FEDERICA GIOVANELLA

WIRELESS COMMUNITY NETWORKS: INQUADRAMENTO LEGISLATIVO E QUESTIONI DI RESPONSABILITÀ CIVILE NEL SISTEMA ITALIANO

SOMMARIO: 1. Introduzione. — 2. Cosa sono e come funzionano le Wireless Community Networks. — 3. Il quadro normativo di riferimento. — 4. Possibili implicazioni in termini di responsabilità civile. — 4.1. Responsabilità della WCN. — 4.2. Responsabilità dell'utente. — 4.3. Responsabilità dell'Internet Service Provider. — 5. Spunti di riflessione e ipotesi di risoluzione delle questioni prospettate. — 6. Conclusioni.

1. Introduzione.

Risulta ormai difficile immaginare un mondo senza connessioni: le tecnologie comunicative hanno modificato radicalmente la società. Fra di esse, Internet ha sicuramente avuto un ruolo da protagonista. Soprattutto nelle nuove generazioni la necessità di essere sempre in contatto e di poter comunicare velocemente è diventata un'esigenza costante. Proprio la voglia di comunicare e di confrontarsi è alla base della nascita delle Wireless Community Networks (WCN).

Le WCN sono reti che nascono da gruppi di cittadini che installano nodi wireless sui tetti o sui balconi delle loro case, con il fine di creare una rete indipendente, da usare per veicolare i propri servizi. Esse permettono inoltre di portare connettività ad Internet in zone scoperte dagli operatori commerciali.

* Il presente scritto è stato preventivamente sottoposto a referaggio anonimo affidato ad un componente il Comitato Scientifico dei Referenti della Rivista secondo le correnti prassi nella comunità dei giuristi.

** Questo lavoro è stato supportato dalla 'Fondazione Cassa di Risparmio di Trento e Rovereto' (Trento) per il tramite del progetto 'Wireless community networks: aspetti giuridici, sociologici e tecnici di un nuovo fenomeno d'aggregazione sociale', finanziato nel 2013. I miei ringraziamenti vanno al dott. Leonardo Maccari (Dipartimento di Ingegneria e Scienza dell'Informazione, Università di Trento) per l'essenziale spiegazione del funzionamento dei meccanismi sottostanti alle WCN e alla loro diffusione, ma soprattutto per avermi coinvolta in questa stimolante ricerca.

Con l'allargarsi della comunità, le WCN diventano non solo uno strumento per accedere Internet, ma anche e soprattutto un mezzo di comunicazione svincolato dalle logiche di mercato, partecipato dalla popolazione, che aiuta la coesione delle comunità, di particolare interesse soprattutto per i luoghi più isolati in termini di accesso ad altri mezzi di comunicazione.

Nonostante le loro potenzialità, sottolineate anche dall'Organizzazione per la Cooperazione e lo Sviluppo Economico [3], fino ad oggi queste reti sono state studiate prevalentemente da ingegneri e sociologi [4], mentre la loro analisi è stata trascurata dalle altre scienze, inclusa la ricerca giuridica [5].

Questo articolo tenta di colmare parzialmente questo vuoto, fornendo un inquadramento giuridico alle WCN e analizzandone le potenziali criticità in tema di responsabilità civile. Il contesto esaminato sarà quello europeo, con particolare riferimento al sistema italiano. Numerose WCN sono infattipresenti in diversi paesi europei e stanno attualmente fiorendo anche nel nostro ordinamento [6].

Il contributo si articola nel modo seguente: dopo aver fornito una breve spiegazione tecnica del funzionamento delle WCN (par. 2), si delineerà il quadro normativo di riferimento (par. 3), per poi passare ad illustrare le potenziali criticità in termini di responsabilità di civile (par. 4), con le relative ipotesi risolutive (par. 5), seguite da delle brevi conclusioni (par. 6).

2. Cosa sono e come funzionano le Wireless Community Networks.

Una WCN è una rete wireless organizzata mediante un approccio "bottom-up", in cui persone che si identificano come una

[3] Cf. OECD, Development of Wireless Local Area Networks in OECD Countries, OECD Digital Economy Papers, No. 71, 2003, OECD Publishing, at: *http://dx.doi-.org/10.1787/233145088433.*

[4] Si vedano ad esempio: R. Flickenger, *Building Wireless Community Networks. Implementing the Wireless Web*, Sebastopol, 2001; I.F. Akyildiz, X.Wang, W.Wang, *Wireless mesh 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. Si vedano anche i seguenti progetti finanziati dall'Unione Europea mediante il 7° Programma Quadro: *www.confine-project.eu, www.clommunity-project.eu.* Sul fronte sociologico si vedano, fra i molti, A. Powell, *WiFipublics: producing community and technology*, 11 *Information, Communication and Society* 1068, 2008; L. Forlano, *Anytime? Anywhere?: Reframing debates around community and municipal wireless networking*, 4 *Journal of community informatics*, 2008; P. Antoniadis et al, *Community building over Neighborhood Wireless Mesh Networks*, 27 *IEEE Society and Technology* 48, 2008.

[5] Rarissime eccezioni sono costituite dai seguenti contributi: 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>.

[6] 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

comunità, creano una rete autogestita e "comunità-centrica". Queste reti permettono l'interazione fra utenti (per esempio attraverso messaggi, chiamate, condivisione di contenuti) e possono portare connettività ad Internet laddove non sia disponibile. Sebbene le WCN non debbano essere pensate come un modo per ottenere un collegamento Internet gratuito, esse possono comunque costituire una valida alternativa nelle zone dove gli operatori commerciali non offrono i propri servizi, per esempio per ragioni di profitto.

Dal punto di vista tecnologico, le WCN sono reti "mesh multihop", cioè reti Wi-Fi basate su nodi distribuiti, in cui ciascun nodo partecipa all'instradamento del traffico verso la destinazione finale (sia essa all'interno della rete o in Internet). Ogni nodo, infatti, genera traffico e, al tempo stesso, "trasporta" il traffico di altri nodi. Queste reti non hanno bisogno di pianificazione preventiva, quindi possono estendersi gradualmente fino a coprire intere regioni.

Fra le loro caratteristiche vi sono quella della affidabilità e della semplicità di installazione. Si considerano affidabili in quanto basate su strutture "ridondanti": se i dati cercano di seguire un determinato percorso e tale percorso non è percorribile, per esempio perché un nodo non è funzionante o è scollegato, la rete ridirige automaticamente i dati attraverso un altro percorso. Per quanto concerne la semplicità di installazione, l'aggiunta di un nuovo nodo è una semplice operazione "plug and play" che, insieme all'economicità di costi per un "access point", fanno delle WCN una tecnologia di facile implementazione [7].

Affinché la rete sia connessa ad Internet è sufficiente che uno o più nodi della rete vi siano connessi: tali nodi, detti "gateway" faranno, appunto, da "ponti" fra la rete e Internet. Così facendo, ciascun utente potrà connettersi ad Internet per mezzo di uno o più *gateway*.

Per come sono strutturate, queste reti permettono la connessione di migliaia di nodi, tanto che in alcune regioni le WCN sono diventate un fenomeno di massa: è questo il caso di Atene e Barcellona [8].

Le WCN si basano spesso su software e protocolli aperti e ne condividono il pensiero [9]. Come detto, nascono attraverso un

[7] Si veda iC2 Institute, *Austin's Wireless Future*, January 2004, 32-33 <http://repositories.lib.utexas.edu/handle/2152/14550>.

[8] Sono la Athens Wireless Metropolitan Network (http://awmn.net) e la rete Guifi in Catalonia (http://guifi.net). 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>.

[9] Si vedano a tal proposito le "istruzioni per partecipare" alla rete Ninux: http://wiki.ninux.org/FAQ#NinuxOrgFAQ. Posso_partecipare.3F. Sembrerebbe esserci una sovrapposizione fra il pensiero "open" e le WCN, come si evince dal "Wireless Commons Manifesto": "Wehaveformed the Wi-

approccio "bottom-up", che si riflette nell'assenza di una organizzazione gerarchica: esse mancano di una amministrazione centrale o di un qualunque organo con funzioni di controllo o con poteri rappresentativi. Normalmente ciascun utente è responsabile (solo) del proprio nodo e la rete non è altro che una struttura spontanea basata sulla sottostante comunità.

Fra le tante peculiarità delle WCN vi è anche quella dell'anonimato. Non solo tale anonimato si realizza all'interno della rete, ma esso persiste anche nel caso di tentativi di riconoscimento di chi si "celi" dietro agli schermi. Invero, sebbene come accade nel contesto di Internet, ciascun nodo sia contraddistinto da un indirizzo IP, ogni utente sceglie autonomamente il proprio indirizzo e lo può cambiare in ogni momento. In aggiunta a questa volatilità, non esiste alcun organismo che registri gli indirizzi IP degli utenti e le identità ad essi associate, come effettuato invece dagli *Internet Service Providers* (ISP) nel contesto di Internet. Ciò significa che, anche laddove si conoscesse un indirizzo IP, non si potrebbe con alcuna certezza risalire al soggetto che di tale indirizzo fosse in un determinato momento il titolare.

Date queste premesse occorre ora fornire un inquadramento giuridico di queste reti, al fine di comprendere quale disciplina sia loro applicabile.

3. Il quadro normativo di riferimento.

Il quadro normativo di riferimento si sostanzia nel c.d. "Codice delle comunicazioni elettroniche", ovverosia il d.lgs. 1° agosto 2003, n. 259 (Cod. Com. El.). Il Codice nasce principalmente come risposta attuativa ad un pacchetto di direttive europee del 2002 a regolamentazione del settore delle comunicazioni elettroniche [10]. Tali direttive si pongono come seconda fase di un lungo cammino percorso dall'Unione Europea in tema di telecomunicazioni, avviatosi nei primi anni '90 con la volontà di permettere la

reless Commonsbecause a global wireless network iswithinourgrasp. We will work to define and achieve a wireless commons built using shared spectrum, and able to connect people everywhere. We believe there is value to an independent and global network which is open to the public. We will break down commercial, technical, social and political barriers to the commons. The wireless commons bridges one of the few remaining gaps in universal communication without interference from middlemen and meddlers" (all'url: http://www.wirelesscommons.org).

[10] 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 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/CEdel 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). In materia di regolazione delle comunicazioni elettroniche si vedano per

privatizzazione di tali servizi [11] e giunto oggi ad un ulteriore passaggio, con la terza riforma avutasi nel 2009 con il cosiddetto "Pacchetto Telecom" [12]. Lo stesso tracciato è seguito dal Codice: esso nasce con l'esigenza, come detto, di implementare il pacchetto di direttive europee del 2002, ma al contempo riordina in un unico testo la normativa in materia. Concentrandoci in questa sede solo sulla normativa oggi vigente e con riferimento unicamente a quanto concerne le WCN, occorre innanzitutto analizzare se e in che modo sia ad oggi regolamentata la creazione ed installazione di una rete wireless comunitaria.

Il Cod. Com. El. al Titolo III regola le "Reti e servizi di comunicazione elettronica ad uso privato". Il suo art. 104 richiede una autorizzazione generale per una serie di attività, anche qualora esse possano qualificarsi come "private". Tuttavia, in quest'ultimo caso, esiste un'ampia deroga al regime generale applicato per le reti "ad uso pubblico". Tale deroga permette una vasta libertà d'uso in numerose fattispecie e, in aggiunta a ciò, il

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.

[11] Le prime direttive europee sono datate 1990: 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.

[12] 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 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. "Betterregulation"). Sull'evoluzione del sistema si veda F. Bassan, *Dalle telecomunicazioni alle comunicazioni elettroniche: motivi e percorsi di una riforma permanente*, in F. Bassan (cur.), *Diritto delle comunicazioni elettroniche*, cit., 3 ss.; V.M. Sbrescia, *L'Europa delle comunicazioni elettroniche*, cit., 1 ss.

regime autorizzatorio per le reti ad uso privato differisce da quello generale [13].

Il menzionato regime generale di autorizzazione è incardinato sulla nozione di "servizi di comunicazione elettronica", rinvenibile nella dir. 2002/21 c.d. "direttiva quadro", recepito nell'art. 1 Cod. Com. El. che 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, lettera *a*), del decreto legislativo 9 aprile 2003, n. 70, non consistenti interamente o prevalentemente nella trasmissione di segnali su reti di comunicazione elettronica" [14]. Tale definizione è da interpretarsi nel senso che sono soggetti ad autorizzazione i servizi consistenti nel trasmettere segnali attraverso reti di comunicazione elettronica (con mezzi elettromagnetici), ma sono invece esclusi da tale autorizzazione i servizi che forniscano solo contenuti [15].

Si deve intendere per autorizzazione, secondo l'art. 1, lett. *g*) "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". Sempre l'art. 1, lett. *ff*) definisce "servizio di comunicazione elettronica ad uso privato: un servizio di comunicazione elettronica svolto esclusivamente nell'interesse proprio dal titolare della relativa autorizzazione generale". Inoltre, il titolare di autorizzazione generale ad uso privato può utilizzare le reti di comunicazione solo per trasmettere dati ed attività di propria pertinenza, con esplicito divieto di effettuare traffico per conto terzi (co. 1, art. 101).

Una stretta interpretazione di queste disposizioni fra propendere per la non qualificabilità delle WCN come reti "ad uso privato" [16].

È possibile tuttavia che le WCN non siano soggette ad autorizzazione alcuna. Ed invero, l'art. 99 prevede che una serie di

[13] A. Boso Caretta, *La disciplina del regime autorizzatorio. Le misure di armonizzazione*, in F. Bassan (cur.), *Diritto delle comunicazioni elettroniche*, cit., 67.

[14] Art. 2, lett. *c*), Dir. 2002/21/CE e art. 1, lett. *gg*), d.lgs. 259/2003. Per la definizione di "servizi della società dell'informazione" v. *infra* paragrafo 4.1.

[15] A. Boso Caretta, *La disciplina del regime autorizzatorio. Le misure di armonizzazione*, 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*.

[16] Cf. 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, *Il codice delle comunicazioni elettroniche*, cit., 473 ss.

attività, elencate all'art. 105, siano "in ogni caso libere". L'art. 105 infatti elenca sotto la rubrica "Libero uso" diverse attività, fra cui le "reti locali di tipo radiolan e hiperlan" (lett. *b*). A questa categoria, che fa riferimento ai collegamenti Wi-Fi, sono da ascrivere anche le WCN, che si basano principalmente su frequenze di 2.4, 5.4-5.7 GHz [17].

Peraltro, se, fino al 2012, utilizzare questo tipo di tecnologia con collegamenti al di fuori del proprio fondo soggetto ad autorizzazione generale, le modifiche, introdotte dal d.lgs. 28 maggio 2012, n. 70 per implementare le due direttive del 2009 sulle comunicazioni elettroniche [18], sottraggono a questa limitazione alcune attività, fra cui anche le reti locali radiolan e hiperlan [19].

Appare pertanto piuttosto lineare, ad oggi, l'applicazione delle norme del Cod. Com. El. alle reti wireless: fintanto che la tecnologia utilizzata non muterà, esse potranno rientrare nelle libere utilizzazioni, senza che nulla occorra ai fini della loro creazione ed installazione.

Diversa è l'ipotesi della condivisione della rete wireless dell'utente privato. Al di là delle considerazioni di tipo contrattuale fra utente e *provider*, di cui si dirà successivamente, si deve dare conto delle diverse norme che si sono susseguite nell'ultimo decennio in materia.

Si ricorderà che il c.d. "Decreto Pisanu", d.l. 27 luglio 2005, n. 144, convertito, con modificazioni, in legge 31 luglio 2005, n. 155, aveva previsto, tra le varie misure a contrasto del terrorismo internazionale, anche alcune limitazioni all'utilizzo di reti di comunicazione, fra cui il Wi-Fi. In particolare, 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" [20]. 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 [21].

---

[17] 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

[18] Le già citate Dir. 2009/136/CE e Dir. 2009/140/CE.

[19] La menzionata lett. *b*) dell'art. 105 Cod.Com. El., è stata infatti privata delle parole "nell'ambito del fondo, ai sensi dell'articolo 99, comma 5" dall'articolo 70, co. 1, d.lgs. 28 maggio 2012, n. 70, recante modifiche al decreto legislativo 1° agosto 2003, n. 259, 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.

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

[21] Art. 1, co. 1, lett. *b*), D.M. 16 agosto 2005, n. 19023: "identificare chi accede ai servizi telefonici e telematici offerti, prima dell'accesso stesso o dell'offerta di credenziali di accesso, acquisendo i dati

I vincoli discendenti dal Decreto Pisanu erano temporalmente limitati al 31 dicembre 2011 [22]: non essendo intervenuta alcuna ulteriore proroga, tali obblighi possono oggi considerarsi caduti [23].

Si deve peraltro dar conto delle ulteriori specificazioni previste nel d.l. 21 giugno 2013, n. 69, c.d. "Decreto del fare" [24], che all'art. 10 ha liberalizzato l'accesso ad Internet per il tramite di tecnologie Wi-Fi. Lo stesso articolo ha inoltre specificato che quando l'offerta di accesso ad Internet non sia attività commerciale prevalente del gestore del servizio, non si applicano le disposizioni qui illustrate del Decreto Pisanu (ad oggi, come visto, decadute), né le disposizioni relative all'"Autorizzazione generale per le reti e i servizi di comunicazione elettronica" di cui all'art. 25 Cod. Com. El.

In definitiva, dunque, pare potersi affermare che ad oggi non occorra alcuna autorizzazione per l'installazione di una rete wireless comunitaria, né occorra effettuare l'identificazione degli utenti che vi prendono parte. Ciò sia in considerazione del fatto che né la WCN può considerarsi "gestore del servizio", né, *a fortiori*, l'offerta di accesso ad Internet costituisce la sua attività prevalente.

Questa brevissima inquadratura regolamentativa deve chiudersi con un'annotazione: l'applicabilità delle previsioni qui richiamate sottostà alle difficoltà di individuare, come più sotto si illustrerà, un responsabile della rete stessa, che sotto questo profilo si rivela pienamente come entità acefala.

4. Possibili implicazioni in termini di responsabilità civile.

Sebbene ad oggi non esista alcun caso concreto scaturito dall'uso delle WCN, è possibile immaginare diverse questioni giuridiche che possono scaturire dalla diffusione di queste reti comunitarie.

Innanzitutto ci si può rappresentare alcuni usi illeciti che di esse possano essere fatti: basti pensare ad ipotesi di azioni diffamato-

anagrafici riportati su un documento di identità, nonché il tipo, il numero e la riproduzione del documento presentato dall'utente". Si veda inoltre l'art. 4 dello stesso decreto: "Accesso alle reti telematiche attraverso tecnologia senza fili — 1. I soggetti che offrono accesso alle reti telematiche utilizzando tecnologia senza fili in aree messe a disposizione del pubblico sono tenuti ad adottare le misure fisiche o tecnologiche occorrenti per impedire l'uso di apparecchi terminali che non consentono l'identificazione dell'utente, ovvero ad utenti che non siano identificati secondo le modalità di cui all'art. 1".

[22] 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 (modificato 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).

[23] Il co. 4, art. 7, Decreto Pisanu fu abrogato già dall'art. 2, co. 19, D.L. 29 dicembre 2010, n. 225.

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

rie, allo scambio illecito di materiale protetto da diritto d'autore, o all'organizzazione di attività criminose.

Parallelamente, appare interessante considerare le modalità di auto-regolamentazione interne alle reti stesse: gli utenti, pur in assenza di regole scritte o contratti, tendono di fatto ad attenersi a dei codici di condotta interni. Chi vuole entrare a far parte della rete e del progetto sottostante ne deve condividere i principi di partecipazione e di diffusione della conoscenza. Spetta agli altri componenti della comunità decidere se un nuovo arrivato possa o meno far parte della comunità e del progetto. Nell'eventualità in cui un utente già parte della rete si comporti in modo non consono ai principi non scritti esistenti all'interno di essa, esistono dei metodi tecnologici per escludere tale utente dalla rete. Discende da quanto brevemente illustrato che un campo di indagine interessante sarebbe legato alle "norme sociali", considerate come standard e regole informali interne ad un determinato gruppo, che regolano il comportamento di quello specifico gruppo [25].

Tra le varie implicazioni possibili, questo articolo si concentra sulle questioni di responsabilità civile, con particolare riferimento al contesto italiano così come influenzato dalle regolamentazioni europee in materia di comunicazioni elettroniche e di società dell'informazione. Più specificatamente si considereranno tre diversi casi di responsabilità, a seconda del soggetto implicato:

a) il primo riguarda la stessa WCN: può la stessa rete essere considerata come entità responsabile nel caso di azioni illecite perpetrate al suo interno?

b) Il secondo caso concerne la responsabilità del singolo utente, sia per le azioni da egli stesso perpetrate, sia per le azioni perpetrate da altri nel caso tale utente sia nodo *gateway*.

c) La terza ipotesi concerne l'ISP per il caso in cui l'attività illecita sia realizzata attraverso un *gateway*. Il *provider* può essere considerato responsabile per un'attività illecita perpetrata attraverso tale nodo?

Nei prossimi paragrafi si tenterà di fornire una risposta a questi quesiti, tenendo presente che non esistono regole che prendano specificatamente in considerazione una tecnologia come quella

[25] Sotto il profilo dell'enforcement, dato che ogni nodo non è altro che una piccolo 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*, 89 Va.L.Rev. 505, 2003; M.F. SCHULTZ, *Copynorms: Copyright and Social Norms*, in P.K. YU (cur.), *Intellectual Property and Information Wealth*, Westport, 2006, 201.

delle WCN, né vi sono, ad oggi, come detto, casi giurisprudenziali cui fare riferimento.

4.1. *Responsabilità della WCN.*

È possibile pensare a delle ipotesi di responsabilità della rete qualora azioni dannose siano perpetrate all'interno della rete stessa. Si rifletta ad esempio sullo scambio illecito fra utenti di materiale coperto da diritto d'autore; sulla diffusione di dati personali; su un comportamento diffamatorio. Si possono inoltre ipotizzare questioni più strettamente legate alla tecnologia della rete, come la diffusione di virus o attacchi hacker.

Per potersi avere una responsabilità della rete per quanto compiuto dagli utenti, sarebbe indubbiamente necessaria l'esistenza di una regola che prevedesse specificatamente una responsabilità per fatto illecito altrui, stante il ben noto paradigma secondo cui ciascuno è responsabile solo per le proprie azioni, salvo diversa previsione.

Quando tale previsione vi sia, essa è normalmente da associarsi alla peculiare relazione fra il possibile responsabile e uno o più elementi del fatto illecito [26], e si ricollega normalmente aduna condotta omissiva: si risponde per aver omesso di sorvegliare, per aver omesso di controllare, e via dicendo. Spesso, inoltre, il soggetto su cui la responsabilità ricade è scelto perché diverrebbe eccessivamente costoso o di fatto impossibile raggiungere e punire l'effettivo soggetto agente [27].

Sebbene il codice civile avesse inizialmente introdotto un numero esiguo di casi in cui un soggetto può essere considerato responsabile per il fatto altrui, la legislazione speciale si è premurata di disciplinare nuove fattispecie [28]. Fra di esse occorre prendere in considerazione la responsabilità dei c.d. "prestatori di servizi" o intermediari di Internet, altrimenti detti Internet Service *Provider*. Di ciò occorre trattare per via del parallelismo fra *providers* e WCN e della possibile analogia di tale normativa al contesto delle reti comunitarie.

È noto che la disciplina della responsabilità degli intermediari di Internet sia di derivazione comunitaria. In particolare, il d.lgs. 9

[26] M. Franzoni, *L'illecito*, Milano, 2010, 678-679.

[27] C. VanDam, *EuropeanTort 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, *L'illecito*, cit., 680.

[28] 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).

aprile 2003, n. 70 ha recepito, essenzialmente senza modifiche, la Dir. 2000/31/CEc.d. "sul commercio elettronico" [29]. È ugualmente noto come la scelta di imporre una responsabilità indiretta in capo agli ISP per il fatto degli utenti discenda dal ruolo strategico che tali intermediari svolgono nel contesto dellarete Internet [30]. Nei primi anni della sua diffusione, Internet appariva come un luogo, non solo non governato, ma pressoché non governabile. L'incapacità di raggiungere il vero autore di un fatto illecito spinse fin da subito a riconoscere negli ISP i soli soggetti tracciabili, con il risultato che questi ultimi furono talvolta ritenuti responsabili ben oltre le loro capacità. Nelle prime controversie, infatti, in assenza di una specifica disciplina, le corti applicavano le regole generali della responsabilità civile, finendo per assimilare il *provider*al gestore di un'attività pericolosa, oppure applicavano leggi speciali previste per altri settori, per cui il *provider* era considerato al pari dell'editore di una testata giornalistica [31].

La scelta di responsabilizzazione dell'ISP dipende dunque indubbiamente anche dall'agilità con cui è raggiungibile il *provider* rispetto al singolo utente di Internet, nonché dalla sua capacità economica [32].

La disciplina dettata dal d.lgs. 70/2003 considera i *provider* responsabili delle azioni perpetrate dagli utenti solo qualora gli intermediari non si confacciano a determinati requisiti individuati nel decreto stesso. In altre parole: fintanto che un ISP si

[29] 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.

[30] Non sarebbe responsabilità indiretta, bensì responsabilità per fatto proprio secondo M. Franzoni, *L'illecito*, 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.*, 2003, 1157; G. Cassano, I.P. Cimino, *Il nuovo regime di responsabilità dei providers: verso la creazione di un novello "censore telematico"*, in *Contratti*, 2004, 88.

[31] 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*, 2010, 329-330; M. Franzoni, *La responsabilità del* provider, in *AIDA*, 1997, 248; G. Spedicato, *La responsabilità extracontrattuale del* provider *per violazioni del diritto d'autore*, in *Ciberspazio e diritto*, 2003, 116; A. Piazza, *La responsabilità civile dell'Internet* Provider, in *Contratto e impresa*, 2004, 130. 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 questa *Rivista*, 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.

[32] Questa non è altro se non l'applicazione, in via legislativa, della c.d. "deeppocketstheory", per cui si veda G. Calabresi, *The Costs of Accidents: A Legal and Economic Analysis*, New Haven, 1970, 40 ss.

adegua agli specifici comportamenti richiesti dalla normativa, non può essere ritenuto responsabile di quanto compiuto dagli utenti [33].

La direttiva 2000/31 e il conseguente d.lgs. 70/2003 individuano tre diverse categorie di *provider*: "mere conduit", "caching", e "hosting" [34]. Senza entrare in dettaglio, basti qui dire che a ciascuna di queste attività è correlato un diverso livello di implicazione nel contesto di Internet, cui si ricollega un diverso livello di oneri cui attenersi onde evitare di incorrere in responsabilità. Si badi bene che, in nessun caso, il *provider* è tenuto ad una sorveglianza del traffico e ciò in base all'art. 17, d.lgs. 70/2003 (già art. 15, Dir. 2000/31) [35].

Come menzionato, le WCN possono essere per molti versi assimilate ad Internet, se consideriamo che quest'ultima altro non è se non un insieme di reti fatte di migliaia di nodi [36]. Data questa

[33] 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. "safeharbors". Anche il sistema USA considera diversi *provider*s e diversi oneri a seconda dell'attività svolta da questi. Tuttavia, v'è una pesante 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*, 52 *Fed. Comm. L.J.* 647, 2000; D.S. Ardia, *Free Speech Savior or Shield for Scoundrels: An Empirical Study of Intermediary Immunity Under Section 230 of the Communications Decency Act*, 43 *Loy. L.A. L. Rev. 373*, 2010.

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*, 16 *C.L.S.Rev.* 4 (2000), 231; P. Baistrocchi, *Liability of Intermediary Service Providers in the EU Directive on Electronic Commerce*, 19 *Santa Clara Computer & High Tech. L.J.* 1 (2003), 111; T. Verbiest, G. Spindler, G.M. Riccio, A.VanderPerre, *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*, 10 *Vanderbilt J. Of Entertainment And Tech. Law 1*, 2007, 179; B. Brown, *Fortifying the Safe Harbors: Reevaluating the DMCA in a Web 2.0 World*, 23 *Berkeley Tech. L.J.* 1 (2008), 437; R.Reese, *The Relationship Between the ISP Safe Harbors and Ordinary Rules of Copyright Liability*, 32 *Colum. J.L. & Arts* 4, 2009, 427.Infine, per una comparazione fra i due approcci si veda il contributo di M.Peguera, *The DMCA SafeHarbors and Their European Counterparts: A Comparative Analysis of Some Common Problems*, 32*Colum.-VLA J.L.&Arts*, 2009, 481.

[34] Si vedano gli artt. 12-14, Dir. 2000/31/CE e gli artt. 14-16, d.lgs. 70/2003.

[35] 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. Sociétébelgedesauteurs, compositeurs et éditeurs SCRL (SABAM)*, deciso il 26 novembre 2011 e C-360/2010, *SABAM v. Netlog NV*, deciso il 31 marzo 2012.

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

similitudine, è possibile applicare in via analogica la disciplina dettata per gli ISP?

Prima di analizzare tale possibilità occorre ricordare che la struttura delle WCN è del tipo "peer-to-peer", dove ciascun nodo genera dati e, al contempo, instrada i dati di altri nodi. Non esiste un nodo centrale c.d. "access point", sebbene alcuni siano strategicamente più importanti o più "trafficati" di altri. In questo senso, le reti comunitarie differiscono fortemente dalla rete Internet, in cui, come più volte detto, i *provider* sono stati scelti anche in considerazione del loro ruolo strategico e funzionale.

Chiaramente, al fine di comprendere se la disciplina relativa ai *provider* sia o meno essere applicabile alle reti di cui ci occupiamo, occorre interpretare le parole della direttiva e del decreto di recepimento ed analizzarne il campo di applicazione [37].

Da un punto di vista soggettivo, la Dir. 2000/31 si riferisce a ogni "prestatore" di servizi, inteso come "la persona fisica o giuridica che presta un servizio della società dell'informazione" [38]. Un "servizio della società dell'informazione" è da intendersi come "qualsiasi servizio prestato normalmente dietro retribuzione, a distanza, per via elettronica e a richiesta individuale di un destinatario di servizi" [39].

Per comprendere queste definizioni occorre rifarsi alla giurisprudenza della Corte di Giustizia, soprattutto per la controversa espressione "dietro remunerazione". Secondo l'art. 50 del Trattato delle Comunità Europee [40], "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".

Secondo quanto stabilito nel caso *Belgio v Humbel*, qualunque corrispettivo per un'attività economica può essere considerato una "remunerazione" [41]. Essa non dev'essere necessariamente né diretta né monetaria, né occorre che sia l'utente finale a pagare

[37] In considerazione del fatto che il d.lgs. 70/2003 di trasposizione della dir. 2000/31 ne è una copia quasi pedissequa, si parlerà in questa sede principalmente della norma europea, ciò permettendo di dare un'illustrazione di più ampio spettro, senza che tale approccio implichi dimenticarsi dell'ordinamento italiano.

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

[39] 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 1998che 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 1998relativa 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.

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

[41] C-263/86, *Belgian State v René Humbel and Marie-ThérèseEdel*, 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

per il servizio: si considera remunerazione a questi fini anche il ritorno derivante da pubblicità e affini [42].

Per essere tale, inoltre, un servizio deve essere *normalmente* prestato dietro remunerazione. Si possono concepire due diverse interpretazioni dell'avverbio "normalmente": esso può fare riferimento a ciò che normalmente avviene nello stesso mercato; oppure può fare riferimento a come normalmente il soggetto implicato offre quel servizio [43]. La seconda ipotesi è più intuitiva delle prima, per la quale, affinché un *provider* possa essere soggetto alla Direttiva occorre che la maggioranza dei *provider* nello stesso mercato offrano lo stesso servizio dietro remunerazione la maggioranza delle volte [44].

Per quanto concerne le WCN, esse non operano in un vero e proprio mercato, e, pur a voler considerare il loro operare come un servizio offerto, tale servizio è indubbiamente gratuito. Lo scopo delle reti comunitarie è quello di permettere la circolazione di dati ed informazioni all'interno della rete stessa, eventualmente consentendo la connessione alla rete Internet.

È pur vero, tuttavia, che il diffondersi delle reti e l'allargarsi delle comunità può portare ad assimilare le WCN agli ISP [45]: esse infatti possono offrire un servizio di scambio dati che normalmente è offerto dietro remunerazione da parte degli intermediari di Internet. Date queste premesse, la direttiva 2000/31, e così il d.lgs. 70/2003, parrebbero applicabili anche alle reti comunitarie.

Nondimeno, la struttura stessa delle WCN impone ulteriori considerazioni. Si è detto della mancanza di organizzazione gerarchica di queste reti, che nascono e si sviluppano in modo spontaneo. Non sono enti con una struttura determinata, al cui vertice vi sia un soggetto o un organo responsabile. Diverrebbe pertanto pressoché impossibile agire nei confronti della "rete" come soggetto danneggiante: non avendosi alcuna soggettività giuridica, non si avrebbe tantomeno alcun soggetto passivamente legittimato al giudizio.

Chiaramente, questo aspetto prescinde dalle prescrizioni della Dir. 2000/31 e necessita, invece, di essere declinato all'interno del sistema giuridico di ciascun stato membro. Per quanto concerne l'Italia, un siffatto quadro non permetterebbe di ottenere ristoro di un danno subito. Diverso sarebbe nel caso in cui la comunità si

fra il prestatore ed il destinatario del servizio".

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

[43] 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/eu/news/legal-analysis-single-market-information-society-smart-20070037>, 12, nota n. 58.

[44] DLA Piper, *EU study on the legal analysis of a Single Market for the Information Society, New rules for a new age?*, cit., 12, nota n. 58.

[45] Della medesima idea già J.S. Hatcher, *Mesh Networks: A Look at the Legal Future*, cit., 19.

organizzasse sotto forma di associazione [46]: quand'anche si trattasse di associazione non riconosciuta, ciò implicherebbe l'esistenza di soggetti responsabili dell'operato dell'associazione.

Il problema da ultimo illustrato, vale a dire l'impossibilità di ottenere efficacemente tutela, permane qualunque regime di responsabilità si voglia adottare nei confronti delle WCN, fintanto che queste continuino ad essere un fenomeno spontaneo.

Invero, non esistendo alcuna previsione che possa colpire le WCN come responsabili indirette delle azioni egli utenti, si potrebbe pensare ad una responsabilità concorrente, per esempio per aver fornito gli strumenti per mezzo dei quali l'azione dannosa è stata perpetrata. Per quanto riguarda il contesto italiano ciò implicherebbe un riferimento necessario all'art. 2055 c.c. Quest'interpretazione, che si analizzerà nel prossimo paragrafo con riferimento ad un'altra fattispecie, non supera tuttavia, come detto, la problematica dell'attribuzione di responsabilità ad un ente, la WCN, che è assolutamente privo di qualunque configurazione giuridica.

4.2. *Responsabilità dell'utente.*

Qualora l'azione illecita sia perpetrata da un utente, è possibile rappresentarsi due ipotesi di responsabilità ulteriori rispetto a quelle già viste.

Un utente potrebbe essere responsabile, infatti, non solo per le sue stesse condotte, ma anche, per l'ipotesi di un utente titolare di un nodo *gateway*, per le condotte altrui effettuate nella rete Internet attraverso tale nodo.

In questo caso tornano a giocare un ruolo predominante le norme civilistiche in tema di responsabilità. Se la prima fattispecie, infatti, sarebbe indubbiamente riconducibile al più classico dei fatti *ex* art. 2043 c.c., la seconda fattispecie potrebbe essere di nuovo considerata come una responsabilità di tipo concorrente e, quindi, solidale *ex* art. 2055 c.c [47]. Si potrebbe invero ipotizzare, come più sopra effettuato in relazione alle reti, che l'utente *gateway*, permettendo la connessione ad Internet di altri utenti,

[46] Si veda ad esempio il caso di Ninux Roma, che è parte di un progetto sociale più ampio facente capo ad una associazione ONLUS (cf: 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 Trih. 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".

[47] 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 questa *Rivista*, n. 1/2013, 130 ss.

fornisca gli strumenti idonei alla condotta illecita, in questo modo prendendovi causalmente parte.

Ancora una volta, nondimeno, la struttura stessa della WCN frustrerebbe le possibilità di *enforcement* di qualsivoglia diritto violato. Infatti, come precedentemente illustrato, un'altra peculiare caratteristica delle reti comunitarie è che, pur esistendo un indirizzo IP legato a ciascun nodo, ogni utente sceglie il proprio e lo modifica a piacimento; a ciò si aggiunga che non esistono registri o *data base* che contengano questi indirizzi. Da ciò discende che, evidentemente, la possibilità di identificare l'utente responsabile è prossima allo zero.

Permarrebbe, tuttavia, la possibilità di identificare l'utente-nodo *gateway*. Egli, infatti, essendo connesso alla rete Internet è dotato di indirizzo IP: il *provider* che fornisce la connettività sarà quindi in grado di combinare dati di accesso e dati identificativi al fine di poter fornire l'identità del soggetto.

Ciò non sarebbe comunque garanzia di un'efficace tutela. È invero noto che, per le ipotesi di violazione del diritto d'autore per c.d. "file sharing", i giudici italiani hanno seguito la corrente di pensiero che, non solo ritiene l'indirizzo IP dato personale, ma soprattutto considera i dati personali degli utenti prevalenti rispetto alla tutela del diritto d'autore [48]. Senza entrare ora nel dettaglio e senza effettuare considerazioni valutative, ciò ha oggettivamente frustrato le aspettative di *enforcement* dei titolari di diritti d'autore.

Sebbene la soluzione applicabile vari da caso a caso e debba tenere in debita considerazione i diritti effettivamente coinvolti, è

[48] 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'Article29 Data ProtectionWorking 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: How to Strike the Balance?*, 18 *International Journal of Law and Information Technology* 50, 2008, 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 questa *Rivista*, 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 sul punto 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 questa *Rivista*, 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

possibile che lo stesso trattamento spetterebbe a chi volesse tutelarsi nei confronti di un utente-nodo *gateway* per aver subito la violazione di un diritto.

4.3. *Responsabilità dell'ISP.*

Un'ultima ipotesi di responsabilità concerne gli ISP per l'eventualità che un illecito sia perpetrato sulla rete Internet, per mezzo di un nodo *gateway*.

Come accennato, la Dir. 2000/31 differenzia, mediante gli articoli 12, 13 e 14, tre tipi di *provider* a seconda delle loro funzioni. Secondo l'art. 14 del decreto di recepimento, il *provider* di "mero trasporto" ("mereconduit" nella versione della Direttiva), è l'intermediario che trasmette informazioni fornite da un destinatario del servizio o che fornisce accesso alle reti di comunicazione. L'art. 15 definisce il *caching provider* come quello 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.

Infine, l'art. 16 considera *hosting provider* quello che memorizza le informazioni fornite da un destinatario del servizio.

Brevemente, si può dire che *caching* e *hosting provider* sono di fatto responsabili per le attività di memorizzazione, seppur con differenti modalità, delle informazioni a richiesta del destinatario, e per non rimuoverle qualora siano tenuti a farlo [49]. La direttiva e il decreto di recepimento considerano responsabili questi intermediari indipendentemente dalla fonte da cui le informazioni memorizzate e/o non rimosse provengono. Si pensi al caso di immagini o parole diffamatorie postate su un sito. Conseguentemente, nel caso qui ipotizzato, è possibile ritenere che per questi due tipi di intermediari non vi sia alcuna differenza in termini di responsabilità se l'informazione proviene da un soggetto non connesso ad Internet "direttamente".

Per quanto concerne il *provider* di mero trasporto, il discorso è parzialmente differente giacché, diversamente da quanto accade per gli altri due *provider*s, esiste fra esso e l'utente un rapporto

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*, 24 *Computer L.&Secur.Rep.* 268, 2008; K.BRIMSTED, G. CHESNEY, *The ECJ'sjudgement in Promusicae: The unintendedconsequences — music to the ears of copyright owners or a privacy headache for the future? A comment*, 24*Computer L. & Secur. Rep.* 275, 2008; M.DECATA, *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 della identificazione del soggetto responsabile v. G. RESTA, *Anonimato, responsabilità, identificazione: prospettive di diritto comparato*, in questa *Rivista*, n. 2/2014, 189-191; 196-202.

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

contrattuale. Pertanto, a prescindere dall'applicazione delle previsioni di cui all'art. 14 d.lgs. 70/2003, un *provider* potrebbe limitare la propria responsabilità attraverso specifiche clausole contrattuali. Esistono già numerosi casi di contratti contenenti clausole che vietano all'utente di condividere la propria connessione [50].

Nell'ipotesi in cui l'utente-nodo *gateway* dovesse contravvenire alle disposizioni contrattuali si renderebbe non solo responsabile in via contrattuale, ma potrebbe essere anche considerato quale garante per eventuali danni che il *provider* si trovasse a dover risarcire a causa della condotta illecita perpetrata mediante la connessione del *gateway* [51].

Peraltro, come già illustrato, laddove la condotta illecita fosse posta in essere da un utente terzo rispetto al cliente del *provider*, tale utente terzo non sarebbe identificabile. Al contrario, sarebbe identificabile mediante il proprio indirizzo IP l'utente *gateway*. In questo modo l'utente *gateway* potrebbe essere caricato della responsabilità di azioni altrui per aver violato il contratto. Ciò potrebbe fungere da forte deterrente all'apertura del nodo e, quindi, alla connessione della WCN alla rete Internet [52].

5. Spunti di riflessione e ipotesi di risoluzione delle questioni prospettate.

Emerge dai precedenti paragrafi che l'applicabilità di norme

[50] 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 (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.

[51] Su una materia affine alla presente raggiungono le stesse conclusioni G. Giannone Codiglione, *Indirizzo IP, Reti Wi-Fi e responsabilità per illeciti commessi da terzi*, cit.; D. MacSíthigh, *Law In The Last Mile: Sharing Internet Access ThroughWifi*, 6 SCRIPTed 2, 2009, 366-369. Sulle problematiche relative alla condivisione di connessioni Wi-Fi si vedano anche R. Robertet al, *WiFi Roaming: Legal Implications and Security Constraints*, 16 *IJLIT* 3, 2008, 217-218; R.V. Hale, *Wi-Fi Liability: Potential Legal Risks in Accessing and Operating Wireless Internet*, 21 *Santa Clara Computer & High Tech. L.J.* 3, 2005, 548; B.D. Kern, *Whacking, Joyriding and War-Driving: Roaming Use of Wi-Fi and the Law*, 21 *Santa Clara Computer & High Tech. L.J.* 101, 2004.

[52] Esistono tuttavia delle possibilità tecniche per cui il traffico generato da un nodo, in questo caso il gateway, venga instradato su reti "anonimizzate". Si veda ad esempioil software Tor: https://www.torproject.org/, su cui K.D. Watson, *The Tor Network: A Global Inquiry into the Legal Status of Anonymity Networks*, in 11 *Wash. U. Global Stud. L. Rev.* 715, 2012; M. Rady, *Anonymity Networks: New Platforms for Conflict and Contention*, *MIT Political Science Department Research Paper No. 2013-5*, 2013, disponibileall'url: http://ssrn.com/abstract=2241536 or http://dx.doi.org/10.2139/ssrn.2241536.Inoltre, si consideri 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.

esistenti alle WCN risulta particolarmente ostica se non impossibile. Se, per un verso, la regolamentazione delle comunicazioni elettroniche parrebbe applicabile, per altro verso, l'effettività di tale regolamentazione rimarrebbe frustrata dalla struttura stessa delle rete comunitaria. Ciò vale per lo più anche per le norme di responsabilità civile "ordinarie". Pertanto, le risultanze di eventuali controversie future sono ad oggi difficili da prevedere.

Attualmente le WCN si stanno espandendo sia in termini di nodi e, quindi, di soggetti coinvolti, sia in termini geografici: non solo le esistenti comunità si stanno allargando, ma nuove comunità sono in fase di creazione. La loro diffusione è di particolare importanza nei paesi in via di sviluppo, soprattutto laddove esistano regimi autoritari: esse permettono infatti la comunicazione con mezzi paralleli a quelli "ordinari" in condizioni di forte anonimato, senza dimenticare che possono portare connettività in luoghi che, per le logiche di mercato, rimarrebbero altrimenti isolati. Per questi motivi, le reti comunitarie rappresentano un potente strumento per la democrazia [53].

Discende da queste considerazioni che un eventuale regime di responsabilità dovrebbe riuscire nel difficile compito di bilanciare da un lato la necessità e il diritto ad ottenere tutela per le violazioni subite, dall'altro le potenzialità e i benefici della rete, soprattutto con riferimento all'anonimato e alla libertà di espressione.

È possibile immaginare diversi regimi di responsabilità a seconda del soggetto ritenuto responsabile. Per come le reti comunitarie sono strutturate, i regimi possibili si concentrerebbero sulla rete e/o sugli utenti.

Per aversi una responsabilità della rete, occorrerebbe una sua formalizzazione. Ciò potrebbe ad esempio discendere da un'imposizione governativa concernente autorizzazioni e concessioni per la nascita e lo sviluppo della rete, diversamente da quanto ad oggi previsto. Tali imposizioni comporterebbero la formalizzazione della WCN sotto forma di associazione o altro ente giuridico, con la conseguenza che esisterebbe un soggetto o un organo responsabile dell'attività svolta nella rete.

Un approccio di questo genere, tuttavia, potrebbe avere un impatto fortemente negativo sugli scopi e i benefici delle reti comunitarie: una delle caratteristiche delle WCN è infatti la loro spontaneità e privatezza (sia in termini di riservatezza che di proprietà). Peraltro, l'imposizione di un regime di responsabilità a carico della sola rete come ente, permetterebbe agli utenti di

[53] Come già detto, di ciò si è avveduta anche l'OECD. Cfr. *supra* nota n. 1. Per la correlazione fra anonimato, Internet e democrazia, si veda il saggio di M. CUNIBERTI, *Democrazie, dissenso politico e tutela dell'anonimato*, in questa *Rivista*, n. 2/2014, 111.

schermarsi dietro ai propri computer, senza alcun effetto deterrente.

Inoltre, come già illustrato, se gli ISP sono stati scelti quali enti responsabili perché economicamente capaci, le WCN non avrebbero alcun bacino da cui attingere nel caso di condanna a risarcimento del danno. Anche se è vero che nel momento stesso in cui si prevedesse una determinata procedura per l'autorizzazione alla nascita di una WCN, ordinamento potrebbe richiedere un patrimonio adatto allo scopo, che potrebbe essere una soluzione a questa problematica [54].

Una seconda ipotesi di soluzione potrebbe concentrare la responsabilità sui singoli utenti. Se, da un punto di vista giuridico, non occorrerebbero nuove regole, in quanto altro non sarebbe che l'applicazione dell'art. 2043 c.c., da un punto di vista tecnico sarebbe necessaria l'introduzione di sistemi di riconoscimento. Anche a voler immaginare l'imposizione di un siffatto sistema di riconoscimento per il tramite di una specifica normativa, tale sistema di riconoscimento andrebbe a colpire fortemente, ancora una volta, le peculiarità della rete: ciò infatti farebbe venire meno l'anonimato di cui queste reti godono [55]. Per certi versi, ciò potrebbe apparire auspicabile o addirittura necessario, per altro verso, soprattutto nell'ottica della democraticità delle WCN, ciò inciderebbe in modo radicale sulle potenzialità delle reti comunitarie.

Infine, non si deve dimenticare che, come più sopra evidenziato, un sistemadi identificazione non sarebbe garanzia di effettività di tutela, stante gli ostacoli già incontrati nell'ambiente Internet da parte dei titolari di taluni diritti nell'*enforcement* di quest'ultimi.

Un'ulteriore possibilità sarebbe data da un regime combinato. Sarebbe possibile rendere la rete responsabile per talune fattispecie, quali la diffusione di virus o altre ipotesi che si potrebbero tecnicamente prevedere e prevenire, al contempo addossando agli utenti la responsabilità delle loro azioni, quali diffamazioni, diffusioni di dati personali e via dicendo. Questo regime combinato, tuttavia, sarebbe evidentemente molto incisivo sia sul fronte dell'anonimato degli utenti, sia sul fronte della spontaneità della rete, in quanto necessiterebbe, da un lato, dell'introduzione di sistemi di riconoscimento e dall'altro, di una formalizzazione

[54] Ad esempio: se si trattasse di associazione riconosciuta, sarebbe necessario, come noto un "patrimonio adeguato alla realizzazione dello scopo" (art. 1, co. 3, DPR 10 febbraio 2000, n. 361).

[55] 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 questa *Rivista*, 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 uu controllo da parte di un soggetto terzo e imparziale circa la sussistenza dell'illecito contestato ".

della rete combinata ad altri strumenti tecnici, quali sistemi di filtraggio dei contenuti. Peraltro, se il parallelo fra WCN e ISP reggesse, strumenti di filtraggio di tale genere sarebbero incompatibili con l'art. 15 Dir. 2000/31, come la stessa Corte di Giustizia ha evidenziato [56].

Da quanto fin qui illustrato discende che, ad oggi, lo stato delle reti comunitarie non sembra permettere, almeno a prima vista, di conciliare gli obiettivi e le peculiarità di tali reti, con la necessità di assicurare un'effettiva protezione dei diritti, sia interna che esterna alla comunità.

Occorre pertanto chiedersi se, di fronte a questo genere di tecnologia, il legislatore sia effettivamente in grado di intervenire e se, in ogni caso, tale intervento sia desiderabile. È possibile infatti che queste reti si auto-regolamentino: come accennato, non esistono all'interno della rete delle norme o dei contratti su cui le relazioni fra utenti si basano. Gli utenti si attengono a norme non scritte, a manifesti, a decaloghi, a "principi ispiratori" [57]. Chi entra nella rete ne condivide idee e regole. Se un utente non rispetta questi principi, c'è la possibilità di escluderlo tecnicamente dalla rete stessa.

Stante l'esistenza di queste attitudini comportamentali, sarebbe possibile incentivare l'adozione di codici di comportamento in ciascuna rete comunitaria, corredati da apposite sanzioni "sociali". In considerazione del fatto che gli utenti tengono particolarmente al funzionamento della rete, sarebbe possibile imporre un dovere di sorveglianza diffuso fra gli utenti, che, nel momento in cui sospettassero di comportamenti scorretti o illeciti, potrebbero riferirne ad uno specifico comitato, creato all'uopo. Tale comitato potrebbe poi agire nei confronti di tale soggetto, posto che ciascuno conosce i nodi (anche se non i soggetti) che gli sono attigui.

Da un punto di vista tecnico, nulla vieta che ciascuna comunità si doti di sistemi di filtraggio interno. In questo senso, un nodo gateway potrebbe fungere da filtro per i contenuti che gli altri nodi tentino di immettere in Internet [58].

Una soluzione di tal genere implicherebbe una organizzazione interna e un monitoraggio degli utenti che non sarebbe, però, centralizzato, bensì diffuso fra i membri della comunità. Questo non necessiterebbe peraltro di precedenti autorizzazioni o concessioni governative e, se ogni comunità si organizzasse al meglio nello scegliere i propri membri e nel monitorarli, il rischio del

[56] Cf. i cosiddetti casi "Scarlet" e "Netlog", sopra nota n. 33.

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

[58] Suggerisce questa soluzione J.S. HATCHER, *Mesh Networks: A Look at the Legal Future*, cit., 13.

verificarsi di attività illecite si ridurrebbe. Testare questa ipotesi necessiterebbe di uno studio approfondito delle nome sociali regolatrici delle WCN. Ciò permetterebbe una maggiore presa di coscienza del funzionamento di queste tecnologie e, soprattutto, delle comunità ad esse sottostanti. In questo senso, il ruolo del legislatore potrebbe essere quello di comprendere se un suo intervento potrebbe o meno innescare o incentivare un circolo virtuoso di norme sociali al fine di ridurre i casi di comportamenti illeciti [59].

Questo approccio è quello che, evidentemente, avrebbe il minor impatto sulla struttura e l'idea delle WCN. Tuttavia, anche laddove effettivamente si riducesse al minimo la probabilità di fatti illeciti, i casi che concretamente verificassero presenterebbero i problemi più sopra evidenziati in punto di efficacia di tutela del diritto leso.

6. Conclusioni.

Ancora una volta la nascita e la diffusione di una tecnologia — di comunicazione, in questo caso — mette alla prova il tessuto normativo esistente ed impone al giurista una riflessione sul caso concreto prima e, sull'ordinamento nel suo complesso, poi.

Lo scopo del presente contributo era quello di illustrare l'inquadramento legislativo del fenomeno delle WCN e di analizzare ipotetiche situazioni di responsabilità civile scaturenti dalla diffusione e dall'uso di tali reti.

Come illustrato, questo genere di tecnologia appare difficilmente governabile dalle presenti normative. L'architettura tecnologica rende arduo il tentativo di dare effettività alla tutela di qualsivoglia diritto.

Si è tentato di immaginare delle soluzioni possibili che, oltre a permettere una effettiva tutela, rispettino le peculiarità e proteggano le potenzialità delle reti comunitarie.

Per ora non vi sono casi concreti in cui testare la tenuta delle regolamentazioni odierne e della struttura delle WCN. Tuttavia, è bene che i giuristi si interroghino su questa nuova tecnologia, anche come chiave di lettura del sistema nel suo complesso. Le reti comunitarie potrebbero infatti dimostrarsi un terreno di gioco

[59] Per una spiegazione di come la legge possa influenzare le norme sociali si veda 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 dello stesso autore: R.C. Ellickson, *Order Without Law: How Neighbors Settle Disputes*, Cambridge (MA), 1991, spec. 284 ss.; E.A. Posner, *Law and Social Norms*, Cambridge (MA), 2009, nonchè R.H. McAdams, *The origin, development, and regulation of norms*, 96 *Mich. L. Rev.* 338 (1997), spec. 391 e ss.

molto scivoloso per l'applicazione delle norme come fino ad oggi l'abbiamo vissuta.

Abstract

Wireless Community Networks (WCNs) are wireless networks based on outer reach technologies managed by local communities, without a centralized structure. WCNs are territorial infrastructures which allow, also through Internet connectivity, the inclusion of people and places which would otherwise be left out of telecommunications market. Engineers and sociologists have been studying these networks for many years, while legal scholars have paid very scant – if none – attention to the phenomenon. The article attempts to fill this gap, analyzing the legal context applicable to WCNs, as well as the possible implications of the diffusion of these networks in terms of civil liability.