UNIVERSITÀ DEGLI STUDI DI TRENTO
Facoltà di Giurisprudenza

RETI DI LIBERTÀ

Wireless Community Networks: un'analisi interdisciplinare

a cura di

ROBERTO CASO e FEDERICA GIOVANELLA

2015

IL DIRITTO CIVILE A CONFRONTO CON LE NUOVE TECNOLOGIE: *WIRELESS COMMUNITY NETWORKS* E RESPONSABILITÀ EXTRACONTRATTUALE[*]

Federica Giovanella

SOMMARIO: *1. Introduzione. 2. Peculiarità delle WCN e loro riflessi sul diritto (o «perché il diritto si deve occupare delle WCN»). 3. Quadro normativo: applicabilità del codice delle comunicazioni elettroniche alle WCN. 4. WCN e responsabilità civile. 4.1. Responsabilità del singolo utente. 4.2. Responsabilità dell'Internet Service Provider. 4.3. Responsabilità della WCN. 5. Possibili soluzioni prospettabili. 6. Riflessioni conclusive.*

1. Introduzione

Nell'epoca in cui ci troviamo appare ormai impossibile immaginare una società senza connessioni comunicative. Le cosiddette «information and communication technologies» (ICTs) hanno profondamente plasmato la società, a tal punto da essere diventate oltremodo necessarie nella maggioranza delle nostre attività quotidiane. Si pensi ad esempio alle comunicazioni effettuate con telefoni cellulari e *smartphone*, alle indicazioni stradali ottenute dai navigatori satellitari o, più di recente, da *smartphone* e *tablet*, nonché alle miriadi di attività lavorative ormai impensabili senza un *personal computer* e una connessione ad Internet. Proprio Internet può essere considerata la tecnologia che ha maggiormente influito sulla società contemporanea in termini quantità e qualità di comunicazioni: la necessità di un continuo contatto e di una costante rintracciabilità è oggi molto sentita, soprattutto nelle generazioni più giovani. Il far parte di una «rete», sia in senso sociale che comunicati-

[*] Il presente contributo è una versione modificata, sviluppata e aggiornata di un precedente contributo pubblicato ne *Il diritto dell'informazione e dell'informatica*, n. 6/2014.

vo, è oggigiorno non soltanto un comportamento normale, ma anche un'esigenza.

La nascita delle Wireless Community Networks (WCN – o «reti wireless comunitarie» – RWC) è probabilmente figlia di queste necessità comunicative. Per meglio dire, la nascita di queste reti è da ascriversi a diversi fattori, fra cui indubbiamente anche la volontà e l'esigenza di comunicare e confrontarsi.

Come si evince dal primo capitolo del presente libro[1], le WCN sono reti spontanee, nascenti da gruppi di cittadini che installano nodi wireless sui tetti o sui balconi delle loro case. Lo scopo principale che spinge alla creazione di queste reti è il loro alto grado d'indipendenza e di anonimato, che permette la veicolazione di diversi servizi. Fra le varie potenzialità di queste reti, vi è anche quella di saper portare connettività a Internet in zone scoperte dagli operatori commerciali.

L'allargarsi della comunità, sia in termini di numero di nodi sia di numero di soggetti, permette che queste reti passino dal semplice ruolo di strumento per accedere a Internet al ruolo ben più cruciale di mezzo di comunicazione, svincolato da logiche di mercato e partecipato dalla popolazione. Attraverso questo mezzo si agevola la coesione della comunità stessa, con importanti rilievi pratici positivi soprattutto per i luoghi che si presentano più isolati in termini di accesso ad Internet e ad altri mezzi comunicativi.

Sebbene le WCN mostrino molte potenzialità, evidenziate anche dall'Organizzazione per la Cooperazione e lo Sviluppo Economico[2], esse presentano indubbi profili di criticità dal punto di vista del diritto. Ciò nonostante, ad oggi queste reti sono state analizzate in maniera prevalente soltanto da ingegneri e scienziati dell'informazione o da sociologi[3]. La loro analisi sotto il profilo giuridico è stata per lo più ne-

[1] Faccio riferimento al contributo di Leonardo Maccari e Tania Bailoni in questo volume.

[2] Si veda il *report* dell'OECD, *Development of Wireless Local Area Networks in OECD Countries*, *OECD Digital Economy Papers*, No. 71, 2003, <http://dx.doi.org/10.1787/233145088433>.

[3] Fra i moltissimi contributi in materia di scienza dell'informazione si vedano quali esempi: R. FLICKENGER, *Building Wireless Community Networks. Implementing the Wireless Web*, Sebastopol, 2001; I.F. AKYILDIZ, X. WANG, W. WANG, *Wireless mesh*

gletta[4]. Ciò è particolarmente vero in relazione agli aspetti più strettamente legati alla responsabilità civile nascente dalla diffusione e utilizzazione delle reti comunitarie.

Il presente contributo si pone lo scopo, da un punto di vista della legislazione euro-italiana, di iniziare a colmare l'esistente vuoto dottrinale, analizzando le WCN sotto il profilo delle potenziali criticità che le stesse possono presentare in tema di responsabilità extracontrattuale. L'analisi sarà preceduta da un breve inquadramento legislativo, al fine di aiutare una maggiore comprensione giuridica del fenomeno nella sua interezza. L'analisi della sola normativa italiana, sebbene possa ad un primo sguardo sembrare semplicistica e riduttiva, si pone in realtà come caso studio, anche in considerazione del fatto che nel nostro ordinamento esistono e stanno fiorendo numerose reti wireless comunitarie[5].

Il contributo si articola nel modo seguente: nel prossimo paragrafo si analizzeranno le caratteristiche delle reti comunitarie e gli effetti di tali caratteristiche sulle norme di responsabilità extracontrattuale; si passerà poi, nel terzo paragrafo, ad illustrare il quadro normativo applicabile. Il

---

networks: a survey, 47 *Computer Networks* 445, 2005; J. ISHMAEL, S. BURY, D. PEZAROS, N. RACE, *Deploying Rural Community Wireless Mesh Networks*, 12 *IEEE Internet Computing* 4, 22, 2008; e più di recente: L. MACCARI, R. LO CIGNO, *A Week in the Life of Three Large Wireless Community Networks*, in *Ad Hoc Networks*, 2014, in corso di pubblicazione. Si vedano anche i seguenti progetti finanziati dall'Europa mediante il VII Programma Quadro: www.confine-project.eu, www.clommunity-project.eu. Sul fronte sociologico si considerino, fra i molti: A. POWELL, *WiFi Publics: Producing Community and Technology*, in *Information, Communication and Society*, n. 8/2008, 1068; L. FORLANO, *Anytime? Anywhere?: Reframing Debates around Community and Municipal Wireless Networking*, in *Journal of community informatics*, n. 1/2008; P. ANTONIADIS ET AL., *Community building over Neighborhood Wireless Mesh Networks*, in *IEEE Society and Technology*, n. 1/2008, 48.

[4] Rare eccezioni sono costituite dai seguenti contributi: M. DULONG DE ROSNAY, *Peer-to-peer as a Design Principle for Law*, in *Journal of Peer Production*, 2014, in corso di pubblicazione. P. DE FILIPPI, *It's Time to Take Mesh Networks Seriously (and not just for the Reasons You Think)*, Wired.com, 1 February 2014, <http://www.wired.com/opinion/2014/01/its-time-to-take-mesh-networks-seriously-and-not-just-for-the-reasons-you-think/>; J.S. HATCHER, *Mesh Networks: A Look at the Legal Future*, 2005, <http://ssrn.com/abstract=814984>.

[5] Per una lista delle WCN attualmente presenti nel nostro Paese si consulti: http://en.wikipedia.org/wiki/List_of_wireless_community_networks_by_region#Italy.

quarto paragrafo sarà dedicato alla disamina delle situazioni da cui possono scaturire problematiche di responsabilità extracontrattuale, considerando di volta in volta i vari soggetti implicati. Nel successivo paragrafo si tenterà di fornire alcune possibili soluzioni. L'ultimo paragrafo sarà costituito da brevi riflessioni conclusive.

2. Peculiarità delle WCN e loro riflessi sul diritto (o «perché il diritto si deve occupare delle WCN»)

Come anticipato, la tematica delle reti wireless comunitarie è stata oggetto di ampi e approfonditi studi soprattutto in materie tecniche, quali l'ingegneria informatica e la scienza dell'informazione. Anche altre branche del sapere se ne sono occupate in minor misura, come nel caso della sociologia. Altre ancora non hanno, di fatto, mai indagato questo fenomeno. In quest'ultima categoria rientra a pieno titolo la scienza giuridica, i cui studiosi non hanno, ad oggi, posto particolare attenzione alle WCN, fatte salve alcune rare eccezioni[6].

Volendo immaginare una motivazione sottostante a tale scarsa attenzione, potremmo pensare alla mancanza di implicazioni giuridiche derivanti dalle WCN. In verità, sebbene ad oggi non esistano casi concreti pendenti o decisi innanzi agli organi giurisdizionali, numerose possono essere le conseguenze giuridiche connesse alla diffusione e all'uso delle reti comunitarie senza fili.

Prima di addentrarsi nella disamina di tali possibili conseguenze, è bene illustrare quali profili delle WCN siano di interesse per il diritto. Più in dettaglio, occorre considerare le caratteristiche che rendono queste reti un fenomeno diverso e peculiare nel panorama delle tecnologie della comunicazione.

Cercando di riassumere in poche righe le tipicità delle WCN, e senza ripetere quanto già da altri meglio descritto[7], occorre innanzitutto ribadire come queste reti nascano con un approccio «bottom-up», ovvero «dal basso», attraverso l'iniziativa di persone che si formano una

[6] Si vedano i contributi già citati in nota n. 4.

[7] Si veda il capitolo di Leonardo Maccari e Tania Bailoni in questo volume, nonché i contributi citati *supra* in nota n. 3.

comunità. Su queste basi le persone creano reti autogestite che hanno nella comunità stessa il loro senso d'esistenza. Lo scopo di queste reti è essenzialmente quello di permettere l'interazione fra gli utenti, per esempio con messaggi o chiamate. Per il modo in cui queste reti sono concepite e costruite, esse possono anche consentire una connessione ad Internet. Di fatto, pertanto, sebbene le WCN non debbano essere intese come gratuiti sostituti di una connessione ad Internet, esse permettono di portare connettività laddove, per i motivi più disparati, non sia disponibile.

Queste reti sono basate su una tecnologia distribuita, in cui ciascun nodo genera traffico e al contempo «trasporta» il traffico di altri nodi. Affinché la rete possa connettersi ad Internet è sufficiente che anche uno o più di uno di questi nodi sia connesso ad Internet. Tali nodi fungono da porte (sono invero detti «gateway») e permettono che la rete sia collegata ad Internet.

L'approccio *bottom-up* che caratterizza le WCN si riflette nell'assoluta mancanza di un'organizzazione gerarchica. Non esiste infatti alcuna amministrazione centrale o un qualsivoglia organo che abbia funzioni di controllo e gestione o anche soltanto con poteri rappresentativi. Ciascun utente è responsabile solo del proprio nodo e la rete è semplicemente una struttura spontanea che si basa sulla sottostante comunità e attraverso di essa si alimenta.

Senza voler anticipare ciò di cui si parlerà diffusamente nei prossimi paragrafi, basti qui accennare che l'assenza di un centro di imputazione nelle WCN si rivela particolarmente rilevante per l'applicabilità delle vigenti normative. Ciò vale sia per la regolamentazione amministrativa di queste, sia per l'applicabilità delle norme di responsabilità civile.

A fianco di queste peculiarità, fra le molteplici caratteristiche delle reti wireless comunitarie ha un'indubbia importanza l'elevato livello di anonimato goduto dagli utenti. Ciò è dovuto principalmente all'assenza di misure di registrazione e archiviazione degli indirizzi IP. Infatti, proprio come accade nell'ambiente di Internet, ciascun nodo (e, quindi, ciascun utente) è identificato da un *Internet Protocol address*. Vi è però una profonda differenza nelle modalità di gestione di questi numeri nei due contesti. Nel caso di Internet, l'indirizzo IP (sia esso statico o dinamico) è assegnato dal gestore dei servizi che fornisce la connessione

alla rete Internet. Gli ISP sono inoltre tenuti a registrare e archiviare questi dati, quantomeno per fini contabili[8]. Nel caso delle WCN, invece, sono gli stessi utenti ad assegnarsi un indirizzo IP che può essere modificato in ogni momento. Se da un punto di vista teorico ogni nodo potrebbe essere identificabile attraverso l'IP di cui si è dotato, praticamente ciò non è possibile, in quanto non esistono *data base* o registri in cui gli indirizzi siano memorizzati a futuro utilizzo. Date queste premesse appare di fatto impossibile risalire con certezza al nodo e, quindi, al soggetto che fosse titolare di un determinato indirizzo IP in un determinato momento.

Anche questa caratteristica delle reti wireless comunitarie, proprio come l'inesistenza di un centro di responsabilità, ha un forte impatto sull'applicabilità di alcune norme giuridiche di rilievo, *in primis* quelle strettamente connesse alla responsabilità extracontrattuale.

Da un punto di vista giuridico, infine, è interessante considerare le modalità di regolamentazione interna di queste reti. Invero, sebbene non esistano regole scritte oppure contratti, gli utenti si autoregolamentano attenendosi a codici di condotta interni. Chi voglia entrare a far

[8] Già a partire dalla Dir. 97/66/CE (del Parlamento europeo e del Consiglio, del 15 dicembre 1997, sul trattamento dei dati personali e sulla tutela della vita privata nel settore delle telecomunicazioni), trasposta nel nostro ordinamento con d.lgs. 13.05.1998, n. 171 (di modifica della L. 31 dicembre 1996, n. 675, di attuazione della Dir. 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati) esistono in capo ai gestori di servizi di telecomunicazione una serie di obblighi in fatto di archiviazione dei dati del traffico degli utenti/abbonati. Tali obblighi sono stati rafforzati con la Dir. C.d. «Data retention» (Dir. 2006/24/CE del Parlamento europeo e del Consiglio, del 15 marzo 2006, riguardante la conservazione di dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione – di modifica della direttiva 2002/58/CE del Parlamento europeo e del Consiglio, del 12 luglio 2002, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche) che, anche ai fini di contrastare il terrorismo internazionale, prevedevano obblighi di conservazione dei dati del traffico per un minimo di 6 mesi fino ad un massimo di 24. Tale ultima direttiva è stata di recente dichiarata invalida dalla Corte di Giustizia dell'Unione europea perché interferiva in modo eccessivo con i fondamentali diritti di riservatezza della vita privata e di protezione dei dati personali (CGE 8 aprile 2014, cause riunite C-293/12 eC-594/12).

parte della rete, della comunità e del progetto ad esse sottostante, deve condividerne i principi di partecipazione e diffusione della conoscenza[9]. L'idoneità di un «candidato» è vagliata dagli utenti già facenti parte della comunità: se essi ritengono che tale nuovo entrato non si comporti in modo consono ai principi non scritti esistenti all'interno della stessa, possono escluderlo dalla rete attraverso modalità tecniche. Ciò vale, ovviamente, anche per soggetti che siano già parte della rete e cessino di rispettare le norme interne. Conseguentemente, da un punto di vista giuridico, questo «ordinamento interno» meriterebbe una certa attenzione, quale espressione di norme sociali, considerate come standard e regole informali interne ad un determinato gruppo, che regolano il comportamento di quello specifico gruppo[10].

Chiudendo questo breve paragrafo che accenna alle particolarità delle reti in esame, si vuole chiarire che, sebbene l'analisi dei risvolti giuridici delle WCN possa apparire un mero esercizio grammaticale, ciò è solo parzialmente vero. Infatti, anche se ad oggi non si riscontrano controversie, queste reti registrano una sempre maggiore diffusione e un costante allargamento in termini di copertura territoriale e di numeri di nodi-utenti connessi. La tecnologia su cui queste reti sono basate permette la connessione di migliaia di nodi, per cui già oggi alcune WCN sono un fenomeno di massa che raccoglie migliaia di utenti, come nei casi Atene e Barcellona[11].

---

[9] Si veda il Pico Peering Agreement: http://www.picopeer.net/PPA-it.html. La rete comunitaria di Firenze e Roma (www.ninux.org) richiede all'utente di accettare le regole del Pico Peering Agreement quale requisito di accesso alla WCN.

[10] Invero, dato che ogni nodo non è altro che una piccola antenna che ha un determinato raggio d'azione, spostare l'antenna in una diversa direzione significa estromettere uno o più nodi e, in particolare, i nodi di coloro che non sono più accettati dalla comunità. Questi comportamenti così come, più in generale, la stessa architettura delle reti comunitarie, richiamano il funzionamento delle tecnologie di peer-to-peer per la condivisione di file, che molti Autori hanno ritenuto essere governate da norme sociali. Si vedano ad esempio L. STRAHILEVITZ, *Charismatic Code, Social Norms, and the Emergence of Cooperation on the File-Sharing Networks*, in *Virginia Law Review*, n. 3/2003, 505; M.F. SCHULTZ, *Copynorms: Copyright and Social Norms*, in P.K. YU (cur.), *Intellectual Property and Information Wealth*, Westport, 2006, 201.

[11] Sono la Athens Wireless Metropolitan Network (http://awmn.net) e la rete Guifi in Catalonia (http://guifi.net), sulle quali si veda il capitolo di Leonardo Maccari e Ta-

Effettuate queste premesse si passerà ora ad illustrare brevemente il quadro normativo in cui esse si inscrivono, con lo scopo di comprendere se e in che modo le normative oggi esistenti in tema di comunicazioni elettroniche siano o meno applicabili alle reti qui esaminate.

3. Quadro normativo: applicabilità del codice delle comunicazioni elettroniche alle WCN

Fra i primi interrogativi il giurista si pone di fronte ad una nuova tecnologia, vi è indubbiamente quello della sua «legalità». Per quanto riguarda le reti wireless comunitarie, ciò è da intendersi innanzitutto come valutazione circa i requisiti giuridici che sono alla base della creazione e dello sviluppo di un'infrastruttura come quella in esame. È noto, infatti, che i sistemi di comunicazione sono regolamentati a vari livelli, in primo luogo dal diritto amministrativo. Peraltro, la disciplina delle comunicazioni elettroniche si basa su numerosi interventi dell'Unione europea che, nell'intento di regolamentare i mercati delle comunicazioni elettroniche, ha inciso a più riprese sulla normativa ad esse relativa.

Venendo al sistema italiano, le norme di riferimento si sostanziano nel c.d. «Codice delle comunicazioni elettroniche», ovverosia il d.lgs. 1° agosto 2003, n. 259 (Cod. Com. El.). Come menzionato, i copiosi interventi dell'Unione europea in materia hanno fortemente inciso sulla normativa del nostro Paese in materia, tanto da necessitare l'emanazione di un testo unico che potesse ricomprendere l'intera disciplina, ripensandola in modo organico. Il Codice, infatti, rappresenta in primo luogo la risposta ad un pacchetto di direttive europee emanate nel corso del 2002, con lo scopo di regolamentare il settore (e il mercato) delle comunicazioni elettroniche[12]. Le direttive del 2002 rappresentano un

---

nia Bailoni nel presente volume. Molte altre reti sono sparse per l'Europa e negli altri continenti: se ne veda una lista all'url: <http://en.wikipedia.org/wiki/List_of_wireless_community_networks_by_region>.

[12] Ci si riferisce a: Dir. 2002/19/CE del Parlamento europeo e del Consiglio, del 7 marzo 2002, relativa all'accesso alle reti di comunicazione elettronica e alle risorse correlate, e all'interconnessione delle medesime (direttiva accesso); Dir. 2002/20/CE

importante *step* all'interno di un lungo percorso di normazione europea in materia di telecomunicazioni iniziato nel 1990 allo scopo di raggiungere la privatizzazione dei servizi[13]. Tale percorso si è incessantemente protratto fino al 2009, quando sono state emanate ulteriori direttive, che sono usualmente ricondotte, assieme ad un regolamento dello stesso anno, sotto l'etichetta «Pacchetto Telecom»[14]. Il Codice delle Comuni-

---

del Parlamento europeo e del Consiglio, del 7 marzo 2002, relativa alle autorizzazioni per le reti e i servizi di comunicazione elettronica (direttiva autorizzazioni); Dir. 2002/21/CE del Parlamento europeo e del Consiglio, del 7 marzo 2002, che istituisce un quadro normativo comune per le reti ed i servizi di comunicazione elettronica (direttiva quadro); Dir. 2002/22/CE del Parlamento europeo e del Consiglio, del 7 marzo 2002, relativa al servizio universale e ai diritti degli utenti in materia di reti e di servizi di comunicazione elettronica (direttiva servizio universale).

Sulla regolazione delle comunicazioni elettroniche si vedano per tutti: M. CLARICH, G.F. CARTEI, *Il codice delle comunicazioni elettroniche*, Milano, 2004; F. DONATI, *L'ordinamento amministrativo delle comunicazioni*, Torino, 2007; G. MORBIDELLI, F. DONATI (cur.), *La nuova disciplina delle comunicazioni elettroniche*, Torino, 2009; F. BASSAN (cur.), *Diritto delle comunicazioni elettroniche*, Milano, 2010; V.M. SBRESCIA, *L'Europa delle comunicazioni elettroniche*, Napoli, 2011.

[13] Dir. 90/387/CEE del Consiglio, del 28 giugno 1990, sull'istituzione del mercato interno per i servizi delle telecomunicazioni mediante la realizzazione della fornitura di una rete aperta di telecomunicazioni (Open Network Provision - ONP); Dir. 90/388/CEE della Commissione, del 28 giugno 1990, relativa alla concorrenza nei mercati dei servizi di telecomunicazioni. Successivamente si ebbero: Dir. 96/19/CE della Commissione, del 13 marzo 1996, che modifica la direttiva 90/388/CEE al fine della completa apertura alla concorrenza dei mercati delle telecomunicazioni; Dir. 97/13/CE del Parlamento europeo e del Consiglio, del 10 aprile 1997, relativa ad una disciplina comune in materia di autorizzazioni generali e di licenze individuali nel settore dei servizi di telecomunicazione; Dir. 97/33/CE del Parlamento europeo e del Consiglio del 30 giugno 1997 sull'interconnessione nel settore delle telecomunicazioni e finalizzata a garantire il servizio universale e l'interoperabilità attraverso l'applicazione dei principi di fornitura di una rete aperta (ONP); Dir. 98/10/CE del Parlamento europeo e del Consiglio del 26 febbraio 1998 sull'applicazione del regime di fornitura di una rete aperta (ONP) alla telefonia vocale e sul servizio universale delle telecomunicazioni in un ambiente concorrenziale. Successivamente vi furono le direttive del 2002 citate *supra* in nota n. 8.

[14] Regolamento (Ce) n. 1211/2009 del Parlamento europeo e del Consiglio del 25 novembre 2009 che istituisce l'Organismo dei regolatori europei delle comunicazioni elettroniche (BEREC) e l'Ufficio; Dir. 2009/136/CE del Parlamento europeo e del Consiglio del 25 novembre 2009 recante modifica della direttiva 2002/22/CE relativa al

cazioni Elettroniche segue lo stesso percorso. Come accennato, esso è nato dall'esigenza e con lo scopo di implementare il gruppo di direttive europee del 2002, divenendo così l'occasione per un riordino della normativa in materia di telecomunicazioni.

Venendo ora alla tematica delle WCN, ci si soffermerà soltanto sulle norme del codice a tutt'oggi in vigore e sulle disposizioni che alle reti in esame possono applicarsi. Occorre in primo luogo interrogarsi sull'esistenza di norme che regolino la creazione ed installazione di una *wireless community network*.

L'art. 104 del Codice rende necessario l'ottenimento di una «autorizzazione generale» per una serie di attività, anche laddove esse possano essere qualificate come «private». Esiste tuttavia una gamma di deroghe applicabili alle reti che non siano ad «uso pubblico», regolate dal Titolo III del Codice, rubricato «Reti e servizi di comunicazione elettronica ad uso privato». Le deroghe ammettono ampia libertà di utilizzo in diverse fattispecie e si affiancano ad un regime autorizzatorio che, per le reti ad uso privato, differisce da quello generale[15].

Il regime generale di autorizzazione è imperniato sulla nozione di «servizi di comunicazione elettronica», come fornita dalla dir. 2002/21 c.d. «direttiva quadro». L'art. 1 Cod. Com. El. considera tali «i servizi, forniti di norma a pagamento, consistenti esclusivamente o prevalentemente nella trasmissione di segnali su reti di comunicazione elettronica, compresi i servizi di telecomunicazioni e i servizi di trasmissione nelle reti utilizzate per la diffusione circolare radiotelevisiva […] esclusi i servizi della società dell'informazione di cui all'articolo 2, comma 1,

---

servizio universale e ai diritti degli utenti in materia di reti e di servizi di comunicazione elettronica; Dir. 2009/140/CE del Parlamento europeo e del consiglio del 25 novembre 2009 recante modifica delle direttive 2002/21/CE che istituisce un quadro normativo comune per le reti ed i servizi di comunicazione elettronica, 2002/19/CE relativa all'accesso alle reti di comunicazione elettronica e alle risorse correlate, e all'interconnessione delle medesime e 2002/20/CE relativa alle autorizzazioni per le reti e i servizi di comunicazione elettronica (direttiva c.d. «Better regulation»).

Sull'evoluzione del sistema si veda F. BASSAN, *Dalle telecomunicazioni alle comunicazioni elettroniche: motivi e percorsi di una riforma permanente*, in F. BASSAN (cur.), *op. cit.*, 3 ss.; V.M. SBRESCIA, *op. cit.*, 1 ss.

[15] A. BOSO CARETTA, *La disciplina del regime autorizzatorio. Le misure di armonizzazione*, in F. BASSAN (cur.), *Diritto delle comunicazioni elettroniche*, cit., 67.

lettera a), del decreto legislativo 9 aprile 2003, n. 70, non consistenti interamente o prevalentemente nella trasmissione di segnali su reti di comunicazione elettronica»[16].

Lasciando per un attimo da parte la categoria dei «servizi della società dell'informazione» di cui ci occuperemo più avanti, la definizione riportata va interpretata nel senso che l'autorizzazione è obbligatoria per quei servizi che consistono nel trasmettere segnali, attraverso reti di comunicazione elettronica (con mezzi elettromagnetici), ma sono invece esclusi da tale autorizzazione i servizi che forniscano solo contenuti[17].

A mente di tale obbligatorietà, occorre comprendere cosa si intenda per autorizzazione. Si occupa di tale compito l'art. 1, lett. g) che definisce l'autorizzazione come «il regime giuridico che disciplina la fornitura di reti o di servizi di comunicazione elettronica, anche ad uso privato, ed i relativi obblighi specifici per il settore applicabili a tutti i tipi o a tipi specifici di servizi e di reti di comunicazione elettronica, conformemente al Codice».

Per la definizione di «servizio di comunicazione elettronica ad uso privato» possiamo fare nuovamente riferimento all'art. 1, lett. ff) che considera tale «un servizio di comunicazione elettronica svolto esclusivamente nell'interesse proprio dal titolare della relativa autorizzazione generale». A ciò va aggiunta l'ulteriore caratteristica, o meglio: restrizione, dettata dall'art. 101, co. 1, secondo cui chi sia titolare di autorizzazione generale ad uso privato può usare le reti di comunicazione solamente per trasmettere dati ed attività di propria pertinenza, con esplicito divieto di effettuare traffico per conto terzi.

Un'interpretazione letterale di queste disposizioni farebbe propendere per la non qualificabilità delle reti wireless comunitarie come «reti ad uso privato»[18], con la conseguenza che occorrerebbero una serie di au-

[16] Art. 2, lett. c), Dir. 2002/21/CE e art. 1, lett. gg), d.lgs. 259/2003.

[17] A. BOSO CARETTA, *op. cit.*, 68. Questa definizione, al pari, come si vedrà, di quella di «servizio della società dell'informazione», è caratterizzata dalla questione della «fornitura di norma a pagamento», su cui si vedano le considerazioni *infra*.

[18] Cfr. l'interpretazione della norma fornita da F. BONELLI, *Uso privato ed uso aperto al pubblico di «reti alternative» di telecomunicazioni (art. 101)*, in M. CLARICH, G.F. CARTEI, *op. cit.*, 473 ss.

torizzazioni e vi sarebbero diverse limitazioni alla nascita e allo sviluppo di queste reti sul nostro territorio.

Occorre tuttavia considerare altre disposizioni del Codice, tra cui quella dell'art. 99 che prevede che alcune attività siano «in ogni caso libere». Tali attività «libere» sono elencate all'art. 105, rubricato «Libero uso», che include fra suddette attività, alla lett. b), anche quelle delle «reti locali di tipo radiolan e hiperlan» (lett. b). Rientrano in questa categoria, che si riferisce ai collegamenti Wi-Fi, anche le WCN, che si basano principalmente su frequenze di 2.4, 5.4-5.7 GHz[19]. Ne consegue che le reti wireless comunitarie non necessitano, ad oggi, di alcuna autorizzazione.

Uno scenario parzialmente differente si riscontrava prima del 2012. L'utilizzo delle tecnologie alla base delle WCN al di fuori del proprio fondo era da considerarsi soggetto ad autorizzazione generale in base sia al dettato dell'art. 105 che ai sensi dell'art. 104 co. 1, lett. c) n. 3.

La già menzionata lett. b) dell'art. 105, infatti, prevedeva che fossero ad uso libero «le apparecchiature che impiegano frequenze di tipo collettivo, senza alcuna protezione, per collegamenti a brevissima distanza con apparati a corto raggio, compresi quelli rispondenti alla raccomandazione CEPT/ERC/REC 70-03» fra cui rientravano le «reti locali di tipo radiolan e hiperlan nell'ambito del fondo»[20].

[19] Si veda la spiegazione fornita sul sito della rete wireless di Roma-Firenze: http://wiki.ninux.org/LeggiWireless. Per ulteriori delucidazioni si veda il portale dell'Ispettorato territoriale della Liguria per il Ministero dello sviluppo economico: http://www.comunicazioniliguria.it/wifi.html.

[20] Per la definizione di «ambito del proprio fondo», l'art. 105 richiama l'art. 99 co. 5 Cod. Com. El. L'art. 99 rubricato «Installazione ed esercizio di reti e servizi di comunicazione elettronica ad uso privato», recita al co. 5: «Sono in ogni caso libere le attività di cui all'articolo 105, nonché la installazione, per proprio uso esclusivo, di reti di comunicazione elettronica per collegamenti nel proprio fondo o in più fondi dello stesso proprietario, possessore o detentore purché contigui, ovvero nell'ambito dello stesso edificio per collegare una parte di proprietà del privato con altra comune, purché non connessi alle reti di comunicazione elettronica ad uso pubblico. Parti dello stesso fondo o più fondi dello stesso proprietario, possessore o detentore si considerano contigui anche se separati, purché collegati da opere permanenti di uso esclusivo del proprietario, che consentano il passaggio pedonale o di mezzi».

L'art. 104 considerava l'autorizzazione generale in ogni caso necessaria per l'installazione o esercizio di sistemi che impiegano bande di frequenze di tipo collettivo «[s]enza alcuna protezione, mediante dispositivi rispondenti alla raccomandazione della Conferenza europea delle amministrazioni delle poste e delle telecomunicazioni (CEPT) CEPT/ERC/REC 70-03, relativi all'installazione od esercizio di reti locali radiolan o hiperlan al di fuori del proprio fondo, ovvero reti hiperlan operanti necessariamente in ambienti chiusi o con vincoli specifici derivanti dalle prescrizioni del Piano nazionale di ripartizione delle frequenze».

A modificare entrambe le suddette disposizioni è intervenuto il d.lgs. 28 maggio 2012, n. 70, attuativo delle direttive del 2009 sulle comunicazioni elettroniche[21]. In particolare l'art. 70, co. 1, d.lgs. 70/2012, ha inciso sull'art. 105 Cod. Com. El., andando a privare la lett. b) delle parole «nell'ambito del fondo, ai sensi dell'articolo 99, comma 5». Tale modifica consente oggi la lettura dell'art. 105 nel senso che sono di libero uso le «reti locali di tipo radiolan e hiperlan», senza ulteriori specificazioni.

Lo stesso d.lgs. 70/2012 è intervenuto, a mezzo dell'art. 69, anche sull'art. 104 Cod. Com. El., abrogando la menzionata lett. c) e, quindi, sottraendo dall'autorizzazione generale le attività ivi elencate.

Da quest'analisi interpretativa emerge che, attualmente, il Codice delle Comunicazioni Elettroniche non richiede alcuna autorizzazione per l'installazione di una WCN: fintanto che la tecnologia alla base di tali reti non muterà, essere rientreranno nelle libere utilizzazioni, senza necessità di ottenere autorizzazioni o licenze.

Diversa situazione e diversa interpretazione sono da effettuare con riferimento alla condivisione della rete wireless da parte dell'utente privato. Lasciando da parte le considerazioni relative al contratto intercorrente fra utente e *provider*, su cui ci si soffermerà successivamente, si devono qui illustrare le normative susseguitesi in materia negli ultimi dieci anni.

[21] «Modifiche al decreto legislativo 1° agosto 2003, n. 259, recante codice delle comunicazioni elettroniche in attuazione delle direttive 2009/140/CE, in materia di reti e servizi di comunicazione elettronica, e 2009/136/CE in materia di trattamento dei dati personali e tutela della vita privata».

Fra gli interventi normativi più noti e, al contempo, più invasivi in materia, si deve annoverare il c.d. «Decreto Pisanu», vale a dire il d.l. 27 luglio 2005, n. 144, convertito, con modificazioni, in legge 31 luglio 2005, n. 155.

Tale decreto, che si faceva carico di introdurre alcune misure a contrasto del terrorismo internazionale *post* «11 settembre 2001», poneva una serie di limitazioni all'utilizzo di reti di comunicazione, fra le quali il wi-fi. A fini di tutela della sicurezza pubblica si prevedeva la necessaria «preventiva acquisizione di dati anagrafici riportati su un documento di identità dei soggetti che utilizzano postazioni pubbliche non vigilate per comunicazioni telematiche ovvero punti di accesso ad Internet utilizzando tecnologia senza fili»[22]. Ciò era stato ulteriormente specificato dal D.M. 16 agosto 2005, n. 19023, adottato ai sensi dell'art. 7, co. 4, del Decreto Pisanu, di cui dettagliava gli obblighi appena menzionati, per cui diventava necessario, ai sensi dell'art. 1, «identificare chi accede ai servizi telefonici e telematici offerti, prima dell'accesso stesso o dell'offerta di credenziali di accesso, acquisendo i dati anagrafici riportati su un documento di identità, nonché il tipo, il numero e la riproduzione del documento presentato dall'utente»[23]. A ciò si doveva aggiungere la previsione di cui all'art. 4 del medesimo decreto ministeriale, secondo cui i soggetti che offrivano «accesso alle reti telematiche utilizzando tecnologia senza fili in aree messe a disposizione del pubblico [erano] tenuti ad adottare le misure fisiche o tecnologiche occorrenti per impedire l'uso di apparecchi terminali che non [consentivano] l'identificazione dell'utente, ovvero ad utenti che non [fossero] identificati secondo le modalità di cui all'art. 1»[24].

Le disposizioni del Decreto Pisanu erano destinate, fin dalla nascita, ad avere una validità temporanea. Numerose modifiche prorogarono tale validità fino al 31 dicembre 2011[25]. Non essendo il legislatore ulte-

[22] Art. 7, co. 4, d.l. 144/2005, invariato nella legge di conversione.

[23] Art. 1 («Obblighi dei titolari e dei gestori»), co. 1, lett. b), D.M. 16 agosto 2005, n. 19023.

[24] Art. 4, D.M. 16 agosto 2005, n. 19023 rubricato «Accesso alle reti telematiche attraverso tecnologia senza fili».

[25] Il testo iniziale del d.l. prevedeva che gli obblighi si estendessero solo fino al 31.12.2007; il comma fu modificato più volte, a partire dalla legge di conversione (mo-

riormente intervenuto con successive proroghe, gli obblighi e le limitazioni posti dal Decreto Pisanu possono oggi dirsi caduti[26].

Oltre a quanto fin qui visto, si deve rendere conto di alcune più recenti misure di liberalizzazione e di apertura all'accesso ad Internet attraverso wi-fi. In particolare, l'art. 10 d.l. 21 giugno 2013, n. 69 – meglio noto come «Decreto del fare»[27] – ha liberalizzato l'accesso ad Internet attraverso tecnologie di wi-fi. Più in particolare, tale articolo sancisce che l'offerta al pubblico di accesso ad Internet mediante wi-fi non richiede l'identificazione personale dell'utente-utilizzatore. Inoltre, quando l'offerta di accesso non sia attività commerciale prevalente del gestore (è il caso, ad esempio, di un bar o un circolo sportivo), non si applicano le disposizioni di cui all'art. 25 Cod. Com. El. relative all'«Autorizzazione generale per le reti e i servizi di comunicazione elettronica».

Sommando tutto quanto fin qui esposto, appare evidente che in questo momento l'installazione di una rete wireless comunitaria non richiede alcuna autorizzazione. Né tali reti sono sottoposte a obblighi di identificazione degli utenti che vi prendono parte, indipendentemente dal fatto che la rete comunitaria sia connessa ad Internet o meno. Ed invero la WCN non può considerarsi quale «gestore del servizio» di accesso, né l'offerta di connessione ad Internet costituisce la sua attività prevalente.

Questa breve disamina effettuata con riferimento al quadro legislativo applicabile necessita di una annotazione finale: qualunque previsione normativa esistente o futura trova e troverà un ostacolo nella difficoltà, fattuale ancor prima che giuridica, di individuare un soggetto responsabile della rete, sia esso un singolo o un'entità collettiva.

---

dificato poi con: art. 34, co. 1, d.l. 31 dicembre 2007, n. 248; art. 11, co. 1, d.l.. 30 dicembre 2008, n. 207; art. 3, co. 1, d.l. 30 dicembre 2009, n. 194; art. 2, co. 19, d.l. 29 dicembre 2010, n. 225).

[26] Il co. 4, art. 7, Decreto Pisanu, relativo alla preventiva acquisizione dei dati anagrafici degli utenti che utilizzassero reti pubbliche, fu abrogato già dall'art. 2, co. 19, d.l. 29 dicembre 2010, n. 225.

[27] Decreto convertito, con modificazioni, in Legge 9 agosto 2013, n. 98 - Disposizioni urgenti per il rilancio dell'economia (Decreto del fare).

4. WCN e responsabilità civile

Il fenomeno delle WCN rappresenta l'ennesimo esempio di un classico problema: quanto nasce una nuova tecnologia, il diritto si deve evolvere, adattarsi, plasmarsi, al fine di rispondere alle sollecitudini che tale nuova tecnologia gli pone[28].

Come accennato, in questo momento non esiste alcun caso concreto vagliato dalle corti che riguardi le WCN, né in termini della loro installazione e diffusione, né in termini di eventuali controversie nascenti dal loro utilizzo.

Non risulta però difficile immaginare eventuali usi illeciti che di queste reti possano farsi. Si pensi ad esempio ad azioni di tipo diffamatorio, a scambi di contenuti protetti da diritto d'autore, all'organizzazione di attività criminose e via discorrendo.

Fra le possibili conseguenze giuridiche ci si soffermerà in questo scritto solamente sulle questioni di responsabilità civile e, più nello specifico, con riferimento al contesto italiano così come modellato dalle normative di derivazione europea in tema di comunicazioni elettroniche e di servizi della società dell'informazione.

Immaginando le possibili implicazioni, è possibile immaginare quantomeno tre diversi casi di responsabilità, facenti capo a ciascuno dei soggetti che reggono le WCN: utenti e rete stessa. Si può innanzitutto pensare all'ipotesi in cui sia il singolo utente ad essere ritenuto responsabile per le azioni da lui stesso perpetrate oppure per le azioni che un utente terzo effettui qualora tale utente sia titolare di un nodo *ga-*

[28] Questo assunto è il punto di partenza della dottrina di «law and technology», su cui si vedano, a fini introduttivi, i seguenti contributi: A. COCKFIELD, J. PRIDMORE, *Symposium: Toward a General Theory of Law and Technology: A Synthetic Theory of Law and Technology*, in *Minnesota Journal of Law Science & Technology*, n. 2/2007, 441; G. PASCUZZI, *Il diritto dell'era digitale*, Bologna, 2010; R. BROWNSWORD, *Rights, Regulation, and the Technological Revolution*, Oxford, 2008; N. COX, *Technology and Legal Systems*, Aldershot, 2006; R.E. SUSSKIND, *The Future of Law: Facing the Challenges of Information Technology*, Oxford, 1996; AA.VV., *Proceedings of the First Law and Technology Conference*, Houston, 1983. Si veda in proposito anche il celeberrimo lavoro di L. LESSIG, *Code and Other Laws of Cyberspace*, New York, 1999, disponibile, nella versione 2.0, anche online all'url: http://codev2.cc/download+remix/Lessig-Codev2.pdf.

teway. Sempre con riferimento all'ipotesi di apertura della rete comunitaria ad Internet, una seconda possibilità concerne la responsabilità dell'ISP per il caso in cui un'attività illecita sia realizzata mediante il *gateway*: può un *provider* essere considerato responsabile per tale attività? Infine bisogna interrogarsi sulla possibile responsabilità (ed imputabilità) della rete nel suo complesso, per le azioni illecite che siano perpetrate «al suo interno».

Ciascuna di queste ipotesi sarà ora analizzata nel dettaglio, allo scopo di tentare di immaginare possibili scenari in risposta ad eventuali casi concreti che si dovessero presentare, pur tenendo in considerazione che vi sono regole che regolino espressamente le WCN, né vi sono casi giurisprudenziali cui fare riferimento.

4.1. Responsabilità del singolo utente

Da un punto di vista strettamente logico-giuridico, il primo soggetto che è chiamato a rispondere di un illecito è, ovviamente, il materiale autore dello stesso. In particolare, si possono immaginare due casi in cui un utente di una rete wireless comunitaria possa essere considerato responsabile: innanzitutto per le sue stesse condotte, e, in secondo luogo, qualora agisca anche come «nodo-gateway», anche per eventuali condotte altrui effettuate nel contesto di Internet e perpetrate per mezzo di tale nodo.

In simili ipotesi le norme che verrebbero innanzitutto in rilievo sarebbero evidentemente le norme civilistiche in tema di responsabilità extracontrattuale. Per quanto concerne la prima ipotesi, più precisamente, il caso sarebbe riconducibile all'area di applicabilità dell'art. 2043 c.c. Il secondo scenario, invece, potrebbe essere considerato una fattispecie di responsabilità concorrente e, quindi solidale ai sensi dell'art. 2055 c.c.[29]. La condotta dell'utente gateway potrebbe infatti considerarsi come un contributo causale all'illecito: fornendo la connessione ad Internet ad altri soggetti, l'utente gateway procura gli strumenti idonei alla condotta illecita, prendendovi causalmente parte.

[29] Sarebbe possibile ipotizzare l'applicabilità anche degli artt. 2050 e/o 2051 c.c. secondo G. GIANNONE CODIGLIONE, *Indirizzo IP, Reti Wi-Fi e responsabilità per illeciti commessi da terzi*, in *Dir. Inf.*, n. 1/2013, 130 ss.

L'applicabilità teorica di queste norme finisce però per diventare inapplicabilità pratica, a fronte della struttura e delle peculiarità della rete comunitaria. Invero, il primo passo per l'*enforcement* di un diritto violato sarebbe quello di identificare e, quindi, convenire in giudizio l'utente responsabile. Tuttavia, se si considera quanto precedentemente illustrato circa l'identificabilità degli utenti della rete, si ricorderà che pur esistendo per ciascun utente un indirizzo IP, tale indirizzo può essere modificato a piacimento dal singolo utente e, in aggiunta, non esistono registri in cui gli *IP numbers* siano archiviati. Come si potrebbe dunque ricondurre al singolo utente un determinato comportamento illecito? È noto che anche nell'ambiente di Internet, per comprendere da quale computer provenga l'attività illecita occorre abbinare indirizzo IP e nome dell'abbonato. Quest'operazione si rivela tuttavia impossibile per le reti qui analizzate, per cui la possibilità di identificare l'utente autore dell'illecito è prossima allo zero: le potenzialità di tutela si riducono drasticamente.

Parzialmente diverso sarebbe il discorso con riferimento all'utente-nodo *gateway*. Tale soggetto, infatti, avendo una connessione ad Internet è anche titolare di un indirizzo IP. Mediante la collaborazione del suo *access provider* sarebbe possibile rinvenire l'identità di questo utente, identificabile attraverso il suo indirizzo IP.

È presto detto, tuttavia, che anche questa possibilità non si dimostra una garanzia di risultato. A molti sarà noto che nei casi di violazione del diritto d'autore mediante «file-sharing» i giudici italiani hanno tutelato i dati personali degli utenti, considerando tali anche gli indirizzi IP, e attribuendo a questi un peso maggiore di quello dato al diritto d'autore[30]. La conseguenza fu che l'interpretazione così fornita frustrò le aspettative di tutela dei titolari di diritto d'autore.

[30] Nelle controversie instaurate dai titolari di diritto d'autore contro utenti finali sospettati di aver condiviso illecitamente dei file tutelati, molti sono stati gli interrogativi sulla configurabilità dell'indirizzo IP come dato personale. A favore di tale interpretazione si veda ad esempio l'opinione 2/2002 dell'Article 29 Data Protection Working Party che ritenne tali dati protetti dalle direttive 95/46 e 97/66 in materia di protezione dei dati personali (http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm#h2-11); permangono dubbi sul punto, si vedano ad esempio: F. COUDERT, E. WERKERS, *In the Aftermath of the Promusicae Case:*

Tornando al mondo delle WCN, sebbene l'interpretazione e la soluzione varino da caso a caso e dipendano anche dagli interessi e dai diritti effettivamente in gioco, va tenuto presente che, anche in ipotesi di identificabilità degli utenti-gateway, non necessariamente si avrebbe effettiva identificazione, secondo quando appena illustrato. A ciò si aggiunga che spesso gli utenti delle WCN utilizzano *software* per l'anonimizzazione, riducendo, se possibile, ulteriormente, la rintracciabilità delle loro identità[31].

How to Strike the Balance?, in *International Journal of Law and Information Technology*, 1/2008, 50 spec. 57 ss.; P. SAMMARCO, *Alla ricerca del giusto equilibrio da parte della Corte di Giustizia UE nel confronto tra diritti fondamentali nei casi di impiego di sistemi tecnici di filtraggio*, in *Dir. Inf*., 2012, 297.

Indipendentemente dalla qualificazione dell'indirizzo IP come dato personale, fu soprattutto la richiesta avanzata dalle case discografiche di ottenere i dati identificativi degli utenti cui gli indirizzi IP appartenevano che diede adito ad un forte dibattito. Nel caso del contesto italiano le controversie finirono col far prevalere la protezione dei dati personali degli utenti, a discapito della tutela del diritto d'autore. Si vedano in merito C. BLENGINO, M.A. SENOR, *Il caso «Peppermint»: il prevedibile contrasto tra protezione del diritto d'autore e tutela della privacy nelle reti peer to-peer*, in *Dir. Inf*., n. 4-5/2007, 835; R. CASO, *Il conflitto tra copyright e privacy nelle reti Peer to Peer: in margine al caso Peppermint – Profili di diritto comparato*, in *Dir. Internet*, n. 5/2007, 471; G. FOGLIA, *La privacy vale più del diritto d'autore: note in materia di filesharing e di sistemi peer-to-peer*, in *Dir. industriale*, n. 6/2007, 598; M. GAMBINI, *Diritto d'autore e tutela dei dati personali: una difficile convivenza in Rete*, in *Giur. it*., n. 2/2009, 509. La questione raggiunse anche la Corte di Giustizia, nella C-275/06, Productores de Música de España (Promusicae) v Telefónica de España SAU, decisa il 28 gennaio 2008, sulla quale si vedano S. KIERKEGAARD, *ECJ Rules on ISP Disclosure of Subscribers' Personal Data in Civil Copyright Cases*, in *Computer Law & Security Report*, n. 3/2008, 268; K. BRIMSTED, G. CHESNEY, *The ECJ's Judgement in Promusicae: The Unintended Consequences – Music to the Ears of Copyright Owners or a Privacy Headache for the Future? A Comment*, in *Computer Law & Security Report*, n. 3/2008, 275; M. DE CATA, *Il caso «Peppermint». Ulteriori riflessioni anche alla luce del caso «Promusicae»*, in *Riv. dir. industriale*, n. 4-5/2008, 404. Più in generale, sul problema dell'identificazione del soggetto responsabile v. G. RESTA, *Anonimato, responsabilità, identificazione: prospettive di diritto comparato*, in *Dir. Inf*., n. 2/2014, 189-191; 196-202.

[31] Esistono diverse tecnologie con cui è possibile rendere anonimo il traffico generato da un nodo della rete, deviandolo su reti anonimizzate. Si veda l'esempio del *software* «Tor»: https://www.torproject.org/, sul quale si leggano K.D. WATSON*, The Tor Network: A Global Inquiry into the Legal Status of Anonymity Networks*, in *Washington*

Queste difficoltà alla tutela dei diritti dimostrano gli ostacoli che una struttura tecnologica come quella delle reti wireless comunitarie pone sulla strada della responsabilità extracontrattuale intesa in senso «classico». Agire direttamente nei confronti dell'utente finale sarebbe la soluzione più immediata e più corretta, anche in considerazione della regola generale per cui ciascuno è responsabile solo delle proprie azioni. Tuttavia, tale soluzione è tecnologicamente (pressoché) impossibile.

Queste falle nella tutela contro gli utenti delle WCN invitano a considerare ulteriori soggetti che possano o debbano essere considerati quali possibili convenuti. Occorre pertanto ora analizzare due ulteriori ipotesi: il caso in cui l'azione illecita sia commessa e si consumi all'interno della WCN, per cui la stessa rete potrebbe essere considerata come soggetto responsabile; nonché il caso in cui ad essere chiamato in causa sia il provider che fornisce l'accesso al nodo gateway.

Tali due possibili ipotesi saranno ora analizzate, partendo da quest'ultima.

4.2. Responsabilità dell'Internet Service Provider

Una seconda ipotesi di responsabilità concerne i fornitori dei servizi telematici, ovverosia gli Internet Service Provider, nell'eventualità che un nodo funga da *gateway*.

Questa «apertura» del nodo pone il *provider* in una situazione di inconsapevole rischio: esso potrebbe in effetti essere sottoposto al pericolo che altri utenti, oltre al suo cliente, pongano in essere comportamenti illeciti.

Quale soluzione si potrebbe fornire in questi casi? Potrebbe il *provider* essere considerato responsabile per le azioni commesse da questi soggetti? E cosa accadrebbe all'utente *gateway*?

University Global Studies Law Review, n. 3/2012, 715; M. RADY, *Anonymity Networks: New Platforms for Conflict and Contention*, in *MIT Political Science Department Research Paper*, n. 5/2013, <http://ssrn.com/abstract=2241536>. Si veda tuttavia il recente studio che dimostra che l'81% degli utenti Tor può essere de-anonimizzato attraverso l'analisi delle informazioni di *routing*: M. ANDERSON, *81% of Tor Users Can Be Deanonymised by Analysing Router Information, Research Indicates*, in *The Stack*, 14 novembre 2014 <http://thestack.com/chakravarty-tor-traffic-analysis-141114>.

Al fine di rispondere a queste domande, occorre qui fare un passo indietro e illustrare, seppur molto brevemente, la disciplina che l'Unione europea ha pensato per la responsabilità degli ISP. Questi intermediari furono scelti come entità responsabili per le azioni degli utenti, in considerazione sia della struttura di Internet che della loro peculiare funzione in tale struttura.

La responsabilità dei *provider* integra un tipico caso di responsabilità per fatto altrui. È noto che la responsabilità per fatto del terzo richiede una specifica previsione in quanto, di norma, ciascuno è responsabile solo per le proprie azioni.

La *ratio* sottesa alle previsioni di responsabilità per fatto altrui è normalmente quella dell'esistenza di una peculiare relazione fra il potenziale responsabile e uno o più elementi del fatto illecito[32]. Si pensi all'ipotesi della responsabilità del lavoratore per i fatti dei dipendenti o alla responsabilità del genitore per i fatti dei figli. In queste ipotesi è evidente che la responsabilità è imputata a tali soggetti sulla base della peculiare relazione fra tali soggetti e il soggetto agente.

Generalmente questa peculiare figura di responsabilità extracontrattuale scaturisce da condotte omissive: omissioni di sorveglianza, di controllo, di vigilanza e via dicendo. Essa è perciò imputata a chi meglio saprebbe sorvegliare o controllare il soggetto che pone in essere l'attività illecita. Si pensi di nuovo al caso dei genitori o del datore di lavoro: essi sono considerati nella posizione migliore per vigilare le attività, rispettivamente, di figli e dipendenti.

Talvolta la scelta di imporre una responsabilità extracontrattuale su un soggetto terzo rispetto al soggetto agente dipende anche da motivazioni d'opportunità: potrebbe, infatti, essere eccessivamente costoso o di fatto impossibile punire il reale soggetto agente[33].

Nel momento di emanazione del nostro codice civile il numero di casi in cui vi era l'imposizione di una responsabilità per fatto altrui era esiguo. Nel tempo, anche in considerazione dell'evolversi della società,

---

[32] M. FRANZONI, *L'illecito*, Milano, 2010, 678-679.

[33] C. VAN DAM, *European Tort Law*, Oxford, 2006, 437-438. Invero «[l]o scopo della responsabilità per fatto altrui è di garantire al danneggiato la possibilità di conseguire il risarcimento, poiché questi può rivolgersi nei confronti di più soggetti, o del soggetto che è più solvibile», M. FRANZONI, *op. cit.*, 680.

la legislazione speciale ha introdotto e disciplinato nuove fattispecie[34]. Fra esse rientra a pieno titolo la responsabilità dei prestatori di servizi di cui qui ci occupiamo.

Come accennato, la scelta di imporre una responsabilità indiretta in capo a questi soggetti discende indubbiamente dal loro ruolo strategico nel contesto di Internet[35], che ne permette la raggiungibilità da parte della vittima di un comportamento illecito. A ciò si sommi la loro capacità economica che è maggiore garanzia per gli eventuali danneggiati in un'azione di risarcimento[36]. La disciplina della responsabilità degli intermediari nasce con la Dir. 2000/31/CE, c.d. «Direttiva sul commercio elettronico»[37], recepita all'interno del nostro ordinamento con il d.lgs. 9 aprile 2003, n. 70, che ha introdotto la disciplina nel nostro ordinamento senza sostanziali modifiche rispetto al testo originale.

L'introduzione di questa disciplina fu quanto mai scelta felice se consideriamo che nei primi momenti in cui Internet cominciava a diffondersi l'interpretazione delle leggi esistenti si poneva come potenzia-

[34] A mero titolo esemplificativo si ricordano: la responsabilità indiretta dello Stato per incidente nucleare (L. 31 dicembre 1062, 1860); la responsabilità del produttore (D.P.R. 24 maggio 1988, n. 224, oggi inserito nel c.d. «Codice del consumo», d.lgs. 6 settembre 2005, n. 206); la responsabilità civile indiretta della banca intermediaria nei danni cagionati dalla condotta illecita del proprio promotore finanziario (art. 31, d.lgs. 24 febbraio 1998, n. 58 – Testo unico finanza).

[35] Non sarebbe responsabilità indiretta, bensì responsabilità per fatto proprio secondo M. FRANZONI, *op. cit*., 340-341. Sulla materia della responsabilità del *provider* si vedano per tutti le monografie di T. PASQUINO, *Servizi telematici e criteri di responsabilità*, Milano, 2003; F. DI CIOMMO, *Evoluzione tecnologica e regole di responsabilità civile*, Napoli, 2003 e M. GAMBINI, *Le responsabilità civili dell'Internet service provider*, Napoli, 2006; M. DE CATA, *La responsabilità civile dell'internet service provider*, Milano, 2010. Si vedano inoltre, fra i moltissimi contributi: G.M. RICCIO, *La responsabilità degli internet providers nel d.lgs. n. 70/03*, in *Danno e resp*., n. 12/2003, 1157; G. CASSANO, I.P. CIMINO*, Il nuovo regime di responsabilità dei providers: verso la creazione di un novello «censore telematico»*, in *Contratti*, n. 1/2004, 88.

[36] Questa non è altro se non l'applicazione, in via legislativa, della c.d. «deep pockets theory», per cui si veda G. CALABRESI, *The Costs of Accidents: A Legal and Economic Analysis*, New Haven, 1970, 40 ss.

[37] Direttiva 2000/31/CE del Parlamento europeo e del Consiglio dell'8 giugno 2000 relativa a taluni aspetti giuridici dei servizi della società dell'informazione, in particolare il commercio elettronico, nel mercato interno.

le ostacolo allo sviluppo della Rete. Invero, l'apparente impossibilità di rinvenire il reale responsabile del fatto illecito spingeva ad attribuire agli ISP ogni responsabilità, in considerazione del fatto che essi apparivano i soli soggetti rintracciabili. Questo approccio comportò che gli intermediari furono ritenuti talvolta responsabili anche oltre le loro effettive capacità. Basti pensare che nelle prime controversie le corti applicarono le regole generali della responsabilità civile, finendo per assimilare il provider al custode di una cosa ai sensi dell'art. 2051 c.c. oppure al gestore di un'attività pericolosa *ex* art. 2050 c.c. In altre occasioni i *provider* si videro applicate norme speciali inerenti altri settori, per cui furono, ad esempio, equiparati agli editori di testate giornalistiche[38].

La disciplina speciale introdotta dalla Dir. 2000/31 e, conseguentemente, dal d.lgs. n. 70/2003 considera gli ISP responsabili delle azioni effettuate dagli utenti solo qualora gli intermediari non si adeguino a determinati requisiti individuati dalla normativa stessa. Vale a dire: se un provider si adegua a quanto specificamente richiesto dal decreto, esso andrà esente da responsabilità per quanto compiuto dagli utenti[39].

---

[38] Per alcuni spunti sulla situazione antecedente l'introduzione di un'apposita disciplina, corredati dalle più importanti sentenze al proposito si vedano S. ALVANINI, *La responsabilità dei service provider*, in *Dir. industriale*, n. 4/2010, 329-330; G. SPEDICATO, *La responsabilità extracontrattuale del provider per violazioni del diritto d'autore*, in *Ciberspazio e diritto*, n. 1/2003, 116; A. PIAZZA, *La responsabilità civile dell'Internet* Provider, in *Contratto e impresa*, n. 1/2004, 130; M. FRANZONI, *La responsabilità del provider*, in *AIDA*, 1997, 248. V. inoltre M. FRANZONI, *L'illecito*, cit., 340-341 e note bibliografiche ivi citate. Per una qualificazione del *provider* come editore di stampa quotidiana si veda Trib. Napoli, (ord.) 8 agosto 1997, in *Giust. civ.*, 1998, I, 259 ss.; Trib. Macerata, (ord.) 2 dicembre 1998, in *Riv. Dir. Ind.*, 1999, 35 (v. sul tema V. ZENO-ZENCOVICH, *La pretesa estensione alla telematica del regime della stampa: note critiche*, in *Dir. Inf.*, n. 1/1998, 15); per una responsabilità del *provider* discendente da una omissione di vigilanza, si veda Trib. Cuneo, (ord.) 23 agosto 1997, in *Aida*, 1997, 500.

[39] Come noto, la direttiva europea si ispira allo USA Digital Millennium Copyright Act (DMCA). Più in particolare, il sistema statunitense introdusse nel 1998 l'Online Copyright Infringement Liability Limitation Act (OCILLA) contenente una serie di previsioni, che esentano dai danni, costi, spese legali ed altri esborsi monetari i *provider* che si qualifichino per tali c.d. «safe harbors». Anche il sistema USA considera diversi *provider*s e diversi oneri a seconda dell'attività svolta da questi. Tuttavia, v'è una pe-

La disciplina in esame si applica a tutte le possibilità attività illecite dell'utente, non distinguendo per materia o per gravità dell'atto. Il d.lgs. n. 70/200 individua tre differenti categorie di intermediari agli artt. 14, 15, 16, rispettivamente: «mere conduit», «caching» e «hosting» *providers*[40].

A ciascuna di tali attività è correlato un diverso grado di implicazione nel contesto di Internet, cui fa da contraltare un diverso livello di oneri cui il *provider* deve attenersi al fine di andare esente da responsabilità. Va specificato che, peraltro, in nessun caso agli intermediari può

---

sante differenza fra le due regolamentazioni data dall'ambito di applicazione: mentre la disciplina europea si applica qualunque sia il diritto violato, la disciplina statunitense riguarda esclusivamente le violazioni del *copyright*. Gli USA avevano già introdotto in precedenza una disciplina relativa alla responsabilità dei provider, che oggi si applica ad ipotesi diverse da quelle del *copyright infringement*. Faccio riferimento alla Section 230 del Communications Decency Act del 1996, su cui si vedano fra i molti: J.A. FRIEDMAN, F.M. BUONO, *Limiting Tort Liability for Online Third-Party Content under Section 230 of the Communications Act*, in *Federal Communications Law Journal*, n. 3/2000, 647; D.S. ARDIA, *Free Speech Savior or Shield for Scoundrels: An Empirical Study of Intermediary Immunity Under Section 230 of the Communications Decency Act*, in *Loyola Los Angeles Law Review*, n. 2/2010, 373.

Per un'analisi della Dir. 2000/31 si rinvia a R. JULIÀ-BARCELÓ, K.J. KOELMAN, *Intermediary Liability: Intermediary Liability in the E-Commerce Directive: So Far so Good, but It's not Enough*, in *Computer Law & Security Review*, n. 4/2000, 231; P. BAISTROCCHI, *Liability of Intermediary Service Providers in the EU Directive on Electronic Commerce*, in *Santa Clara Computer & High Technology Law Review*, n. 1/2002, 111; T. VERBIEST, G. SPINDLER, G.M. RICCIO, A. VAN DER PERRE, *Study on the Liability of Internet Intermediaries*, 2007, <http://ec.europa.eu/internal_market/e-commerce/docs/study/liability/final_report_en.pdf>. Per una panoramica della disciplina introdotta dal DMCA si faccia riferimento, fra i tanti, a: L.B. PATTEN, *From Safe Harbor to Choppy Waters: YouTube, the Digital Millennium Copyright Act, and a Much Needed Change of Course*, in *Vanderbilt Journal of Entertainment and Technology Law*, n. 1/2007, 179; B. BROWN, *Fortifying the Safe Harbors: Reevaluating the DMCA in a Web 2.0 World*, in *Berkeley Technology Law Journal*, n. 1/2008, 437; R. REESE, *The Relationship Between the ISP Safe Harbors and Ordinary Rules of Copyright Liability*, in *Columbia Journal of Law & the Arts*, n. 4/2009, 427. Infine, per una comparazione fra i due approcci si veda il contributo di M. PEGUERA, *The DMCA Safe Harbors and Their European Counterparts: A Comparative Analysis of Some Common Problems*, in *Columbia Journal of Law & the Arts*, n. 4/2009, 481.

[40] Si vedano gli artt. 12-14, Dir. 2000/31/CE.

essere imposto un obbligo di sorveglianza del traffico o di ricerca attiva di fatti o circostanze indicatrici di attività illecite[41].

Pur non potendo entrare nel dettaglio, possiamo rapidamente descrivere i tre tipi di provider come segue:

1) il *provider* di «mero trasporto» («mere conduit» nella versione della Direttiva) di cui all'art. 14 d.lgs. n. 70/2003, è l'intermediario che trasmette informazioni fornite da un destinatario del servizio o che fornisce accesso alle reti di comunicazione. Si tratta di fatto dell'«access provider» cioè il provider che permette agli utenti l'accesso ad Internet;
2) il *caching provider* (art. 15) è l'intermediario che trasmette, su una rete di comunicazione, informazioni fornite da un destinatario del servizio e a tale scopo effettua la memorizzazione automatica, intermedia e temporanea di informazioni fornite da un destinatario del servizio;
3) l'*hosting provider*, infine, memorizza le informazioni fornite da un destinatario del servizio (art. 16).

Dalle definizioni discende che *caching* e *hosting provider* sono responsabili per la loro attività di memorizzazione di informazioni a richiesta del destinatario, sebbene con differenti modalità, seguita da una mancata rimozione nell'ipotesi in cui siano tenuti a farlo[42]. La direttiva e il decreto di recepimento non specificano ulteriori requisiti dell'informazione, se non che sia «a richiesta del destinatario». Questo dimostra che non ha rilevanza la fonte da cui provengono le informazioni memorizzate e non rimosse quando dovuto. Nel contesto qui esaminato ciò significa che questi due tipi di *provider* saranno ritenuti responsabili per la mancata rimozione di informazioni quando obbligatoria, indipendentemente dalla provenienza di tali informazioni da un utente interno o esterno ad una WCN, cioè, indipendentemente dal fatto che l'utente sia connesso «direttamente» ad Internet o per il tramite di un nodo *gateway*.

[41] Art. 15, Dir. 2000/31 e art. 17, d.lgs. 70/2003.Ciò è stato a più riprese ribadito anche dalla Corte di Giustizia Europea; si vedano i celebri casi C-70/10, *Scarlet Extended SA v. Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*, deciso il 26 novembre 2011 e C-360/2010, *SABAM v. Netlog NV*, deciso il 31 marzo 2012.

[42] Si vedano sul punto i requisiti previsti dagli artt. 15 e 16.

Un diverso discorso, almeno parzialmente, deve farsi per il *provider* di mero trasporto. A differenza di quanto accade per gli altri intermediari, questo genere di *provider* è legato ad un utente da un rapporto contrattuale. Alle previsioni di cui all'art. 14, d.lgs. 70/2003, vanno pertanto a sommarsi le clausole contrattuali specifiche di ciascun contratto: a prescindere dall'applicazione delle limitazioni della responsabilità di cui all'art. 14, l'intermediario potrebbe limitare la propria responsabilità attraverso clausole contrattuali *ad hoc*. Già oggi, numerosi contratti contengono clausole che, per esempio, vietano all'utente-abbonato di condividere la propria connessione con terzi, o che impongono allo stesso un uso corretto del servizio, vietandone l'utilizzo improprio[43].

Se un utente contravvenisse a queste disposizioni, si troverebbe ovviamente a violare il contratto, dovendo rispondere a titolo di responsabilità contrattuale. In aggiunta, egli potrebbe essere ritenuto garante per eventuali danni che il *provider* si dovesse trovare a risarcire a causa della condotta illecita perpetrata da un terzo attraverso il *gateway*[44].

[43] A mero titolo di esempio si vedano le «Clausole generali di contratto» di Telecom Italia per il servizio ADSL: la clausola n. 7 vieta che l'accesso ad internet sia ceduto ad altri utenti; le clausole 11 e 12 si riferiscono invece all'uso corretto e non improprio del servizio. Tra gli usi vietati vi è quello di servirsi del *provider* Telecom Italia «per comunicazioni e corrispondenza contro la morale, l'ordine pubblico o con lo scopo di recare molestia alla quiete pubblica o privata, di recare offesa o danno diretto o indiretto a chiunque» (clausola n. 11); vi è inoltre l'impegno dell'abbonato «ad astenersi da ogni violazione dei sistemi e della sicurezza delle reti che possano dar luogo a responsabilità civile e penale» (clausola n. 12) (clausole reperibili all'url: http://www.telecomitalia.it/sites/default/files/files/documentation/Condizioni_Gen_Contratto_Alice_0.pdf). A contrario, esistono alcuni provider che permettono questa pratica. Si veda a tal proposito, come esempio, la lista dei «wireless friendly» ISP statunitensi all'url: https://www.eff.org/pages/wireless-friendly-isps.

[44] Su una materia affine alla presente raggiungono le stesse conclusioni G. GIANNONE CODIGLIONE, *op. cit.*; D. MAC SÍTHIGH, *Law in the Last Mile: Sharing Internet Access Through Wifi*, in *SCRIPTed*, n. 2/2009, 366-369. Sulle problematiche relative alla condivisione di connessioni Wi-Fi si vedano anche R. ROBERT ET AL., *WiFi Roaming: Legal Implications and Security Constraints*, in *International Journal of Law and Information Technology*, n. 3/2008, 217-218; R.V. HALE, *Wi-Fi Liability: Potential Legal Risks in Accessing and Operating Wireless Internet*, in *Santa Clara Computer & High Technology Law Journal*, n. 3/2005, 548; B.D. KERN, *Whacking, Joyriding and*

Anche in questo caso esistono già contratti in cui vi sono clausole che impegnano il cliente a mantenere indenne l'intermediario per i casi di danni derivanti dalla violazione delle norme contrattuali, inclusi, evidentemente, anche quelli causati a terzi[45].

Va infine ricordato che, come più sopra illustrato, se la condotta fosse posta in essere da un soggetto terzo rispetto all'utente-abbonato, tale terzo non sarebbe identificabile, in quanto manca nelle WCN un sistema che offra la riconoscibilità dei partecipanti alla comunità. Diversamente, il nodo-*gateway* sarebbe identificabile tramite il proprio indirizzo IP. Questa disparità potrebbe comportare per l'utente del nodo-*gateway* un'eccessiva responsabilità per i fatti compiuti dai terzi tramite tale nodo. Questo scenario potrebbe fungere da deterrente all'apertura del nodo e, conseguentemente, all'apertura della rete intera ad Internet, anche se si deve ricordare che esistono modalità di anonimizzazione che potrebbero in qualche modo «proteggere» l'utente gateway[46].

4.3. Responsabilità della WCN

Va infine vagliata la possibilità che sia la rete stessa ad essere considerata quale soggetto responsabile delle attività dannose perpetrate all'interno della stessa. Si pensi ad esempio all'ipotesi di scambio di materiale pedo-pornografico fra utenti, alla diffusione di dati e informazioni personali altrui, a comunicazioni diffamatorie.

Affinché si possa parlare di una responsabilità della rete per le attività compiute dagli utenti, è innanzitutto necessario che la rete abbia una propria soggettività giuridica. Ad oggi, infatti, come si evince da

---

War-Driving: Roaming Use of Wi-Fi and the Law, in *Santa Clara Computer & High Technology Law Journal*, n. 1/2004, 101.

[45] Si veda di nuovo il contratto di Telecom Italia richiamato in nota n. 43, clausola n. 11: «Il Cliente si impegna a mantenere indenne Telecom Italia da ogni perdita, danno, responsabilità, costo o spese, incluse anche le spese legali, derivanti da ogni violazione delle suddette norme».

[46] Si veda quanto già riportato in nota n. 31. Si consideri inoltre la decisione Cass. Pen., 11 novembre 2008, n. 6046, in *Foro it*., 2009, II, 562 e in *Danno e resp*., 2009, 1049 con nota di Chiarolla, in cui la Suprema Corte ritenne non responsabile il titolare di un «internet point» per una diffamazione perpetrata attraverso di terminali di connessione ad internet ad opera di soggetti che non furono identificati.

quanto fin qui illustrato, le WCN non hanno un'organizzazione che permetta una soggettivizzazione giuridica.

A ciò si aggiunga che, anche laddove fossimo di fronte a reti che hanno una loro soggettività, ad esempio perché organizzate in un'associazione, sarebbe comunque necessaria una regola che imputasse specificatamente alla WCN la responsabilità per fatto altrui. Come più sopra ricordato, infatti, la regola generale vuole che ciascuno sia responsabile soltanto per le proprie azioni, salvo diverse previsioni, esattamente come avviene per la responsabilità degli Internet Service Provider per i fatti degli utenti.

Le WCN possono sotto alcuni profili essere assimilate alla rete Internet, la quale, invero, è un insieme di reti fatte di migliaia di nodi[47], quali quelli che compongono le reti wireless comunitarie. In considerazione di questa somiglianza, si potrebbe pensare ad un'applicazione analogica della disciplina relativa agli intermediari di Internet, più sopra brevemente illustrata. Se, ad un primo sguardo, parrebbe possibile effettuare quest'analogia, occorre in realtà considerare più nel dettaglio la struttura e le peculiarità delle WCN. Esse sono infatti delle reti di tipo «peer-to-peer», dove, cioè, ciascun nodo genera dati e «trasporta» dati di altri nodi, considerati fra loro come «pari». Anche se, di fatto, alcuni nodi hanno un ruolo più importante in termini strategici o di quantità delle informazioni instradate, non esiste un nodo centrale del tipo «access point», attraverso cui passino tutte le informazioni o la stragrande maggioranza delle stesse. In ciò le reti wireless comunitarie differiscono grandemente da Internet, che si basa su nodi nevralgici e centrali gestiti dai provider, che, anche per questo, sono stati scelti quali responsabili per i fatti degli utenti.

Data questa premessa, per poter comprendere se la normativa relativa agli ISP possa applicarsi anche alle WCN, occorre analizzare ed interpretare la Dir. 2000/31 e il suo ambito di applicazione. Del decreto di recepimento ci si limiterà ad effettuare qualche breve richiamo, in considerazione del fatto che esso non diverge sostanzialmente in alcunché dal testo normativo europeo.

---

[47] F. DACOSTA, *Ugly truth about mesh networks*, dailywireless.org, 28 giugno 2004, all'url: http://www.dailywireless.org/2004/06/28/ugly-truth-about-mesh-networks/.

La richiamata direttiva delinea il proprio campo di applicabilità soggettivo riferendosi ai «prestatori di servizi», da intendersi quali persone fisiche o giuridiche che prestino un servizio della società dell'informazione[48]. Quest'ultimo è a sua volta definito come «qualsiasi servizio prestato normalmente dietro retribuzione, a distanza, per via elettronica e a richiesta individuale di un destinatario di servizi»[49].

Al fine di meglio comprendere queste definizioni e di individuare l'ambito applicativo della direttiva in esame è necessario fare riferimento alle interpretazioni che di essa ha dato la Corte di Giustizia dell'Unione europea. Fra le locuzioni più controverse vi è quella di «servizio dietro remunerazione». Tale locuzione è parte della legislazione comunitaria da sempre, in quanto già nei Trattati collegata alla libera circolazione di beni e servizi. Invero, ai sensi dell'art. 50 del Trattato delle Comunità Europee[50], «sono considerate come servizi le prestazioni fornite normalmente dietro retribuzione, in quanto non siano regolate dalle disposizioni relative alla libera circolazione delle merci, dei capitali e delle persone».

Si consideri il caso *Belgio c. Humbel*[51], in cui la Corte di Giustizia ha stabilito che qualunque corrispettivo per un'attività economica possa essere considerato «remuneration». Non si deve infatti necessariamente trattare né di una remunerazione diretta, né di una remunerazione monetaria. Non occorre nemmeno che sia il cliente/utente finale a pagare

[48] Art. 2, lettera (b), Dir. 2000/31/CE.

[49] L'art. 2, lettera (a), Dir. 2000/31/CE fa riferimento ai «servizi della società dell'informazione» come definiti dall'art. 1(2) della Dir. 98/34/CE del Parlamento europeo e del Consiglio del 22 giugno 1998 che prevede una procedura d'informazione nel settore delle norme e delle regolamentazioni tecniche, come modificata dalla Dir. 98/48/CE del Parlamento europeo e del Consiglio del 20 luglio 1998 relativa ad una modifica della direttiva 98/34/CE che prevede una procedura d'informazione nel settore delle norme e delle regolamentazioni tecniche, che fornisce la definizione riportata.

[50] Oggi art. 57 della versione consolidata del Trattato sul funzionamento dell'Unione europea.

[51] C-263/86, *Belgian State c. René Humbel and Marie-Thérèse Edel*, deciso il 27 settembre 1988. Si veda nello specifico il par. 17, dove la Corte di Giustizia sancì «[l]a caratteristica essenziale della retribuzione va quindi rintracciata nella circostanza che essa costituisce il corrispettivo economico della prestazione considerata, corrispettivo che è generalmente pattuito fra il prestatore ed il destinatario del servizio».

per il servizio: sono pertanto riconducibili alla categoria «remuneration» anche i ritorni economici derivanti da pubblicità e annunci[52].

L'art. 50, peraltro, considera «servizi» le prestazioni che «normalmente» sono prestate dietro remunerazione. Tale avverbio è stato interpretato in due diversi modi. Innanzitutto prendendo a riferimento ciò che normalmente avviene nello stesso mercato; in secondo luogo tenendo presente le modalità di erogazione dei propri servizi normalmente seguite dal soggetto sotto indagine[53]. Se questa seconda interpretazione appare più lineare e intuitiva, la prima richiede un maggiore sforzo di comprensione. Infatti, affinché si applichi la direttiva ad uno specifico *provider*, è necessario che normalmente la maggioranza degli intermediari nello stesso mercato offrano lo stesso servizio dietro remunerazione nella maggioranza dei casi[54].

Le reti wireless comunitarie non operano in un vero e proprio mercato e, in ogni caso, il servizio che esse offrono – ammesso che così lo si possa qualificare – è assolutamente gratuito. Come più volte illustrato, infatti, lo scopo delle reti comunitarie è quello di fare in modo che dati ed informazioni possano circolare all'interno della rete, mediante una varietà di servizi creati e condivisi dagli utenti, nonché, eventualmente, fuoriuscire dalla comunità attraverso la connessione ad Internet. Non va tuttavia sottaciuto che il diffondersi delle reti e il loro allargarsi in termini di numero di nodi connessi potrebbe portare ad un'assimilazione delle reti comunitarie agli Internet Service Provider[55]. Le WCN possono infatti offrire un servizio di scambio di dati accostabile a quello che normalmente gli ISP offrono dietro remunerazione. Questo potrebbe portare ad un'interpretazione della Dir. 2000/31 e del d.lgs. 70/2003 secondo cui essi sarebbero applicabili anche alle reti comunitarie.

---

[52] C- 352/85, *Bond van Adverteerders c. Paesi Bassi*, deciso il 26 aprile 1988.

[53] Si veda DLA PIPER, *EU study on the legal analysis of a Single Market for the Information Society, New rules for a new age?, Liability of online intermediaries*, 2009 <http://ec.europa.eu/digital-agenda/en/news/legal-analysis-single-market-information-society-smart-20070037>, 12, nota n. 58.

[54] DLA PIPER, *op. cit.*, 12, nota n. 58.

[55] Della medesima idea già J.S. HATCHER, *op. cit.*, 19.

Questa interpretazione «prima facie» impone in realtà alcune ulteriori considerazioni. Si è detto e ripetuto che queste reti mancano di una struttura gerarchica, in quanto nascono dal basso e si sviluppano in modo spontaneo. Non hanno una struttura al cui vertice si ponga un soggetto o un organo responsabile. Ciò pone una barriera difficilmente superabile all'applicabilità delle norme e, nello specifico, alla Dir. 2000/31 e al suo decreto attuativo d.lgs. 70/2003: non vi è infatti alcun soggetto giuridico che, da un punto di vista di diritto sostanziale, possa essere considerato responsabile, né, a maggior ragione, un soggetto che possa essere passivamente legittimato al giudizio e chiamato in causa a fini risarcitori.

Tale aspetto s'impone come ostacolo non solo per la Dir. 2000/31 o il corrispondente d.lgs. 70/2003, ma per qualunque normativa – italiana o straniera – che si voglia applicare alle WCN. Per quanto più in particolare concerne il nostro ordinamento, un possibile diverso scenario sarebbe dato dal caso in cui la comunità si organizzasse sotto forma di associazione[56]: anche se si trattasse di un'associazione non riconosciuta, vi sarebbero soggetti da potersi considerare responsabili dell'operato dell'associazione.

Va inoltre ricordato che il quadro normativo di riferimento per quanto riguarda le WCN richiede agli ISP una serie di autorizzazioni prima di avviare la propria attività. Come più sopra illustrato, tali autorizzazioni non sono necessarie per le reti comunitarie, e ciò concorre a qualificarle come soggetti diversi dai *provider*.

La descritta acefalia delle WCN, che comporta la totale assenza di soggettività giuridica, sfocia in una quasi totale impossibilità di ottenere efficacemente tutela, indipendentemente da qualsivoglia regime di re-

[56] Si veda ad esempio il caso di Ninux Roma, che è parte di un progetto sociale più ampio facente capo ad una associazione ONLUS (cfr.: http://www.fusolab.net/component/k2/666-ninux). Lo stesso dicasi, ad esempio, della rete wireless di Barcellona guifi.net, che è parte di una fondazione: http://blogs.guifi.net/fundacio/. Va in questo contesto riportata la recente sentenza Trib. Roma, 9 luglio 2014 (reperibile all'url: https://upload.wikimedia.org/wikipedia/foundation/a/ad/Angelucci_judgement.pdf), relativa a «Wikimedia Foundation»: la fondazione è stata considerata non responsabile legalmente per quanto gli utenti caricano liberamente sui progetti «Wikimedia», primo fra tutti la celeberrima enciclopedia libera «Wikipedia».

sponsabilità esistente o futuribile. Infatti, non esistendo previsioni che sanzionino le reti comunitarie per i comportamenti degli utenti, si potrebbe considerare l'applicazione della responsabilità concorrente. Si potrebbe per esempio considerare che la rete ha concorso al fatto illecito fornendo gli strumenti necessari con cui il singolo utente ha perpetrato l'azione dannosa. Nel contesto italiano ciò significherebbe applicare l'art. 2055 c.c. Tuttavia, di nuovo, la mancanza di una qualsivoglia soggettività giuridica, e, conseguentemente, di organi rappresentativi o governativi della rete, crea un vuoto di tutela, nei confronti di un ente privo di qualunque configurazione giuridica.

È indispensabile pertanto interrogarsi su possibili scenari alternativi, soprattutto in una prospettiva *de iure condendo*.

5. Possibili soluzioni prospettabili

Si evince da quanto fin qui narrato che l'applicabilità di norme già esistenti alle WCN risulta particolarmente difficile, se non addirittura impossibile. La regolamentazione delle comunicazioni elettroniche, in astratto applicabile, risulta di fatto inapplicabile in ragione della struttura stessa della rete comunitaria. Il medesimo ostacolo si incontra quando si tenti di applicare alle reti comunitarie le disposizioni di responsabilità civile «classiche». Da ciò discende che non risulta semplice o forse nemmeno possibile effettuare dei pronostici per ipotetiche controversie.

Ad oggi, le reti comunitarie si stanno allargando sia in termini di nodi – e, pertanto, di utenti connessi – sia in termini geografici: le comunità esistenti si stanno allargando e nuove comunità sono in fase di creazione.

Questo genere di strumenti è di particolare importanza soprattutto in Paesi dove non vi siano governi democratici: esse infatti permettono comunicazioni con mezzi alternativi e paralleli a quelli «ordinari», in condizioni di forte anonimato. Inoltre, possono portare connettività in luoghi che restano fuori dalle logiche del mercato e, pertanto, isolati dalle comunicazioni. Ecco che, dunque, anche a parere dell'Organizza-

zione per la Cooperazione e lo Sviluppo Economico, queste reti rappresentano uno strumento fondamentale per la democrazia[57].

Tenendo in considerazione quanto fin qui premesso, discende che un ipotetico regime di responsabilità dovrebbe conciliare da un lato la necessità ed il diritto ad ottenere tutela da parte di chi subisca violazioni, dall'altro le potenzialità e gli effetti positivi della rete, soprattutto in relazione all'anonimato, quale tecnica strumentale ad una maggiore libertà di espressione.

Si possono ipotizzare diversi regimi di responsabilità, a seconda del soggetto da ritenersi di volta in volta responsabile. Per come le WCN sono articolate, i regimi possibili si concentrano ovviamente sulla rete e/o sugli utenti della stessa.

Se si intendesse introdurre un regime di responsabilità in capo alla rete, occorrerebbe in prima battuta pensare una regolamentazione che ne induca la formalizzazione. Si pensi ad esempio ad un'imposizione governativa che, diversamente da quanto oggi avviene, richieda autorizzazioni e/o concessioni per la creazione e lo sviluppo delle WCN. Simili imposizioni avrebbero la conseguenza di formalizzare la rete comunitaria sotto forma di associazione o di altro ente giuridico. Ciò, a sua volta, implicherebbe l'esistenza di un soggetto o di un organo responsabile dell'attività svolta nella rete.

Questo approccio potrebbe però generare conseguenze negative su scopi e benefici delle reti comunitarie. Come si è più volte ribadito, infatti, fra le principali caratteristiche delle WCN vi sono la spontaneità e la loro privatezza, quest'ultima da intendersi sia in termini di riservatezza che di proprietà privata. A monte, l'imposizione di un regime di responsabilità in capo alla sola rete/ente, permetterebbe lo «schermarsi» degli utenti dietro ai propri computer che, non potendo essere identificati, non subirebbero alcun effetto deterrente[58].

A ciò si deve aggiungere un ulteriore rilievo. Si è detto che i *provider* sono stati scelti quali soggetti responsabili nel contesto di Internet

[57] Cfr. *supra* nota n. 2. Per la correlazione fra anonimato, Internet e democrazia, si veda il saggio di M. CUNIBERTI, *Democrazie, dissenso politico e tutela dell'anonimato*, in *Dir. Inf*., n. 2/2014, 111.

[58] Rimane aperta la possibilità che, ricorrendone i presupposti, gli utenti rispondano personalmente in quanto soci.

sia per la posizione nevralgica che rivestono, sia per la loro capacità economica per le ipotesi di risarcimento. Ad oggi le WCN non hanno alcun patrimonio che potrebbe fungere da garanzia in questi casi. Va da sé che, nel caso in cui si dovesse prevedere che tutte le WCN fossero sottoposte ad una procedura autorizzativa, lo stesso ordinamento potrebbe prevedere l'attribuzione di un patrimonio adatto allo scopo, che supererebbe questa problematica[59]. Tuttavia, si ripete, questa possibilità frustrerebbe le caratteristiche di approccio «bottom-up» e di condivisone che ad oggi denotano le reti comunitarie.

Una possibile seconda ipotesi sarebbe incentrata sugli utenti e, più precisamente, potrebbe imporre su di essi la responsabilità delle loro stesse azioni. Da un punto di vista giuridico, invero, ciò non costituirebbe alcuna novità, ma sarebbe meramente l'applicazione dell'art. 2043 c.c. al contesto delle WCN. Da un punto di vista tecnico, tuttavia, sarebbe necessario introdurre un sistema di identificazione degli utenti. Pur volendo immaginare una regolamentazione che imponga un siffatto sistema di riconoscimento, una norma di tal genere andrebbe nuovamente a frustrare le peculiarità della rete: verrebbe infatti meno l'anonimato di cui gli utenti che usano queste reti godono[60]. Se, sotto alcuni aspetti, un simile approccio potrebbe apparire auspicabile, al fine di ottenere una tutela effettiva dei diritti lesi, sotto altri aspetti si andrebbe ad incidere troppo profondamente sulle reti wireless, soprattutto sulle loro potenzialità in termini di libertà di espressione e democrazia.

Non si deve dimenticare, inoltre, che un eventuale sistema di identificazione non sarebbe comunque necessariamente garanzia di una tutela efficace: come più sopra evidenziato, infatti, gli ostacoli incontrati nel

[59] Vale a dire: si prenda l'esempio dell'associazione riconosciuta, per cui sarebbe necessario, come noto, un «patrimonio adeguato alla realizzazione dello scopo» (art. 1, co. 3, DPR 10 febbraio 2000, n. 361).

[60] Si può in questo contesto mutuare quanto sostenuto per il contesto di Internet da G.E. VIGEVANI, *Anonimato, responsabilità e trasparenza nel quadro costituzionale italiano*, in *Dir. Inf.*, n. 2/2014, 221: «Compito precipuo del legislatore sarebbe dunque quello di individuare meccanismi di identificazione del responsabile che non sacrifichino in modo eccessivo le garanzie individuali e che prevedano un controllo da parte di un soggetto terzo e imparziale circa la sussistenza dell'illecito contestato».

mondo di internet per l'*enforcement* di alcuni diritti, potrebbero riproporsi anche in questa sede.

Si potrebbe infine prendere in considerazione un regime «combinato» attribuire la responsabilità alla rete per talune fattispecie, imponendo anzitutto che essa assuma una soggettività giuridica (si pensi alla diffusione di virus o altre fattispecie «tecnicamente» individuabili) e agli utenti per altre fattispecie (come ad esempio per le diffamazioni). Un siffatto regime avrebbe tuttavia la conseguenza di incidere in modo molto profondo sia sull'anonimato degli utenti sia sulla spontaneità della rete. Invero esso imporrebbe sia un sistema di identificazione degli utenti, sia una formalizzazione della rete che dovrebbe anche implementare sistemi tecnici di monitoraggio, quali, ad esempio, filtri dei contenuti. Quest'ultima ipotesi, peraltro, potrebbe essere in contrasto con le attuali normative. L'art. 15 Dir. 2000/31 – recepito con art. 17, d.lgs. 70/2003 – prescrive che gli Stati membri non possano imporre ai *provider* un obbligo di sorveglianza sul traffico e sulle informazioni che trasmettono o che memorizzano, né un obbligo generale di attivarsi per ricercare fatti o circostanze indice di attività illecite. Conseguentemente, un sistema che imponesse filtraggi sarebbe in contrasto con tali norme, come chiarito a più riprese anche dalla Corte di Giustizia dell'Unione europea[61].

Il quadro fin qui descritto sembra dimostrare che le caratteristiche delle reti wireless comunitarie non permettano di conciliare le potenzialità e gli effetti positivi di tali reti, con la necessità di tutela dei diritti, sia interna sia esterna alle reti medesime.

È necessario quindi chiedersi se, di fronte a queste tecnologie, il legislatore possa intervenire efficacemente e se, indipendentemente da tale efficacia, un intervento legislativo sia effettivamente desiderabile.

Le WCN sembrano auto-regolamentarsi: non vi sono delle norme scritte o dei contratti su cui le relazioni fra gli utenti si basino. Esistono soltanto «principi ispiratori», manifesti e decaloghi[62], a cui si aggiungono norme non scritte. Chi entra a far parte di queste comunità deve condividerne idee e regole. Qualora un utente non rispetti questi princi-

[61] Cfr. i cosiddetti casi «Scarlet» e «Netlog», *supra* nota n. 41.

[62] Si veda la pagina a ciò dedicata della rete wireless comunitaria di Firenze: http://wiki.ninux.org/Manifesto.

pi, v'è modo di escluderlo dalla comunità attraverso accorgimenti tecnici.

Sulla base di queste considerazioni, un possibile intervento statale potrebbe incentivare l'adozione di codici di comportamento nascenti all'interno delle comunità, la cui violazione potrebbe essere socialmente sanzionabile. Considerata l'importanza che gli utenti attribuiscono alla rete, al suo funzionamento e al suo perdurare, essi stessi finirebbero per monitorarsi gli uni gli altri. Ciascuna rete potrebbe istituire un comitato deputato a vagliare i comportamenti dei membri e a prendere decisioni per eventuali azioni contro i membri stessi. Se, infatti, i soggetti non sono identificabili, ciascun nodo è conosciuto (quantomeno) dai nodi ad esso attigui. Un simile schema porterebbe alla selezione dei soggetti più motivati e più interessati alla vita della comunità.

Fatte salve le considerazioni più sopra esposte circa gli obblighi di sorveglianza, per aumentare l'effettività dei controlli interni, le reti potrebbero applicare dei sistemi di filtraggio: i nodi gateway potrebbero anche fungere da filtri per le informazioni ed i dati che gli altri nodi tentassero di immettere nella rete Internet[63].

Si tratterebbe di implementare un'organizzazione interna alle WCN e un sistema di monitoraggio diffuso e interno, differente dal classico approccio centralizzato e accentrato tipico del controllo proveniente dall'esterno. Se ciascuna comunità fosse in grado di scegliere al meglio i propri membri e monitorarli, il rischio del verificarsi di comportamenti illeciti si ridurrebbe.

È evidente che tentare effettivamente un intervento di questo tipo necessiterebbe uno studio approfondito dell'*an* e del *quomodo* delle norme sociali esistenti nelle reti comunitarie, anche al fine di meglio comprendere il funzionamento delle reti e, soprattutto, delle sottostanti comunità. Accertata l'esistenza e l'estensione di norme sociali, il legislatore dovrebbe considerare non soltanto l'opportunità di un suo intervento, ma anche le conseguenze di un simile intervento all'interno di una comunità che già si auto-regolamenta. Il legislatore dovrebbe inoltre considerare anche le modalità di un proprio intervento allo scopo di

[63] Suggerisce questa soluzione J.S. HATCHER, *op. cit.*, 13.

tentare di incentivare le esistenti norme sociali in un circolo virtuoso che permetta di ridurre i comportamenti illecitamente rilevanti[64].

Ammesso che una simile regolamentazione possa essere introdotta, essa sarebbe da preferirsi in quanto solo lievemente impattante sul funzionamento e su ciò che potremmo definire come la «filosofia» delle WCN. Chiaramente, anche nella migliore delle ipotesi, non tutti i casi di attività illecite verrebbero eliminati. I casi che concretamente dovessero verificarsi continuerebbero a presentare i problemi evidenziati in termini di tutela dei diritti ed efficacia dei rimedi ad oggi approntati dall'ordinamento.

6. Riflessioni conclusive

Emerge chiaramente dalle pagine che precedono come ancora una volta la nascita e la diffusione di una nuova tecnologia possano mettere a dura prova il tessuto normativo esistente. Nel caso specifico, l'emersione di una nuova tecnologia di comunicazione pone in luce tutte le limitazioni di un impianto normativo – quello della responsabilità extracontrattuale – che è basato su concetti e categorie radicate in tempi lontani. Ciò impone al giurista l'obbligo di interrogarsi e di riflettere su tali concetti e categorie, non già necessariamente per ribaltarli o eradicarli, ma per conciliarli con le peculiarità dei nuovi scenari. Questo breve contributo non aveva tale pretesa, ma si prefiggeva solamente di fornire alcuni spunti di riflessione sul rapporto fra reti wireless comunitarie e responsabilità extracontrattuale.

Si è dimostrato che il quadro normativo attuale non permette un'effettività della tutela, a fronte delle particolarità tecnologiche delle reti analizzate.

---

[64] Si vedano a proposito del ruolo del legislatore in merito alle norme sociali R.C. ELLICKSON, *The Evolution of Social Norms: A Perspective from the Legal Academy*, in M. HECHTER, K.D. OPP (cur.), *Social Norms*, New York, 2001, 35. Si consideri, più in generale, il celebre lavoro di R.C. ELLICKSON, *Order without Law: How Neighbors Settle Disputes*, Harvard, 1991, spec. 284 ss., nonché R.H. MCADAMS, *The Origin, Development, and Regulation of Norms*, in *Michigan Law Review*, n. 2/1997, 338, spec. 391 ss.

Nell'illustrare le ipotesi risolutive si è tenuto conto delle peculiarità e delle potenzialità delle reti comunitarie, che potrebbero essere fortemente danneggiate da strumenti di regolamentazione troppo incisivi. Un interessante campo di indagine, quindi, è quello delle norme sociali, al fine di definire se esse esistano, come si atteggino e quali siano le potenzialità delle stesse nel delimitare i comportamenti illeciti.

Sebbene ad oggi non vi siano casi concreti nei quali possa essere testata la tenuta delle regolamentazioni attuali e della struttura delle reti comunitarie, è necessario interrogarsi sulle possibilità di queste nuove tecnologie e del diritto nei loro confronti. La capacità del diritto di rispondere ai mutamenti dipende anche dall'interpretazione che la dottrina, da sempre sensibile ai cambiamenti sociali, anche – o forse soprattutto – quando scaturenti dalla diffusione di nuove tecnologie.

Bibliografia

AA.VV., *Proceedings of the First Law and Technology Conference*, Houston, 1983

AKYILDIZ I.F., WANG X., WANG W., *Wireless Mesh Networks: A Survey*, 47 *Computer Networks* 445, 2005

ALVANINI S., *La responsabilità dei service provider*, in *Dir. industriale*, n. 4/2010, 329

ANDERSON M., *81% of Tor Users Can Be De-Anonymised by Analysing Router Information, Research Indicates*, in *The Stack*, 14 novembre 2014 <http://thestack.com/chakravarty-tor-traffic-analysis-141114>

ANTONIADIS P. ET AL., *Community Building over Neighborhood Wireless Mesh Networks*, in *IEEE Society and Technology*, n. 1/2008, 48

ARDIA D.S., *Free Speech Savior or Shield for Scoundrels: An Empirical Study of Intermediary Immunity Under Section 230 of the Communications Decency Act*, in *Loyola Los Angeles Law Review*, n. 2/2010, 373

BAISTROCCHI P., *Liability of Intermediary Service Providers in the EU Directive on Electronic Commerce*, in *Santa Clara Computer & High Technology Law Review*, n. 1/2002, 111

BASSAN F. (cur.), *Diritto delle comunicazioni elettroniche*, Milano, 2010

BASSAN F., *Dalle telecomunicazioni alle comunicazioni elettroniche: motivi e percorsi di una riforma permanente*, in ID. (cur.), *Diritto delle comunicazioni elettroniche*, Milano, 2010

BLENGINO C., SENOR M.A., *Il caso «Peppermint»: il prevedibile contrasto tra protezione del diritto d'autore e tutela della privacy nelle reti peer to-peer*, in *Dir. Inf.*, n. 4-5/2007, 835

BONELLI F., *Uso privato ed uso aperto al pubblico di «reti alternative» di telecomunicazioni (art. 101)*, in CLARICH M., CARTEI G.F., *Il codice delle comunicazioni elettroniche*, Milano, 2004

BOSO CARETTA A., *La disciplina del regime autorizzatorio. Le misure di armonizzazione*, in BASSAN F. (cur.), *Diritto delle comunicazioni elettroniche*, Milano, 2010

BRIMSTED K., CHESNEY G., *The ECJ's Judgement in Promusicae: The Unintended Consequences – Music to the Ears of Copyright Owners or a Privacy Headache for the Future? A Comment*, in *Computer Law & Security Report*, n. 3/2008, 275

BROWN B., *Fortifying the Safe Harbors: Reevaluating the DMCA in a Web 2.0 World*, in *Berkeley Technology Law Journal*, n. 1/2008, 437

REESE R., *The Relationship Between the ISP Safe Harbors and Ordinary Rules of Copyright Liability*, in *Columbia Journal of Law & the Arts*, n. 4/2009, 427

BROWNSWORD R., *Rights, Regulation, and the Technological Revolution*, Oxford, 2008

CALABRESI G., *The Costs of Accidents: A Legal and Economic Analysis*, New Haven, 1970

CASO R., *Il conflitto tra copyright e privacy nelle reti Peer to Peer: in margine al caso Peppermint – Profili di diritto comparato*, in *Dir. Internet*, n. 5/2007, 471

CASSANO G., CIMINO I.P., *Il nuovo regime di responsabilità dei providers: verso la creazione di un novello «censore telematico»*, in *Contratti*, n. 1/2004, 88

CLARICH M., CARTEI G.F., *Il codice delle comunicazioni elettroniche*, Milano, 2004

COCKFIELD A., PRIDMORE J., *Symposium: Toward a General Theory of Law and Technology: A Synthetic Theory of Law and Technology*, in *Minnesota Journal of Law Science & Technology*, n. 2/2007, 441

COUDERT F., WERKERS E., *In the Aftermath of the Promusicae Case: How to Strike the Balance?*, in *International Journal of Law and Information Technology*, 1/2008, 50

COX N., *Technology and Legal Systems*, Aldershot, 2006

CUNIBERTI M., *Democrazie, dissenso politico e tutela dell'anonimato*, in *Dir. Inf.*, n. 2/2014, 111

DACOSTA F., *Ugly Truth about Mesh Networks*, dailywireless.org, 28 giugno 2004 <http://www.dailywireless.org/2004/06/28/ugly-truth-about-mesh-networks>

DE CATA M., *Il caso «Peppermint». Ulteriori riflessioni anche alla luce del caso «Promusicae»*, in *Riv. dir. industriale*, n. 4-5/2008, 404

DE CATA M., *La responsabilità civile dell'internet service provider*, Milano, 2010

DE FILIPPI P., *It's Time to Take Mesh Networks Seriously (And Not Just for the Reasons You Think)*, Wired.com, 1 February 2014, <http://www.wired.com/opinion/2014/01/its-time-to-take-mesh-networks-seriously-and-not-just-for-the-reasons-you-think/>

DI CIOMMO F., *Evoluzione tecnologica e regole di responsabilità civile*, Napoli, 2003

DLA PIPER, *EU study on the legal analysis of a Single Market for the Information Society, New rules for a new age?, Liability of online intermediaries*, 2009 <http://ec.europa.eu/digital-agenda/en/news/legal-analysis-single-market-information-society-smart-20070037>

DONATI F., *L'ordinamento amministrativo delle comunicazioni*, Torino, 2007

DULONG DE ROSNAY M., *Peer-to-peer as a design principle for law*, in *Journal of Peer Production*, 2014

ELLICKSON R.C., *Order without Law: How Neighbors Settle Disputes*, Harvard, 1991

ELLICKSON R.C., *The Evolution of Social Norms: A Perspective from the Legal Academy*, in HECHTER M., OPP K.D. (cur.), *Social Norms*, New York, 2001, 35

FLICKENGER R., *Building Wireless Community Networks. Implementing the Wireless Web*, Sebastopol, 2001

FOGLIA G., *La privacy vale più del diritto d'autore: note in materia di filesharing e di sistemi peer-to-peer*, in *Dir. industriale*, n. 6/2007, 598

FORLANO L., *Anytime? Anywhere?: Reframing Debates around Community and Municipal Wireless Networking*, in *Journal of Community Informatics*, n. 1/2008

FRANZONI M., *L'illecito*, Milano, 2010

FRANZONI M., *La responsabilità del* provider, in *AIDA*, 1997, 248

FRIEDMAN J.A., BUONO F.M., *Limiting Tort Liability for Online Third-Party Content under Section 230 of the Communications Act*, in *Federal Communications Law Journal*, n. 3/2000, 647

GAMBINI M., *Diritto d'autore e tutela dei dati personali: una difficile convivenza in Rete*, in *Giur. it*., n. 2/2009, 509

GAMBINI M., *Le responsabilità civili dell'Internet service provider*, Napoli, 2006

GIANNONE CODIGLIONE G., *Indirizzo IP, Reti Wi-Fi e responsabilità per illeciti commessi da terzi*, in *Dir. Inf.*, n. 1/2013, 130

HALE R.V., *Wi-Fi Liability: Potential Legal Risks in Accessing and Operating Wireless Internet*, in *Santa Clara Computer & High Technology Law Journal*, n. 3/2005, 548

HATCHER J.S., *Mesh Networks: A Look at the Legal Future*, 2005, <http://ssrn.com/abstract=814984>

ISHMAEL J., BURY S., PEZAROS D., RACE N., *Deploying Rural Community Wireless Mesh Networks*, 12 *IEEE Internet Computing* 4, 22, 2008

JULIÀ-BARCELÓ R., KOELMAN K.J., *Intermediary Liability: Intermediary Liability in the E-Commerce Directive: So Far so Good, but It's not Enough*, in *Computer Law & Security Review*, n. 4/2000, 231

KERN B.D., *Whacking, Joyriding and War-Driving: Roaming Use of Wi-Fi and the Law*, in *Santa Clara Computer & High Technology Law Journal*, n. 1/2004, 101

KIERKEGAARD S., *ECJ Rules on ISP Disclosure of Subscribers' Personal Data in Civil Copyright Cases*, in *Computer Law & Security Report*, n. 3/2008, 268

LESSIG L., *Code and Other Laws of Cyberspace*, New York, 1999 <http://codev2.cc/download+remix/Lessig-Codev2.pdf>

MAC SÍTHIGH D., *Law in the Last Mile: Sharing Internet Access through Wifi*, in *SCRIPTed*, n. 2/2009, 366

MACCARI L., LO CIGNO R., *A Week in the Life of Three Large Wireless Community Networks*, in *Ad Hoc Networks*, 2014

MCADAMS R.H., *The Origin, Development, and Regulation of Norms*, in *Michigan Law Review*, n. 2/1997, 338

MORBIDELLI G., DONATI F. (cur.), *La nuova disciplina delle comunicazioni elettroniche*, Torino, 2009

OECD, *Development of Wireless Local Area Networks in OECD Countries*, OECD Digital Economy Papers, No. 71, 2003, <http://dx.doi.org/10.1787/23314508843>

PASCUZZI G., *Il diritto dell'era digitale*, Bologna, 2010

PASQUINO T., *Servizi telematici e criteri di responsabilità*, Milano, 2003

PATTEN L.B., *From Safe Harbor to Choppy Waters: YouTube, the Digital Millennium Copyright Act, and a Much Needed Change of Course*, in *Vanderbilt Journal of Entertainment and Technology Law*, n. 1/2007, 179

PEGUERA M., *The DMCA Safe Harbors and Their European Counterparts: A Comparative Analysis of Some Common Problems*, in *Columbia Journal of Law & the Arts* 4, n. 4/2009, 481

PIAZZA A., *La responsabilità civile dell'Internet* Provider, in *Contratto e impresa*, n. 1/2004, 130

POWELL A., *WiFi Publics: Producing Community and Technology*, in *Information, Communication and Society*, n. 8/2008, 1068

RADY M., *Anonymity Networks: New Platforms for Conflict and Contention*, in *MIT Political Science Department Research Paper*, n. 5/2013, <http://ssrn.com/abstract=2241536>

RESTA G., *Anonimato, responsabilità, identificazione: prospettive di diritto comparato*, in *Dir. Inf.*, n. 2/2014, 171

RICCIO G.M., *La responsabilità degli internet providers nel d.lgs. n. 70/03*, in *Danno e resp.*, n. 12/2003, 1157

ROBERT R. ET AL., *WiFi Roaming: Legal Implications and Security Constraints*, in *International Journal of Law and Information Technology*, n. 3/2008, 217

SAMMARCO P., *Alla ricerca del giusto equilibrio da parte della Corte di Giustizia UE nel confronto tra diritti fondamentali nei casi di impiego di sistemi tecnici di filtraggio*, in *Dir. Inf.*, 2012, 297

SBRESCIA V.M., *L'Europa delle comunicazioni elettroniche*, Napoli, 2011

SCHULTZ M.F., *Copynorms: Copyright and Social Norms*, in YU P.K. (cur.), *Intellectual Property and Information Wealth*, Westport, 2006, 201

SPEDICATO G., *La responsabilità extracontrattuale del provider per violazioni del diritto d'autore*, in *Ciberspazio e diritto*, n. 1/2003, 116

STRAHILEVITZ L., *Charismatic Code, Social Norms, and the Emergence of Cooperation on the File-Sharing Networks*, in *Virginia Law Review*, n. 3/2003, 505

SUSSKIND R.E., *The Future of Law: Facing the Challenges of Information Technology*, Oxford, 1996

VAN DAM C., *European Tort Law*, Oxford, 2006

VERBIEST T., SPINDLER G., RICCIO G.M., VAN DER PERRE A., *Study on the liability of Internet intermediaries*, 2007, <http://ec.europa.eu/internal_market/e-commerce/docs/study/liability/final_report_en.pdf>

VIGEVANI G.E., *Anonimato, responsabilità e trasparenza nel quadro costituzionale italiano*, in *Dir. Inf.*, n. 2/2014, 221

WATSON K.D., *The Tor Network: A Global Inquiry into the Legal Status of Anonymity Networks*, in *Washington University Global Studies Law Review*, n. 3/2012, 715

ZENO-ZENCOVICH V., *La pretesa estensione alla telematica del regime della stampa: note critiche*, in *Dir. Inf.*, n. 1/1998, 15.

COLLANA
'QUADERNI DELLA FACOLTÀ DI GIURISPRUDENZA'

UNIVERSITÀ DEGLI STUDI DI TRENTO

1. *L'applicazione delle regole di concorrenza in Italia e nell'Unione europea. Atti del IV Convegno Antitrust tenutosi presso la Facoltà di Giurisprudenza dell'Università di Trento* - (a cura di) GIAN ANTONIO BENACCHIO, MICHELE CARPAGNANO (2014)

2. *Dallo status di cittadino ai diritti di cittadinanza* - (a cura di) FULVIO CORTESE, GIANNI SANTUCCI, ANNA SIMONATI (2014)

3. *Il riconoscimento dei diritti storici negli ordinamenti costituzionali* - (a cura di) MATTEO COSULICH, GIANCARLO ROLLA (2014)

4. *Il diritto del lavoro tra decentramento e ricentralizzazione. Il modello trentino nello spazio giuridico europeo* - (a cura di) ALBERTO MATTEI (2014)

5. *European Criminal Justice in the Post-Lisbon Area of Freedom, Security and Justice* - JOHN A.E. VERVAELE, with a prologue by Gabriele Fornasari and Daria Sartori (Eds.) (2014)

6. *I beni comuni digitali. Valorizzazione delle informazioni pubbliche in Trentino* - (a cura di) ANDREA PRADI, ANDREA ROSSATO (2014)

7. *Diplomatici in azione. Aspetti giuridici e politici della prassi diplomatica nel mondo contemporaneo* - (a cura di) STEFANO BALDI, GIUSEPPE NESI (2015)

8. *Il coordinamento dei meccanismi di stabilità finanziaria nelle Regioni a Statuto speciale* - (a cura di) ROBERTO TONIATTI, FLAVIO GUELLA (2014)

9. *Reti di libertà. Wireless Community Networks: un'analisi interdisciplinare* - (a cura di) ROBERTO CASO, FEDERICA GIOVANELLA (2015)