Modelli di cybersecurity e prevenzione dei cyber crimes

Aporie della legislazione vigente, problematiche applicative e prospettive de iure condendo

24 Gennaio 2025

Università degli Studi di Napoli Federico II
Dipartimento di Scienze Politiche
Aula Spinelli - Via L. Rodinò, 22 Napoli

9.30 Apertura dei lavori

Saluti Istituzionali
Matteo Lorito, Rettore Università degli Studi di Napoli, Federico II
Paola De Vivo, Direttrice Dipartimento Scienze Politiche - Università degli Studi di Napoli, Federico II
Fabio Villone, Direttore DIETI - Università degli Studi di Napoli, Federico II
Carlo Colapietro, Principal Investigator - Università degli Studi Roma Tre
Giacomo Di Gennaro, Responsabile Unità di Ricerca Università degli Studi di Napoli, Federico II

Sezione Prima (ore 10.15 - 11.45)
Chair: Carlo Colapietro, Università degli Studi Roma Tre
Roberto Flor, Università degli Studi di Verona
Simon Pietro Romano, Università degli Studi di Napoli, Federico II
Pasquale Troncone, Università degli Studi di Napoli, Federico II
Bruno Frattasi, Agenzia Cybersicurezza nazionale (*in attesa di conferma*)

11.45 - 12.05 Coffe Break

Sezione Seconda (ore 12.05 - 13.50)
Chair: Giacomo Di Gennaro, Università degli Studi di Napoli, Federico II
Andrea Alberico, Università degli Studi di Napoli, Federico II
Ivano Gabrielli, Direttore Servizio Centrale Polizia Postale e delle Comunicazioni
Vincenzo Molinese, Generale dei Carabinieri, Comandante del ROS Roma

14.00 - 15.00 Fast Lunch

Sezione Terza (ore 15.05 - 17.00)
Chair: Pasquale Troncone, Università degli Studi di Napoli, Federico II
Giorgio Ventre, Università degli Studi di Napoli, Federico II
Vania Maffeo, Università degli Studi di Napoli, Federico II
Francesco Zorzi, Senior Advisor in Cybersecurity
Giovanni Cocozza, Università degli Studi di Napoli, Federico II

Il Convegno è organizzato dall'Unità di ricerca della Federico II (Responsabile Prof. Giacomo Di Gennaro), nell'ambito del Progetto PNRR Hard Disc, Spoke 1 "Human, social, and legal aspects", iniziativa "Security rights in cyberspace", Project "Law and regulation for a better-safe cyberspace (cyber rights)".

Finanziato dall'Unione europea NextGenerationEU
Ministero dell'Università e della Ricerca
Italiadomani
Consiglio Nazionale delle Ricerche
SERICS

Linee di indirizzo sui contenuti del Convegno del 24 gennaio 2025

La sicurezza informatica sta assumendo un ruolo sempre più importante nella società moderna fondata sulla operatività di una Rete globale dei sistemi e delle informazioni che ne vengono trattate. Una Rete che si sviluppa con infrastrutture che, oltre a coprire il territorio nazionale, si interconnettono secondo un circuito tecnologico transnazionale. Ne sono fruitori inevitabili i settori economici nevralgici del sistema imprenditoriale italiano e le istituzioni pubbliche che invocano una puntuale e tempestiva tutela per attività che si sviluppano secondo gli indirizzi della digitalizzazione integrale dei propri apparati operativi, indirizzati anche a un risparmio di spesa con la dematerializzazione dei processi.

Se da un lato gli sviluppi della tecnologia digitale si pongono in linea funzionale con gli sviluppi dell'economia nazionale, dall'altro esiste una precisa istanza di tutela in ordine a queste attività cui, per ragioni di asincronia, non si riesce a fare fronte in maniera soddisfacente. L'aggressione portata alla funzionalità dei sistemi informatici e i progetti di predare informazioni sensibili che fanno capo a strutture critiche di apparati di sicurezza dello Stato e di soggetti economici operanti nei mercati assume un tale livello di rischio imponderabile che impone interventi di difesa efficaci di natura tecnologica e normativa. Basti pensare ai grandi archivi dati che si stanno costituendo nel settore militare, in quello sanitario, in quello dell'intelligence, in quello giudiziario. Tuttavia, l'evoluzione legislativa e la pratica giudiziaria non riescono a tenere il passo dei progressi della tecnologia informatica e questo ritardo genera serie incertezze nella fase degli investimenti economici e severi danni nella fase operativa.

Un tale assetto così fortemente dinamico sfugge, dunque, a un puntuale governo e agli efficaci controlli del diritto che finisce per intervenire solo su vicende in essere per rimediare introducendo nuovi e più adeguati assetti regolativi e soluzioni di natura preventiva per sventare ingerenze, intrusioni e danni da parte di terzi soggetti ostili. Sulla scorta delle indicazioni e degli obblighi normativi di conio sovranazionale, il nostro ordinamento si sta dotando progressivamente di nuovi strumenti giuridici per affrontare il problema. Alla base, tuttavia, manca un progetto complessivo di natura legislativa, così come il costituendo settore della cybersicurezza è del tutto carente di mezzi, personale e risorse finanziarie adeguate.

Intanto il campo normativo (legislativo e giurisprudenziale) si allarga di giorno in giorno in maniera convulsa. Cresce il bisogno di protezione rispetto a fatti predatori, dotati di incontrollabile aggressività, commessi con i mezzi informatici e con essi cresce l'attenzione e il livello di intervento disordinato del legislatore nazionale, in carenza di un disegno razionale organico dell'intervento regolativo.