

Wireless: problemi tecnici e giuridici

Michele Iaselli, Avvocato, Funz. Ministero della Difesa

Il termine wireless (dall'inglese senza fili) indica i sistemi di comunicazione fra dispositivi elettronici che non fanno uso di cavi, al contrario dei sistemi tradizionali basati su connessioni cablate. Per *wireless local area network* (Wlan), si intende una "rete locale senza fili", cioè tutte le reti locali di computer che non utilizzano dei collegamenti via cavo per connettere fra loro gli *hosts* della rete.

Le onde radio vengono utilizzate dalle reti tipo Wi-Fi, reti che devono coprire ambienti eterogenei dove le diverse postazioni da collegare non sono necessariamente visibili. Wi-Fi, abbreviazione di *Wireless Fidelity*, è il nome commerciale delle reti locali senza fili (Wlan) basate sulle specifiche Ieee 802.11, infrastrutture relativamente economiche e di veloce attivazione, che permettono di realizzare sistemi flessibili per la trasmissione di dati usando frequenze radio, estendendo o collegando reti esistenti ovvero creandone di nuove.

Nel 2001 venne ratificato il protocollo 802.11a, approvato nel 1999. Questo standard utilizza lo spazio di frequenze nell'intorno dei 5 Ghz e opera con una velocità massima di 54 Mbit/s sebbene nella realtà la velocità reale disponibile all'utente sia di circa 20 Mbit/s. La velocità massima può essere ridotta a 48, 36, 34, 18, 9 o 6 se le interferenze elettromagnetiche lo impongono.

Quasi ogni Stato ha emanato una direttiva diversa per regolare le frequenze ma, dopo la conferenza mondiale per la radiocomunicazione del 2003, l'autorità federale americana ha deciso di rendere libere le frequenze utilizzate dallo standard 802.11a. Quest'ultimo, però, non ha riscosso i favori del pubblico, così come è accaduto, invece, per lo standard l'802.11b, che si era già molto diffuso (e in molti paesi l'uso delle frequenze a 5 Ghz è tuttora riservato).

Prima della ratifica ufficiale dello standard, avvenuta nell'estate del 2003, vi erano dei produttori indipendenti che fornivano delle apparecchiature basate sulle specifiche non definitive dello standard. Nel giugno del 2003 venne ratificato lo standard 802.11g, che utilizza le stesse frequenze di quello 802.11b e fornisce una banda teorica di 54 Mbit/s. Nel gennaio 2004 lo Ieee avviò lo studio di un nuovo standard per realizzare reti wireless di dimensioni metropolitane. La velocità reale di questo standard dovrebbe essere di 100 Mbit/s (quella fisica dovrebbe essere prossima a 250 Mbit/s), quindi, dovrebbe essere cinque volte più rapido del protocollo 802.11g e ben quaranta volte più rapido dell'802.11b.

Ma nonostante la varietà di standard il vero problema delle reti wireless, estremamente convenienti per i bassissimi costi della tecnologia, rimane la sicurezza.

Le versioni originali dei protocolli 802.11 erano basati sulla crittografia Wep (*Wired Equivalent Privacy*). Nel 2001 un gruppo di ricercatori dell'università di Berkeley presentò un lavoro che evidenziò le falle di sicurezza del protocollo 802.11. Sia lo Ieee sia la Wi-Fi Alliance si misero al lavoro per progettare un'evoluzione dello standard di sicurezza Wep. Quest'ultima annunciò nel 2003 la realizzazione del Wpa (*Wi-Fi Protected Access*), che rimuoveva la maggior parte dei problemi di sicurezza rendendo le reti wireless discretamente sicure. Nel 2004 vennero rilasciate dallo Ieee le specifiche dello standard 802.11i, che rendeva le reti wireless molto sicure e la Wi-Fi Alliance lo adottò subito con il nome di Wpa2.

In effetti il sistema di protezione Wep, acronimo di *Wired Equivalent Privacy* non è infallibile. Esso utilizza l'algoritmo RC4 in modalità sincrona. Si basa su un sistema a crittazione con due chiavi, una pubblica (chiamata Initialization Vector, di 24 bit) e una privata, inizialmente codificata con una lunghezza di 40 bit, successivamente aumentati a 128 bit quando la legge americana sull'esportazione di tecniche crittografiche lo ha permesso. La lunghezza di soli 24 bit dell'Initialization Vector permette la creazione di un numero relativamente limitato di codici di crittazione, che fra l'altro non devono nemmeno cambiare ad ogni trasmissione, secondo lo standard: monitorando quindi per un certo tempo una rete wireless è possibile creare una tabella contenente tutte le possibili chiavi di decrittazione, utilizzandole quindi per intercettare i dati e inserirsi nella rete.

Con il diffondersi dei collegamenti via cavo o via ADSL si è avuto un notevole incremento degli utenti che realizzano piccole reti locali per condividere il collegamento a Internet; molte di queste sono wireless. D'altronde le reti wireless rappresentano ormai una importante forma di connessione: il mercato per i dispositivi wireless è stimato in forte crescita, come il relativo giro d'affari, che è passato da 300 milioni di dollari nel 1998 a oltre 2 miliardi nel 2006.

Data la scarsa competenza (in media) dei realizzatori di queste reti "casalinghe" capita spesso che le Wlan non usino alcuna crittografia, al massimo Wep. Queste reti naturalmente sono insicure e possono essere forzate con semplicità, permettendo l'intercettazione del traffico wireless e l'accesso abusivo alla rete, che, fra l'altro, non permette di rintracciare *a posteriori* gli autori di comportamenti pericolosi o illegali.

Si è diffusa nell'underground informatico l'abitudine di segnalare la presenza di reti wireless non sicure o addirittura senza nessuna forma di protezione. È stato creato un linguaggio convenzionale per identificare le reti wireless accessibili mediante simboli grafici disegnati sui muri. La stessa pratica di cercare reti wireless vulnerabili è detta *wardriving*, mentre quella di segnalarle con segni murali è detta *warchalking*.

Purtroppo la rete wireless non potrà mai essere sicura al 100% ma molto si può fare autenticando gli indirizzi hardware (Mac Address) dei Nic o configurando apposite regole sui firewall. Alternativamente, si può instradare sulla rete wireless un canale VPN (Virtual Private Network) cifrato, ottenendo

un livello di sicurezza sicuramente paragonabile a quello di una rete cablata, anche se purtroppo in questo modo si perderà qualcosa in termini di efficienza e prestazioni.

Il problema è che ormai in aree commerciali molto frequentate, come aeroporti, stazioni ferroviarie o alberghi, è possibile trovare servizi commerciali di connettività wireless (*HotSpots*), che, però, normalmente identificano i loro utenti. Inoltre proprio di recente i Ministri della Difesa Arturo Parisi e delle Comunicazioni Paolo Gentiloni hanno raggiunto un'intesa per l'avvio in Italia delle nuove tecnologie di telecomunicazioni wireless, approvando il percorso per l'introduzione del Wi-Max in Italia.

In altri termini il wireless ormai è una realtà e per quanto potranno essere adottati diversi accorgimenti come quelli menzionati in precedenza il problema sicurezza rimarrà sempre molto grave.

In caso di violazione della rete, al di là delle varie figure di reato riconducibili all'accesso abusivo, sono ipotizzabili varie forme di violazione della privacy, come il furto di identità che ormai sta assumendo una particolare gravità negli ultimi tempi.

In effetti il progressivo sviluppo delle comunicazioni elettroniche ha determinato la crescita esponenziale di nuovi servizi e tecnologie. Se ciò ha comportato, da un lato, indiscutibili vantaggi in termini di semplificazione e rapidità nel reperimento e nello scambio di informazioni fra utenti della rete Internet, dall'altro, ha provocato un enorme incremento del numero e delle tipologie di dati personali trasmessi e scambiati, nonché dei pericoli connessi al loro illecito utilizzo da parte di terzi non autorizzati.

Si è così maggiormente diffusa l'esigenza di assicurare una forte tutela dei diritti e delle libertà delle persone, con particolare riferimento all'identità personale e alla vita privata degli individui che utilizzano le reti telematiche.

Indubbiamente in ragione delle peculiarità del settore e dell'estrema rapidità con cui la tecnologia va evolvendosi, sono opportunamente destinati a svolgere un ruolo determinante, sul piano della disciplina dei trattamenti e delle garanzie per gli interessati, i codici deontologici e di buona condotta previsti da ultimo dal d.lgs. 30 giugno 2003, n. 196.

Le diverse questioni emerse nella materia in esame confermano peraltro la necessità di una cooperazione internazionale, anche in ragione del recepimento in Italia del principio di stabilimento, che può limitare il potere di intervento dell'Autorità rispetto ai trattamenti di dati personali effettuati da soggetti situati all'estero.

Anche sul fronte dell'e-government esistono indubbe difficoltà non solo in Italia ma anche in Europa e in un documento recentemente reso pubblico i Garanti europei hanno analizzato la situazione corrente e le prospettive di sviluppo in tema di e-government, sottolineandone le implicazioni in chiave di

protezione dei dati personali e richiamando l'attenzione sui possibili rischi del mancato coordinamento fra governi nazionali e autorità di protezione dati.

Lo sviluppo di moderne tecnologie e di nuovi servizi di comunicazione elettronica ha reso, quindi, necessario un ulteriore adeguamento della normativa sulla protezione dei dati personali in ambito italiano ed internazionale.

Sul punto, in Italia, il recente Codice per la protezione dei dati personali ha compiuto una ricognizione innovativa delle preesistenti norme sul trattamento dei dati nel settore delle telecomunicazioni (d.lgs. n. 171/1998, come modificato dal d.lgs. n. 467/2001), completando nello stesso tempo il recepimento della direttiva n. 2002/58/CE, relativa alla tutela della vita privata nel settore delle comunicazioni elettroniche.

La disciplina introdotta in materia dal Codice, riproponendo un criterio già presente nella normativa comunitaria, adotta un approccio "tecnologicamente neutro", ossia valido ed applicabile a tutte le forme di comunicazione elettronica a prescindere dal mezzo tecnico utilizzato.

Naturalmente rimane il rischio che la diffusione dei documenti elettronici come la Carta Nazionale dei Servizi e l'interconnessione di archivi informatici possano comportare una riduzione dei diritti della persona e della riservatezza dei dati personali.

Ciò anche in considerazione del fatto che su questi profili l'Italia non è dotata di una legislazione in tutto idonea a contemperare le esigenze di semplificazione e razionalizzazione dell'attività economica e commerciale con quelle di tutela della persona, anche in attuazione delle prescrizioni e dei principi generali già contenuti nella normativa comunitaria.

Al riguardo, l'Autorità Garante per la tutela dei dati personali, nell'esercizio della funzione consultiva di cui è titolare, ha più volte segnalato, negli anni precedenti, la necessità di individuare con maggiore attenzione e proporzionalità la tipologia dei dati da inserire nei documenti elettronici, i soggetti che possono eventualmente accedere alle varie categorie di dati e le garanzie per gli interessati.

Lo sviluppo della rete ha inoltre contribuito, secondo il Garante, alla concezione di un "corpo elettronico" della persona ripartito in diverse banche dati.

Oggi le potenziali aggressioni del diritto all'identità personale non provengono esclusivamente da atti, fisici o immateriali, che comportano un'invasione della propria sfera privata. L'evoluzione tecnologica, infatti, se da un lato ha reso sempre più semplici ed accessibili i meccanismi attraverso i quali la pretesa di solitudine dell'individuo tende ad essere compressa, dall'altro ha offerto forme di protezione e di prevenzione dalle intrusioni indesiderate che consentono di risolvere o quanto meno di attenuare in radice questo fenomeno. Cosicché diventa essenziale non tanto evitare che altri violino il pur diritto fondamentale

di essere lasciati soli, quanto consentire che ogni individuo possa disporre di un agile diritto di controllo rispetto alle tante informazioni di carattere personale che altri possano aver assunto.

Difatti, nell'attuale era tecnologica le caratteristiche personali di un individuo possono essere tranquillamente scisse e fatte confluire in diverse banche dati, ciascuna di esse contraddistinta da una specifica finalità. Su tale presupposto può essere facilmente ricostruita la c.d. *persona elettronica* attraverso le tante tracce che lascia negli elaboratori che annotano e raccolgono informazioni sul suo conto.

Ma è necessario ed auspicabile che le giuste preoccupazioni del Garante vadano risolte sul piano istituzionale facendo tra l'altro ricorso a quegli strumenti che lo stesso Codice mette a disposizione.

Si deve ricordare innanzitutto che l'obiettivo delle nuove tecnologie è quello di migliorare la qualità della vita dei cittadini nel rispetto della sicurezza e della privacy. Qualsiasi problematica inerente i rapporti tra nuove tecnologie e privacy va sempre risolta inquadrandola nell'ambito di una considerazione globale dei benefici socio-economici che scaturiscono dall'innovazione tecnologica. Ad esempio non possono trascurarsi i grandi vantaggi rappresentati dalle banche dati presenti in Rete oltre che nello svolgimento dell'attività amministrativa, anche nel migliorare in generale la qualità della vita dei cittadini e nel promuovere le attività produttive ed economiche. Le banche dati, per la loro stessa natura, non sono un male; ciò che è preoccupante, ai fini della tutela dei diritti delle persone e della sicurezza delle informazioni, è sicuramente l'uso che delle stesse può farsi. Diventa, quindi, necessario sotto questo profilo governare i processi di sviluppo e promuovere le regole per il rispetto dei diritti.

Per questo, bisogna ammettere che il nuovo codice della privacy costituisce un avanzamento della consapevolezza civile in un'era di accelerata e pervasiva evoluzione tecnologica.

Con l'approvazione del decreto legislativo n. 196 del 30 giugno 2003, il quadro delle misure di protezione dei dati personali è stato profondamente modificato. I meccanismi di adeguamento previsti renderanno il Codice meno soggetto all'obsolescenza di fronte all'avanzare delle tecnologie, restando peraltro immune da tecnicismi e mantenendo invece una sufficiente generalità e indipendenza da specifiche tecnologie.

In questo senso, il Codice ha fatto proprio l'obiettivo di ripristino del principio giuridico della norma a carattere generale ed astratto che sia applicabile anche alle fattispecie future che l'evoluzione tecnologica può presentare.