Internet tra diritti e giurisprudenza

Monica Suerz

Abstract

La rete si configura come una sorta di "banco prova" per un'autonomia normativa che vede gli stessi utenti, al contempo, sia quali produttori di regole che soggetti alle loro regole. Questa autonomia trova ragion d'essere non tanto in costruzioni di natura teorica (ergo, opzioni valoriali) ma nell'impossibilità di un ordinamento giuridico gerarchizzato sovranazionale di intervento. Tutti noi siamo quindi in definitiva demandati a meccanismi di auto-regolamentazione del sistema e, al di là di essa, al senso di responsabilità delle aziende, dei programmatori, di noi stessi utenti. Ma per regolamentare l'agire all'interno della rete non bastano i codici o le indicazioni di "galateo". Si rende necessario il passaggio dalla dimensione etica - imperativa per la coscienza del singolo o di ristretti insiemi di persone - alla dimensione politico-giuridica - prescrittiva per tutti i cittadini - sulla base di una riflessione giuridica costantemente sollecitata da fondamentali intuizioni etiche che, in genere, si pongono alla base di ogni indispensabile aggiornamento del diritto. Ma sotto questo punto di vista il diritto deve pure volgere ad un equilibrio di valori aventi un connotato di stretta proporzionalità tra risposte, limiti e confini. Poiché ogni confinamento, che non voglia essere discriminazione, deve essere e portare a paritetiche garanzie.

Parole chiave

Rete e reati;
Internet e giurisprudenza;
Giurisdizione e competenze;
Casi giudiziari.

> *Permettendo a sistemi adattivi complessi di interagire tra loro,internet ha cambiato il modo in cui prendiamo le decisioni. Sempre più spesso non sono i singoli esseri umani a decidere,ma una complicata rete formata da esseri umani e macchine. Anche se siamo stati noi a crearla, non l'abbiamo progettata. Si è evoluta da sola. Il rapporto che ci unisce è similea quello che abbiamo con il nostro ecosistema biologico. Siamo codipendenti e non la controlliamo completamente.*
>
> W.D. Hillis[1]

Sommario

1. La disciplina giuridica

Internet e le varie reti hanno reso possibile l'utopia della libertà di volere e di pensare qualsiasi cosa, perché hanno tolto apparentemente ogni vincolo di gerarchia o di subordinazione. Ognuno è un tassello a sé stante in una rete orizzontale senza capi, né vertici, senza limiti all'esercizio della propria volontà. Perché questa libertà non diventi anarchia occorre regolamentazione. La lotta al crimine informatico non rappresenta dunque soltanto una necessità per ristabilire l'ordine giuridico violato, ma aiuta anche indirettamente nell'opera di prevenzione di questi specifici reati. A questo proposito occorre sempre tenere conto di un'importante e costante circostanza, ovvero la vulnerabilità della società informatizzata

1 W.D. Hillis, fisico ed informatico. Citazione rinvenibile sul settimanale "*Internazionale*", 29 gennaio/4 febbraio 2010, n. 831, p. 39.

e la sua preponderante dipendenza dalla tecnologia dell'informazione. Infatti, ciò che si rileva è il quotidiano avanzare della tecnologia sulla stessa tecnologia, spesso senza pause né tempi sufficienti ad un assorbimento di tutte le novità che si ripercuotono in tutti i campi, ivi compreso quello della comunicazione e del diritto, anche processuale. Nell'attuale contesto ogni soggetto, compresi gli avvocati ed i magistrati, è chiamato a moltiplicare le sue energie e sforzi al fine di non veder calpestati diritti fondamentali nell'individuo; diritti che hanno il loro fondamento non solo nella Costituzione, ma altresì nel Trattato di Lisbona entrato in vigore il 1 dicembre 2009. Nonostante le difficoltà che una materia soggetta a così rapida evoluzione – quale è l'informatica – oppone a qualsiasi forma di stabile disciplina, questa non può essere sottratta all'esigenza di una riconduzione a principi fondamentali. Ciò attraverso la contrapposizione fra libertà di fare e di dire con la necessità di rispettare i diritti, anche fondamentali, degli altri, quindi con i limiti legislativi ed etici alle violazioni di questi diritti. Infatti, sebbene la rapidità dell'innovazione tecnologica di Internet renda impossibile un reale tentativo di pianificazione, ciò non esclude la possibilità di approntare opportuni rimedi giuridici a specifici problemi che sorgono nella rete. Un sistema normativo stabile, di cui gli operatori devono tener conto nello svolgere la loro attività, deve necessariamente adeguarsi alla natura di Internet: quindi, da un lato, alle caratteristiche tecniche e, dall'altro, alla peculiarità dei rapporti sociali ed economici che si sviluppano nella rete. Sono questi gli imprescindibili doveri da adempiere, nell'attuale era "digitale", per non trasformare la rete in una giungla senza regole che può comportare un calpestio di inviolabili diritti fondamentali per ogni individuo e per la collettività. La soluzione adottata finora è quella di regolare le controversie secondo le regole del diritto internazionale privato, ovvero nell'ambito dell'Unione Europea secondo le norme adottate da questo ordinamento sovranazionale e implementate negli Stati membri[2]. Nonostante vi siano strumenti pattizi di diritto internazionale, come i trattati del WIPO[3] in materia di protezione del diritto d'autore, questi tuttavia non coprono tutte le problematiche di natura giuridica che possono sorgere *online*.

Il più recente orientamento della Corte di Giustizia dell'Unione Europea, proprio miran-

convenzione di Budapest del 2001 in materia di criminalità informatica. Le novità introdotte con tale provvedimento in materia penale sono numerose. Sono state infatti introdotte inedite fattispecie di reato tese a penalizzare sia i cd. reati informatici "puri" – reati, cioè, che penalizzano quelle condotte che aggrediscono beni informatici – sia i reati informatici "spuri" – reati comuni commessi per mezzo di un sistema informatico - . Pensiamo a:
- Art. 495 *bis* C.P. – Falsa dichiarazione o attestazione al certificatore di firma elettronica sull'identità o su qualità proprie o di altri;
- Art. 640 *quinquies* C.P. – Frode informatica del soggetto che presta servizi di certificazione di firma elettronica;
- Art. 615 *quinquies* C.P. – Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico);
- Art. 635 *bis* C.P. – Danneggiamento di informazioni, dati e programmi informatici;
- Art. 635 *ter* C.P. – Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità;
- Art. 635 *quater* C.P. – Danneggiamento di sistemi informatici e telematici;
- Art. 635 *quinquies* C.P. - Danneggiamento di sistemi informatici o telematici di pubblica utilità;
- Art. 24 *bis.* – Delitti informatici e trattamento illecito di dati.

Altro reato informatico, di più risalente introduzione nel nostro ordinamento e sul quale la recente sentenza del 27.10.2011 della Corte di Cassazione S.S. U.U. è stata chiamata a dirimere (anche se non sono state tuttora depositate le motivazioni), è il reato all'art. 615 *ter* c.p., ovvero «*se integri la fattispecie criminosa di accesso abusivo ad un sistema informatico o telematico protetto la condotta di accesso o di mantenimento nel sistema posta in essere da soggetto abilitato ma per scopi o finalità estranei a quelli per i quali la facoltà di accesso gli è stata attribuita*».

Per quanto attiene alle modifiche intervenute con la legge di ratifica della Convenzione di Budapest, bisogna sottolineare come esse attengano per la maggior parte la materia dei mezzi di ricerca della prova prevedendo l'estensione della loro applicazione a dati di natura informatica, a dati cioè caratterizzati da due caratteristiche fondamentali: l'immaterialità e la fragilità.

3 La *World Intellectual Property Organization* è un'agenzia specializzata delle Nazioni Unite per quanto concerne il diritto d'autore e la proprietà intellettuale delle opere di ingegno e d'arte.

2 Certo è che sotto il profilo dell'adeguamento del sistema sanzionatorio si è fatto sicuramente di più. Ciò, soprattutto, per mezzo della L. 48/2008 di ratifica della

do ad un bilanciamento tra i diritti fondamentali (come l'accesso alla medesima Internet, la riservatezza, il diritto di manifestare liberamente il pensiero, di accedere alla conoscenza), ha inteso garantire la peculiare struttura della Rete con le pretese patrimoniali della tutela dei diritti d'autore. La Corte ha statuito che occorre tenere «presenti le condizioni derivanti dalla tutela dei diritti fondamentali applicabili» e che quindi le direttive europee[4] «devono essere interpretate nel senso che ostano all'ingiunzione ad un fornitore di accesso ad Internet di predisporre un sistema di filtraggio di tutte le comunicazioni elettroniche che transitano per i suoi servizi, in particolare mediante programmi *"peer-to-peer"*, applicato a tutta la sua clientela, a titolo preventivo, a sue spese esclusive, e senza limiti nel tempo, idoneo ad identificare nella rete di tale fornitore la circolazione di file contenenti un'opera musicale, cinematografica o audiovisiva rispetto alla quale il richiedente affermi di vantare diritti di proprietà intellettuale, onde bloccare il trasferimento di file il cui scambio pregiudichi il diritto d'autore»[5]. Tale decisione ribadisce il principio di neutralità della Rete.

La virtualità della Rete influisce non solo sull'avvicinamento alla stessa da parte degli utenti, bensì pure sulla trasformazione, o per lo meno sull'adattamento, dei concetti giuridici tradizionali collegati alla protezione dei diritti fondamentali a questo tipo di ambiente.

2. Privacy e riservatezza

Il rapporto tra uso dei *social network*, riservatezza e diritto all'oblio si fa sempre più stretto e l'analisi della casistica giurisprudenziale consente di coglierne la portata concreta. A questo proposito è interessante analizzare il caso giudiziario conosciuto come "GoogleVideo contro Vividown" inerente alla tutela della riservatezza e della dignità della vittima di un atto di cyberbullismo. Nell'autunno 2006 veniva caricato su Google Video un video realizzato con un videofonino che illustrava un ragazzo disabile oggetto di denigrazione da parte dei suoi compagni in orario scolastico. Oltre allo sdegno dell'opinione pubblica tale fatto ha provocato l'interesse della magistratura inquirente, che ha formulato il rinvio a giudizio alcuni manager di Google per due capi di imputazione: il primo relativo all'integrazione di una fattispecie di diffamazione[6] (dalla quale gli imputati sono stati assolti poiché al momento tale fattispecie non era prevista quale reato penale), mentre il secondo relativo alla violazione del codice della *privacy*[7] relativamente alla diffusione *online* di dati sensibili della vittima, ovvero il suo stato di salute. Il Tribunale di Milano ha condannato a 6 mesi di reclusione i dirigenti di Google con la condizionale esclusivamente in riferimento alla seconda incriminazione. Nella sua lunghissima motivazione, il giudice monocratico di prime cure ha ricostruito la serie di comunicazioni avvenute tra gli operatori di Google sulla cancellazione del video, al fine di dimostrare come i gestori del *website* cercassero di guadagnare delle posizioni sul mercato del *video-sharing*, e quindi appetibilità dei loro spazi pubblicitari, trascurando gli adempimenti di legge in materia di *privacy*. Tale sentenza ha suscitato diverse perplessità tra gli operatori e tra i commentatori in relazione alla condanna del *provider* per la pubblicazione *online* da parte di terzi di materiali lesivi della *privacy* altrui[8]. Tuttavia si osservi come, se da un lato tale disciplina sia limitata al commercio elettronico, dall'altro Google Video (e servizi assimilabili, come la medesima YouTube controllata da Google) non possono più essere considerati fornitori di servizi neutri, in quanto essi svolgono un vero e proprio ruolo di natura editoriale relativamente ai materiali pubblicati con classifiche di gradimento, inserzioni pubblicitarie e di intervento sui materiali. Un dato oggettivo

4 Nella specie la 2000/31/CE, relativa al commercio elettronico; la 2001/29/CE, sulla protezione del diritto d'autore; la 2004/48/CE, sul rispetto dei diritti di proprietà intellettuale; la 95/46/CE, in materia di protezione dei dati personali; la 2002/58/CE, relativa alla vita privata e alle comunicazioni elettroniche.

5 Corte europea di giustizia, 24 novembre 2011, C-70/10, Scarlet v. Sabam.

6 Per violazione degli artt. 110, 40, 595, commi 1 e 3.

7 D. Lgs. 30 giugno 2003, n. 196.

8 I commentatori critici della sentenza si basano sull'art. 15 della Direttiva 2000/31/CE rubricato "Assenza dell'obbligo generale di sorveglianza".

emerge da questa sentenza: l'assenza di espliciti riferimenti comunitari in tema di *privacy*. Non è infatti nemmeno stata citata la Carta dei diritti fondamentali dell'Unione Europea per richiamare la necessarietà della protezione della parte lesa, seppur già vincolante al momento della pubblicazione del dispositivo e nonostante l'esplicito riferimento, contenuto nella medesima, alla riservatezza dei dati sensibili dei soggetti sottoposti a quel tipo di riprese. A questo proposito soccorre il diritto comparato, dove, in un caso analogo, ovvero la pubblicazione di commenti denigratori e ingiuriosi consistenti in *hate speech*, la Court of Appeal of the State of California ha statuito che, trattandosi di cyberbullismo, tale azione non possa avvalersi delle garanzie di libertà di espressione fornite dal First Amendment del Bill of Rights della Costituzione americana, poiché il contenuto diffamatorio configura un reato. Ne conseguirebbe quindi che la tutela del soggetto debole dalla pubblicazione di dati ovvero immagini diffamatorie *online* implicherebbe un aspetto delicato, ancora più profondo della rivendicazione del diritto all'oblio, in riferimento alla tutela della dignità della vittima. Si tratta di un elemento essenziale del dovere di solidarietà verso i più deboli, dovere che non deve venire – e non viene – meno neanche sul Web. Il problema però diventa di gestione ancora più difficile sulle piattaforme di condivisione sociale dei contenuti, come Facebook. Sebbene ivi lo svelamento dei propri dati o materiali (come fotografie, video, commenti, note e così via) avvenga, generalmente, senza il consenso dell'avente diritto, questo comportamento tuttavia non è da considerarsi pienamente illegale, poiché, nel momento in cui ci si iscrive alla piattaforma, si accettano le condizioni d'uso nonché il rischio ad essa connesso, ovvero la possibilità che dati personali inerenti l'utente vengano dispersi. È peraltro difficile verificare come vengano posti in essere i rimedi a disposizione degli utenti lesi nella loro *privacy*, perché, relativamente alle piattaforme di *social networking* come Facebook, le decisioni giurisprudenziali sono ancora rare.

Per quanto concerne l'ordinamento nazionale, secondo la giurisprudenza di merito è tenuto al risarcimento a titolo di danno morale colui il quale leda diritti e valori costituzionalmente garantiti, quali la reputazione, l'onore o il decoro altrui, mediante l'invio di messaggi offensivi condivisi su Facebook. Nel caso di specie si trattava della condivisione su Facebook, da parte dell'*ex-boyfriend* di una ragazza, di frasi canzonatorie dei difetti fisici della giovane. La giurisprudenza di legittimità ha considerato le molestie, perpetrate attraverso il reiterato invio alla persona offesa di sms e/o di messaggi di posta elettronica - o comunque postati sui cd. *social network*, proprio come Facebook - nonché quelle attuate con la divulgazione di filmati ritraenti rapporti sessuali avuti con la medesima, come integrazione alla condotta tipica del delitto di atti persecutori[9].

L'esperienza comparatistica fornisce un interessante parametro di confronto: i giudici federali americani hanno iniziato a delineare cosa costituisca violazione della *privacy* su Facebook, e quindi sia censurabile, da cosa sia semplicemente inopportuno o disgustoso, e quindi sia tutelato dalla libertà di manifestazione del pensiero. Nel caso di specie, un gruppo di allievi infermieri aveva seguito un corso in ostetricia e ginecologia presso un ospedale di Olathe, nel Kansas. Alla fine del corso alcuni di loro avevano chiesto di potersi fotografare con la placenta di una paziente rilasciata durante il parto. Una di essi pubblicò la sua foto sulla sua pagina di Facebook, provocando la sua espulsione dal corso. La ragazza fece causa per venire riammessa, argomentando che non era stato rispettato il suo diritto al Due Process, poiché sanzionata senza contraddittorio. La domanda fu accolta dai giudici. Per quanto concerne il merito della vicenda, la Corte ha enucleato due argomenti di interesse: a) dal momento in cui il docente concede il permesso di fotografare le persone che tengono in mano la placenta, questi deve fondatamente supporre che successivamente le immagini verranno postate sul più popolare *social network* del mondo; b) fotografare tale materiale umano non viola la *privacy* di alcuno, perché dalle immagini non è possibile risalire a chi appartenga la placenta stessa. In altra causa, giudici statali hanno al-

9 Art. 612 *bis* c.p.

tresì affermato come non sia necessario il consenso per venire taggati in una foto caricata su Facebook. La decisione è stata presa all'interno di un procedimento di affido di minori. Il padre ha portato, quale prova giudiziaria, una foto pubblicata su Facebook che rappresentava la madre mentre beveva alcoolici, nonostante la controindicazione medica correlata all'assunzione di psicofarmaci per la cura di un disturbo comportamentale della signora. Le difese della donna, rigettate della corte, argomentavano che essa è stata fotografata e taggata su Facebook senza il suo consenso. Questo provvedimento pone due questioni: da un lato, quale sia la possibile difesa della *privacy* su Facebook, completamente negata in questo caso; dall'altro, fino a quando le foto digitali potranno venire considerate come affidabili mezzi di prova per la rappresentazione della realtà, considerata la facile reperibilità di software in grado di modificarle.

3. Reati informatici

L'utilizzo di Internet, pur rappresentando una vitale opportunità per il sistema economico-sociale, può diventare un possibile centro di criminalità capace di generare notevoli danni a livello globale senza trovare una risposta adeguata nella normativa, che dovrebbe essere concordata a livello globale. Inizialmente, infatti, ciascun Stato aveva una propria normativa di riferimento, anche se Convenzioni o Trattati internazionali prevedevano la cooperazione in campo penale tra alcuni Stati Europei ed extra Europei. Sebbene iniziative di sensibilizzazione per la cooperazione nella lotta alla criminalità informatica siano state successivamente messe in campo dalle Nazioni Unite, dall'OECD, dall'Unione Europea, dal G8 e da altre organizzazioni, nel frattempo l'evoluzione della tecnologia digitale ha portato alla convergenza ed alla rapida globalizzazione delle reti informatiche. È aumentato parallelamente il rischio che le reti informatiche e le informazioni in formato elettronico possano essere utilizzate per commettere reati, anche se tramite queste reti è pure possibile conservare e trasferire le prove connesse a tali reati. Ciò nonostante soltanto il primo luglio 2004 entrò in vigore la Convenzione di Budapest, risultato di quattro anni di lavoro da parte di esperti non solo del Consiglio d'Europa, ma anche di altre nazioni non facenti parte dell'Unione Europea (come Stati Uniti, Canada, Giappone). Alcuni degli obiettivi della Convenzione sono

:

- perseguire una politica comune in campo penale finalizzata alla protezione della società civile contro la criminalità informatica;
- facilitare l'individuazione, l'investigazione e l'esercizio di una azione repressiva comune;
- avere incriminazioni omogenee, sanzioni comuni ed una giurisdizione legittimata a perseguire e punire questi reati globali.

Nel creare un deterrente per le azioni dirette contro la segretezza, l'integrità e la disponibilità dei dati ovvero dei sistemi e delle reti informatiche, così come un dissuasivo per l'uso improprio di questi sistemi nonché delle reti e delle informazioni (come, ad esempio, archivi ospedalieri in materia di trasfusioni), la Convenzione è stata costretta a misurarsi con il difficile compito di garantire un bilanciamento tra l'interesse per l'azione repressiva ed il rispetto dei diritti umani fondamentali, da un lato, e la necessità di tutelare gli interessi legittimi nell'uso e nello sviluppo delle tecnologie informatiche, dall'altro.

Per quanto concerne poi il piano del Diritto Penale Sostanziale, la Convenzione prevede che ogni Paese debba prevedere e sanzionare i seguenti reati perpetrati contro la riservatezza, l'integrità e la disponibilità dei dati e dei sistemi informatici, ossia:

- l'accesso illegale ad un sistema informatico;
- l'intercettazione abusiva;
- l'attentato all'integrità dei dati;
- l'attentato all'integrità di un sistema;
- l'abuso di apparecchiature;
- la falsificazione informatica;
- la frode informatica;
- i reati relativi alla pornografia infantile;
- i reati contro la proprietà intellettuale e diritti collegati.

Sempre sul piano del Diritto Penale Sostanziale, particolare attenzione viene inoltre posta alla responsabilità delle persone giuridiche in materia di reati informatici. La Convenzione, nell'ambito della responsabilità della persona giuridica, chiede infatti agli Stati membri di modulare il tipo di responsabilità (civile - penale - amministrativa) oltre ad applicare sanzioni penali e non penali, che siano effettive, proporzionate e dissuasive, o altre misure (incluse sanzioni pecuniarie). Ciò in quanto i reati hanno sempre più come oggetto privilegiato le aziende.

Per quanto concerne il nostro Paese, l'Italia ratifica la Convenzione di Budapest con L. 18.3.2008, n. 48 ed è uno dei primi Paesi ad introdurre una legge organica in tema di delitti informatici[10]. Così non è, però, per la materia della responsabilità delle persone giuridiche, che prevede il solo art. 24 *bis* inserito nel corpo del D.Lgs. 231/2001: "Delitti informatici e trattamento illecito dei dati". In concreto non è errato asserire che la normativa richieda un maggior sforzo organizzativo agli Enti non solo per l'estensione delle fattispecie di reato, ma per l'esposizione degli stessi Enti ad una "responsabilità amministrativa" da reato, ovvero di una "colpa organizzativa" per non essersi dotati di meccanismi interni necessari per la prevenzione dei reati informatici. In Italia, peraltro, il diritto penale dell'informatica si è sviluppato con una tendenza tecnofobo-moralista, che spesso non discerne fra strumento e suo utilizzo, fra gravità dei reati e adeguatezza della pena, fra diritto alla libera espressione ed alla *privacy* e tendenza a porre freni e controlli. Tanto che si è depenalizzato il falso in bilancio, ma si persegue il ragazzino che scarica musica con il *peer to peer*.

Benché pure altri Paesi sottoscrittori della Convenzione di Budapest si siano dotati di una normativa, il panorama globale risulta frammentario, dando vita a rischi di censura nei Paesi che non si uniformino al diritto internazionale. Certo è che le dimensioni (numeriche, geografiche ed economiche) di questa tipologia di reati nonché le modalità di esecuzione e la specificità di chi li commette richiedono nuovi approcci culturali, tecnologici e normativi per garantire risposte adeguate ed innovative. Risposte che devono essere necessariamente globali, sebbene si ponga l'interrogativo di chi debbano essere gli autori delle regole mondiali.

Gli U.S.A. hanno lanciato, a tal proposito, un'importante campagna di sensibilizzazione sul *cyber-crime*. Determinante è stato in tal senso l'incontro nel maggio 2011 tra il Primo Ministro David Cameron ed il Presidente Barack Obama. Avuto riguardo di questo, l'International Cyber Conference a Londra del 7.11.2011 ha raccolto il messaggio e fissato alcuni importanti principi, tra i quali emerge che:

- il *cyber-space* dovrebbe essere regolato da norme di comportamento non impartite dall'alto a livello governativo, ma condivise con gli *stakeholders* (i veri *players*) e basate su opportunità, libertà, innovazione e rispetto dei diritti umani;
- la *cyber security* non dovrebbe essere il pretesto per operare una subdola censura;
- i *cyber-criminals* non sono il vero problema e che la condotta *online* dei cittadini non dovrebbe essere valutata dall'alto, ma gestita da politiche governative trasparenti e chiare.

In definitiva, Internet è strumento democratico e pretende un approccio democratico.

4. Internet nella giurisprudenza

Internet è sia strumento "veicolare" di giurisprudenza (cioè di diffusione o disseminazione giurisprudenziale) sia oggetto di decisioni giurisprudenziali. La gran parte delle giurisdizioni superiori straniere consente, infatti, la consultazione gratuita dei provvedimenti giurisprudenziali *online* da parte del pubblico specializzato e non. Si permette così la realizzazione dell'accesso alla giustizia non solo come diritto all'accesso alle Corti, ma anche alla conoscenza (non squisitamente accademica o professionale bensì pure divulgativa) delle decisioni prese delle stesse. Per quanto concerne poi le decisioni giurisprudenziali attinenti ad Internet quale oggetto dei provvedimenti, nella dottrina si è dato spazio all'analisi delle

10 L. 23.12.1993, n. 547.

fattispecie accadute pure in altri ordinamenti. Ciò a conferma di come Internet si sia rivelata essere il più forte ed efficiente veicolo di imitazione giuridica oggi a nostra disposizione. Non capita di rado, infatti, che i giudici nel decidere le fattispecie in materia di diritto della Rete facciano riferimento a sentenze straniere attraverso la comparazione quando vi sia un problema simile in altri ordinamenti. In tal modo è possibile avere una risposta armonizzata. Questo rende manifesto come la prassi internazionale sia spesso strumento veicolare per lo scambio di modelli e, soprattutto, di cultura giuridica e di come Internet ne moltiplica, in modo quasi esponenziale, gli effetti.

Un'autorevole dottrina, appoggiata peraltro politicamente da alcuni Paesi emergenti come ad esempio il Brasile, ha proposto un approccio unitario al tema della protezione dei diritti umani. Ci si sta riferendo all'Internet Bill of Rights. Nell'ottica di riconoscere la valenza di diritto fondamentale dell'accesso ad Internet[11], la medesima dottrina ha proposto una modifica alla Costituzione italiana con l'introduzione di un apposito disposto[12]. Tuttavia al momento tale proposta non ha avuto seguito. A parere della suddetta dottrina è altresì opportuno concentrare l'attenzione sulla trasparenza e sul controllo in riferimento ai giganti della Rete, ossia ai quei centri di potere, soprattutto economici, che con le loro direttive aziendali possono minare i diritti fondamentali di milioni di persone che utilizzano i servizi forniti dagli stessi[13]. Se da un lato il Congresso americano ha proposto un progetto - cd. Global Online Freedom Act - che obbliga dette compagnie ad informare uno specifico comitato[14] di tutti i casi in cui sono stati filtrati o cancellati contenuti su richiesta di governi stranieri, dall'altro la proposta dell'Internet Bill of Rights vuole mantenere una dimensione globale del rispetto dei diritti fondamentali su Internet. Questo approccio di tipo multilivello è appropriato alla portata sovranazionale del rispetto dei diritti fondamentali collegato sia a dinamiche sociali ed economiche sia a poteri politici e costituzionali. Va osservato peraltro che, in una dimensione globale come la nostra, si sta gradualmente affermando una comunità di corti senza confini, in quanto questa risulta essere formata sia da organi di tipo sovranazionale (come ad esempio la Corte europea dei diritti umani, la Corte interamericana dei diritti umani e la Corte di giustizia delle comunità europee) sia da organi giudiziari nazionali, forti della persuasività acquisita dalle loro decisioni spesso di grande risonanza. Il caso tipico di questo modello è proprio Internet, dove giudici nazionali diversi non solo si citano tra loro nella soluzione di tematiche rilevanti inerenti il cyberspazio, ma formano pure un formante giurisprudenziale che vorrebbe essere, o per lo meno tenta di diventare, omogeneo.

5. Giurisdizione e competenza: le questioni aperte

Sotto diverso profilo è poi da tenere presente come la diffusione – in costante crescita nel nostro Paese – dell'utilizzo del *web* in svariati ambiti della vita economica e di relazione metta in crisi tutta una serie di principi dell'ordinamento che costituivano una base imprescindibile prima dell'era digitale: mi riferisco in particolare al principio cd. "di territorialità" che mostra tutti i suoi limiti con la diffusione delle comunicazioni in rete[15].

Numerose sono le difficoltà che possono sorgere nel momento in cui si tratta di individuare criteri certi su cui, ad esempio, fondare la giurisdizione e la competenza ovvero di risolvere le questioni preliminari concernenti l'ammissibilità e la proponibilità della relativa domanda giudiziale[16]. Tali incertezze possono

11 Come affermato dal Rapporto La Rue presentato alle Nazioni Unite l'11 maggio 2011.

12 Rubricato quale art. 21 bis, ovvero con l'emendamento dell'art. 21.

13 Basti pensare a Google, Yahoo!, Microsoft, Facebook.

14 Istituito presso il Dipartimento di Stato.

15 Sottolineando come i reati informatici siano potenzialmente privi di barriere spazio-temporali, ad es. M. Guernelli, *L'uso di strumenti o sistemi informatici per la realizzazione di reati in materia patrimoniale*, in "Riv. dir. pen. ec.", 2007, 192 ss; F. Resta, *La responsabilità penale del provider: tra laissez faire ed obblighi di controllo*, in "Giur. Merito", 2004, 1739 ss.

16 Il problema è stato già ampiamente rilevato in materia di reati informatici a proposito dell'imprecisa for-

tradursi in una tale dilatazione dei tempi da privare le eventuali sanzioni di efficacia deterrente, se non persino di impedire, in molti casi, di giungere ad una pronuncia sul merito. In tal modo viene però favorita l'ulteriore propagazione, o addirittura l'impunità, di talune delle condotte illecite in questione proprio in settori che coinvolgono diritti e libertà fondamentali della persona[17]. Tra gli esempi di incertezze interpretative su questioni di carattere preliminare per mancati riferimenti al web indico la recente disciplina della mediazione obbligatoria[18] che prevede, tra le materie interessate, anche quella relativa alla «diffamazione con il mezzo della stampa o con altro mezzo di pubblicità». Se l'esperimento del tentativo di mediazione nei casi di cui all'art. 5 è, come noto, condizione di procedibilità per la proposizione della relativa azione in giudizio, si tratta di valutare – in mancanza di riferimenti al web – se la diffamazione che fosse posta in essere via Internet rientri o meno in tale previsione. Ne consegue che la vittima di un tale illecito si troverebbe in situazione di incertezza su profili preliminari che condizionano alla base l'esercizio dell'azione per la tutela di diritti e con costi non trascurabili. Gran parte della giurisprudenza precisa infatti che la diffamazione realizzata via internet non possa essere equiparata a quella a mezzo stampa o con altri mezzi di pubblicità[19]. La stessa Cassazione di recente ha affermato, con riguardo alla fattispecie della diffamazione via web, che «ai fini dell'individuazione della competenza, sono inutilizzabili, in quanto di difficilissima, se non impossibile individuazione, criteri oggettivi unici, quali, ad esempio, quelli di prima pubblicazione, di immissione della notizia nella rete, di accesso al primo visitatore» e che pertanto non possano trovare applicazione né la regola stabilita dall'art. 8 c.p.p. né quella fissata dall'art. 9, comma 1, c.p.p.[20]. Detto ciò, precisa ulteriormente che «Attese le peculiari modalità di diffusione di notizie lesive dell'altrui reputazione allocate in un sito web (...) non può neppure sostenersi l'automatica trasposizione dei criteri fissati per i reati di diffamazione commessi con il mezzo della stampa»[21]. Ad esiti non diversi giunge la giurisprudenza in sede civile, evidenziando come il danno causato da un articolo che compaia su Internet sia del tutto autonomo ed indipendente da quello invece realizzato dalla pubblicazione dello stesso sulla versione cartacea del giornale[22]. Un'interessante sentenza è stata, ad esempio, resa nel 2010 dal Tribunale di Monza, che, a proposito di un caso di violazione dell'onore e della riservatezza realizzato tramite Facebook, non ha mancato di sottolineare la peculiarità dello strumento utilizzato da parte del suo autore per attuarla[23]. In particolare, il

mulazione utilizzata dalla Convenzione di Budapest (ratificata con legge 18 marzo 2008, n. 48) che definisce "competenza" quella che dovrebbe invece intendersi come "giurisdizione" determinando così non poche incertezze interpretative. Sul punto tra gli altri, M. Di Bitonto, La ratifica della Convenzione del Consiglio d'Europa sul cybercryme: profili processuali, in "Dir. Internet", 2008, 503 ss.

17 Per alcune considerazioni sul punto, si veda ad esempio il recente contributo di A. RICCI, *Il valore economico della reputazione nel mondo digitale. Prime considerazioni,* in "Contr. e impresa", 2010, 6, 1297 ss.

18 Art. 5 del D.lgs. 4 marzo 2010, n. 28.

19 Nel senso di differenziare la diffamazione via internet da quella a mezzo stampa, si vedano ad esempio Cass. pen., 26 Cass.pen., 15 maggio 2008, n. 24018, in "Guida al dir.", 2008, 33, 103; Trib. Milano, 15 marzo 2010, in "Foro Ambrosiano", 2010, 1, 23; e già Trib. Oristano, 25 maggio 2000, in "Riv.it.dir.proc.pen.", 2001, 1405. Un'ipotesi applicativa di un certo interesse è quella della responsabilità del direttore di un quotidiano *online* per diffamazione, a proposito della quale si esclude l'applicazione dell'art. 57 c.p. in quanto espressamente riferita alla pubblicazione mediante carta stampata: in tal senso, Cass.pen., 16 luglio 2010, n. 35511, in "Giur.it.", 2011, 6, con nota di M. Mascalzoni, *Sulla responsabilità del direttore di un quotidiano online per diffamazione*. Si registra tuttavia un orientamento giurisprudenziale volte invece ad applicare alla diffamazione via web la stessa diffamazione aggravata di cui all'art. 595, comma 3, c.p.: così, Cass.pen., 26 aprile 2011, n. 16307; Cass., 26 gennaio 2011, n. 2739 in "Dir. Pen. e Processo", 2011, 10, 1233; ed anche Trib. Bari, 20 maggio 2003, in "Giur. Merito", 2003, 1806. E su tali temi di recente anche S. Peron, *Internet, regime applicabile per i casi di diffamazione e responsabilità del direttore,* in "Resp. civ. e prev.", 2011, 1, 85.

20 Così Cass., 26 gennaio 2011, n. 2739, cit.

21 *Ibidem*.

22 Trib. Trani, 3 dicembre 2009, in" Giur. It.", 2010, 7, con nota di R. Lombardi, *Nota in tema di articolo diffamatorio via internet.*

23 Trib. Monza, 2 marzo 2010, in *Resp.civ.*, 2010, 5, 394; e

danno che si realizzasse e che continuerebbe a realizzarsi mediante l'immissione dell'articolo diffamatorio sul web, senza limiti di tempo finché non intervenisse un provvedimento interdittivo del giudice, sarebbe dotato «di propria reiterata e continuata efficacia lesiva» rispetto a quello realizzato con la pubblicazione sul cartaceo e per tale motivo aggraverebbe in modo particolare la lesione della personalità[24]. Si rende allora necessario riflettere su quali soluzioni potrebbero essere adottate al fine di non lasciare negli ordinamenti delle lacune; lacune che vanno a minare, alla base, l'esercizio di diritti in sede giudiziale con prospettazione di lungaggini e moltiplicazioni di costi al riguardo. In tale prospettiva si potrebbe, ad esempio, pensare alla previsione di un procedimento esperibile nelle fasi iniziali del processo di primo grado o di eventuale procedura arbitrale – con modalità e termini da definire – di tipo sommario che si concluda, in sostanza, con un provvedimento reclamabile e con esclusione della previsione di ricorso ordinario per Cassazione. Ciò è analogo a quanto si verifica per i provvedimenti emessi dal Giudice in sede di reclamo attraverso provvedimenti cautelari[25]. Una volta risolte le questioni di carattere pregiudiziale e/o preliminare, in tale fase ipotizzata, non dovrebbe più esservi il pericolo, dopo molti anni, di trattare lo stesso caso davanti ad altro Giudice[26]. Occorrerebbero in proposito, ovviamente, anche delle convenzioni internazionali il più possibili uniformi, al fine del riconoscimento di criteri condivisi in tema di giurisdizione e competenza dei fenomeni relativi all'utilizzo della rete. Del resto, nell'ottica di invocare la necessità di regole certe ed idonee a definire in modo celere le questioni preliminari e pregiudiziali di giurisdizione e competenza, possono essere richiamati anche taluni principi generali di rilevanza sovranazionale. Così il diritto del cittadino ad un processo giusto e di ragionevole durata trova fondamento oltre che nell'art. 111, comma 2, della nostra Costituzione anche nella stessa Carta dei diritti fondamentali dell'Unione europea – la cui applicazione è stata garantita dal Trattato di Lisbona, entrato in vigore il 1 dicembre 2009 – il cui art. 47 (Diritto a un ricorso effettivo e a un giudice imparziale) appunto stabilisce che «Ogni persona i cui diritti e le cui libertà garantiti dal diritto dell'Unione siano stati violati ha diritto ad un ricorso effettivo dinanzi ad un giudice, nel rispetto delle condizioni previste nel presente articolo» (comma 1) ovvero che «Ogni persona ha diritto a che la sua causa sia esaminata equamente, pubblicamente ed entro un termine ragionevole da un giudice indipendente e imparziale, precostituito per legge»[27]. Spunti altrettanto interessanti possono essere colti nell'art. 1, paragrafo 3-*bis* della Direttiva CE del 25 novembre 2009 n. 140 con cui si prevede che «i provvedimenti adottati dagli Stati membri riguardanti l'accesso o l'uso di servizi e applicazioni attraverso reti di comunicazione elettronica, da parte degli utenti finali, devono rispettare i diritti e le libertà fondamentali delle persone fisiche, garantiti dalla convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali e dai principi generali del diritto comunitario» (comma 1). La stessa previsione dispone altresì che «Qualunque provvedimento di questo tipo riguardante l'accesso o l'uso di servizi e applicazioni attraverso reti di comunicazione elettronica, da parte degli utenti finali, che ostacolasse tali diritti o libertà fondamentali può essere imposto soltanto se appropriato,

per un commento anche M.L. Bixio, *Social network e danno morale da diffamazione*, in "Riv. dir. inf. e informatica", 2010, 3, 467.

24 In questi termini, R. Lombardi, *Nota in tema di articolo diffamatorio via internet*, cit. nella nota sopra.

25 Si veda art. 669-*terdecies* c.p.c.

26 G. Siniscalchi, *Efficienza della giustizia civile, richiamo di Draghi. Sarà la volta buona?*, in www.osservatoriosullalegalita.org; sito consultato il 12/04/2013.

27 Tra le altre norme della Carte dei diritti fondamentali che possono assumere rilevanza in tale *contest* si possono menzionare, ad esempio, gli artt. 1 (dignità umana), 6 (diritto alla libertà e alla sicurezza), 7 (rispetto della vita privata e familiare), 8 (protezione dei dati di carattere personale) e 17 (diritto di proprietà). E si veda anche A. Giarda, *Il reato di stalking: profili procedurali*, intervento al convegno "*Mobbing* e *stalking*. Aspetti penali, procedurali e civili", 26 marzo 2011, che appunto ricorda come i principi fondamentali che reggono il sistema penale sono quelli di "stretta legalità penale" e di "stretta legalità processuale".

proporzionato e necessario nel contesto di una società democratica e la sua attuazione deve essere oggetto di adeguate garanzie procedurali conformemente alla convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali e ai principi generali del diritto comunitario, inclusi un'efficace tutela giurisdizionale e un giusto processo. Tali provvedimenti possono di conseguenza essere adottati soltanto nel rispetto del principio della presunzione d'innocenza e del diritto alla *privacy*. Deve essere garantita una procedura preliminare equa ed imparziale, compresi il diritto della persona e delle persone interessate di essere ascoltate, fatta salva la necessità di presupposti e regimi procedurali appropriati in casi di urgenza debitamente accertata conformemente alla convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali. Deve essere garantito il diritto ad un controllo giurisdizionale efficace e tempestivo» (comma 2).

È opportuno sottolineare, in tale contesto, l'importanza della recente sentenza della Corte di Giustizia Europea secondo la quale «in caso di asserita violazione dei diritti della personalità per mezzo di contenuti messi in rete su un sito internet, la persona che si ritiene lesa ha la facoltà di esperire un'azione di risarcimento, per la totalità del danno cagionato, o dinanzi ai giudici dello Stato membro del luogo di stabilimento del soggetto che ha emesso tali contenuti, o dinanzi ai giudici dello Stato membro in cui si trova il proprio centro di interessi. In luogo di un'azione di risarcimento per la totalità del danno cagionato, tale persona può altresì esperire un'azione dinanzi ai giudici di ogni Stato membro sul cui territorio un'informazione messa in rete sia accessibile oppure lo sia stata.

Questi ultimi sono competenti a conoscere del solo danno cagionato sul territorio dello Stato membro del giudice adito».

La Corte stessa ha altresì precisato che «l'art. 3 della Direttiva del Parlamento Europeo e del Consiglio 8 giugno 2000, 2000/31/CE, relativa a taluni aspetti giuridici dei servizi della società dell'informazione, in particolare il commercio elettronico, nel mercato interno ("direttiva sul commercio elettronico") deve essere interpretato nel senso che esso non impone un recepimento in forma di norma specifica di conflitto.

Nondimeno, per quanto attiene all'ambito regolamentato, gli Stati membri devono assicurare che, fatte salve le deroghe autorizzate, alle condizioni previste dall'art. 3, n. 4 della direttiva 2000/31, il prestatore di un servizio del commercio elettronico non sia assoggettato a prescrizioni più rigorose di quelle previste dal diritto sostanziale applicabile nello Stato membro di stabilimento di tale prestatore»[28]. Si tratta di una pronunzia che sarà sicuro punto di riferimento nella soluzione dei problemi in tema di giurisdizione e competenza di cui sopra.[29] Anche alla luce di tale sentenza sembrerebbe urgente la necessità di previsioni di discipline globali uniformi, al fine non solo di prestare effettiva tutela a diritti inviolabili dell'individuo, ma pure per non calpestare le garanzie e le libertà fondamentali dei *server provider* e degli utenti della rete in generale. Il tema è estremamente delicato, dovendosi trovare il giusto equilibrio tra esigenze parimenti meritevoli di tutela. In proposito rilevo che su tali profili di grande rilevanza, attualità e delicatezza si è avviata recentemente, il 1 novembre 2011 presso il Queen Elizabeth Conference Center di Londra, una conferenza internazionale sul web con la partecipazione di molti Paesi nonché di numerosi protagonisti delle innovazioni della rete. Ciò a conferma della grande importanza delle tematiche da affrontare per la ricerca di soluzioni auspicabilmente globali ed idonee a trovare un giusto equilibrio anche tra sicurezza e tutela dei diritti.[30]

28 Così si legge nella sentenza della Corte di Giustizia UE (Grande Sezione) in data 25 ottobre 2011 nei procedimenti riuniti C-509/09 e C-161/10.

29 Per un puntuale richiamo e commento di tale pronuncia si veda l'articolo di G.Mira Marq, *Diffamazione online, Corte UE: fatto all'estero, processato nello Stato del danneggiato*, nel sito dell'Osservatorio sulla legalità e sui diritti Onlus: http://www.osservatoriosullalegalita.org/11/acom/10ott2/2929gabueinternet.htm; sito visitato il 23/04/2013.

30 Per qualche news di aggiornamento, con riferimento a tale conferenza mondiale, si veda l'articolo *Sicurezza di Internet: c'è rischio di censura* in data 2 novembre 2011 all'URL www.romagnanoi.it; sito visitato il 12/04/2013.

Il 21 settembre 2011, peraltro, il Comitato dei ministri del Consiglio d'Europa ha adottato una dichiarazione sui principi della *governance* in rete, in cui riafferma la difesa dei diritti e delle libertà ed individua come autori delle regole di gestione della rete – di concerto – tutti i soggetti portatori d'interessi, dai governi alle associazioni, ai tecnici ed agli stessi utenti[31]. Essa afferma tra l'altro che «I meccanismi di *governance* della rete devono garantire la tutela di tutti i diritti e le libertà fondamentali ed affermare la loro universalità, l'indivisibilità, l'interdipendenza e interrelazione in conformità con il diritto internazionale dei diritti umani. Essi devono inoltre garantire il pieno rispetto della democrazia e dello Stato di diritto e dovrebbero promuovere lo sviluppo sostenibile. Tutti gli attori pubblici e privati dovrebbero riconoscere e difendere i diritti umani e le libertà fondamentali nelle loro operazioni e attività, così come nella progettazione di nuove tecnologie, servizi e applicazioni. Essi devono essere consapevoli degli sviluppi che portano alla valorizzazione dei – così come le minacce per – diritti e le libertà fondamentali, e pienamente partecipare agli sforzi volti a riconoscere i diritti emergenti». Inoltre «lo sviluppo e la realizzazione di accordi di *governance* di Internet dovrebbero garantire, in modo aperto, trasparente e responsabile, la piena partecipazione di governi, settore privato, società civile, comunità tecnica ed utenti, tenendo conto dei loro specifici ruoli e responsabilità. Lo sviluppo internazionale delle politiche pubbliche legate ad Internet e i meccanismi di *governance* di Internet dovrebbe consentire la piena partecipazione e pari di tutti gli attori di tutti i Paesi». Ancora, «gli utenti devono essere pienamente autorizzati ad esercitare i loro diritti e le libertà fondamentali, prendere decisioni informate e partecipare ad accordi di *governance* di Internet, in particolare nei meccanismi di *governance* e nello sviluppo di Internet legate all'ordine pubblico, in piena fiducia e libertà [...]. Gli utenti dovrebbero avere il più ampio accesso ad Internet, a contenuti, applicazioni e servizi di loro scelta, anche se non sono offerti gratuitamente, tramite appositi dispositivi di loro scelta. Misure di gestione del traffico che hanno un impatto sul godimento dei diritti e delle libertà fondamentali, in particolare il diritto alla libertà di espressione e di comunicare e ricevere informazioni senza riguardo a frontiere, così come il diritto al rispetto della vita privata, devono soddisfare i requisiti di diritto internazionale sulla tutela della libertà di espressione e di accesso all'informazione ed il diritto al rispetto della vita privata». A giugno 2011 anche le Nazioni Unite hanno preso una posizione ufficiale sul diritto a connettersi in rete. In un rapporto[32] del Relatore speciale dell'ONU, Frank La Rue, sulla promozione e la protezione del diritto alla libertà di opinione e di espressione si legge infatti: «Togliere l'accesso degli utenti ad Internet è una misura sproporzionata, qualunque ne sia il motivo, compresa la tutela del *copyright*. È una violazione dell'art. 19, paragrafo 3, della Convenzione internazionale dei diritti civili e politici». La relazione delinea poi quattro casi eccezionali che abilitano gli Stati a proibire ed a criminalizzare in base al diritto internazionale: pedopornografia, incitamento a commettere genocidio, incitamento alla discriminazione, all'odio o alla violenza ed incitamento al terrorismo. Il rapporto ONU raccomanda che gli Stati si astengano dal criminalizzare tutte le altre forme di espressione e delinea anche le garanzie che devono essere osservate per prevenire la censura dei contenuti con la giustificazione di obiettivi apparentemente legittimi. Certo è che tale argomento presenta ogni giorno nuove sfide che dovranno essere affrontate con costanza e lungimiranza.

Monica Suerz è laureata in Comunicazione e Pubblicità (curriculum aziendale-pubblicitario). Attualmente laureanda in Scienze della Comunicazione pubblica, d'impresa e pubblicità presso l'Università degli Studi di Trieste

monicasuerz@gmail.com

31 Si vada al link https://wcd.coe.int/ViewDoc.jsp?id=1835773; sito visitato il 12/04/2013.

32 Si vada al link http://www.ohchr.org/Documents/Issues/Opinion/A.66.290.pdf; sito visitato il 12/04/2013.