WP 3
Progetto FICO

Come indicato nel progetto FICO il WP 3 (Conti, Falcinelli, Gnaldi) riguarda la definizione dell'ambito di applicazione progettuale, l'analisi dello stato dell'arte e degli attuali strumenti di investigazione in ambito cyber-crime/cyber-security e dei progetti in corso di sviluppo. Questa attività si concretizza in un **documento** di sintesi relativo allo stato dell'arte, relativo soprattutto alle lacune e agli spazi possibili di intervento. Ciò anche grazie a un'interpretazione della sicurezza informatica dalla voce degli esperti (interviste semi-strutturate).
Si tratta di un'analisi sugli aspetti giuridici, statistici e sociali che riguardano l'esistenza o meno di banche dati, centri di calcolo, software. Quali reati in rete dovrebbero riguardare? Quali caratteristiche hanno tali reati in rete (truffe, cyber terrorismo, corruzione, offensivi identità personale)? Si tenterà di focalizzare l'attenzione sui software e su bisogni/necessità per un processo per l'analisi automatizzata delle immagini in formato digitale.
In secondo luogo, si procede a una selezione di tipologie di cyber-crimes/casi studio e dei domini specifici di analisi relativi a corruzione, cyber-terrorismo, reti reati offensivi dell'identità personale. Che casi di studio esistono dalla cronaca? Che cosa esiste ? e che cosa manca? Se manca perché manca? È un problema tecnico, legislativo, burocratico? La risposta a tali domande include la contestualizzazione dei diversi casi-studio; la ricostruzione delle dinamiche criminale-vittima-testimone rispetto alle specifiche del caso; e l'individuazione delle vulnerabilità e dei comportamenti anomali e/o illegali.
Ciò esita in un **report** sulle possibili vittime dei cyber-crime individuati e sulle dinamiche del crimine e in un **seminario** dedicato all'individuazione e approfondimento dei casi studio.
Il terzo luogo, avviene o la selezione di possibili fonti open source e definizione delle metodologie per l'estrazione dei dati oppure, laddove assenti, la descrizione delle lacune che riguardano le fonti open source idonee a seconda del cyber-crime considerato, esplicitando gli eventuali bisogni in un report sulle fonti disponibili e sul loro possibile utilizzo in ambito corruzione, cyber-terrorismo, reati offensivi dell'identità personale.
Ciò comporta una possibile definizione delle metodologie e delle task d'analisi dei dati in base al tipo di cyber-crime ed elaborazione di metriche di valutazione dell'accuratezza ed efficienza dei risultati, che esiterebbero in un **report** su metodologie d'analisi e metriche di valutazione in ambito corruzione, cyber-terrorismo, reati offensivi dell'identità personale.
In sintesi, il lavoro del WP 3 riguarda l'individuazione dei bisogni e delle necessità relative a banche dati per la sociologia, la statistica sociale e per la giurisprudenza: ciò avviene tramite l'esplicitazione dei bisogni e delle necessità che riguardano lo stato dell'arte cioè l'esistente e le possibili modalità per colmare le lacune; i bisogni per la realizzazione di banche dati e software capaci di gestire e di aggiornare automaticamente una banca dati di giurisprudenza penale, di merito e di legittimità, su argomenti specifici che riguardano i reati penali in rete. Quindi, i software e le banche dati non sono intesi non come un prodotto dell'esito del lavoro, ma come orizzonte per ragionare sui bisogni esistenti, ossia i bisogni per la realizzazione di banche dati e/o l'accesso a banche dati esistenti e centri di calcolo .