ICT E DIRITTO

Rubrica a cura di

Antonio Piva, David D'Agostini

Scopo di questa rubrica è di illustrare al lettore, in brevi articoli, le tematiche giuridiche più significative del settore ICT: dalla tutela del *domain name* al *copyright* nella rete, dalle licenze software alla *privacy* nell'era digitale. Ogni numero tratterà un argomento, inquadrandolo nel contesto normativo e focalizzandone gli aspetti di informatica giuridica.

La tecnologia Wi-Fi e l'accesso alle reti

David D'Agostini, Antonio Piva

1. Premessa

Con la pubblicazione sulla Gazzetta Ufficiale del cd. Decreto Milleproroghe, i media hanno dato ampio risalto alla notizia che dal 1° gennaio 2011 sono venute meno le disposizioni del decreto Pisanu relative al Wi-Fi: ne sono seguiti commenti entusiasti (soprattutto sul web) e molti hanno festeggiato il Wi-Fi finalmente libero. Ma cosa si intende con tale sigla e, soprattutto, cosa cambia oggi alla luce delle nuove disposizioni di legge? In questo articolo cercheremo di dare risposta a tale domanda non prima di aver debitamente introdotto l'argomento da un punto di vista tecnico e illustrato il quadro normativo di riferimento.

2. Aspetti tecnici

Nelle telecomunicazioni, il termine "Wi-Fi" indica l'insieme delle tecnologie dedicate alla connettività che permettono a diversi tipi di dispositivi di collegarsi tra loro attraverso una rete locale senza fili, detta anche WLAN (*Wireless Local Area Network*).
Una rete Wi-Fi è, dunque, una rete di telecomunicazioni, paragonabile a una rete a copertura cellulare di piccola scala (locale), che fa uso di dispositivi di ricetrasmissione radio chiamati *access point; per access point*, quindi, si intende qualsiasi dispositivo che permette all'utente di collegarsi a una rete *wireless*[1].
L'*access point* può essere collegato fisicamente a una rete cablata oppure via onde radio ad altri *access point*, i quali ricevono e inviano segnali radio ai dispositivi collegati, mediante antenne e apparati di ricetrasmissione, permettendo così la connessione sotto forma di radiocomunicazione.
La parte di rete che interfaccia gli *access point* ai terminali di utenza costituisce la rete di accesso, mentre la rete LAN (*Local Area Network*) cablata, cui gli *access point* sono collegati, rappresenta la rete di trasporto.
Quando un *access point* è collegato a una rete cablata, esso funge da interfaccia tra la rete di accesso *wireless* e la parte cablata di trasporto, implementando un cambio di protocollo per il trasferimento dell'informazione tra le due parti di rete. Ciascun *access point* determina una cella di copertura di circa 200 m di diametro, in quanto la potenza di trasmissione è limitata da normative specifiche di sicurezza legate al rischio elettromagnetico (100 mW). È possibile collegare più *access point* alla medesima rete cablata oppure tra di loro in modalità *wireless* per creare in tal modo una rete più grande.
Un *access point* può anche fungere da bridge (ponte) se trasmette informazioni tramite collegamento *wireless* agli altri *access point*, ciascuno dei quali è collegato ad un segmento della re-

[1] Il decreto del Ministro delle Comunicazioni del 28 maggio 2003 all'art. 1 definisce l'*access point* quale "*strumento di accesso per un numero variabile di utenti tra la rete Radio-LAN e la struttura di rete di telecomunicazioni*".

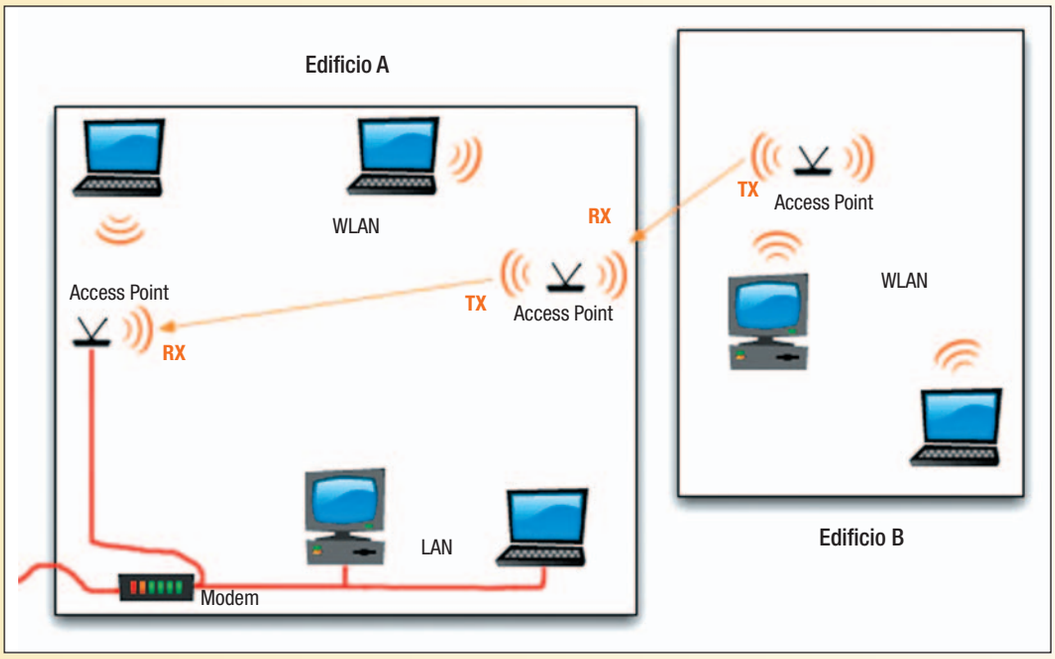

FIGURA 1

Esempio di rete costituita da una LAN cablata e una WLAN realizzata mediante alcuni access point che forniscono la connettività anche all'esterno dell'edificio principale (edificio A). Le frecce fra gli access point rappresentano un esempio di comunicazione dove "TX" indica la trasmissione e "RX" la ricezione. Si tenga presente che la comunicazione fra access point è bidirezionale

te cablata. In tal modo i diversi segmenti di rete cablata vengono interconnessi.

I singoli *access point* hanno il compito di inviare in *broadcast*[2] ai dispositivi ricetrasmittenti *wireless*, presenti nel loro raggio di copertura, il *Service Set IDentifier* (SSID) che identifica la rete o le reti che stanno servendo. L'insieme delle stazioni servite dagli *access point* è detto BSS (*Basic Service Set*). La rete globale ottenuta dalla rete WLAN realizzata tramite gli *access point* e la rete LAN cablata può essere collegata alla rete Internet tramite un *router* e usufruire di tutti i servizi di connettività offerti da un *Internet Service Provider* (ISP). Nella figura 1 è illustrato un esempio di rete in cui una parte è cablata e costituisce la rete LAN all'interno dell'edificio A e una parte è servita da alcuni *access point* che forniscono la connettività alle postazioni di lavoro, realizzando una WLAN che si estende anche all'edificio limitrofo (edificio B).

A seconda delle antenne montate sugli *access point*, si possono realizzare due diversi tipi di copertura: le antenne omnidirezionali vengono solitamente utilizzate per fornire la connettività all'interno di uffici, o comunque in zone private relativamente piccole; invece, con raggi d'azione più grandi, si possono coprire aree pubbliche o aperte al pubblico (come aeroporti, centri commerciali ecc.).

Con un *access point* omnidirezionale è possibile coprire con banda larga fino a una distanza di 100 m teorici (uso domestico) se non vi è alcuna barriera in linea d'aria; per contro le antenne direttive hanno una portata di chilometri anche in presenza di barriere in linea d'aria, e sono proprio questi collegamenti a consentire il raggiungimento della banda larga nei territori scoperti dalla rete cablata.

A parte l'utilizzo domestico delle reti *wireless*, gli accessi Wi-Fi (chiamati anche *hot spot*) sono ormai disponibili anche in aeroporti, stazioni ferroviarie, internet caffè, esercizi commerciali ecc. e anche gli enti pubblici, soprattutto i Comuni, molto spesso installano reti *wireless* in aree pubbliche a disposizione della cittadinanza. La fonte di connettività a banda larga cui l'*hot spot* si ap-

[2] Il termine broadcast indica la radiodiffusione circolare in cui un sistema trasmittente invia delle informazioni ad un insieme di sistemi riceventi non definito a priori.

poggia può essere un collegamento via cavo (ADSL o HDSL) oppure via satellite.
Con riferimento agli standard di comunicazione, quello internazionale per le reti *wireless* è l'IEEE 802.11, che specifica sia l'interfaccia tra il dispositivo *client* e l'*access point* sia tra dispositivi *client wireless*. La famiglia 802.11 comprende tre protocolli dedicati alla trasmissione delle informazioni (a, b, g), il protocollo 802.11i dedicato alla sicurezza, e altri standard (c, d, e, f, h, ecc.) che riguardano estensioni dei servizi base e miglioramenti di servizi già disponibili. Di questi, i più diffusi sono i protocolli b, g ed n. L'802.11b e 802.11g utilizzano lo spettro di frequenze nell'intorno dei 2,4 GHz e hanno capacità di trasmissione di 11 Mbit/s e 24,7 Mbit/s rispettivamente. L'802.11 n è il più recente dei tre, con una capacità di trasmissione di 100 Mbit/s e la possibilità di trasmettere sia a 2,4 GHz che a 5,4 GHz.
Esiste anche un'altra famiglia di standard, la IEEE 802.16 su cui si basa la tecnologia WiMAX, che consente l'accesso a reti di telecomunicazioni a banda larga e senza fili. WiMAX rispetto a Wi-Fi risulta superiore sotto due aspetti: la velocità di trasmissione e l'ampiezza della copertura delle celle. Infatti, a differenza del Wi-Fi pensato per reti casalinghe o comunque interne, il WiMAX nasce per reti esterne, con distanze raggiungibili anche di svariati chilometri. Non vi è però conflitto fra le due tecnologie: siccome le reti IEEE 802.16 utilizzano lo stesso protocollo interno (LLC), standardizzato come IEEE 802.2, queste possono essere collegate a WLAN IEEE 802.11 e servire per incanalamenti comuni.
Dato che l'IEEE fornisce solo un insieme di specifiche, ma non prevede alcun test o certificazione che garantisca che un prodotto rispetti tali specifiche, è nata, nel 1999, l'associazione *Wi-Fi Alliance*, costituita da un gruppo di industrie produttrici di componenti per schede Wi-Fi, al fine di certificare l'interoperabilità dei prodotti e per diffondere le reti Wi-Fi. Attualmente l'Alliance si occupa solo degli standard a, b e g, oltre che degli standard di sicurezza come il WEP, il WPA e il nuovo 802.11i, conosciuto anche come WPA2.
Le versioni originali dei protocolli 802.11 utilizzavano la crittografia WEP (*Wired Equivalent Protocol*) che si basa sull'algoritmo di cifratura RC4. L'implementazione adottata per lo standard 802.11 era però molto debole e facilmente forzabile. In risposta alle numerose falle scoperte nel sistema WEP, nel 2003 la Wi-Fi Alliance annunciò la nascita del nuovo protocollo WPA (*Wi-Fi Protected Access*) come un'evoluzione del WEP che ne rimuove alcuni problemi di sicurezza rendendo le reti *wireless* discretamente sicure. Nel 2004 vennero rilasciate, infine, le specifiche dell'IEEE 802.11i che rende le reti wireless molto sicure e che fu immediatamente adottato dalla Wi-Fi Alliance sotto il nome di WPA2, che utilizza come algoritmo di codifica l'AES (*Advanced Encryption Standard*). Grazie alla diffusione dei collegamenti ADSL via cavo si è registrata una notevole proliferazione di piccole reti *wireless* private, realizzate dagli utenti per condividere il collegamento a Internet. In queste situazioni capita spesso che non si utilizzi alcuna crittografia, o al massimo si usi il WEP. Questo rende le reti insicure e vulnerabili dal punto di vista della sicurezza, in quanto possono essere forzate con semplicità, permettendo a chi accede abusivamente alla rete di usufruire indebitamente della connessione e di intercettare il traffico *wireless*[3].

3. Quadro normativo

Dopo aver tratteggiato i profili tecnici delle comunicazioni elettroniche senza fili, passiamo ora a illustrare le principali norme di diritto.
Fino al 2001 il riferimento legislativo per l'utilizzo di apparecchiature operanti nelle bande di frequenza [2,4 - 2,4835] GHz (comunemente detta banda a 2.4 GHz), [5,15 - 5,350] GHz e [5,47 - 5,725] GHz (comunemente dette bande a 5 GHz), utilizzate per la trasmissione *wireless* LAN, era dato dal Decreto del Presidente della Repubblica n. 447 del 5 Ottobre 2001.
Il decreto stabiliva che tali frequenze potessero essere impiegate solo nell'ambito di LAN a uso privato, mentre per connettere una WLAN alla rete pubblica occorreva un'autorizzazione generale del Ministero nonché il pagamento di un canone.
A partire dal gennaio 2002, il regolamento di attuazione dello stesso DPR 447/01 consente l'utilizzo di dispositivi di WLAN che operano sulle bande di frequenza appositamente assegnate, senza più la necessità di richiedere alcuna concessione.
Il quadro regolamentare definitivo per l'utilizzo della tecnologia Wi-Fi in ambito pubblico viene

[3] Si veda anche "*L'accesso abusivo ai sistemi informatici e telematici: Aspetti giuridici e informatici di un attacco hacker*" nella rivista Mondo Digitale n. 2 giugno 2004.

dato dal cosiddetto *decreto Gasparri* del 28 maggio 2003, che regola le condizioni per il rilascio delle autorizzazioni generali per la fornitura al pubblico dell'accesso Radio-LAN alle reti e ai servizi di telecomunicazioni: la delibera dell'Autorità per le Garanzie nelle Comunicazioni 102/03/CONS precisa che non è necessario disporre di licenza o autorizzazione per l'erogazione di servizi di connettività di rete nel caso l'attività commerciale non abbia come oggetto principale l'attività di telecomunicazioni (si pensi al caso di bar, alberghi, centri commerciali ecc.).
L'intera materia delle telecomunicazioni (compresi argomenti quali gli standard di comunicazione sopra citati, le frequenze e così via) trova, in seguito, compiuta disciplina nel d.lgs. 1 agosto 2003 n. 259, meglio noto come "*Codice delle comunicazioni elettroniche*".

Riquadro 1

Direttive europee sulle comunicazioni elettroniche

2002/19/CE direttiva relativa all'accesso alle reti di comunicazione elettronica e alle risorse correlate e all'interconnessione delle medesime (direttiva accesso);

2002/20/CE direttiva relativa alle autorizzazioni per le reti e i servizi di comunicazione elettronica (direttiva autorizzazioni);

2002/21/CE direttiva che istituisce un quadro normativo comune per le reti e i servizi di comunicazione elettronica (direttiva quadro);

2002/22/CE direttiva relativa al servizio universale e ai diritti degli utenti in materia di reti e di servizi di comunicazione elettronica (direttiva servizio universale);

2002/77/CE direttiva relativa alla concorrenza nei mercati delle reti e dei servizi di comunicazione elettronica.

Riquadro 2

Il Registro degli Operatori di Comunicazione (ROC)

Elenco istituito dalla Legge 31 luglio 1997 n. 249 al quale debbono obbligatoriamente iscriversi:

1. i soggetti destinatari di concessioni o autorizzazione in materia di comunicazione;

2. le imprese concessionarie di pubblicità da trasmettere mediante impianti radiofonici o televisivi o da diffondere su giornali quotidiani o periodici;

3. le imprese di produzione e distribuzione dei programmi radiofonici e televisivi;

4. le imprese editrici di giornali quotidiani, di periodici o riviste e le agenzie di stampa di carattere nazionale;

5. le imprese fornitrici di servizi telematici e di telecomunicazioni ivi compresa l'editoria elettronica e digitale.

La tenuta e la regolamentazione del ROC sono affidate all'Autorità per le Garanzie nelle Comunicazioni (AGCOM).

Tale testo ha unificato e regolamentato l'intera normativa delle comunicazioni elettroniche, prendendo le mosse da alcune fondamentali direttive dell'Unione Europea del 2002 (riquadro 1).
Nel Codice si trovano le disposizioni inerenti le autorizzazioni per i servizi di comunicazione elettronica, i diritti di uso delle frequenze radio, nonché gli adempimenti amministrativi che il fornitore di connettività in modalità *wireless* deve affrontare per esercitare l'attività.
In particolare, secondo il combinato disposto dell'art. 25 del Codice e del menzionato DM 28 maggio 2003, la fornitura del servizio Wi-Fi in locali aperti al pubblico o in aree confinate a frequentazione pubblica quali aeroporti, stazioni ferroviarie e marittime e centri commerciali risulta subordinata a un'autorizzazione generale.
Il soggetto interessato deve presentare al Ministero delle Comunicazioni[4] una dichiarazione contenente l'intenzione di iniziare la fornitura di reti o servizi di comunicazione elettronica; tale dichiarazione costituisce denuncia di inizio attività (cosiddetta D.I.A.). L'abilitazione a iniziare l'attività decorre dall'avvenuta presentazione della dichiarazione e nel rispetto delle disposizioni sui diritti di uso delle frequenze radio. Il Ministero, entro 60 giorni dalla presentazione della dichiarazione, è tenuto a verificare la sussistenza dei presupposti richiesti e può disporre il divieto di prosecuzione dell'attività, con provvedimento motivato da notificare agli interessati entro il medesimo termine.
I titolari di tale autorizzazione (rilasciata per un periodo massimo di venti anni, rinnovabile) per poter esercitare la suddetta attività sono tenuti all'iscrizione nel registro degli operatori di comunicazione, noto con l'acronimo ROC (riquadro 2).
Per quanto concerne gli impianti Wi-Fi, il Codice detta in maniera puntuale anche i procedimenti relativi alle infrastrutture, prevedendo che "*l'installazione di torri, di tralicci, di impianti radiotrasmittenti, di ripetitori di servizi di telecomunicazione, di stazioni radio base per reti radio a larga banda punto-multipunto*" sia realizzabile, ordinariamente, con l'autorizzazione dell'Ente locale competente, vale a dire del Comune. Invece nel caso di installazione di impianti con potenza

[4] Il Ministero delle Comunicazioni tiene un elenco aggiornato dei fornitori di reti e di servizi di comunicazione elettronica, consultabile anche sul proprio sito Internet http://www.comunicazioni.it

in singola antenna uguale o inferiore ai 20 W, risulta sufficiente presentare la menzionata denuncia di inizio attività, con conseguente applicazione del principio del silenzio-assenso dopo 90 giorni: in pratica, decorso il termine di 90 giorni dalla denuncia di inizio attività senza alcun riscontro negativo da parte della Pubblica Amministrazione, sarà possibile procedere all'installazione di dispositivi Wi-Fi a uso pubblico di potenza uguale o inferiore ai 20 W.
Per ulteriori aspetti e per i limiti di esposizione ai campi elettromagnetici, il Codice rinvia espressamente alle vigenti norme in materia di elettrosmog[5].
Gli operatori di reti Wi-Fi sono, infine, tenuti a inviare la descrizione di ciascun impianto installato ai Comuni e ai competenti ispettorati territoriali del Ministero delle Comunicazioni.
Per completezza si deve menzionare anche un altro decreto del Ministero delle Comunicazioni (il cosiddetto Decreto Landolfi) che il 4 ottobre 2005, modificando il precedente decreto Gasparri del 28 maggio 2003, ha liberalizzato l'erogazione di servizi Wi-Fi. In particolare:

- l'art. 1 liberalizza il servizio su tutto il territorio nazionale;
- l'art. 2 obbliga i soggetti autorizzati a consentire l'accesso indipendentemente dalla tecnologia utilizzata, favorendo gli accordi di r*oaming* tra operatori diversi; inoltre questa norma introduce il cosiddetto "*Diritto d'antenna*" (l'installazione di apparati e antenne deve essere garantita a condizioni "*eque, trasparenti e non discriminatorie*" e non ci possono essere quindi installazioni di apparati in esclusiva per alcuni operatori);
- l'art. 4 mantiene il regime di autorizzazione generale per i soggetti che vogliono fornire servizi Wi-Fi.

4. Il decreto Pisanu

Se le norme sopra elencate, *in primis* il Codice delle comunicazioni elettroniche, rivestono un'importanza fondamentale per gli operatori del settore Wi-Fi, contenendo l'insieme delle disposizioni alle quali i medesimi si devono attenere nell'esercizio della propria attività, per tutti gli utenti finali ben più rilevante è stato l'impatto con il cosiddetto Decreto Pisanu.
Per spiegare tale normativa è necessario ricordarne i presupposti. Come noto, nel luglio 2005 lo scenario internazionale registrò una recrudescenza del terrorismo di matrice islamica: il 7 luglio a Londra vennero compiuti quattro attentati che causarono 52 morti e circa 700 feriti; il 23 luglio a Sharm el-Sheikh esplosero tre bombe uccidendo una sessantina di persone e ferendone oltre 150.
In tale clima di rinnovata tensione il Governo italiano il 27 luglio 2005 approvò un decreto legge (il n.144, denominato Pisanu dal nome del Ministro dell'interno proponente il testo) contenente "*misure urgenti per il contrasto del terrorismo internazionale*"[6]. Tra le diverse misure introdotte, figurava anche un'integrazione della disciplina amministrativa degli esercizi pubblici di telefonia e internet (art. 7) in cui venivano previsti una serie di obblighi e restrizioni.
In buona sostanza, secondo quanto previsto dalla predetta norma e dal Decreto del Ministero dell'Interno del 16 agosto 2005, l'esercizio pubblico di qualsiasi tipo (bar, ristorante, albergo, rivendita tabacchi ecc.) che offriva al pubblico un servizio di accesso a Internet, anche tramite Wi-Fi, veniva assoggettato ai seguenti obblighi:
a. inviare al Ministero delle Telecomunicazioni la comunicazione prevista dall'art. 25 del Codice delle Telecomunicazioni (quella sopra citata per i fornitori del servizio);
b. richiedere la licenza al questore;
c. identificare il cliente prima di consentirgli l'accesso alla rete; il gestore, inoltre, era tenuto ad adottare le misure fisiche o tecnologiche necessarie per impedire l'accesso (anche tramite Wi-Fi) agli apparecchi terminali da parte di persone che non erano state preventivamente identificate;
d. monitorare le attività svolte dal cliente memorizzando e mantenendo i dati relativi al giorno e all'ora della comunicazione e alla tipologia del servizio utilizzato, abbinabili univocamente al terminale utilizzato (esclusi, comunque, i contenuti delle comunicazioni).
Il gestore doveva, quindi, adottare misure necessarie affinché i dati registrati fossero mantenuti con modalità tali da garantirne l'inalterabilità e la

[5] Sull'argomento si può consultare la legge 22 febbraio 2001 n. 36 - Legge quadro sulla protezione dalle esposizioni a campi elettrici, magnetici ed elettromagnetici.

[6] Il decreto legge 27 luglio 2005 n.144 venne convertito dal Parlamento in appena quattro giorni con la legge 31 luglio 2005 n.155.

non accessibilità da parte di persone non autorizzate; la raccolta e il trattamento di tali dati con modalità informatiche rendeva necessaria la redazione del documento programmatico sulla sicurezza, previsto dal d.lgs 196/2003. Sia i dati raccolti relativi all'identificazione dell'utente che al monitoraggio, dovevano essere resi disponibili agli organi di polizia o alla magistratura, se richiesti.
Il Decreto Pisanu, quindi, invalida la delibera dell'Autorità per le Garanzie nelle Comunicazioni 102/03/CONS, prevedendo (per ragioni di sicurezza legate al terrorismo) la previa autorizzazione al questore per chiunque metta a disposizione terminali telematici ai propri clienti.
Tali disposizioni sarebbero dovute restare in vigore, secondo quanto previsto inizialmente dal decreto Pisanu, fino al 31 dicembre 2007, ma la loro efficacia è stata prorogata anno dopo anno[7] fino al 31 dicembre 2010.
L'ultimo dei cosiddetti Decreti Milleproroghe (il D.L. 29 dicembre 2010 n.225) dispone che l'obbligo della licenza del questore non sia più a carico di chiunque, ma solo per i soggetti che mettono a disposizione del pubblico apparecchi terminali utilizzabili per le comunicazioni (si ribadisce: anche in modalità Wi-Fi) quale attività principale (vale a dire i soli gestori di *internet point* continuano a necessitare di una speciale licenza): ciò esclude da tale obbligo i gestori di alberghi, ristoranti, caffè e locali pubblici.

[7] Le proroghe sono state stabilite con i seguenti decreti legge: D.L. 28 dicembre 2007 n.248, D.L. 30 dicembre 2008 n.207, D.L. 30 dicembre 2009 n.194.

Inoltre, per costoro viene eliminato il monitoraggio delle operazioni degli utenti, la loro identificazione e l'archiviazione dei relativi dati di navigazione.
Decade pertanto un gravoso onere che aveva finora impedito lo sviluppo del Wi-Fi pubblico in Italia, limitando fortemente anche importanti opportunità commerciali e, comunque, comprimendo la libertà dei cittadini.

5. Conclusione

Si tratta, come detto in premessa, di Wi-Fi finalmente libero anche in Italia? In realtà pare che il Governo intenda applicare un sistema per identificare i dispositivi attraverso i quali le persone si connetteranno attraverso gli *hotspot* pubblici.
La soluzione più probabile potrebbe essere l'identificazione via sms, come già avviene per alcuni *hotspot*: l'utente si collega alla rete, inserisce il proprio numero di cellulare sul quale viene inviato un SMS contenente la password necessaria a proseguire la navigazione.
Si tratta di un metodo sicuramente più semplice rispetto alla raccolta dei documenti cartacei ed eliminerà molta della burocrazia necessaria per l'apertura di *hotspot* pubblici. Tale soluzione appare però ancora molto distante dalle realtà presenti nella maggior parte dei paesi occidentali, dove il Wi-Fi è realmente libero per tutti. Non resta che attendere e vedere come verrà affrontato il problema, auspicando che la soluzione non sia peggiore del vecchio decreto Pisanu.

David D'Agostini avvocato, master in informatica giuridica e diritto delle nuove tecnologie, collabora all'attività di ricerca scientifica dell'Università degli studi di Udine e ha fondato l'associazione "*Centro Innovazione & Diritto*". È componente della Commissione Informatica dei Consigli dell'Ordine del Triveneto, responsabile dell'area "*Diritto & informatica*" della rivista "*Il foro friulano*", membro dell'organo di Audit Interno di Autovie Venete SpA.
E-mail: studio@avvocatodagostini.it

Antonio Piva, laureato in Scienze dell'Informazione, *Vice Presidente dell'ALSI* (Associazione Nazionale Laureati in Scienze dell'Informazione ed Informatica) e Presidente della commissione di informatica giuridica. Docente a contratto di *diritto dell'ICT e qualità* all'Università di Udine. Consulente sistemi informatici e Governo Elettronico nella PA locale, valutatore di sistemi di qualità ISO9000 ed ispettore AICA.
E-mail: antonio@piva.mobi