**Paolo Giardini**
Consulente per la sicurezza delle Informazioni
Eucip Certified Informatics Professional
AIP – OPSI – AIPSI – CLUSIT - ISSA - FORMEZ - ILS

# Wireless e Privacy

**Assisi - 20 maggio 2008**

# OPSI - AIP

- OPSI - Osservatorio Privacy e Sicurezza Informatica nasce in seno all'Associazione Informatici Professionisti.
- Ha come scopo lo studio delle problematiche relative alla Sicurezza informatica ed ai rischi legati alla tutela dei dati personali e confidenziali.
- Promuove la cultura della Sicurezza Informatica.
- Si propone come centro di concertazione e di confronto tra le varie associazioni, gruppi e aziende pubbliche e private che si occupano di sicurezza.
- Rappresenta AIP presso il Garante Privacy al tavolo per la redazione del Codice Deontologico per i servizi di telecomunicazione.

# Argomenti

- Installazioni wireless:  la normativa,il Codice delle Comunicazioni, le linee guida del CNIPA
- Accesso ad Internet: fra Decreto Antiterrorismo e Codice della Privacy, passando per il Codice delle Comunicazioni ed i decreti Gasparri e Landolfi
- Controllo delle emissioni elettromagnetiche
- Videosorveglianza e privacy: un problema in più se è wireless
- Il Garante Privacy: controlli in corso

# La normativa sul Wireless

# La normativa di riferimento

La normativa che regola il settore delle trasmissioni radio ed in particolare le Wlan è molto variegata ed ha subito molte modifiche nel corso degli anni. Qui vengono elencate solo le principale norme.

- DPR 318/97 regolamento attuazione direttive comunitarie settore telecom
- D.M. 8/7/2002 Piano nazionale delle ripartizioni delle frequenze e successive modifiche del 20/2/2003
- DPR 447/01 Regolamento servizi telecomunicazioni privati
- D.Lgs 198/2002
- D.M. 28/5/2003 regolamentazione servizi wi-fi uso pubblico
- Delibera AGCOM 102/03/CONS
- D.Lgs 259/2003 Codice delle comunicazioni elettroniche
- D.L. 144 27/7/2005 – L. 31/7/2005 n.155  Decreto Pisanu
- D.M. 4/10/2005 Decreto Landolfi

# Le frequenze radio

Le frequenze utilizzabili per i vari servizi sono stabilite dal PNRF (piano nazionale di ripartizione delle frequenze) emanato con il DM 8.7.2002.

Le frequenze che ci interessano, ovvero quelle "unlicensed" sono definite ISM (Industrial – Scientific – Medical) e sono 2400-2500 Mhz, 5725-5875 MHz  e 24-24,250 Ghz

In queste bande lavorano, ad esempio,  telecomandi, forni a microonde, Bluetooth, Wlan

# Normativa dal 2001 al 2005

Fino al 2001 il **DPR 447/2002** stabiliva la necessità di acquisire una autorizzazione ed il pagamento di un canone per la connessione di una Wlan alla rete pubblica, mentre era permesso l'uso esclusivamente privato.

Il *Decreto Gasparri* del 2003 regola le condizioni per il rilascio delle autorizzazioni generali per la fornitura al pubblico dell'accesso delle Wlan alle reti ed ai servizi di telecomunicazioni eliminando la necessità di concessione ministeriale e delegando gli enti locali.

La **delibera 102/03/cons** dell'Autorità Garante per le comunicazioni specifica che non necessita di autorizzazione chi non faccia della connettività l'attività principale

Il 1/8/2003 viene emanato il **codice delle comunicazioni elettroniche** che unifica e regolamenta la disciplina, pur lasciando dei dubbi sulla normativa per le Wlan

# Normativa dal 2005

Nel 2005, il decreto Pisanu per il contrasto al terrorismo impone obbligo di autorizzazione da parte della Questura e registrazione degli utenti e dei dati di navigazione per chi offra il servizio al pubblico.

Si deve attendere l'ottobre del 2005 con il decreto Landolfi per la definitiva "liberalizzazione" dei servizi wireless dando possibilità di installare Wlan in aeroporti, stazioni, ecc.

Tale decreto, in vigore tutt'ora, ripristina il regime delle autorizzazioni generali per i soggetti che vogliano fornire servizi Wlan, comprese URP e biblioteche. Tale autorizzazione è da richiedere alla Direzione generale per i servizi di comunicazione elettronica e radiodiffusione del Ministero delle Comunicazioni.

Sono state da pochi giorni pubblicate (6/5/2008) dal CNIPA le Linee Guida per l'introduzione delle tecnologie Wireless nella Pubblica Amministrazione.

# Riassumendo

- Nessun obbligo se gli apparati Wlan vengono utilizzati per uso privato, anche fra edifici distinti purché non si attraversi suolo pubblico e che l'accesso non sia pubblico, rispettando i limiti di potenza imposti.
- Per uso al pubblico,  è necessaria una autorizzazione generale e se si tratta di servizi di navigazione internet devono essere identificati gli utilizzatori.
- Per la installazione di apparati ripetitori, tralicci, ponti radio (GSM,. UMTS, ecc. deve essere richiesta autorizzazione all'Ente Locale competente. Se la potenza in antenna non supera i 20 W è sufficiente la denuncia di inizio attività. Vale il principio di silenzio - assenso.
- L'ente locale deve verificare tramite le ARPA che vengano rispettati i limiti di emissioni elettromagnetiche come stabilito dalla legge 22/2/2001 n. 36.

# Videosorveglianza e Wlan

# Videosorveglianza urbana

- L’adozione di sistemi di videosorveglianza è oggi in crescita costante. Questi sistemi trattano dati personali: la voce e l’immagine, infatti, sono da considerarsi, in base alla Direttiva 95/46/CE ed alla normativa italiana, informazioni riferite ad una persona identificata o identificabile.
- Date le dimensioni assunte dal fenomeno, specie negli ultimi anni, e le problematiche che l’utilizzo di nuove tecnologie solleva, il Garante è intervenuto per individuare un punto di equilibrio tra esigenze di sicurezza, prevenzione e repressione dei reati, e diritto alla riservatezza e libertà delle persone.

# Il garante e la Videosorveglianza

- Nel luglio del 2000 è stata portata a termine la prima indagine sulla presenza di telecamere visibili in Italia.
- Nel novembre 2000 il Garante ha adottato un provvedimento contenente un "decalogo" con le regole per garantire il rispetto delle norme sulla privacy e sulla tutela della libertà delle persone, in particolare assicurando la proporzionalità tra mezzi impiegati e fini perseguiti.
- Il 29 aprile 2004 è stato pubblicate un provvedimento generale che individua specifici obblighi per i vari ambiti nei quali viene operata videosorveglianza.

# La tutela della Privacy

In estrema sintesi, la videosorveglianza è permessa se:

- Vengono definite le finalità, esplicite e legittime, rispetto alle competenze assegnate per legge
- Vengono rispettati i principi di pertinenza e non eccedenza
- Viene limitato il tempo di conservazione allo stretto necessario
- Vengono nominati per iscritto gli incaricati ed i responsabili
- Viene fornita anche sinteticamente una adeguata informativa

# Provvedimento 29/4/2004

Vengono introdotti ulteriori specifici obblighi

- Verifica preliminare da parte del titolare
- Documentazione delle scelte
- Eventuale richiesta di autorizzazione e notifica al Garante

Sono inoltre indicate le regole per i soggetti pubblici che intendano effettuare videosorveglianza.

E' comunque il caso di ricordare che il soggetto pubblico non deve richiedere il consenso dell'interessato.

# Videosorveglianza e P.A.

Una PA può effettuare videosorveglianza solo per svolgere funzioni istituzionali.

Ad esempio non è lecito perseguire finalità di prevenzione ed accertamento di reati che competono all'autorità giudiziaria ed alle forze di polizia.

Risulta parimenti priva di giustificazione l'installazione di impianti di videosorveglianza al solo fine (come risulta da casi sottoposti al Garante), di controllare il rispetto del divieto di fumare o gettare mozziconi, di calpestare aiuole, di affiggere o di fotografare, o di altri divieti relativi alle modalità nel depositare i sacchetti di immondizia entro gli appositi contenitori.

# Videosorveglianza e P.A.

Quando il soggetto pubblico è realmente titolare di un compito attribuito dalla legge in materia di sicurezza pubblica o di accertamento, prevenzione e repressione di reati, per procedere ad una videosorveglianza di soggetti identificabili deve ricorrere un'esigenza effettiva e proporzionata di prevenzione o repressione di pericoli concreti e specifici di lesione di un bene (ad esempio, in luoghi esposti a reale rischio o in caso di manifestazioni che siano ragionevolmente fonte di eventi pregiudizievoli).

# Un codice deontologico

- Il Garante ha avviato nel 2002 le procedure per l'adozione di un codice deontologico e di buona condotta del settore che fissi regole precise e garanzie riguardo alla raccolta, all'uso e alla conservazione delle immagini.
- Attualmente (seminario del 16/5/2008 con il Presidente dell'Autorità Garante Prof. Pizzetti) non è dato conoscere quando termineranno i lavori.

# Telecamere wireless

- La connessione via cavo è dispendiosa ed a volte  difficile da implementare per difficoltà intrinseche.
- Per questo motivo vengono sempre più usate le telecamere wireless,  via radio o su  Wlan.

# Problematiche di sicurezza

Dati gli obblighi di sicurezza legati al trattamento di dati personali, sarà necessario prendere in considerazione le problematiche legate all'utilizzo di sistemi di videosorveglianza dotati di telecamere che trasmettono via radio.

- La principale problematica è legata al segnale radio che può essere ricevuto da chiunque si trovi nella zona di irradiamento dell'antenna. Basta un ricevitore adeguato e l'immagine ripresa sarà disponibile.

# Problematiche di sicurezza

Altri problemi derivano dalla facilità con la quale le trasmissioni radio sono disturbate da interferenze, casuali o volute. Basta un apparato chiamato "Jammer" dal costo di poche centinaia di euro per impedire qualunque ripresa.

# Problematiche di sicurezza

Utilizzando la tecnologia Wlan wireless 802.11 b/g la situazione non cambia di molto. E' assolutamente banale individuare la telecamera e connettersi alla rete con un notebook per intercettare le immagini o bloccare le riprese. L'utilizzo di crittografia WEP è praticamente ininfluente ed anche le wlan con crittografia WPA possono essere craccate.

# L'attività 2008 del Garante

L’attività ispettiva del Garante sulla privacy per il 2008 prevede controlli sulle telecamere di videosorveglianza.

In particolare saranno effettuati controlli su tutto il territorio nazionale sia per verificare il rispetto delle regole dettate dal Garante nel 2000 e nel 2004 (vedi il decalogo sulla corretta videosorveglianza ed il provvedimento generale del 2004) sia per acquisire informazioni generali sull’attuale diffusione sul territorio di sistemi di videosorveglianza da parte di soggetti pubblici e privati.

# Altre cose di cui parlare...

- Sicurezza degli apparati Bluetooth
- Sicurezza delle Wlan 802.11x
- Sicurezza dei telefoni cellulari
- Sicurezza dei telefoni cordless
- Protocolli Wi-max ed Hiperlan
- Sicurezza VoIP

# Maggiori informazioni

http://www.garanteprivacy.it/garante/doc.jsp?ID=1002987
http://www.garanteprivacy.it/garante/doc.jsp?ID=1003482
http://www.garanteprivacy.it/garante/doc.jsp?ID=31019
http://www.urpcomunicazioni.it/ambiente.htm
http://www.urpcomunicazioni.it/servizi_telecomunicazioni.htm
http://www.garanteprivacy.it/garante/doc.jsp?ID=47020
http://www.elettrosmog.it/Leggi.htm
http://www.garanteprivacy.it/garante/doc.jsp?ID=40041
http://www.ambiente.it/impresa/legislazione/leggi/2001/legge36-2001.htm
http://www.elettrosmog.it/leggi/DL257.htm
http://www.urpcomunicazioni.it/nuovo_pnrf.htm
http://www.camera.it/parlam/leggi/01036l.htm

# Grazie per l'attenzione

*paolo.giardini@aipnet.it*

*http://www.aipnet.it - http://opsi.aipnet.it - http://www.solution.it*