

## Progetto e Piano di Formazione

### **Tecniche di privacy preserving per la protezione di sistemi cyber fisici**

Le attività di questo assegno di ricerca, della durata di 12 mesi, si concentreranno principalmente sullo studio delle tecniche di protezione della privacy e della loro applicazione nelle smart city, inserendosi nell'ambito del progetto "Approccio sistemico alla prevenzione e mitigazione dei rischi relativi a cybersecurity, cyber resilienza e safety (EcoCyber)" del progetto "SEcurity and Rights in the CyberSpace" (SERICS). Gli obiettivi principali comprendono la progettazione, implementazione e validazione di nuovi meccanismi di protezione della privacy per salvaguardare le grandi quantità di dati e informazioni generate dai dispositivi Internet of Things (IoT) che caratterizzano le moderne smart city. In particolare, l'assegnista si concentrerà sull'integrazione delle tecniche emergenti di preservazione della privacy, come Zero-Knowledge Proof (ZKP), differential privacy (DP) e homomorphic encryption in modo da garantire la sicurezza dei dati raccolti e generati nelle smart city. Inoltre, si esploreranno approcci basati su Decentralized Identifier (DID) e Verifiable Credential (VC) per consentire agli utenti di mantenere il controllo sui propri dati personali e di condividerli in modo sicuro, riducendo così la dipendenza da entità centralizzate e aumentando la fiducia nell'ecosistema delle smart city. Infine, l'assegnista dovrà valutare anche l'utilizzo di queste tecniche in contesto di modelli di intelligenza artificiale distribuiti come federated learning.

Il programma di formazione dell'assegno prevede le seguenti attività organizzate nel periodo di un anno:

- Ricerca sullo stato dell'arte
- Progettazione di soluzioni di privacy preserving
- Sviluppo software e test sul campo delle soluzioni progettate

Sono inoltre previste attività di gruppo orientate alla predisposizione di materiali e prototipi. Saranno anche maturate esperienze significative relativamente a: redazione di documenti di carattere divulgativo e presentazione di risultati e prototipi alla comunità scientifica e ad aziende del territorio.