



Denominazione	Diritto e cybersecurity
Moduli componenti	
Settore scientifico-disciplinare	GIUR-01/A; GIUR-14/A
Anno di corso e semestre di erogazione	5° anno, 2° semestre
Lingua di insegnamento	italiano
Carico didattico in crediti formativi universitari	8 CFU
Numero di ore di attività didattica assistita	56 ore: (48 ore – didattica erogativa; 8 ore – didattica interattiva)
Docente	Prof. Francesco Ricci (responsabile dell'insegnamento, 3 CFU); Prof. Donato Maria Matera (3 CFU); Prof. Massimiliano Lanzi (2 CFU)
Risultati di apprendimento specifici	● Conoscenza e capacità di comprensione Alla fine del corso gli studenti avranno acquisito una conoscenza approfondita dei problemi giuridici in materia di sicurezza informatica, in particolare del quadro regolatorio europeo e nazionale della cybersecurity, della protezione dei dati personali nel contesto digitale, della disciplina giuridica dei beni digitali e della loro circolazione, nonché dei profili di responsabilità civile e penale connessi all'uso di sistemi informatici e di intelligenza artificiale. ● Capacità di applicare conoscenza e comprensione Alla fine del corso gli studenti saranno in grado di analizzare autonomamente fattispecie concrete di rischio informatico, di individuare le misure giuridiche e organizzative adeguate alla gestione del rischio cyber, di valutare la conformità di sistemi e processi digitali alle normative vigenti e di selezionare i rimedi applicabili in caso di violazione degli obblighi di sicurezza o di lesione dei diritti connessi ai beni digitali. ● Autonomia di giudizio Alla fine del corso gli studenti saranno in grado di compiere scelte autonome e consapevoli in ordine alle misure di sicurezza giuridicamente adeguate, di valutare criticamente le implicazioni normative delle scelte tecnologiche adottate e di orientarsi tra le diverse opzioni di tutela disponibili in caso di incidente informatico, data breach o uso illecito di sistemi di intelligenza artificiale. ● Abilità comunicativa Alla fine del corso gli studenti saranno in grado di esporre con chiarezza e rigore i meccanismi di funzionamento del quadro regolatorio della



	cybersecurity, di illustrare le ragioni delle scelte normative e delle soluzioni interpretative adottate in materia, nonché di fare luce sui principali problemi applicativi connessi alla gestione del rischio informatico e alla tutela dei diritti nel contesto digitale.
Programma	Il corso di Diritto e Cybersecurity ha per oggetto il quadro giuridico della sicurezza informatica inteso come l'insieme delle discipline che le fonti europee, nazionali ed extrastatali dispongono con riguardo ai seguenti argomenti: a) Il quadro regolatorio della cybersecurity: nozioni fondamentali e interessi protetti; fonti europee e nazionali: Cybersecurity Act, NIS 2, Cyber Resilience Act, DORA, legge 90/2024; ACN e perimetro di sicurezza nazionale cibernetica [Ricci]; b) Cybersecurity e protezione dei dati personali: principi di integrità, riservatezza e accountability nel GDPR; misure tecniche e organizzative adeguate; ruoli e responsabilità; il data breach [Ricci]; c) Cybersecurity e Intelligenza Artificiale: requisiti di robustezza, accuratezza e cybersicurezza dei sistemi ad alto rischio nell'AI Act; disciplina nazionale; valore giuridico dei principi etici; IA generativa come strumento e come bersaglio di attacchi [Ricci]; d) Contrattazione algoritmica, smart contract e blockchain: automazione, volontà e imputazione degli effetti; sicurezza dei registri distribuiti; patologie e rimedi [Ricci]; e) Identità digitale, documento informatico e firme elettroniche: eIDAS e eIDAS 2; wallet europeo di identità digitale; valore giuridico e probatorio del documento informatico; furto di identità e uso abusivo di credenziali [Ricci]; f) I beni digitali: qualificazione giuridica delle risorse digitali; controllo, circolazione e tutele; possesso e spossessamento digitale; blockchain e trasferimento di token [Matera]; g) La patrimonializzazione dei dati personali e i profili successori delle risorse digitali; conflitti sui beni digitali e casistica giurisprudenziale [Matera]; h) Intelligenza artificiale e responsabilità civile: responsabilità da insicurezza informatica; danno da data breach; responsabilità del produttore di software; responsabilità delle piattaforme; assicurazione del rischio cyber [Matera]; i) La tutela penale dei sistemi e delle infrastrutture digitali: reati informatici; ransomware e frontiere penali del Dark Web [Lanzi]; j) Intelligenza artificiale e responsabilità penale: nuove fattispecie introdotte con la L. 132/2025; deepfake e aggravante dell'IA [Lanzi]; k) Nuove frontiere della responsabilità colposa nell'uso lecito di sistemi di IA: self-driving car e robot medicali [Lanzi].
Tipologie di attività didattiche previste e relative modalità di svolgimento	L'insegnamento sarà strutturato in lezioni di didattica frontale e in attività di didattica interattiva. L'attività didattica sarà dunque caratterizzata da lezioni teoriche e da esercitazioni che avranno ad oggetto l'approfondimento di singoli istituti, attraverso l'analisi di casi pratici. Ai fini della Didattica Interattiva (DI) saranno svolte n. 3 esercitazioni, due da 3 ore ed una da 2 ore (in distance). Le lezioni di Didattica interattiva (DI) saranno svolte dal Prof. Francesco Ricci e/o dal Prof. Massimiliano Lanzi e/o dal Prof.



	Donato Maria Matera e/o dal Dott. Carlo Moretti, secondo le modalità che verranno comunicate a lezione e sulla piattaforma "Google Classroom". Oltre alle lezioni di didattica frontale ed interattiva, gli studenti potranno accedere ad attività di tutoraggio con cadenza settimanale finalizzato a dare loro supporto nell'apprendimento e nell'autovalutazione della propria preparazione.
Metodi e criteri di valutazione dell'apprendimento	L'esame finale consiste in un colloquio orale della durata di circa 20 minuti (fatta salva la possibilità di concedere un tempo maggiore a favore dello studente) volto a verificare il conseguimento degli obiettivi del corso e la conoscenza dei temi oggetto del programma.
Criteri di misurazione dell'apprendimento e di attribuzione del voto finale	La valutazione dell'apprendimento prevede l'attribuzione di un voto finale espresso in trentesimi. Il voto finale deriva dalla valutazione complessiva della prova e risulta dalla verifica del livello dei risultati di apprendimento raggiunti. La risposta ad ogni domanda sarà calcolata in trentesimi ed il voto finale sarà individuato in base alla media aritmetica dei voti assegnati a ciascuna risposta.
Propedeuticità	Diritto privato 1; Diritto Privato 2; Diritto Penale
Materiale didattico utilizzato e materiale didattico consigliato	• (a cura di Ranieri Razzante), Manuale di cybersicurezza, 2ª ed., Pacini Giuridica, 2026 • Il programma deve essere integrato con le seguenti letture, disponibili sulla piattaforma Google Classroom: F. Ricci, Le clausole vessatorie nei contratti online, in Contratto e Impresa Europa, 2014; F. Ricci, Le nuove scritture nell'era del documento informatico, in Liber Amicorum per Giuseppe Vettori, 2022; F. Ricci, Smart Contract e autonomia privata, in Rivista di Diritto Privato, 2025; M. Lanzi, Uso di strumenti a intelligenza artificiale e imputazione della responsabilità penale: difficoltà ricostruttive e prospettive di intervento, in Diritto di difesa, 2024; B. Fragasso, Profili penalistici della legge sull'intelligenza artificiale: osservazioni a prima lettura, in Sistema penale, 2025. • Lo studio deve essere integrato con la consultazione dei testi normativi considerati durante il corso, i quali si possono scaricare dai seguenti siti Internet: - https://www.normattiva.it - https://eur-lex.europa.eu/advanced-search-form.html