territoriale. Conseguentemente, occorre individuare linee di confine non più fisiche, ma inevitabilmente logiche. Ciononostante, è pur vero che dagli inizi degli anni Novanta ogni azione compiuta in Rete ha una disciplina di riferimento, spesso corredata da sanzioni anche gravi.

Non solo in Italia, ma anche nel resto del mondo l'evoluzione del diritto sulle nuove tecnologie ha via via normato tutti gli aspetti della vita digitale e dei comportamenti online, arrivando a toccare qualsiasi ambito.

Dunque, secondo i giuristi di diritto positivo, ogni attività che si svolge in Rete è disciplinata da una norma cui occorre prestare attenzione, perché «*la Rete è un luogo profondamente concreto e capace di accogliere nel suo seno, nel bene e nel male, le più umane esigenze*»[16].

In che misura *effettivamente* il diritto regoli il comportamento nel

Cosmopolitismo contemporaneo. Moralità, politica, economia, Perugia, 2009, pp. 311-325.

[13] L. Lessig, *Code Version 2.0.*,New York, 2006, p. 47 ss.

[14] A. Miconi, *Reti. Origini e struttura della network society*, Roma-Bari, 2011, p. 56 ss.; L. Lessig, *Code Version 2.0.*, cit., p. 61.

[15] Per l'espressione "normocentrismo", cfr. C. Sarra, *Le fonti del diritto e il problema dell'individuazione del giuridico*, Padova, 2002.

[16] P. Costanzo, *Internet* (voce), in *Digesto delle Discipline Pubblicistiche*, vol. XVIII, Torino, 2000, p. 349 ss.

cyberspazio è una questione a sé. Il diritto, comunque sia, «*continues to threaten an expected return. Legislatures enact, prosecutors threaten, courts convict*»[17].

Il cyberspazio è di per sé uno spazio del mondo reale, non solo perché da quest'ultimo può essere regolato, ma soprattutto perché gli utenti del cyberspazio vivono nella realtà fisica: «*Cyberspace is not, and never could be, the kingdom of mind; minds are attached to bodies, and bodies exist in the space of the world. And Cyberspace as such as does not preexist its users*»[18]. L'unicità del paradigma del *cyberspace as place* risiede nella particolare interazione che esso realizza tra potere normativo e progettazione tecnica (elemento qualificante di questo spazio, che va continuamente esaminata). È solo traducendo queste specificità in leggi e in politiche mirate che potrà avviarsi un progetto di regolazione del cyberspazio, ancorato a un approccio di carattere pragmatico[19].

In contrapposizione a questa prospettiva (il diritto "doma" il *code),* la corrente *cyber-libertaria* ha rivendicatola natura libertaria della Rete, qualificandola come un unico spazio virtuale che potesse e dovesse restare scevro da qualsiasi tipo di regolazione (*a-regulation or self-regulation*), specie se statale. John Perry Barlow, nella sua ormai mitica *A Cyberspace Independence Declaration* (9 feb. 1996), declama: «*Governi del Mondo, stanchi giganti di carne ed acciaio, io vengo dal Cyberspazio, la nuova dimora della Mente. A nome del futuro, chiedo a voi, esseri del passato, di lasciarci soli. Non siete graditi fra di noi. Non avete alcuna sovranità sui luoghi dove ci incontriamo*».

Le condotte sfuggono al controllo del governo in ragione dell'anonimità e della multigiurisdizionalità che connotano il cyberspazio: è la stessa natura dello spazio digitale a rendere *irregolamentabile* il comportamento.

In tal senso sono rivelatrici le riflessioni di Johnson e Post, secondo i quali: «*Cyberspace radically undermines the relationship between legally significant (online) phenomena and physical location. The rise of the global computer network is destroying the link between geographical location and: (1) the power of local governments to assert control over online behaviour; (2) the effects of on line behaviour on individuals and things; (3) the legitimacy of a local sovereign's efforts to regulate global phenomena; and (4) the ability of physical location to give notice of which sets of rules apply. The Net thus radically*

[17] L. Lessig, *The Law of the Horse: What Cyberlaw Might Teach*, in *Harvard Law Review*, n. 113/1999, p. 508.
[18] J.E. Cohen, *Cyberspace as/and places*, in *Columbia Law Review*, n. 107/2007, p. 218 ss.
[19] T. Wu, *Cyberspace sovereignty? – Internet and the International System*, in *Harvard Journal Law & Technology*, n. 3/1997, p. 658 ss.

subverts the system of rule-making based on borders between physical spaces, at least with respect to the claim that Cyberspace should naturally be governed by territorially defined rules»[20].

Il cyberspazio non sarebbe dunque uno spazio senza regole, bensì uno spazio distinto e diverso in cui le ormai delegittimate autorità pubbliche dei luoghi reali sono sostituite dagli utenti della Rete, che dettano per se stessi regole atte a realizzare i loro desideri e bisogni. Entrare nel cyberspazio, del resto, è un atto di volontà ben preciso che determina l'accettazione delle regole di Internet: «*No one accidentally strays across the border into cyberspace. To be sure, Cyberspace is not a homogenous place. Crossing into Cyberspace is a meaningful act that would make application of a distinct law of Cyberspace' fair to those who pass over the electronic boundary*»[21].

Ad avviso dei sostenitori del *cyber-libertarianism*, la *governance* del cyberspazio si costruisce dal basso (*bottom-up*): a dettare le regole sono gli stessi utenti, legittimati proprio dall'utilizzo della Rete. La legge, infatti, intesa come «*thoughtful group conversation about core values*»[22] persisterà, ma non potrà – e d'altro canto, nemmeno potrebbe – essere quella stessa applicabile a territori fisici e geograficamente definiti.

Presumere che l'architettura della Rete sarebbe fissata *by default* e il governo sarebbe incapace di adottare misure efficaci in grado di modificarla, rende in parte errata la credenza relativa all'architettura ontologica e normativa del cyberspazio.

Inoltre, a fronte di un approccio particolarmente attento alla struttura della Rete, essa non considera seriamente l'evidente ricaduta di tutte le attività che si svolgono *online* nel mondo reale[23].

Quando si visita il *cyberspace,* non si viaggia verso un luogo: anche nello spazio virtuale un comportamento antisociale è vietato e il soggetto che lo compie, ancorché *online*, resta soggetto alla diretta regolazione dello Stato di residenza[24].

Pur tuttavia, bisogna ammettere che la *self-regulation approach* del cyberspazio coglie una questione reale: la fonte primaria dello spazio in Rete rimane pur sempre un processo decentralizzato di adozione *volontaria* di standard tecnici da parte di operatori di rete (*Internet Service Providers*),

[20] D.R. Johnson, D. Post, *Law and Borders-the Rise of Law in Cyberspace*, in *Stanford Law Review*, n.48/1996, p. 1370, in www.cli.org/X0025_LBFIN.html.
[21] Ivi, p. 1379.
[22] Ivi, p. 1402.
[23] U. Kohl, *Jurisdiction and the Internet. Regulatory competence over Online Activity*, New York, 2007, p. 63.
[24] A. Murray, *Information Technology Law. The law and society*, Oxford, 2013, p. 56 ss.

piattaforme web (*Website Platforms*) e comunità degli utenti (*Virtual Communities*). L'esistenza di differenti sotto-comunità di utenti determina l'eterogeneità delle regole applicabili, tra loro antinomiche. Tali antinomie normative sono superabili mediante l'accesso ad altre e diverse aree della Rete da parte di coloro che non dovessero condividere un determinato corpo di regole vigente in un determinato Stato.

In accordo con l'approccio teorico-giuridico elaborato da Lawrence Lessig, si ritiene che l'architettura del cyberspazio non sia fissata *by default*, bensì in funzione del *design* (*rectius:* del suo *code*). Il *code* è mutevole: potrebbero essere il governo o il mondo delle multinazionali a determinarne una particolare evoluzione. L'architettura del cyberspazio è neutrale. Laddove le architetture del *code* incidono sui vincoli giuridici, questi finiscono per soppiantare anche i valori del diritto.

L'utilizzo dell'architettura per regolare la condotta implica la disarticolazione dei principi stessi su cui si fondano gli ordinamenti giuridici costituzionali contemporanei.

Si pensi ad un virus, tecnicamente un *worm*, che sia in grado di propagarsi a tutti i computer connessi in rete e che riporti alle forze dell'ordine l'eventuale presenza nella memoria fisica di un computer infettato di materiale in un qualche modo vietato, ad esempio immagini di pornografia infantile o piani di attacchi terroristici. Qualora il virus non trovi alcunché di rilevante, in base ai criteri di ricerca predeterminati, esso provvederà ad autodistruggersi. Qui il *code* rappresentato dal virus *worm* si atteggia come un vero e proprio agente morale.

Inoltre, per un sito che accetta il traffico utente, ogni richiesta di accesso ai contenuti è identica alle altre: l'architettura fondamentale del cyberspazio garantisce l'invisibilità alle caratteristiche dell'utente.

In tal senso, in un contesto specifico quale quello del cyberspazio, l'influenza dell'architettura sul diritto – e sul comportamento degli agenti – è particolarmente rilevante, forse più di altri ambiti.

In particolare, proprio a partire dalla chiave di lettura cibernetica, il rapporto fra diritto e architettura emerge come il perno centrale nella configurazione dei comportamenti possibili nel cyberspazio[25]. Ciò non significa, peraltro, che in altri contesti l'architettura non sia uno strumento indispensabile di controllo, ma in un contesto digitale essa diventa un vincolo quasi pervasivo al comportamento[26].

[25] D. Tambini, D. Leonardi, C. Marsden, *Codifying Cyberspace. Communications self-regulation in the age of Internet convergence*, London, 2008, p. 12 ss.

[26] M. Goldoni, *Politiche del codice. Architettura e diritto nella teoria di Lessig*, in *Archivio Marini*, 2007, p. 5 ss.; consultabile in www. archiviomarini.sp.unipi.it/350/1/lessig.pdf.

Nel caso della proprietà intellettuale digitale, ad esempio, il *code* appare *sovrainclusivo* rispetto alla normativa giuridica: quest'ultima favorisce un'implementazione architettonica del *code* tale da favorire i detentori di cospicue percentuali di proprietà intellettuale, così esentando le multinazionali delle telecomunicazioni dalle responsabilità di servizio universale e condivisione delle reti. Nel campo del *copyright* l'architettura digitale, cioè il modo con cui le tecnologie disegnano *ex ante* lo spazio di comportamento degli utenti, ha progressivamente ristretto i margini di libertà (*fair use*) delle scelte individuali.

La società post-Internet determina un'intensificazione della normativa sul *copyright* digitale, posta a sostegno delle grandi imprese produttrici di contenuti digitali: la normativa, infatti, inizia a disciplinare minuziosamente i comportamenti dell'utente-cittadino-consumatore (c.d. *netizen*). Il diritto interagisce col *code* (*co-regulation*)[27], vietando sia l'aggiramento delle protezioni tecnologiche sia la produzione di tecnologie finalizzate all'elusione delle protezioni medesime[28]. L'architettura, rappresentata dal sistema numerico binario, diventa un vincolo fortissimo per l'individuo, massimamente invasiva delle sue capacità di azione: la proprietà digitale diviene proprietà mimetica dell'architettura (ogni utilizzo di un'opera creativa si trasforma automaticamente in una copia) e pone ora controlli e regole, influendo su legge e mercato[29]. Ad avviso di Lessig, d'ora in poi i controlli sull'accesso ai contenuti non saranno ratificati dai tribunali, ma verranno inseriti dai programmatori tramite il *code*. Diversamente dai controlli introdotti per legge, quelli inseriti dalla tecnologia non formano oggetto di verifica giudiziale[30]. D'altronde, mentre la regola legislativa risulta verificabile e contestabile, altrettanto non può dirsi per la regola tecnologica[31].

Lessig porta l'esempio del caso *Mattel, Inc. v. Cphack*[32] per dimostrare

[27] T.E. Frosini, *Internet come ordinamento giuridico*, in *Percorsi costituzionali*, n. 1/2014, p. 13 ss.

[28] R. Caso, *L'"immoralità" delle regole tecnologiche: un commento alle teorie degli studiosi Burk e Gillespie*, in G. Ziccardi (a cura di), *Nuove tecnologie e diritti di libertà nelle teorie nordamericane*, Modena, 2007, p. 38 ss.

[29] Ad esempio, il sistema delineato dal *Digital Rights Management* (DRM) impone di fatto clausole contrattuali e condizioni d'uso restrittive dell'utilizzo del bene digitale. Attraverso un controllo pervasivo ed invasivo della *privacy* del consumatore, è il titolare del contenuto, prima e più del legislatore, ad impostare i termini dell'equilibrio tra interesse economico proprietario e fruizione del contenuto.

[30] L. Lessig, *Cultura libera: un equilibrio fra anarchia e controllo, contro l'estremismo della proprietà intellettuale*, Milano, 2007, p. 124 ss.

[31] R. Caso, *L'"immoralità" delle regole tecnologiche: un commento alle teorie degli studiosi Burk e Gillespie*, cit., p. 43.

[32] United States Court of Appeals, First Circuit. Microsystems software inc v. Scandinavia

come il software censorio *Cyber Patrol*, ideato dalla Mattel, presenti un'architettura di filtraggio, diretta a impedire l'apertura delle pagine dei siti ritenuti inadatti sul personal computer degli utenti. Quest'architettura estende arbitrariamente i limiti costituzionali del *copyright*, aggirando le garanzie approntate dal Primo emendamento e rendendo, perciò, vana la salvaguardia della *fair use clause*.

Nel caso *Cphack*, la Mattel controllava una società che vendeva *Cyber Patrol*, un software censorio che, in base a determinati contenuti, permetteva di bloccare siti internet.

Il *code* di *Cyber Patrol* non metteva, però, gli utenti in condizione di conoscere i siti e i contenuti bloccati; inoltre, conteneva specifici filtri preimpostati, che l'amministratore non avrebbe potuto autonomamente attivare o disattivare. Nel 1999 due programmatori, lo svedese Eddy Jansson e il canadese Matthew Skala, decisero di elaborare un programma che permettesse di superare i problemi posti da *Cyber Patrol* e di aggirare il *censor software* creato dalla Mattel.

Così, i due programmatori svilupparono *Cphack*, un programma che consentiva agli utenti di disattivare Cyber Patrol e di visualizzare, tramite la tecnica del *reverse engineering*[33], i siti bloccati dal censore.

Per tentare di eliminare il software *Cphack,* la Mattel reagì intraprendendo un'azione giudiziaria.

Dapprima aggiunse, alla lista dei siti bloccati dal *censor software,* gli indirizzi dei siti che mettevano a disposizione il programma di Jansson e Skala; successivamente, si rivolse alla Corte Federale statunitense e sporse querela contro i due programmatori e contro l'associazione per i diritti civili *Peacefire* che li sosteneva, chiedendo un'ingiunzione idonea a inibire la distribuzione del codice e la sua circolazione sul web. Mattel accusò Jansson e Skala di aver violato il copyright. Nell'atto depositato davanti ai giudici, l'azienda sosteneva che, sottoponendo a *reverse engineering* il codice di *Cyber Patrol,* i propri diritti d'autore erano stati violati: si trattava di una procedura posta in essere in violazione della licenza con cui il programma era venduto agli utenti. Per cui, l'uso di *Cphack* era illegale: pur essendo permesso dalla legge, esso risultava contrario alla licenza di vendita; benché nel caso di specie Jansson e Skala non avessero acquistato una copia di *Cyber Patrol*.

I giudici della *Seventh Circuit Court of Appeals* accolsero la richiesta della Mattel e, nello stesso giorno, emisero un'ingiunzione temporanea, finalizzata a far cessare la distribuzione del programma.

online AB, n. 00-1503, 27 september 2000.

[33] Il *reverse engineering* è una tecnica di decifratura in modo che il fruitore sappia che a una specifica sequenza di bit corrispondono lettere, parole e simboli (analogici).

Al di là delle modalità di risoluzione del caso (Mattel comprò i diritti di privativa di *Cphack*!), l'argomentazione addotta dalla Mattel si reggeva implicitamente sulla potenziale capacità del *code* di essere *sovrainclusivo* rispetto al diritto. Infatti, l'essenza del *copyright* consiste nel proteggere gli autori da potenziali furti: significa proteggere la Mattel, ad esempio, da chi dovesse rubare *Cyber Patrol,* per poi utilizzarlo senza averlo pagato. Solitamente, il *copyright* non è finalizzato alla protezione degli autori da critiche (*fair use*). Proibire la critica di quanto è stato fatto in passato non equivale a promuovere il progresso, ma questo era esattamente lo scopo per cui la legge veniva usata in questo caso. Affermare che un contratto, allegato al codice giuridico di *copyright,* bandiva un utente dal criticare il *code* (senza copiare alcunché dall'originale) equivaleva ad utilizzare la legge per limitare le critiche.

Se la legge sul *copyright* deve proteggere il materiale sotto *copyright* e, al contempo, anche il *fair use*, ne consegue che le leggi poste a tutela del *code* (ad esempio, la clausola antielusione prevista dal *Digital Millenium Copyright Act*), a sua volta preposto alla protezione del materiale sotto *copyright*, dovrebbero lasciare spazio al *fair use*. Il caso *Mattel vs Cphack* dimostra esattamente il contrario: il *Digital Millenium Copyright Act* ha permesso che il *code* desse origine a forme ibride di *enforcement,* che il codice legale del copyright non poteva garantire a causa dei vincoli imposti dalla Costituzione e dai principi del Primo emendamento.

4. Lex *Informatica e fonti del diritto*

In Internet il diritto è veicolato attraverso il mezzo tecnico: il *code* non è una legge e non è soggetto a limiti costituzionali, ma trova la sua copertura nella legge e funziona *de facto* come una legge, garantendo a volte maggiore efficacia. Il *code* è una delle inedite forme del *soft law*: una serie di atti, disomogenei quanto a origine e natura ma in vario modo giuridicamente rilevanti, benché privi di effetti giuridici vincolanti[34]. È così che il *code* diventa legge: violare i controlli inseriti nelle tecnologie di protezione e di regolazione dell'accesso in rete equivale a violare *ex ante facto* la legge. L'evoluzione del "*code as law*" in "*code si law*" ha determinato un'anticipazione del momento esecutivo della sanzione. A ben vedere, non solo la tutela diviene preventiva (basata unicamente sulla sussistenza del

[34] M.R. Ferrarese, *Diritto sconfinato. Inventiva giuridica e spazi nel mondo globale*, Roma-Bari, 2006.

duplice requisito del *fumus commissi delicti* e del *periculum in mora*), ma viene aggirata la fase accertativa.

Gli schemi di controllo dei diritti digitali, ad esempio, possono inibire l'accesso al contenuto digitale dopo un certo numero di letture; possono controllare i luoghi nei quali il prodotto viene visualizzato; possono richiedere che il contenuto sia visto in un certo ordine, e così via[35].

È dunque evidente che la tutela preventiva approntata dal provider assuma funzione repressiva più che sanzionatoria, dimostrando come, sul web, la separazione dei poteri sia stata ampiamente superata in favore della titolarità di un unico soggetto che commina ed irroga la sanzioni, con notevole anticipazione della soglia della punibilità. Infine, occorre forse riflettere sull'ambivalente natura di questo genere di tutela: estremamente effettiva, ma scricchiolante sotto il profilo delle garanzie; infatti, non richiedendosi l'effettiva commissione di un illecito al fine di irrogare le sanzioni, ma solo un pericolo presunto di commissione del medesimo, lasciato alla valutazione discrezionale del provider, potrebbero sanzionarsi condotte anche prive di potenzialità offensiva: il *code*, dunque, diverrebbe un diritto finalizzato alla tutela di beni giuridici dal pericolo di lesioni, non più dal danno effettivo.

Le categorie giuridiche tradizionali si sgretolano sotto il peso delle continue innovazioni tecnologiche. Il diritto nel mondo digitale diviene tecnologicizzato, assumendo caratteristiche del tutto peculiari rispetto a quelle assunte nel mondo reale. La tecnica digitale, di cui il *code* è un prodotto, viene assunta come disciplina dei rapporti digitali: il software ed i protocolli permettono la connettività alla rete, ma la loro essenza è una complessa sequenza di bit – zero e uno – che riduce le effettive possibilità per l'utente-cittadino-consumatore (c.d. *netizen*), che naviga nella Rete, di operare in maniera libera e consapevole.

Il diritto non insiste più su un territorio, ma agisce su una rete di relazioni, si plasma globalmente senza soluzione di continuità nell'unico vasto territorio virtuale che copre l'intero pianeta: Internet.

La Rete, che incide sulla configurazione delle fonti del diritto contemporaneo, è l'infrastruttura della globalizzazione.

Il diritto digitale segna irreversibilmente la crisi della sovranità dello Stato: la rigidità del diritto statale si rivela incapace di regolare le nuove modalità delle azioni umane; la destatualizzazione e la delocalizzazione producono un diritto flessibile, che si adatta al modello reticolare del

[35] L. Lessig, *Il futuro delle idee*, Milano, 2006, pp. 181-184. Per un approfondimento sul caso *Cphack*, rinvio a G. Ziccardi, *Libertà del codice e della cultura*, Milano, 2006, pp. 57- 62.

mondo digitale[36].

Sia a livello transnazionale sia a livello internazionale si è venuta a creare una rete di attori globali che concorrono alla creazione del diritto, così sottraendo la potestà legislativa agli Stati nazionali: realtà ormai troppo grandi per confortare la socializzazione primaria e insieme tragicamente troppo piccole per contenere le derive del *networking*[37].

Tra i fattori che hanno concorso all'erosione delle quote di sovranità statale figura la crisi del rapporto di identificazione tra stato e diritto «che ha portato ad assegnare al diritto un carattere territoriale (il territorio è il luogo della sovranità statale). Diversamente, nell'età della globalizzazione, la territorialità tende ad essere sostituita dalla categoria della spazialità. La spazialità è la categoria con la quale il diritto ha affrontato l'interconnessione»[38]. A ben vedere, è la *Lex informatica* a fornire le regole tecniche per realizzare l'interconnessione, poiché la tecnologia attivata dal *code* garantisce una operazione *generativa* di spazio e una *virtualizzazione infinita* delle pratiche sociali.

Internet è il più grande spazio pubblico che il mondo abbia mai conosciuto, un multiverso artificiale di informazioni, uno spazio di vastità imperscrutabili, popolato da oggetti che vanno dalle particelle subatomiche (bit) a tentacolari superammassi di galassie (Google, Facebook, Instagram, ecc.). La confusione tra reti digitali di proprietà privata e spazio digitale pubblico, i molteplici significati di commercializzazione della Rete, l'estrema variabilità configurativa del web hanno fatto sì che il *code* si sviluppasse in modi diversi e sempre più legati alla privatizzazione. Gli utenti, ormai sempre più consumatori, sono diventati sempre meno partecipi dello sviluppo e della diffusione di idee[39]. Come acutamente osservato da Saskia Sassen: «Prima del 1995 […] l'architettura di Internet impediva lo *zoning*, ossia qualsiasi tecnica che faciliti la discriminazione degli accessi o la distribuzione di qualche bene o servizio. Ciò è cambiato con la tendenza a facilitare il commercio elettronico […]. Ciò ha privatizzato lo sforzo di

[36] S. Bertea, C. Sarra, *Dialettica del precedente. Appunti per una collocazione teorica dell'uso del precedente straniero*, in *Ars interpretandi*, n. 1/2016, p. 38.
[37] A. Miconi, *Reti. Origini e struttura della network society*, cit., p. 85.
[38] E. Pariotti, *La giustizia oltre lo stato: forme e problemi*, Torino, 2004, p. 42.
[39] Come osserva lucidamente Somma in merito alla *soft law* come dispositivo ordoliberale: «*Si determina una armonizzazione delegata ad un processo competitivo, inesorabilmente destinata a far soluzioni dannose per i contraenti deboli e in prospettiva ad affossare le politiche sociali nazionali*»; cfr. A. Somma, *Some Like It Soft. Soft law e hard law nella costruzione del diritto privato europeo*, in Id. (a cura di), *Soft law e hard law nelle società postmoderne*, Torino, 2009, p. 167 ss.

disegnare regole per Internet»[40].

Tra il *provider* della struttura informatica e gli utenti si realizza un implicito baratto: l'utente che vuole utilizzare la piattaforma del provider e creare il suo spazio virtuale deve cedere i propri dati al provider proprietario della piattaforma.

Ciò comporta una vera e propria mutazione genetica del trattamento dei dati e della loro concezione, poiché essi entrano a fare parte di quella immensa rete di calcolo che è Internet, passando da componente fondamentale per la costruzione della *personalità digitale* dell'individuo a valore immateriale di scambio. Ogni informazione digitale è riproducibile a costi marginali: facendo un uso massiccio delle licenze a strappo (*Shrink-Wrap License)*, in cui l'accettazione da parte dell'obbligato di tutte le previsioni opera come finzione, le *corporations* che detengono e difendono i diritti di proprietà intellettuale dal *fair use* trasformano le informazioni digitali in un "bene scarso" da cui trarre profitto.

I soggetti che operano in Internet e che possiedono fisicamente i server al cui interno è salvato il codice del software, successivamente offerto agli utenti, si atteggiano quali piccole *nazioni digitali*, in cui si concentra un gran flusso del traffico dati.

La *costituzione digitale* di queste *cyber-nazioni* è rappresentata dalle condizioni generali del contratto[41], vere e proprie clausole vessatorie, con cui i *sovrani digitali* stabiliscono unilateralmente le regole di comportamento da seguire all'interno dei firewall elettronici del proprio spazio web, nonché le modalità di trattamento dei dati personali immessi volontariamente nel loro database dall'utente al momento dell'iscrizione o produzione dei contenuti voluti.

5. *Delocalizzazione e le giurisdizioni del cyberspazio*

La Rete non conosce la localizzazione delle parti di una transazione *online*: non utilizza indirizzi localizzabili in un determinato territorio, non fu creata per l'identificazione geografica dei suoi utilizzatori, né la prevede. Internet fa uso di indirizzi che non hanno un collegamento con il mondo reale, ma che individuano gli utilizzatori del computer da qualche parte nel cyberspazio.

Si potrebbe controargomentare che tali indirizzi contengono informazioni

[40] S. Sassen, *Territorio, autorità, diritti. Assemblaggi dal Medioevo all'età globale*, Milano, 2008, p. 421.

[41] Sulla privatizzazione dello spazio giuridico comune, cfr. A. Somma, *Introduzione critica al diritto europeo dei contratti*, Milano, 2007, p. 69 ss.

per la localizzazione geografica (paragonando in questo modo l'indirizzo IP alla targa di un'automobile del cui conducente non conosciamo l'identità[42]), ma questa non è la regola; difatti, non c'è un rapporto necessario e logico tra un terminale (avente uno specifico indirizzo IP – *Internet Protocol*) e la persona. Si tratta, piuttosto, di un'eccezione rispetto ad una moltitudine di indirizzi (a volte statici, altre volte dinamici, altre volte ancora coperti per mezzo di *proxy server* o da *anonymous remailers*), che si limitano ad indicare solamente la tipologia del titolare della pagina web o il tipo di attività che questo svolge.

Nonostante le innumerevoli difficoltà poste dalla caratterizzazione transnazionale delle nuove tecnologie informatiche, in una conferenza tenuta all'Università di Chicago sul diritto del cyberpazio nel 1996 il giudice Frank Easterbrook affermò che come non vi era mai stato alcun bisogno di un diritto del cavallo, così non vi sarebbe stato alcun bisogno di ricorrere ad un sistema giuridico alternativo, creando un diritto del cyberspazio. Secondo il giudice Easterbrook, solo lo sforzo di parlare di un siffatto diritto avrebbe provocato confusione: infatti, i professori di diritto avrebbero fatto meglio a mettersi da parte, evitando in tal modo di rendersi protagonisti di una sorta di "*multidisciplinary dilettantism*"[43].

In tono provocatorio verso l'uditorio presente al congresso, egli affermò: «*I regret to report that no one at this Symposium is going to win a Nobel Prize any time soon for advances in computer science. We are at risk of multidisciplinary dilettantism, or, as one of my mentors called it, the cross-sterilization of ideas. Put together two fields about which you know little and get the worst of both worlds*»[44].

Continuò poi in termini perentori: «*And if I did know something about computer networks, all I could do in discussing "Property in Cyberspace" would be to isolate the subject from the rest of the law of intellectual property, making the assessment weaker*»[45].

Alla domanda "perché non ci dobbiamo occupare del diritto del cavallo, allo stesso modo in cui non ci dovremmo occupare del diritto del cyberspazio?", il giudice Easterbrook rispose affermando che i corsi di diritto si dovrebbero occupare solo di istituti che possano illuminare l'intero diritto: perché scrivere un diritto del cavallo, quando esistono regole generali che si

[42] F. Cajani, *Internet Protocol. Questioni operative in tema di investigazioni penali e riservatezza*, in *Diritto dell'Internet*, n. 6/2008, p. 545 ss.
[43] F.H. Easterbrook, *Cyberspace and the Law of the Horse*, in *University of Chicago Legal Forum*, 207, 1996, pp. 207-216.
[44] Ibidem.
[45] Ivi, p. 207.

occupano di proprietà, di *torts*, di transazioni commerciali e così via?

Il ragionamento del giudice dimostra che egli aderiva ad un approccio indicato con l'espressione "*Digital Realism*" (o "*Conservative Approach*"), che rappresenta tuttora il più importante metodo nello studio delle forme di regolazione del cyberspazio.

Cercherò di spiegare in che cosa sostiene quest'approccio e quali sono le ragioni che lo rendono debole e inidoneo a regolare Internet.

Sulla scorta delle riflessioni svolte da Lawrence Lessig in risposta al giudice Easterbrook, vorrei prima dimostrare, però, che è possibile riferirsi ad un principio metodologico generale che giustifica lo studio del diritto del cyberspazio, nonostante la particolarità di esso, al quale si legano questioni proprie tanto del mondo degli atomi quanto del mondo dei bit[46].

Detto principio generale riguarda i limiti del diritto come norma e le tecniche per eludere quei limiti. Tale elusione nello spazio reale e in quello cibernetico proviene dal riconoscimento della gamma di strumenti che una società possiede per stabilire costrizioni sul comportamento. Il diritto nel suo senso tradizionale, inteso come norma sanzionata, è solo uno di questi strumenti.

In base all'idea in generale della "nuova scuola di Chicago", il diritto può avere un effetto su questi ultimi, affinché essi impongano un comportamento stabilito e fungano essi stessi da strumenti del diritto. Ovviamente, la scelta fra gli strumenti dipende dalla loro efficacia. Ora, se concentriamo la nostra attenzione sulle regole inerenti il cyberspazio, è possibile osservare cose che altre aree non ci mostrerebbero.

Da un lato, questa metodologia ci permette di comprendere i grossi limiti in cui incorre il *Digital Realism,* laddove opera una perfetta simmetria tra accadimenti e comportamenti del mondo reale e quelli del cyberspazio; dall'altro, essa mette in luce gli esiti, spesso paradossali, a cui giunge la giurisprudenza nell'elaborare test o criteri di competenza giurisdizionale che allargano fittiziamente la territorialità anche su azioni, eventi e conseguenze la cui concretizzazione avviene in un *non-luogo* (principio di ubiquità, teoria del frammento del reato, ecc.): un *non-luogo* logico e concettuale, qual è il Web.

Il modello predisposto da Lessig comprende quattro "strumenti" in grado di intervenire direttamente o indirettamente sulla regolamentazione dei comportamenti.

Il primo di questi elementi viene dalla tradizione giuridica classica: il diritto rimane un elemento importantissimo per intervenire direttamente

[46] O. Pollicino, *La 'transizione' dagli atomi ai bit nel reasoning delle Corti europee*, in *Ragion pratica*, n. 1/2015, pp. 53-82.

sui comportamenti.

Il secondo strumento di regolamentazione è costituito dalle norme, intese come norme sociali e morali, senza alcuna caratterizzazione giuridica.

Il terzo genere di vincolo al comportamento è costituito dal mercato: esso controlla l'accesso o la possibilità di compiere una determinata azione, in particolare attraverso i prezzi stabiliti, per ottenere un qualsiasi genere di bene o servizio.

Il quarto strumento di regolamentazione è l'architettura intesa in senso lato, ossia come organizzazione di uno spazio di qualsiasi genere attraverso l'utilizzo dei materiali che si hanno a disposizione. In un certo senso, l'architettura costituisce la "natura" di un contesto: l'elemento architetturale a volte può essere immodificabile; più spesso, invece, può essere modificato per rivedere l'assetto organizzativo dello spazio interessato.

Ad esempio, il fatto, in sé banale, che una strada venga interrotta per il crollo di un ponte cambia il corso delle azioni umane; oppure la costruzione di una determinata architettura è coessenziale ad una serie di valori e di scopi precisi. Così, per riprendere alcuni degli esempi proposti da Lessig, la ricostruzione di Parigi nel 1853, ordinata da Napoleone III, venne decisa nella consapevolezza che ampi *boulevards* avrebbero reso più difficile l'organizzazione delle rivolte.

I quattro *constraints* al comportamento vengono esercitati in maniera diversa a seconda dei contesti.

Inoltre, i primi due vengono di solito esercitati *ex post*, mentre gli altri due sono generalmente strumenti a cui si ricorre *ex ante*. Questi quattro vincoli possono influenzarsi a vicenda ed agire l'uno sull'altro. In ogni caso, la forza e la capacità regolative di ogni modalità variano a seconda di diversi fattori.

Soprattutto, l'efficacia di ciascuna modalità di controllo muta in accordo all'oggetto da regolare e le modalità esercitano pressioni diverse anche a seconda dell'ambiente nel quale questo viene disciplinato.

A prima vista, può sembrare un'analisi triviale, ma proviamo a pensare ad un semplice comportamento dipendente dall'architettura nell'era pre-Internet rispetto all'era post-Internet:

nello *spazio reale* la pornografia è tenuta fuori dalla portata dei minori; per essi è comunque difficile, anche se non impossibile, acquistare materiale pornografico, sia a causa delle leggi, che proibiscono la vendita di pornografia, sia a causa delle norme sociali, che impongono di evitare coloro che vendono pornografia ai minori, sia, infine, a causa del mercato, perché la pornografia è costosa.

Ecco il punto decisivo della questione: le regole dello spazio reale

dipendono da certe caratteristiche di *design*. Nello spazio reale l'età è un fatto immediatamente conoscibile: ovviamente un ragazzo potrebbe cercare di dissimularla, ma generalmente ciò non accade; infatti, all'adulto che vende o tratta pornografia è intuitivamente nota la minore età del ragazzo. Nello spazio reale l'autenticazione di sé consente facilmente di creare zone che rendono *off-limits* i contenuti osceni dell'espressione.

Nel cyberspazio, invece, l'età non è immediatamente conoscibile: quand'anche le stesse restrizioni di mercato, nonché le stesse leggi e norme sociali, trovassero applicazione al cyberspazio, ogni tentativo di istituire delle zone *off-limits* per la pornografia si scontrerebbe con la difficoltà concreta di accertare l'età.

In tal senso, l'architettura emerge come il perno centrale nella configurazione dei comportamenti possibili nel cyberspazio. L'architettura dell'informazione (di qualsiasi informazione, specie quelle a valenza precettiva) si pone come possibile collante fra i vari contesti di interazione uomo-informazione, da quelli fisici a quelli digitali e viceversa. La compenetrazione di questi ambienti sta avanzando a ritmi tali da rendere sempre più difficile, se non poco logico, distinguere tra diversi corsi d'azione possibili.

Di fronte a questi problemi, la risposta fornita dal diritto internazionale non è sicuramente sufficiente, né può servire a mascherare le tensioni generate dai principi generali del diritto dei singoli stati, i quali invocano l'esclusività delle proprie regole.

Nonostante ciò, il *Digital Realism Approach* afferma che Internet, quale sistema internazionale di comunicazione che unisce persone, istituzioni, società e governi[47], non esiste prima e indipendentemente dagli uomini. Internet, pur non essendo un'entità fisica, viene paragonato giuridicamente all'Antartide, considerata "*a jurisdictional no man's land*"[48]. Non si tratta, in realtà, di spazi senza legge, ma dell'assenza di una potestà dominante[49]. Le convenzioni internazionali ne disciplinano in ogni caso lo statuto ed in esse l'ordinamento giuridico internazionale è sempre presente per disciplinare la coesistenza delle differenti potestà attive nell'area.

Ecco che si affaccia di nuovo la pervasività della metafora *cyberspace as place:* dovunque l'uomo s'insedi, la sua attività viene attratta entro l'ambito di un ordinamento giuridico statale, la cui vigenza costituisce, quindi, un

[47] In tal senso, cfr. *United States District Court for the Eastern District of Pennsylvania, 11 June 1996, ACLU v. Janet Reno. Il testo integrale della sentenza è stato tradotto e commentato da V. Zeno Zencovich, Corte Federale U.S.A. 11 giugno 1996, in Il Diritto dell'Informazione e dell'Informatica, n. 4/5, 1996, pp. 604 ss.*

[48] T. Ballarino, *Internet nel mondo della legge*, Cedam, 1998, p. 5.

[49] Cfr. U.S. Supreme Court, 96 U.S. 511 (1997), *Reno v. ACLU*.

fatto ineliminabile; difatti, non può prospettarsi la tesi del vuoto normativo.

È proprio questo, invece, che manca alle attività o alle azioni su Internet: una regolamentazione transnazionale della giurisdizione che superi la visione classica, ormai inattuale e insufficiente, del diritto internazionale. Internet rinvia all'immagine di uno spazio virtuale, in cui la difficoltà risiede tanto nel definire le relazioni tra spazio reale e virtuale tanto nello stabilire come predisporre un diritto della Rete; esso, infatti, non può essere ancorato a uno spazio territoriale.

Spesso sulla base della sviante analogia tra attività *offline* e attività *online* si applica il diritto internazionale privato: questo succede ad esempio relativamente alle transazioni *online*. Ma ancora una volta, appena si tenta di applicare la regola secondo la quale le persone domiciliate in uno degli stati contraenti indipendentemente dalla loro nazionalità saranno sottoposte alla giurisdizione dello stato del loro domicilio, ci si accorge che questo test non vale per Internet, la cui indeterminatezza geografica pare chiaro che la parola "domicilio" poco si addice al mondo di Internet.

D'altronde, le *corporations* che operano su Internet utilizzano appieno l'autonomia contrattuale ad esse concessa dalla maggior parte degli ordinamenti; si pensi, ad esempio, agli ISP (*Internet Service Provider*)[50]. Sono diventate ormai comuni le cosiddette *Choice of Forum Clauses*, cioè clausole inserite nei contratti da stipularsi *online*, che individuano a priori la Corte competente per le eventuali controversie tra le parti contrattuali.

Ad esempio, la maggior parte degli ISP include unilateralmente nei propri accordi di servizio le clausole relative al *locus fori*; tuttavia, molte attività in Internet non sono commerciali od orientate alle transazioni e la scelta unilaterale *by default* delle clausole sulla competenza giurisdizionale non può riguardare problemi emersi su network aperti e non derivanti da attività non commerciali. Il rischio è quello di una privatizzazione assoluta del governo della Rete e la giurisprudenza non indica ancora quali percorsi giurisdizionali intraprendere per risolvere la vera scelta delle controversie giuridiche originate da tali attività[51].

Il consenso giurisprudenziale a favore della metafora "*cyberspace as place*" è, dunque, all'origine di una prassi su questioni di giurisdizione per attività illecita su Internet, contrattuale ed extracontrattuale, che si è rivelata nel tempo ondivaga, sviante e, spesso, paradossale o impossibile da applicare.

[50] O. Pollicino, *Tutela del pluralismo nell'era digitale: ruolo e responsabilità degli Internet service provider*, in *Percorsi costituzionali*, n. 1/2014, p. 45 ss.

[51] Sul tema della responsabilità giuridica degli ISP, si veda V. Zeno Zencovich, *I rapporti tra responsabilità civile e responsabilità penale nelle comunicazioni su Internet (riflessioni preliminari)*, in *Il Diritto dell'Informazione e dell'Informatica*, 1999, pp. 1050 ss.

Non essendo possibile affrontare approfonditamente in questa sede la ricca casistica giurisprudenziale, mi limiterò ad alcune osservazioni randomizzate[52], tese a dimostrare le numerose criticità causate dall'applicazione del criterio analogico tra azioni illecite offline e azioni illecite online in materia di illeciti transfrontalieri extracontrattuali commessi attraverso Internet.

Al fine di individuare un sistema risolutivo del possibile conflitto di giurisdizione tra vari Paesi astrattamente competenti per la decisione della controversia, nell'ipotesi di illeciti commessi *online* la giurisprudenza statunitense ha elaborato tre criteri alternativi[53]:

1- lo *sliding scale test* o *Zippo test*, che ha riformato il primo test utilizzato dalle Corti federali, ossia quello del *minimum contact*;

2- l'*effects test*;

3- il *targeting test*.

L'antecedente dei "*long-arm statutes*" è rappresentato dal test del *minimum contact,* preso in considerazione dalle Corti statunitensi ben prima dell'avvento di Internet: nel caso *International Shoe Co. v. Washington*[54] la presenza continua, sostanziale e sistematica di un soggetto non residente nell'ambito di una determinata giurisdizione statale determinerebbe la competenza territoriale della Corte di quello Stato, benché non formalmente residente in quel determinato territorio. La presenza costante, sostanziale e sistematica costituirebbe l'elemento sufficiente e necessario (il *minimum contact*) di individuazione dell'autorità giurisdizionale territorialmente competente, a condizione che l'esercizio della giurisdizione non contravvenga alle nozioni tradizionali di ragionevolezza e di giustizia materiale in conformità al *Due Process Clause*.

L'applicazione del *minimum contacts test* alle transazioni effettuate *online* è stata discussa a lungo, portando la giurisprudenza ad abbandonare la distinzione tra *jurisdiction in rem*, *in quasi rem* e *in personam* e a sostituirla con quella tra *general and specific jurisdiction*: la prima ricorre per i contatti intercorsi tra il convenuto e il *locus fori,* senza aver riguardo alla natura delle transazioni; la seconda, invece, ricorre quando è necessario valutare la connessione tra i fatti su cui è fondata la *cause of action* invocata dall'attore

[52] Anche se ormai datata, un'utile panoramica si trova in P. Longhini, *Internet nella giurisprudenza*, Milano, 2003.

[53] Per un'analisi accurata della giurisprudenza americana in tema di giurisdizione digitale si rinvia a A. Thierer, C.W. CrewsJr., *Who Rules the Net? Internet Governance and Jurisdiction*, Washington, 2003.

[54] U.S. Supreme Court, 326 U.S. 310 (1945), *International Shoe Co. v. Washington*.

e il *locus fori*.

Alla luce delle condizioni previste dal *Due Process Clause,* i due comparatisti Von Meheren e Trautman, che avevano rilevato la necessità di abbandonare la distinzione tra competenza *in rem* e competenza *in personam,* ebbero gioco facile a preconizzare che la Corte Suprema aveva imposto sul *minimum contacts test* una successiva evoluzione giurisprudenziale, la quale avrebbe condotto ad abbandonare il criterio della *general Jurisdiction*[55].

Il test del *minimum contacts* venne dunque successivamente declinato in modi differenti rispetto a quello applicato al caso *International Shoe*.

Nel 1996 il criterio venne perfezionato con una versione conosciuta come *sliding scale test*: nel caso *Zippo Dot Com* la Corte si soffermò sulla questione di *jurisdiction* e, più precisamente, sulla competenza della Corte della Pennsylvania nei confronti di Zippo, non residente nel territorio della Pennsylvania. In quell'occasione, la Corte ritenne che l'attività di commercio elettronico della Zippo soddisfacesse la rinnovata versione del *test* del *minimum contact,* basandosi sulla capacità e sull'estensione qualitativa dell'interattività del sito della stessa nel l*ocus fori*.

Questa variante del *minimum contacts test* richiedeva la verifica circa la sussistenza dei seguenti requisiti: quantità dei contatti del soggetto agente, natura e qualità dei contatti medesimi, connessione fra la causa dell'azione ed i contatti, interessi dello Stato nell'affermare il foro di competenza e convenienza dei soggetti.

Una seconda variante del *minimum contacts* test era già stata introdotta nel 1984 dalla Corte Suprema nel caso *Calder v. Jones*[56], la quale, elaborando l'*effects test,* riconobbe la competenza dello Stato della California nei confronti di un convenuto della Florida, poiché l'azione lesiva dei diritti dell'attore – nel caso di specie, la pubblicazione di un articolo lesivo – aveva dispiegato i propri effetti in misura rilevante nello Stato in questione, dove la rivista su cui era stato pubblicato era maggiormente diffusa. Si sostenne che la competenza spettasse a quel foro, in quanto la condotta del convenuto era stata intenzionalmente ed espressamente indirizzata verso la California.

Le criticità del *minimum contacts test* e delle sue successive varianti (*sliding scale test* e *effects test*) sono il prodotto dell'ossessivo sforzo di territorializzare il criterio dell'azione in Internet: l'architettura di Internet farebbe scontare un inconveniente alle azioni di immissione e di ricezione dei dati in rete, il quale sarebbe in grado di paralizzare l'effettività di quei criteri; infatti, attraverso la scelta del luogo di immissione dei dati o del

[55] A.T. von Mehren, D.T. Trautman, *Jurisdiction to Adjudicate: A Suggested Analysis*, in *Harvard Law Review*, 79, 1966, p. 1121 ss.

[56] U.S. Supreme Courts, 465 U.S. 783 (1984), *Calder v. Jones*.

server in cui metterli inizialmente a disposizione dei destinatari o del pubblico, si consentirebbe all'agente di scegliere la legge applicabile.

Più precisamente, l'*effects test* non funziona affatto: l'architettura di Internet rende facile alle persone nascondere la loro identità e la loro posizione; sulla base dell'architettura computazionale, è quindi impossibile pensare di basarsi sull'identità dell'agente al fine di valutare l'attività di servizi fornita dai siti.

Stessa sorte anche per *Zippo test*, che si fonda sulla natura interattiva del sito. Il problema è che il concetto di interattività rimane vago e ambiguo: quanta e quale interattività è condizione sufficiente per determinare la competenza? È ancora tecnicamente possibile suddividere i siti web in passivi ed interattivi? Il test Zippo non è nemmeno in grado di limitare il numero delle giurisdizioni concorrenti: una volta che un sito web è sufficientemente commerciale ed interattivo al di là di un'ipotetica e improbabile soglia fissata dalla Corte, la competenza può essere potenzialmente stabilita per ogni Stato. Decidere dove una *corporation multi-forum* è danneggiata è un problema insolubile in Internet.

Per ovviare ai difetti palesati da *Zippo test* e da *effects test*, si è pensato allora di elaborare un ulteriore test di determinazione della giurisdizione, indicato con l'espressione *targeting test*. Questo test, che presenta "qualcosa in più" rispetto ai primi due, è soddisfatto quando il convenuto ha tenuto un comportamento illecito verso l'attore, nella consapevolezza che quest'ultimo risiedeva nello Stato del foro competente. In pratica il convenuto, al fine di raggiungere un preciso obiettivo, ha tenuto dolosamente un'attività elettronica illecita direttamente nello Stato del foro: egli ha l'intenzione di esplicare detta attività nello Stato competente a giudicare i conflitti che sorgono con le controparti e che ivi risiedono. Il convenuto ha volutamente diretto i propri atti verso il *locus fori*, avvalendosi della legislazione di questo e azionando un sito interattivo nello Stato del foro.

In questo modo, sulla base della verifica della sua intenzione di produrre effetti illeciti diretti *online* nello Stato del foro medesimo, il *targeting test* darebbe maggiore certezza circa la determinazione della competenza giurisdizionale[57].

[57] Si veda in proposito il caso *People v. World Interactive Gaming* 714 NYS 2d 844 (1999). In Europa il *targeting test* è stato utilizzato per decidere il caso *The LICRA v. Yahoo! France* (*Nazi memorabilia*) del 22 maggio 2000. Il giudice francese ha riconosciuto competenza alla Corte parigina, essendosi il danno prodotto in Francia (nonostante l'azione lesiva sia avvenuta in California); in base all'articolo 5 della Convenzione di Bruxelles, in materia di illecito civile è competente il giudice del luogo di verificazione dell'evento dannoso. Esso (cioè la predisposizione di contenuti illeciti caricati sul server, in particolare immagini

A ben vedere, però, anche questo test presenta il difetto della prevedibilità del foro competente: i tribunali possono comunque ignorare completamente i criteri giurisdizionali generalmente accettati e applicare semplicemente il diritto del forum alle controversie legate a Internet; inoltre, rispetto all'architettura di Internet il *targeting test* è di fatto impraticabile: può un sito essere considerato in grado di avere un effetto diretto sul territorio di uno Stato, solo perché non ha messo in pratica delle azioni che prevenissero l'accesso al sito da parte di utenti del territorio dello Stato competente?

Diversamente dall'approccio statunitense, sia in sede nazionale sia in sede europea si è consolidato il principio dell'ubiquità giuridica, in forza del quale l'illecito si considera commesso sul territorio statale non solo quando su di esso si sia verificata in tutto o in parte l'azione o l'omissione, ma pure quando su di esso si sia verificato l'evento che ne è conseguenza.

Più precisamente, il principio di ubiquità, oggi accolto in Europa dalla maggior parte degli ordinamenti giuridici, che dà pari rilievo al luogo di verificazione dell'evento e a quello del compimento dell'azione, fu accolto anche dalla giurisprudenza statunitense e indicato con l'espressione *mosaic theory* nel caso *Playboy Ent. Inc. c. ChuckleberryPubl. Inc.*[58]. Una Corte statunitense ha ritenuto di poter ordinare al gestore di un servizio localizzato su un *server* italiano, ma accessibile anche da parte di utenti americani, di non utilizzare più il marchio Playmen, in quanto contraffazione del marchio Playboy. La Corte statunitense ha, però, riconosciuto di non avere giurisdizione per ordinare la chiusura del sito in Italia ed ha quindi limitato la condanna al pagamento delle somme che il convenuto ha percepito dalla sottoscrizione di abbonamenti per gli utenti americani e all'obbligo di rifiutare qualsiasi richiesta di abbonamento proveniente dagli U.S.A.

In ambito europeo viene in rilievo la sentenza della Corte suprema tedesca sul *Caso CompuServe, Amtsgericht München del 28 maggio 1998*[59]: il luogo nel quale si trova il server contenente i dati illeciti basterebbe in ogni caso ad individuare il *locus commissi delicti*, anche se diverso dal luogo in cui è avvenuta la prima memorizzazione o da quello della successiva produzione di effetti lesivi nel pubblico di destinatari.

inneggianti al nazismo) si era verificato in California, dove il server aveva la propria sede. Ma il danno (la visualizzazione del contenuto) si era prodotto anche in Francia, dove le associazioni che difendono la memoria dell'Olocausto sono legittimate ad agire. Si noti che il giudice parigino ha limitato alla Francia gli effetti dell'inibitoria.

[58] *Playboy Enterprises*, *Inc. v. Chuckleberry Publishing*, *Inc.* 1996 WL 337276 (S.D.N.Y. June 19, 1996).

[59] *CompuServe* (1995) 8340 Ds 465 Js 173158/95 (*Amtsgericht München* 28/05/1998, Felix Somm).

La sentenza ha dimostrato l'estrema difficoltà di considerare separatamente il comportamento posto in essere in un singolo territorio statale rispetto a quello di chi attiva e gestisce il server in altro Stato, sul quale il materiale incriminato sia stato immesso originariamente, memorizzato e reso poi disponibile agli utenti.

La questione è stata risolta nel senso *dell'estesa nozione di luogo* così come previsto dal principio di ubiquità giuridica, la c.d. *Ubiquitats theorie,* alla cui stregua si considera indifferentemente come luogo del fatto sia quello dell'azione od omissione sia quello dell'evento. In questo modo, il luogo nel quale si trova il server contenente dati illeciti basterebbe in ogni caso ad individuare il *locus commissi delicti,* anche se diverso dal luogo in cui sia avvenuta la prima memorizzazione o da quello della successiva produzione di effetti lesivi nel pubblico del destinatario, potendo rappresentare sia il luogo dell'azione, od almeno di quella sua parte consistente nella memorizzazione, riproduzione e trasmissione dei dati mediante il server medesimo, sia quello dell'evento, dato che tramite l'accesso ad esso da parte degli utenti si realizzerebbe anche la diffusione dei contenuti illeciti, se non anche la produzione degli effetti lesivi o della situazione di pericolo prevista dalla fattispecie.

Il criterio dell'ubiquità trova particolare applicazione nell'ambito dei reati commessi in Internet.

In Italia, il principio di ubiquità è previsto dal comma 2 dell'art. 3 del codice penale ed è considerato il contraltare del principio di territorialità previsto dal comma 1.

Analizzando un caso di diffamazione commessa a mezzo Internet, la Cassazione ha fatto ricorso al principio di ubiquità: con sentenza n. 4741 del 17 novembre 2000 ha stabilito che il magistrato italiano può intervenire anche nel caso in cui l'immissione nel web di immagini o frasi lesive della dignità o dell'onore di un cittadino italiano avvenga all'estero[60]. I giudici hanno considerato la diffamazione *online* un reato di evento e hanno affermato che l'elemento psicologico del reato sussiste anche se un soggetto diverso dall'agente o dalla persona offesa clicca sul sito incriminato e visualizza il contenuto diffamatorio. Si giustifica l'applicazione del principio di ubiquità in base a questo assunto: il reato si considera commesso nel territorio italiano non solo quando su di esso sia stata compiuta, in tutto o in parte, l'azione o l'omissione, ma pure quando su di esso si verifichi l'evento che ne è conseguenza. La magistratura italiana può perseguire i delitti contro l'onore anche quando l'*iter criminis* sia iniziato all'estero per mezzo di Internet.

[60] Cass. pen.,Sez. V, 27 dicembre 2000, n. 4741.

Eppure, nella diffamazione *online* sono ipotizzabili sia il tentativo sia il reato impossibile: l'evento non si verifica, in quanto il sito non viene visualizzato da alcuno; l'azione è inidonea, perché il messaggio non è stato immesso in rete. Ciò implica che si sarebbe dovuto considerare quale luogo di verificazione dell'evento offensivo quello in cui il primo cybernauta sia giunto a percepire la notizia diffamatoria.

La Corte, invece, ritiene che si integri il reato *de quo* in relazione agli effetti del discredito che derivano dall'offeso danneggiato nel suo ambiente, non richiedendosi la prova che il visitatore abbia letto la specifica notizia e assumendo rilevanza il mero accesso al sito; la prova della visita del sito da parte di utenti è facilmente accertabile.

In conclusione, allo stato attuale è inevitabile assistere ad una moltiplicazione degli ordinamenti che possono e devono perseguire un illecito commesso in Internet, sia pure in modi e tempi diversi, quando risulti violata la loro legge.

Ma la natura stessa della Rete è causa dell'emergere di numerose criticità. Solo per citarne alcune:

1- Il principio di ubiquità nel caso di specie non esclude una pluralità di fori tutti egualmente competenti;

2- Compressione del principio del giudice naturale ex art. 25 Cost. con un effetto penalizzante per il danneggiato, la cui libertà di scelta viene completamente soppressa;

3- La natura della Rete conduce a situazioni paradossali: non vigendo in ambito sovranazionale il principio del ne bis in idem, l'estensione ubiquitaria della territorialità (la finzione di avere un locus commissi delicti) non salva lo stesso soggetto dall'essere potenzialmente chiamato a rispondere del medesimo reato di fronte ad autorità giudiziarie di stati diversi;

4- Difficoltà insormontabili per identificare i terzi che hanno percepito il reato (pur avendolo classificato quale reato di evento) come seconda persona,

5- Presumendo che il momento della consumazione sia legato all'immissione in Rete del messaggio, viene a prodursi una perfetta coincidenza tra condotta ed evento, che priva quest'ultimo di ogni rilevanza fino ad imporre l'individuazione del locus commissi delicti nel luogo ove è stata realizzata la condotta.

Anche nei casi di violazione dei diritti di proprietà intellettuale, il problema della delocalizzazione si presenta quale maggiore ostacolo. La

giurisprudenza ha affrontato la questione con riguardo alle condotte, chiarendo che la localizzazione del sito all'estero non fa venir meno la giurisdizione del giudice nazionale quando una parte della condotta illecita concorsuale sia avvenuta nel territorio dello Stato. È irrilevante che la frazione di condotta, considerata ai fini della valutazione della giurisdizione, possa considerarsi mero tentativo. Condotte quali quella di "immissione di files" in Rete, così come quella di diffusione, sono suscettibili di essere localizzate all'interno di uno specifico territorio. Anche laddove il *server* in questione fosse posizionato al di fuori dei confini della giurisdizione, una frazione della condotta potrebbe considerarsi compiuta all'interno del territorio di competenza. Tali principi permetterebbero la riassunzione, di fattispecie potenzialmente frazionabili tra diverse competenze, in unico foro. Ne discende, quindi, la volontà di tutelare la parte debole, ovvero il danneggiato, garantendogli una maggiore tutela per mezzo di un riequilibrio della propria posizione, alquanto sbilanciata: altrimenti, egli dovrebbe rincorrere i diversi fori competenti sulla base di una quanto mai complessa individuazione di un univoco ed esclusivo *locus commissi delicti*.

Anche nel caso di specie, le criticità sono le stesse rilevate sopra e il problema generale rimane intatto: al di là della tipologia dell'illecito in oggetto (download o immissione illecita di files), la finzione dell'ubiquità rende davvero effettiva la tutela della vittima? O si predica l'effettività solo perché la finzione evita la disseminazione di diversi fori competenti? Ci sono ragioni solide per asserire che il principio di ubiquità garantisce il raggiungimento di una tutela effettiva?

Nonostante la volontà di creare un "codice per Internet" sotto l'egida dell'UNCITRAL e nonostante la volontà di sviluppare un diritto consuetudinario fondato sui principi dell'arbitrato internazionale (alla maniera della nuova *lex mercatoria*), l'attuale sistema giuridico generale dimostra ancora la sua incapacità di fondare una giurisdizione per Internet tecnicamente separata dal *nomos* della terra.

6. Internet *e* soft law

Diventa essenziale individuare la fonte normativa più adeguata per disciplinare questi fenomeni: deve trattarsi di una fonte negoziale o di una fonte autoritativa? E, in questa seconda ipotesi, a quale livello deve collocarsi

tale fonte[61]?

Questo contributo muove da un semplice assunto: la tecnologia inevitabilmente esercita un condizionamento «non soltanto sulla modalità di trasmissione delle informazioni, ma anche su scelte che condizionano inevitabilmente la disciplina del rapporto, assurgendo a fonte di vero e proprio *rulemaking*»[62].

Il *code* produce la *trasduzione* della legislazione e delle relative forme di tutela giurisdizionale in uno spazio giuridico elettronico concettuale o logico; ciò non significa, però, che "gli Stati siano impossibilitati a regolare il cyberspazio. Significa viceversa che l'unica capacità di regolamentazione [*e di una conseguente efficace giurisdizione*] che essi hanno è quella di intervenire sul codice e sull'architettura del sistema"[63].

Il ruolo delle attuali tecnologie nel determinare possibilità o forme di *governance* o di coordinamento diviene, dunque, una questione importante[64].

I vantaggi della risposta tecnica sono dovuti alla mancanza di confini territoriali, così consentendo elasticità delle regole ed autocontrollo. La coercibilità delle regole volontariamente assunte è garantita dalla forza vincolante del contratto, che è legge tra le parti[65].

In questo senso, Johnson e Post sostengono che le reti elettroniche transnazionali creino un insieme di giurisdizioni diverse da quelle statali, dotate di base territoriale: è poco sensato cercare di replicare per Internet le forme di regolazione degli Stati, rendendosi piuttosto necessario un diritto emergente e decentrato, ma convergente verso norme comuni per il coordinamento reciproco[66].

Ciò determinerebbe una sorta di *federalismo elettronico*: una pluralità, per le differenti sotto-comunità di utenti, di regole applicabili, che generano antinomie superabili mediante l'accesso ad altre e diverse aree della Rete da parte di coloro che non dovessero condividere un determinato corpo di regole.

Per Reidenberg e Lessig, che pongono invece l'accento sulla questione tecnologica, Internet è un ambiente regolato dagli *standard* e dai vincoli

[61] C. Rossello, *Commercio elettronico. La governance di internet tra diritto statuale, auto-disciplina, soft law e lex mercatoria*, Milano, 2006, p. 9.
[62] Ivi, pp. 14-5.
[63] M. Betzu, *Regolare Internet. Le libertà di informazione e di comunicazione nell'era digitale*, Torino, 2012, p. 24.
[64] D. Lehmkuhl, *The Revolution of Domain Names vs. Trademark Conflicts. A Case Study on Regulation beyond the Nation-State and Related Problems*, in *ZeitschriftFürRechtssoziologie*, 1, 2002, pp. 61-78.
[65] D.R. Johnson, D.G. Post, *And How Shall the Net Be Governed? A Meditation on the Relative Virtues of Decentralized, Emergent Law*, 1997; in www.cli.org.emdraft.html.
[66] D.R. Johnson, D. Post, *Law and Borders-the Rise of Law in Cyberspace*, cit., p. 1370 ss.

incorporati nei *software* e negli *hardware*. Reidenberg condivide con Lessig l'opinione secondo cui Internet è destinata a minare ogni *governance* regolatoria basata sul territorio[67]: gli standard tecnici e la loro capacità di stabilire regole limite di default hanno creato e continuano a creare nuovi modelli e fonti di norme negli ambienti delle reti.

Reidenberg nota come, attraverso una precisa configurazione di sistema[68], queste nuove architetture tecnologiche offrano ai governi una scelta sulle regole del flusso di informazioni.

La *Lex informatica*, intesa come insieme delle regole imposte dalla tecnologia per i flussi informativi e per le reti di comunicazione, diventa un sistema di regole parallelo, concorrente e a volte sovrastante le regole giuridiche[69].

Reidenberg, nel suo seminale articolo sulla *Lex Informatica* pubblicato dalla *Texas Law Review* nel 1998, schematizza il confronto tra la regolazione giuridica e la *Lex informatica*[70]:

	Legal Regulation	Lex Informatica
Framework	Law	Architecture standards
Jurisdiction	PhysicalTerritory	Network
Content	Statutory/ Court Expression	Technical Capabilities CustomaryPractice
Source	State	Technologists
CustomizedRules	Contract	Configuration
Customization Process	Low Cost; Moderate cost Standard form High cost negotiation	Off-the-shelf Configuration; Installable Configuration User choice
PrimaryEnforcement	Court	Automated, Self-execution

J.R. Reidenberg, Lex Informatica. 1998, 566.

[67] J.R. Reidenberg, *Lex informatica: the Formulation of Information Policy Rules through Technology*, in *Texas Law Review*, 3, p. 571.
[68] Ivi, pp. 553-593.
[69] H.H. Perritt, *Jurisdiction in Cyberspace*, in *Villanova Law Review*, 1, 1996, p. 41 ss.; J. Hughes, *The Internet and the Persistence of Law*, in *Boston College Law Review*, 44, 2003, p. 359 ss.; A. Murray, *Information Technology Law. The law and society*, cit., p. 9 ss.
[70] J.R. Reidenberg, *Lex informatica: the Formulation of Information Policy Rules through Technology*, cit., p. 566.

Come emerge dalla tabella, nel caso della regolazione giuridica il quadro normativo è rappresentato dalla legislazione mentre nel caso della *Lex informatica* è composto dalle architetture tecnologiche e dagli standard di rete.

Avendo riguardo alla regolamentazione giuridica, la giurisdizione è statale, territoriale e geopolitica, mentre, per la *Lex informatica*, essa è rappresentata dal network e dalle informazioni filtrate e regolate dai codici informatici, da una rete spaziale che travalica i confini geo-giuridici degli Stati.

Se il contenuto della regolamentazione giuridica consiste in norme e sentenze, quello della *Lex informatica* consiste nella capacità tecnica del codice di prestabilire quali attività possono compiere gli utenti della rete.

La fonte normativa, nel caso della regolamentazione giuridica, è il legislatore; nel caso della *Lex informatica*, invece, a costituire la fonte del codice è il programmatore informatico. Condotte e norme sono sempre più incluse nei dispositivi, nelle applicazioni e negli spazi web quale frutto della configurazione dei programmatori: nessun costruttore di *device* incorpora nella sua applicazione meccanismi per farla violare, mentre le regole giuridiche non impediscono la facoltà di poterle disobbedire[71].

L'autonomia delle regole prescelte e decise per la regolamentazione giuridica si esplica nei contratti, nei negozi giuridici e negli accordi negoziali, lasciati tutti alla libertà delle parti secondo il principio dell'autonomia contrattuale e sanzionati secondo il criterio *ex post facto*; diversamente, per la *Lex informatica* essa si riduce drasticamente a regole tecniche, a configurazioni già preimpostate – *ex ante facto* – dai programmatori informatici e a clausole vessatorie unilaterali, che rendono una finzione la libertà negoziale degli utenti.

Nell'ambito della regolamentazione giuridica la personalizzazione e l'autonomia dei processi e dei procedimenti sono rappresentate dal *low cost*, dal costo moderato, dalle forme di contrattazione standard e dall'alto costo di negoziazione; nell'ambito della *Lex informatica* esse consistono nella configurazione installabile, nella scelta dell'utente e nel flusso personalizzato delle informazioni al momento dell'installazione di un programma.

La forza di legge, per la regolamentazione giuridica, è data e assicurata dalle corti e dai tribunali che intervengono, seppur con tempi procedurali dilatati e in qualità di soggetti terzi e imparziali, su domanda di parte; nel caso della *Lex informatica,* invece, per effetto della capacità di elaborazione delle informazioni, l'implementazione della forza di legge è *automatizzata*

[71] M. Hildebrandt, *Smart Technologies and the End(s) of Law. Novel Entanglements of Law and Technology*, Cheltenham, 2015, p. 12.

e contiene già in sé la soluzione. In questo senso la tecnologia digitale condiziona non solo la trasmissione di informazioni ma anche la disciplina dei rapporti intersoggettivi: «l'*enforcement* giuridico è incorporato nella scrittura di un codice che rende eseguibili algoritmicamente le clausole contrattuali»[72].

Come risulta chiaramente dalla tavola di Reidenberg, il provider esercita congiuntamente funzioni che, nel mondo reale, sono assimilabili sia a quella legislativa sia a quella giurisdizionale. L'elisione di quella che, in un giudizio ordinario, potremmo definire "fase istruttoria", rende i provvedimenti assunti dal provider nei confronti dell'autore dell'illecito più simili a provvedimenti cautelari, basati esclusivamente sul *periculum in mora* e sul *fumus boni iuris*.

7. *Conclusione*

Internet è, perciò, sia un insieme di norme sia una struttura dalla logica interna fondata su regole tecniche. Dal punto di vista giuridico, Internet non è un soggetto; la realizzazione dei vari rapporti telematici in Rete richiama, secondo la *vulgata* corrente, l'immagine di un *luogo* dove si instaurano relazioni commerciali, personali o in cui vengono commessi atti illeciti.

La strategia dei tribunali è quella di "vedere ed aspettare", nella convinzione che il sistema di Internet non esisterebbe prima delle azioni e dei comportamenti degli uomini (*cyberspace is not extraterritorial*[73]), ritenendo che si debba attendere per osservare lo sviluppo del network in molti contesti differenti quali il commercio, la pornografia, la privacy e la tassazione.

Si tratta di un errore fatale: organi legislativi e giurisdizionali dimostrano di non aver compreso che il sistema tecnico ha invaso la totalità del vissuto e l'intera pratica sociale; difatti, la relazione con il sistema tecnico è immediata (o de-medializzata). Ormai i *pattern* culturali sono divenuti semplici riflessi dell'ambiente tecnico: è ciò che McLuhan intese esprimere con la celebre formula: «*The medium is the message*»[74].

Anziché arroccarsi a difesa della metafora *cyberspace as place* occorre programmare le tecnologie computazionali affinché siano funzionali ad un

[72] C. Accoto, *Il mondo dato. Cinque brevi lezioni di filosofia digitale*, Milano, p. 106.
[73] A. Etzioni, *The Limits of Privacy*, New York, 1999, pp. 96-99.
[74] J. Ellul, *Il sistema tecnico. La gabbia delle società contemporanee*, Milano, 2004, p. 59.

controllo portato dall'interno dell'infrastruttura[75].

Finché i regolatori pubblici continueranno a immaginare una perfetta simmetria tra azioni *offline* e azioni *online,* nessuna normazione preventiva risulterà efficace[76]: il confine tra *offline* e *online* potrà risultare netto solo agendo sulle scelte di *design* delle *regole virtuali* su Internet[77].

Al fine di bilanciare i limiti e le possibilità del comportamento nel cyberspazio, la sfida normativa consiste dunque nel realizzare una continua interazione tra regolazione statuale o sovranazionale e l'architettura del *code*.

In questo senso e contrariamente a quanto evidenziato in materia di *copyright* dei beni intangibili, la natura preventiva (*ex ante facto*) del *code* potrebbe seguire un percorso inverso, cioè quello dell'incorporazione nelle regole informatiche di valori giuridici condivisi.

In questo modo, il *code* diventa *sottoinclusivo* rispetto alle norme giuridiche: quest'ultime possono incidere sull'uso generale di quelle tecnologie digitali deputate alla realizzazione di un set di valori condivisi (tutela dei soggetti più vulnerabili, libertà di espressione, parità di accesso alle forme di informazione e comunicazione tecnologica, promozione del controllo democratico nella progettazione tecnologica, garanzia di riservatezza dei dati personali).

Lessig propone due esempi in cui il *code* appare la soluzione a problemi di informazione, rispettando un approccio *value-centered design*.

Il primo problema impone di chiedersi se la delimitazione di zone (*zoning*) dell'espressione digitale, avente contenuti adatti ai soli adulti, sia in grado di tenere i minori lontani dalla pornografia.

Il secondo problema, invece, induce a domandarsi se nel cyberspazio sia davvero possibile decidere se partecipare o acconsentire alla nostra sorveglianza e rinunciare, di conseguenza, alla nostra privacy.

La risposta a questi due problemi – nel primo caso, delimitare una zona per la pornografia e, nel secondo caso, scegliere di tutelare una privacy protetta – dipende dall'architettura intrinseca del cyberspazio. La risposta è lasciata alla discrezionalità dei regolatori: dare regole (si pensi, ad esempio, ai principi della *privacy by design*) per il cambiamento dell'assetto tecnico del *code* o lasciare il cyberspazio com'è e, conseguentemente, accettare che finalità condivise siano lasciate al loro destino?

[75] C. Sunstein, *Republic.com. Cittadini informati o consumatori di informazioni?*, Bologna, 2003.
[76] D.J. Solove, *The Future of Reputation. Gossip, Rumor, and Privacy on the Internet*, New Haven, 2007, p. 190.
[77] G. Sartor, *Temi di diritto dell'informatica*, Torino, 2011, pp. 13-17.

Abstract

The central question of this paper is how code (or 'Lex informatica') relates to the competence debate: is it a governance solution separate and outside any competence model? Code is an expression referring to technical choices that impose certain behaviours upon web users. It includes both the establishment of specific rules for the flow of digital information upon the Web, and the possibility to impose procedural limitations upon said flow. The Web becomes simultaneously centralized and decentralized, it adapts and repolarizes itself in infinite variations, eluding territories, structuring immaterial confines within global space. The expression "Code is law" denotes that technological architectures of the internet contain self-organizing codes and regulatory languages that establish and control the rules of access to the digital content of the Web. Code, unlike traditional regulation, does not presuppose or require transparency: it can be effective, whether or not those subject to it are aware of it. This question has from very early on attracted attention in the various legal contexts and resurfaces throughout this paper.