**Il rapporto fra accertamento preventivo e indagini penali in relazione ai dati raccolti dai sistemi di cybersicurezza**

**Descrizione della ricerca**

La ricerca, che si svolge nell'ambito del partenariato esteso PE7 SERICS (*SEcurity and RIghts In the CyberSpace*) Spoke 8, affronta i profili giuridici e informatico giuridici della gestione dei rischi in ecosistemi cyber-fisici del futuro. Proporre metodi e soluzioni originali per contribuire alla resilienza informatica dei futuri sistemi e servizi caratterizzati da componenti digitali sempre più interconnessi e intrinsecamente vulnerabili, come richiesto dall'UE attraverso NIS e NIS2, nonché dall'Agenzia Nazionale per la Cybersicurezza (ACN) rappresenta l'obiettivo prevalente del progetto EcoCyber (*Risk management for future cyber-physical ecosystem*s), in cui la ricerca si colloca.

Il progetto, con un approccio multidisciplinare, pone le basi per una visione olistica della cybersicurezza, che includa anche la resilienza, la privacy, e la sicurezza delle organizzazioni, delle industrie, delle infrastrutture critiche e delle relative filiere - prerogativa essenziale non solo per la fiducia e l'utilizzo dell'innovazione e della connettività, ma anche per sostenere i diritti e le libertà fondamentali degli individui.
Tale approccio è al centro della nuova Strategia per la cybersicurezza della Commissione (2020) che contiene proposte per iniziative di carattere legislativo, di investimento e politico in tre settori di intervento dell'UE: 1) resilienza, sovranità tecnologica e leadership; 2) sviluppo delle capacità operative volte alla prevenzione, alla dissuasione e alla risposta; e 3) promozione di un ciberspazio globale e aperto. Al fine di aumentare il livello di cyberresilienza e cybersicurezza del settore pubblico e privato dell'UE, vengono promossi in particolare la revisione della c.d. direttiva NIS, risultante nella direttiva (UE) 2022/2555 (c.d. NIS2); nuove norme orizzontali in materia di cybersicurezza per i prodotti con elementi digitali, risultanti poi nella proposta di c.d. *Cyber Resilience Act* presentata nel settembre 2022; iii) la creazione di un c.d. 'cyberscudo europeo', disegnato di recente dalla proposta del c.d. *Cyber Solidarity Act.*

Sul piano giuridico e informatico giuridico, la ricerca ha dunque l'obiettivo di condurre un'analisi dei quadri normativi della UE esistenti e futuri basati sul rischio, delle linee guida e degli standard tecnici al fine di supportare e integrare in chiave multidisciplinare le linee di ricerca più propriamente scientifico-tecnologiche del progetto nell'elaborazione di nuovi approcci alla gestione del rischio e di metodi originali di mitigazione e reazione in caso di attacchi informatici, necessari per garantire la sicurezza, la resilienza e la *safety* della società futura.
In chiave processualpenalistica, focus del presente assegno, la ricerca si concentrerà in particolare sull'analisi del rapporto fra accertamento preventivo e indagini penali in relazione ai dati raccolti dai sistemi di cybersicurezza.

**Piano delle attività**

L'assegnista, ponendosi in linea di continuità con il lavoro già svolto, in ambito IUS 16, dal titolare dell'assegno di ricerca già bandito nel primo anno di ricerca, dovrà approfondire l'analisi della normativa europea in materia di cybersicurezza (a partire dalla Direttiva NIS e dalle proposte di *Cyber Resilience Act* e *Cyber Solidarity Act*), evidenziandone in punti di diretta rilevanza con l'ambito penalistico e i punti di contatto che, anche indirettamente, possono avere un'influenza sullo svolgimento di indagini di rilevanza penale.
In secondo luogo, dovranno continuare ad essere analizzate le fonti nazionali che, sia in trasposizione della normativa sovranazionale sia di propria iniziativa, definiscono il quadro normativo che caratterizza lo svolgimento di indagini, di tipo preventivo o penale, in ambito cybersicurezza.

A fronte di tale ricognizione, l'assegnista dovrà quindi incentrare il proprio lavoro sull'analisi degli strumenti, giuridici e - in coordinazione con i risultati prodotti, all'interno del progetto, dal gruppo di ricerca in informatica giuridica – tecnici che possono o dovrebbero essere utilmente impiegati per lo svolgimento di indagini effettive in questo dominio. Lo studio dovrà anche raccogliere e tenere in considerazione standard o linee guida attualmente in uso presso le autorità di contrasto. Partendo da queste basi, l'assegnista dovrà formulare proposte per migliorare (o contribuire a costruire) il sistema di indagine, ponendo attenzione sia alle istanze di efficienza legate alla tutela della sicurezza nazionale, sia, naturalmente, alla necessità di garantire in modo effettivo i diritti fondamentali degli individui coinvolti in queste forme di accertamento.
All'assegnista sarà richiesto di pubblicare i risultati della propria ricerca, nonché organizzare o comunque contribuire ad almeno un incontro informativo specializzato, finalizzato alla crescita di consapevolezza nella comunità accademica sui temi oggetto dell'assegno.