La relazione affronta i principali rischi legati all'uso delle reti Wi-Fi, sempre più diffuse ma anche esposte a numerosi attacchi informatici. Tra questi, si analizzano:

- **Man-in-the-Middle (MITM)**: dove un attaccante intercetta la comunicazione tra due dispositivi.
- **Evil Twin**: un falso hotspot Wi-Fi con nome identico a quello legittimo, usato per rubare dati.
- **Deauthentication Attack**: attacco che disconnette gli utenti per forzarli a riconnettersi, facilitando l'intercettazione.

Viene descritta l'evoluzione dei protocolli di sicurezza wireless:

- **WEP**: ormai considerato insicuro.
- **WPA/WPA2**: miglioramenti ma con vulnerabilità.
- **WPA3**: l'attuale standard più sicuro, basato sul protocollo SAE, ancora poco diffuso.

Dal punto di vista tecnico, si sottolinea l'importanza dei livelli 2 e 3 del modello ISO/OSI, degli algoritmi di cifratura e dei protocolli di autenticazione. La sicurezza di una rete dipende non solo dalla tecnologia ma anche dalla **configurazione**e dall'**educazione degli utenti**.

L'analisi civica evidenzia:

- Il diritto alla privacy, messo a rischio dalle reti pubbliche non protette.
- La responsabilità nella gestione e nella condivisione delle connessioni Wi-Fi.
- Il **digital divide**, che rende più vulnerabili gli utenti meno esperti o privi di accesso a connessioni sicure.
- L'impatto ambientale delle infrastrutture wireless (consumo energetico, smaltimento dispositivi).

Un caso studio reale racconta un attacco *evil twin* avvenuto in un bar a Milano, dove un hacker ha creato una rete fasulla per sottrarre informazioni agli utenti. L'episodio ha spinto il locale a migliorare le misure di sicurezza.

Infine, la relazione propone soluzioni come l'uso di **VPN**, la promozione del protocollo WPA3, campagne di educazione digitale e una maggiore regolamentazione delle reti pubbliche.