di Giovanni Nazzaro

LAWFUL INTERCEPTION OF WI-FI ONBOARD NETWORKS

Giovanni NAZZARO, *Lawful Interception Consultant* e *Security Manager*, ingegnere, è un libero ed indipendente professionista che opera nell'*information technology* e nelle reti di telecomunicazioni, esperto in *security*, *legal* e *compliance* in tali ambiti. Dal 2001 si occupa della progettazione dei sistemi d'intercettazione e di data retention in uso agli operatori di telecomunicazioni mobili, fisse, wifi, satellitari. Direttore di "*Sicurezza e Giustizia*" dal 2011 e della "*Lawful Interception Academy*" dal 2014, è promotore della *LIA Certification* per la certificazione degli apparati LEMF e dei processi aziendali della funzione Judicial Authority Services, secondo i criteri della LIA. Si occupa di formazione ed è docente a contratto per il Ministero di Giustizia, in Master Universitari di I e II livello.

Le reti Wifi sui treni, autobus o aerei sono reti pubbliche e come tali sono soggette all'applicazione dell'art. 96 del Codice delle Comunicazioni elettroniche, ovvero l'operatore di telecomunicazioni che ha richiesto al Mise la licenza deve assicurare alcuni servizi all'Autorità Giudiziaria tra cui l'intercettazione, lo storico delle connessioni, ecc. Invece, le società, imprese o esercizi commerciali che non hanno come attività principale la fornitura di servizi di comunicazione elettronica devono garantire solo l'autenticazione dei propri utenti.

1. *Introduzione*

L'incremento dell'uso di dispositivi mobili per l'informazione e la comunicazione che caratterizza la società moderna è palesemente più evidente in una figura, che più di ogni altra ha bisogno di essere connessa a Internet. Si tratta del passeggero che viaggia in treno, autobus e aereo. Quella che sia la durata del suo viaggio, il passeggero moderno non riesce a rimanere disconnesso troppo a lungo dalla rete. Ed è così che le aspettative dei passeggeri riguardo la connettività hanno cambiato le dotazioni di questi vettori, al punto che la possibilità di connettersi ad una rete Wi-Fi gratuita durante un viaggio è oggi considerato un servizio fondamentale.

2. *La rete Wi-Fi a bordo*

Consentire a centinaia di passeggeri di connettersi a Internet contemporaneamente è un compito arduo per gli operatori del settore, tecnicamente molto più difficoltoso che configurare e gestire una rete Wi-Fi domestica o di ufficio perché l'obiettivo è quello di garantire che ogni passeggero possa navigare su un sito web, consultare la propria email o vedere un video su Youtube in contemporanea ad altri passeggeri che gli sono accanto. Occorre cioè fornire una larghezza di banda sufficiente per ciascun passeggero in un ambiente ad alta densità. Gli operatori del settore sono stati spinti ad adottare, nel complesso, soluzioni che combinino affidabilità, copertura e larghezza di banda affinché possa essere garantita una user experience senza interruzioni.

Vediamo quali possano essere i principali fattori critici in una rete Wi-Fi ad alta densità (rif. https://www.moxa.com).

1. **L'affidabilità del punto di accesso (AP)** che svolge un ruolo centrale nel collegamento dei passeggeri alla rete Wi-Fi di bordo.
2. **Una opportuna larghezza di banda per ciascun passeggero,** che ha bisogno di una connettività di rete senza interruzioni durante il viaggio. Le stime si basano generalmente su studi sull'utilizzo dei dispositivi mobili e sul comportamento dell'u-

tente. In casa o in ufficio, 50 o 100 Mbps possono essere sufficienti per consentire l'accesso a Internet per più dispositivi contemporaneamente. Tuttavia, con i passeggeri che hanno più di un dispositivo e considerando altri fattori che limitano il throughput, i passeggeri possono avere a disposizione anche solo 2 o 3 Mbps di larghezza di banda. Molto dipende anche dalle tecnologie Wi-Fi (a / b / g / n / ac) e quali applicazioni sono utilizzate. Ad esempio, un AP che funziona in modalità 802.11n potrà supportare velocità variabili.

3. **Il rapporto tra AP e numero di utenti**. Per fornire una buona esperienza utente, alcuni studi del settore consigliano di distribuire un AP ogni 60 utenti. Ad esempio, un trasporto ferroviario che trasporta 100 passeggeri richiederà almeno due AP, ciascuno dei quali serve 50 passeggeri. Se non vengono distribuiti abbastanza AP, alcuni passeggeri potrebbero riscontrare una scarsa qualità della connessione. C'è da dire che le applicazioni ad alto utilizzo di banda, come YouTube, influiscono su tale rapporto e riducono il numero di utenti che un AP può servire. La seguente tabella mostra la larghezza di banda richiesta dalle applicazioni comuni.

Applicazione	Bandwidth
Netflix HD Quality	5 Mbps
Netflix DVD Quality	3 Mbps
FaceTime	500 Kbps - 1 Mbps
YouTube	500 Kbps - 1 MbpsWeb
Browsing	1.5 Mbps
Skype (HD)	1 Mbps
Google Hangouts	5 Mbps
Google Play	320 Kbps
Facebook video calls	500 Kbps

Sebbene impegnativo, lo studio di come i requisiti di larghezza di banda delle applicazioni influiscono sulla capacità è un passo importante verso la realizzazione di una rete Wi-Fi ad alte prestazioni e ad alta densità.

4. **Il numero massimo di dispositivi che possono connettersi a un AP**. Quando molti dispositivi tentano di connettersi a un AP, la larghezza di banda disponibile per ciascun dispositivo diminuisce. Bilanciando il carico per ciascun dispositivo, gli operatori del settore possono limitare il numero di dispositivi che si connettono a un AP. Quando viene raggiunto questo limite, l'AP può rifiutare qualsiasi nuova richiesta di connessione, costringendo i nuovi dispositivi a connettersi ad altri AP. Questo è il motivo per cui, ad esempio, viaggiando su un treno o un autobus, pur avendo massima intensità di segnale Wi-Fi, non riusciamo a connetterci alla rete. Inoltre, il bilanciamento del carico potrebbe avvenire per singolo canale, incoraggiando una distribuzione uniforme della larghezza di banda disponibile per tutti i dispositivi.
5. **L'isolamento dei dispositivi per aumentare la sicurezza,** impedendo che dispositivi diversi connessi alla stessa rete Wi-Fi possano comunicare tra loro. Non dimentichiamoci che ogni dispositivo che si collega agli AP di bordo appartiene alla stessa rete, compresi i sistemi di bordo come quelli di trasmissione o altri sistemi di controllo, evitando così anche attacchi informatici dall'interno.

3. Aspetti di interesse per l'Autorità Giudiziaria e le Forze di polizia

Le reti Wi-Fi sui treni, autobus o aerei sono reti pubbliche e come tali sono soggette all'applicazione dell'art. 96 del Codice delle Comunicazioni elettroniche, ovvero l'operatore di telecomunicazioni che ha richiesto al Mise la licenza deve assicurare alcuni servizi all'Autorità Giudiziaria tra cui l'intercettazione, lo storico delle connessioni, ecc. Alcuni impropriamente interpretano tale norma di riferimento attribuendo al titolo di viaggio acquistato la condizione per escludere la caratteristica di rete pubblica, cioè solo chi ha acquistato il titolo di viaggio può accedere alla rete Wi-Fi di bordo. Tale assunto non è certamente valido in quanto l'accesso alla rete Wi-Fi dovrebbe verificare anche il possesso del biglietto.
Questa verifica generalmente non avviene, esponendo l'accesso alla rete Wi-Fi anche a soggetti fisicamente limitrofi al vettore di trasporto. Assumendo che durante la fase di accesso alla rete Wi-Fi venga verificata il possessodel biglietto e quindi la titolarità del viaggio, anche in questo caso non verrebbe meno l'obbligo dettato dall'art. 96 CdC poiché l'aggettivo di "pubblica" riferita alla rete non è certamente legato al valore economico del servizio offerto, quanto piuttosto al fatto che chiunque può utilizzare tale servizio se accetta le condizioni offerte.

Il Codice delle comunicazioni elettroniche, istituito con il Decreto legislativo n.259 del 1 agosto 2003, rimane nel nostro paese il riferimento normativo che disciplina i servizi di comunicazione elettronica per i quali occorre un'autorizzazione generale o una licenza individuale. A tal proposito è utile ricordare la distinzione tra servizi privati e pubblici. Si intende per servizio di comunicazione elettronica ad uso privato il servizio svolto esclusivamente nell'interesse proprio dal titolare della relativa autorizzazione generale o licenza. Il servizio di comunicazione elettronica ad uso pubblico riguarda un servizio fornito dalla società titolare di autorizzazione o licenza, "accessibile" al pubblico.

Assunto quindi che l'offerta di un servizio accessibile al pubblico ha bisogno di un'autorizzazione generale o licenza e che il soggetto richiedente deve garantire, di conseguenza, determinati servizi verso l'Autorità Giudiziaria, vediamo come si è evoluta la disciplina specifica delle reti Wi-Fi.

Il Decreto ministeriale 28.05.2003 (modificato dal d.m. 14.10.2005) rubricato "Regolamentazione dei servizi Wi-Fi ad uso pubblico", all'art. (Oggetto ed ambito di applicazione) prevede che: "Il presente provvedimento fissa le condizioni per il conseguimento dell'autorizzazione generale per la fornitura, attraverso le applicazioni Radio LAN nella banda 2,4 GHz o nelle bande 5 GHz,

dell'accesso del pubblico alle reti e ai servizi di telecomunicazioni in modalità fissa e nomadica".
L'art. 6 (Condizioni dell'autorizzazione generale) del suddetto decreto, prevede che "*il soggetto titolare dell'autorizzazione generale per la fornitura, attraverso le applicazioni Radio LAN, dell'accesso del pubblico alle reti e ai servizi di telecomunicazioni, è tenuto a soddisfare*

Art. 6 DM 28.05.2003	Descrizione	Obbligo
Lettera B)	la sicurezza della rete contro **l'accesso non autorizzato** conformemente alla normativa in materia, il mantenimento dell'integrità della rete, l'interoperabilità dei servizi nonché la protezione dei dati ed in particolare le prestazioni ai fini di giustizia sin dall'inizio dell'attività;	Autenticazione
Lettera K)	l'adozione di opportuni codici di abilitazione e identificazione per **identificare univocamente l'abbonato** e verificarne l'abilitazione all'accesso alla rete tramite l'access point	Identificazione
Lettera L)	il rispetto delle disposizioni vigenti in materia di pubblica sicurezza e tempestiva collaborazione con l'Autorità giudiziaria	Prestazione Obbligatorie verso l'Autorità Giudiziaria

le seguenti condizioni" che sono sintetizzate nella seguente tabella con l'indicazione dell'obbligo derivante.

Nel 2013 il c.d. "decreto del fare" (Decreto-Legge 21 giugno 2013, n. 69, "Disposizioni urgenti per il rilancio dell'economia") ha alleggerito la posizione di alcuni soggetti commerciali. L'art. 10, modificato in fase di conversione dalla legge di conversione de 9 agosto 2013, n.98 prevede che "*L'offerta di accesso alla rete internet al pubblico tramite tecnologia Wi-Fi non richiede l'identificazione personale degli utilizzatori. Quando l'offerta di accesso non costituisce l'attività commerciale prevalente del gestore del servizio, non trovano applicazione l'articolo 25 del codice delle comunicazioni elettroniche, di cui al decreto legislativo 1º agosto 2003, n. 259, e successive modificazioni, e l'articolo 7 del decreto-legge 27 luglio 2005, n. 144, convertito, con modificazioni, dalla legge 31 luglio 2005, n. 155, e successive modificazioni*" ovvero non è richiesta autorizzazione generale al MISE.

Si tratta di una disposizione condivisibile poiché sana definitivamente la posizione di soggetti commerciali che non si sono mai potuti adeguare alla norma precedente in vigore fino al 2013. Pensiamo ad esempio ad un bar o ad una pizzeria che offre l'accesso alla rete Wi-Fi ai propri clienti: questi avrebbero dovuto identificare il proprio cliente che accede alla rete Wi-Fi registrando i dati del suo documento d'identità. Venendo meno per tali soggetti anche l'applicazione dell'art. 25 del CdC, decade anche l'obbligo di garantire le prestazioni obbligatorie verso l'Autorità Giudiziaria. Volendo fare un paragone, è come se tali soggetti fossero stati assimilati ai clienti privati residenziali degli operatori telefonici, che hanno un accesso ADSL o in fibra alla rete telefonica su cui installano un router Wi-Fi che diffonde il segnale della propria rete domestica. La differenza è che, mentre per i soggetti individuati dal decreto ministeriale è obbligatorio evitare l'accesso non autorizzato alla rete Wi-Fi garantendo una preventiva fase di autenticazione tramite username e password (soprattutto in considerazione del fatto che chiunque avvicinandosi al suddetto bar o pizzeria potrebbe connettersi in modo del tutto trasparente), per i clienti privati non esiste uno specifico obbligo normativo ma è fortemente consigliato per questioni di sicurezza, al punto che i router Wi-Fi che si possono acquistare anche dal proprio operatore telefonico sono già predisposti dalla fabbrica per l'accesso tramite username e password.

In definitiva, quindi, da tale panoramica normativa si desume che le società che hanno come attività principale la fornitura di servizi di comunicazione elettronica, devono richiedere al Mise l'autorizzazione generale o licenza, con conseguente obbligo di identificare i propri clienti, assicurare l'autenticazione evitando così l'accesso non autorizzato, garantire verso l'Autorità Giudiziaria prestazioni obbligatorie come l'intercettazione, il tracciamento delle connessioni, la sospensione del servizio, ecc. Per ragioni di sintesi non vengono riportati i dettagli implementativi di tali servizi.
Invece, le società, imprese o esercizi commerciali che non hanno come attività principale la fornitura di servizi di comunicazione elettronica devono garantire solo l'autenticazione dei propri utenti.

E' ovvio che in questo caso possono esserci soggetti che, pur valutando di non avere come attività principale la fornitura di servizi di comunicazione elettronica, decidono comunque di adempiere agli obblighi previsti di chi possiede l'autorizzazione generale. Tale scelta può basarsi sulla valutazione che ne deriverebbe per gli alti volumi di traffico e il numero elevato di utenti in caso di interazioni con l'Autorità Giudiziaria. Ad esempio, si può valutare che la predisposzione centralizzata ed automatica di tali richieste possa garantire un risparmio economico, di risorse umane e di tempo rispetto alla gestione frammentata delle singole richieste. Al contrario è possibile che ci siano soggetti che, ignorando la normativa di riferimento oppure scegliendo di risparmiare sui costi dovuti agli adeguanti necessari per implementare gli obblighi verso l'Autorità Giudiziaria, operino senza tale autorizzazione dichiarando, quindi, che non hanno come attività principale la fornitura di servizi di comunicazione elettronica. Tale ipotesi può trovare applicazione solo per soggetti privati, che quindi subirebbero un esame sulla leicità delle dichiarazioni pregresse nel momento in cui si formalizzi la prima richiesta dell'Autorità Giudiziaria. Ricordiamo infatti che l'art. 6 del Codice delle comunicazioni elettroniche vieta espressamente a Stato, Regioni ed enti locali di fornire direttamente reti e servizi di comunicazione elettronica ad uso pubblico se non attraverso società controllate o collegate. Per erogare questo tipo di servizi le pubbliche amministrazioni devono quindi rivolgersi a operatori autorizzati ai sensi dell'art. 25 del Codice.

A questo punto, in merito all'offerta di un servizio gratuito o meno per l'accesso alla rete Wi-Fi, un utile suggerimento per le società che operano nei trasporti può essere quello di adottare lo schema utilizzato dalle pubbliche amministrazione, affidando tale servizio ad operatori autorizzati.

In Italia abbiamo tre principali esempi:

1. **Trenitalia** (rif. https://www.icomera.com/trenitalia-deploying-latest-icomera-passenger-wi-fi-technology-on-high-speed-frecciarossa-fleets/). All'interno del *press release* si legge che Trenitalia ha affidato alla società Icomera la fornitura dell'accesso a Internet per i passeggeri della sua flotta di treni ad alta velocità "Frecciarossa" ETR1000 ed ETR700 EMU. Icomera è una società controllata di ENGIE Ineo, ha sede a Göteborg in Svezia ed ha uffici negli Stati Uniti, nel Regno Unito, in Germania, Francia e Italia. Si definisce come il principale fornitore mondiale di connettività Internet wireless per il trasporto pubblico. La società Icomera AB risulta aver ottenuto autorizzazione in Italia il 1° febbraio 2019, ai sensi del D.M. 28 maggio 2003 e dell' articolo 25 del Codice delle Comunicazioni Elettroniche.
2. **Alitalia** (rif. http://www.amministrazionestraordinariaalitaliasai.com/pdf/alitalia/allegato_2_alitaliarelazione2017.pdf). All'interno della relazione sulla gestione del gruppo Alitalia nel periodo dal 2 maggio 2017 al 31 dicembre 2017, relativamente al tema "Cabin appearance" si legge che le attività di manutenzione relative alle cabine degli aeromobili sono eseguite internamente da Alitalia su tutta la flotta, mentre la manutenzione dei sistemi di Intrattenimento di bordo e connettività è affidata a Panasonic. La Panasonic Avionics Airlines (PAC) è un fornitore di apparecchiature di intrattenimento in volo, tra cui musica, video on demand, shopping in volo, Internet ed e-mail, servizio telefonico GSM e UMTS tramite la sua affiliata AeroMobile Communications Limited, operatore di rete mobile registrato per l'industria aeronautica e ha sede nel Regno Unito. All'interno del sito web di Alitalia (rif. https://www.alitalia.com/it_it/volare-alitalia/in-volo/connessione-a-bordo.html) è possibile avere notizie più approfondite sul roaming GSM a bordo degli aerei. PAC e Aeromobile hanno in Italia un'autorizzazione del 28 maggio 2015 per fornire al pubblico servizi satellitari sugli aerei di Alitalia.
3. **Flixbus** (rif. https://www.icomera.com/flixbus-awards-icomera-contract/). L'operatore di trasporto internazionale FlixBus ha affidato la realizzazione della connettività Internet ad Icomera prima citata. L'installazione dei primi 1.500 veicoli in Europa e negli Stati Uniti è iniziata nella primavera del 2018 ed è previsto il completamento quest'anno.

L'elenco delle società autorizzate è facilmente reperibile esaminando l'elenco nazionale delle imprese autorizzate ad offrire servizi di comunicazione elettronica ai sensi del Decreto legislativo 259/2003, aggiornato al 27 maggio 2019 per tipologia di servizio (rif. https://www.mise.gov.it/index.php/it/component/content/article?id=68306). Inoltre, è possibile consultare l'elenco delle risorse di numerazione geografiche, non geografiche e mobili assegnate ai gestori di telefonia e quelle disponibili (rif. https://www.mise.gov.it/index.php/it/comunicazioni/telefonia/risorse-di-numerazione).

4. *Eliminato l'obbligo di tracciare il MAC address*

Nella sua forma originaria, l'art. 10, comma 1, del Decreto-Legge 21 giugno 2013, n. 69 prevedeva che "*L'offerta di accesso ad internet al pubblico è libera e non richiede la identificazione personale degli utilizzatori. Resta fermo l'obbligo del gestore di garantire la tracciabilità del collegamento (MAC address)*". La legge di conversione ha fortunatamente eliminato il seguente passaggio "*Resta fermo l'obbligo del gestore di garantire la tracciabilità del collegamento (MAC address)*". Vediamo il motivo.

Ogni computer, tablet o smartphone ha una scheda di circuito che gli consente di connettersi a una rete. Questa scheda viene indicata con l'acronimo di NIC (Network Interface Controller) ed ognuna ha un identificativo hardware noto come MAC (Media Access Control) address. Un MAC address può essere facilmente rintracciato ma non viaggia abbastanza lontano da essere utilizzato, ad esempio, per rintracciare il nostro computer che è stato rubato.

Infatti, sebbene l'indirizzo MAC sia univoco e cablato sulla scheda, esistono alcuni metodi che permettono di camuffarlo, operazione che in gergo tecnico viene detta *MAC spoofing*. La modifica può essere giustificata da motivi di privacy, ad esempio collegandosi ad una rete Wi-Fi libera e non protetta, o per motivi di interoperabilità. In ogni caso queste modifiche sono effettuate a livello software e non sono permanenti: al riavvio del sistema viene ripristinato il MAC address originale memorizzato all'interno del dispositivo hardware.
La versione 10 del sistema operativo Windows consente di configurare l'opzione di utilizzo di "indirizzi hardware casuali" della scheda di rete Wi-Fi ad ogni nuova connessione o per una specifica rete, quindi oggi possiamo fare il MAC spoofing senza alcuna conoscenza di programmazione o senza ricorrere a specifici programmi (rif. https://support.microsoft.com/it-it/help/4027925/windows-how-and-why-to-use-random-hardware-addresses).

Anche ipotizzando che il MAC address non sia stato modificato, tale informazione non supera il primo dispositivo di rete tra il nostro computer e Internet. Per questi motivi il riferimento al MAC address è stato eliminato dalla norma, tuttavia avremmo preferito che nella legge di conversione si fosse ribadito l'obbligo di autenticazione con il tracciamento e la correlazione dell'identificativo utilizzato in tale fase (ad esempio il numero di cellulare a cui inviare la password temporanea).

Nonostante queste limitazioni di natura tecnica, in paesi esteri anche non troppo lontani dall'Italia, nella lista dei termini e condizioni del servizio Wi-Fi offerto a bordo degli aerei si può leggere che il MAC Address è conservato per adempiere alla normativa di riferimento. Ad esempio, analizzando i termini e le condizioni del servizio Wi-Fi offerto dalla Scandinavian Airlines System (SAS), compagnia di bandiera della Danimarca, Norvegia e Svezia, si può leggere "*By accepting these Terms and Conditions you give us permission to process your personal data (e.g. name, EuroBonus membership number, e-mail address and your device MAC address*" ed anche "*The personal data will, except for MAC addresses, be retained for the duration of the flight. MAC addresses will be retained by Viasat Inc for two years after it has been collected in order to enhance the user experience and comply with mandatory legislation*" (rif. https://www.flysas.com/content/dam/sas/pdfs/travel-info/terms-conditions-sas- Wi-Fi.pdf) quindi il MAC address viene conservato addirittura per due anni. ©