

**Convegno annuale del Centro interuniversitario di ricerca
CybeRights**

La riforma della governance europea della cybersicurezza

Università degli Studi di Roma Tre

20 novembre 2026

Call for participation

La cybersicurezza è ormai elemento strutturale della sovranità e dell'autonomia strategica europea.

Negli ultimi anni, l'Unione Europea ha sviluppato un quadro normativo di straordinaria complessità e portata: dalla Direttiva NIS2 al Cyber Resilience Act, dal regolamento sulla cybersicurezza al DORA, dal Data Act al CER (Critical Entities Resilience), fino alla nascente strategia coordinata della difesa nello spazio cyber. Questa architettura normativa non rappresenta soltanto l'evoluzione tecnica e procedurale di una “policy of projects”, ma segna una transizione verso una vera “policy of systems”, dove la gestione della cybersicurezza diventa intrinsecamente legata all'equilibrio fra sicurezza, diritti fondamentali e logiche di mercato, al coordinamento multilivello fra istituzioni europee e nazionali, e alla cooperazione pubblico-privato.

La riforma della governance europea della cybersicurezza incide profondamente su molteplici questioni fondamentali: il ripensamento dei poteri e delle funzioni delle autorità competenti (ENISA, Autorità Competenti Nazionali, agenzie settoriali); la ridefinizione delle responsabilità degli operatori economici e dei fornitori di servizi digitali;

l'equilibrio fra sovranità digitale nazionale e integrazione europea; il ruolo delle tecniche di gestione del rischio e dei meccanismi di cooperazione transnazionale; la compatibilità tra misure di sicurezza e protezione dei diritti dei cittadini. Il Centro CybeRights – Centro interuniversitario costituito nel quadro della Fondazione SERICS – offre una piattaforma ideale per una riflessione interdisciplinare e plurale su questi temi, valorizzando prospettive costituzionali, penali, internazionalistiche, filosofico-giuridiche, privatistiche e comparatistiche.

Il convegno intende raccogliere contributi teorici, empirici e applicativi che, a partire dalle diverse aree disciplinari del Centro, siano in grado di: (i) ricostruire l'architettura multilivello della governance europea della cybersicurezza e i meccanismi di coordinamento fra gli attori; (ii) valutare l'impatto della trasformazione normativa su diritti, doveri e responsabilità di istituzioni, operatori economici e individui; (iii) discutere strumenti sperimentali e modelli di regolazione adattiva (sandbox, osservatori, laboratori congiunti) per un governo del rischio digitale più efficace, trasparente e orientato ai diritti; (iv) proporre approcci innovativi alla formazione, al capacity-building e alla costruzione di una cittadinanza digitale resiliente.

Ambiti tematici della Call

- Profili costituzionali della governance europea della cybersicurezza, fra diritti fondamentali e controllo democratico delle autorità indipendenti;
- Cybersicurezza, Stato di diritto e separazione dei poteri, con riguardo al ruolo dei parlamenti, e delle Corti;
- Diritto penale della cybersicurezza, fra responsabilità degli operatori di servizi essenziali e fornitori di servizi digitali, misure di prevenzione e investigazioni transnazionali
- Cooperazione giudiziaria e di polizia in materia di cybercrime, strumenti UE, e-evidence, circolazione dei dati probatori e garanzie processuali

- Diritto internazionale pubblico e cyberspazio, attribuzione degli attacchi, standards of due diligence, responsabilità degli Stati e cooperazione NATO/UE
- Governance della cybersicurezza nel diritto internazionale, fra standard tecnici, supply chain globali, sanzioni, controlli sulle esportazioni e sicurezza delle infrastrutture critiche
- Rapporti interindividuali nell'ambiente digitale, profili di responsabilità e tutela *cross-border*
- Filosofia del diritto e teoria della regolazione della cybersicurezza, concetti di rischio, responsabilità, legittimazione del potere e modelli di governance policentrica
- Etica della cybersicurezza e dei dati, sicurezza-by-design, autonomia individuale e bilanciamento tra sicurezza, privacy e trasparenza
- Diritto comparato e cybersicurezza, modelli stranieri di allocazione della responsabilità per incidenti cyber, standard di diligenza e comparazione fra ordinamenti extra-UE e UE
- Diritto dell'Unione Europea e cybersicurezza, architettura normativa (NIS2, DORA, CRA, AI Act, CER, Data Act, eIDAS2, ecc.), coordinamento, sovrapposizioni e lacune
- Governance settoriale della cybersicurezza, con focus su finanza, sanità, spazio, energia, trasporti, amministrazioni pubbliche e sui modelli di supervisione e poteri delle autorità
- Cybersicurezza e spazio, coordinamento fra diritto dello spazio e normativa cyber, programmi europei (GOVSATCOM, IRIS, EUSPA-ENISA), resilienza e autonomia strategica
- Formazione, capacity-building e cultura della cybersicurezza, ruolo delle università, delle scuole e delle partnership pubblico-private nella costruzione di una cittadinanza digitale resiliente
- Tutela dei minori online: necessità e proporzionalità degli strumenti di verifica dell'età legati alle esigenze di tutela di tutti i diritti dei minori (e non) e bilanciamento tra privacy e sicurezza nel contesto del c.d. 'Chat Control'

Modalità di partecipazione e tipologie di contributo ammissibili

La Call, in linea con gli obiettivi del Centro, si rivolge ai ricercatori e alle ricercatrici interessati alle tematiche e accoglie proposte in italiano e in inglese, con l'obiettivo di favorire un confronto ampio e interdisciplinare.

In coerenza con questa impostazione, saranno ammesse due diverse modalità di partecipazione.

Prima modalità

Entro il 15 settembre 2026, sarà possibile inviare **brevi contributi scritti**, destinati al “Simposio Virtuale di CyberRights”, da pubblicare sul [sito](#) nella forma di blog post.

Tali contributi dovranno inserirsi negli ambiti tematici della Call e avere funzione di avvio e orientamento della discussione scientifica. I contributi devono contenere un minimo di 1200 e un massimo di 1500 parole. Per i riferimenti bibliografici è necessario utilizzare i collegamenti ipertestuali direttamente nel testo.

La selezione dei contributi proposti avverrà entro il 30 settembre 2026 e, a partire dal 1° ottobre 2026, saranno pubblicati sul Blog CyberRights con cadenza periodica.

Seconda modalità

Entro il 31 ottobre 2026, sarà possibile inviare **poster** oppure **brevi video**, sempre in italiano o in inglese, dedicati ai temi del Convegno.

Tali materiali dovranno essere concepiti come strumenti sintetici ed efficaci di comunicazione della ricerca, idonei a presentare in forma chiara una tesi, una domanda di ricerca, un caso di studio o una proposta interpretativa.

I poster o video proposti saranno selezionati entro il 10 novembre 2026. Determinati autori e autrici, a loro volta selezionati dal Comitato scientifico, saranno invitati a presentarli in sessione plenaria nella forma di “*lightning talks*”: ogni candidata/o avrà a disposizione cinque minuti di tempo per illustrare i risultati principali della propria ricerca.

Tutti gli altri poster ammessi troveranno comunque spazio all'interno del Convegno, secondo modalità espositive che saranno successivamente comunicate, così da garantire un'effettiva valorizzazione dell'insieme dei contributi ricevuti.

Tutti i materiali dovranno esser inviati all'indirizzo **cyberights(at)cyberights.unifi.it** indicando nell'oggetto la modalità di partecipazione e il titolo del contributo.

Pubblicazione post Convegno

È inoltre prevista, a valle del Convegno, la pubblicazione di una **special issue** o di una **raccolta di atti**, dedicata ai temi emersi nel corso dei lavori.

La special issue o la raccolta di atti prevederanno la pubblicazione di una versione estesa dei contributi presentati tramite blog, poster/video e *lightning talks*. Le indicazioni per predisporre la versione estesa verranno condivise tramite apposita comunicazione dopo il Convegno.

La sede editoriale della pubblicazione verrà individuata preferibilmente in una rivista italiana o internazionale.

Comitato scientifico del Convegno

Andrea Simoncini, Alessandro Armando, Raffaella Brighi, Carlo Colapietro, Gianmario Demuro, Antonio Iannuzzi, Erik Longo, Gaetana Morgante, Giovanni Maria Riccio, Giuseppe Verde, Francesca C. Villata

Riferimenti e contatti

<https://www.cyberights.unifi.it/>
[cyberights\(at\)cyberights.unifi.it](mailto:cyberights(at)cyberights.unifi.it)