Insegnamento	Cybersecurity e protezione dei dati
Livello e corso di studio	Corso di laurea magistrale in giurista d'impresa
Settore scientifico disciplinare (SSD)	IUS 01
Anno accademico	*2021-2022*
Anno di corso	
Numero totale di crediti	8
Propedeuticità	Non presente
Docente	Fabio Di Resta Facoltà: Giurisprudenza Nickname: fabio.diresta Email: fabio.diresta@unicusano.it Orario di ricevimento: Consultare il calendario alla pagina seguente del nostro sito verificando gli orari di Videoconferenza http://www.unicusano.it/calendario-lezioni-in-presenza/calendario-area-ingegneristica
Presentazione	Il corso in Cybersecurity e protezione dei dati è suddiviso in due macroaree, la prima riferita alla Cybersecurity, si articola in tredici lezioni nelle quali verranno descritti gli elementi fondamentali della materia con numerosi casi di studio in modo che lo studente possa immediatamente cimentarsi con le fattispecie pratiche. La prime lezioni esamineranno gli elementi definitori della Cybersercurity, seguiranno alcune lezioni sulle nozioni tecniche e sugli istituti giuridici coinvolti nella trattazione della materia. Durante il corso verranno pertanto esaminate le fonti normative europee e nazionali nonchè i principi e i criteri che caratterizzano la materia della Cybersecurity. In tale contesto, si analizzeranno le principali differenze e le analogie con la diversa materia della protezione dei dati personali, tenendo in conto dello scopo, del metodo adottato dal legislatore e delle diverse fonti normative secondo i corrispondenti livelli di gerarchia delle stesse, internazionali, europee e nazionali. La seconda macroarea è riferita invece al quadro normativo sulla protezione dei dati personali, dalle fonti internazionali, alle fonti del diritto europeo alle fonti normative nazionali. In tale contesto, saranno previste ventiquattro lezioni, anche in questo caso i numerosi casi di studio presentati forniscono allo studente la possibilità di applicare la fattispecie astratta della disposizione normativa alla fattispecie concreta. Le prime lezioni introduttive illustreranno le nozioni fondamentali della materia per successivamente concentrarsi sui principi e criteri della protezione dei dati personali. Le successive lezioni in materia di protezione dei dati affronteranno gli adempimenti e le responsabilità di varia natura, civile e amministrativa, connesse all'omessa adozione degli stessi e con riferimento al pregiudizio per i diritti e le libertà fondamentali degli interessati.
Obiettivi formativi	Il corso in Cybersecurity e protezione dei dati ha i seguenti obiettivi formativi: 1. Rivedere le basi della cybersecurity e della protezione dei dati personali 2. Illustrare i principi e criteri principali della cybersecurity 3. Illustrare i principi e criteri principali della protezione dei dati personali 4. Illustrare casi di studio sia ambito di Cybersecurity che in ambito protezione dei dati personali 5. Trasferire allo studente una abilità di analisi delle fattispecie concrete relativamente all'ambito delle due discipline trattate
Prerequisiti	Non sono previste propedeuticità per l'insegnamento.
Risultati di apprendimento attesi	**Conoscenza e capacità di comprensione** Lo studente al termine del Corso avrà dimostrato di conoscere gli argomenti di Cybersecurity e di protezione dei dati personali, ed avrà acquisito la capacità di analisi degli stessi. Inoltre, lo studente acquisirà la conoscenza del quadro normativo dell'insegnamento, inclusi, l'analisi del rischio di impatto sulle reti e sui sistemi informativi in ambito di cybersecurity e ambito di rischi inerenti al trattamento dei dati personali, i soggetti passivi degli obblighi previsti dalle normative applicabili, le responsabilità giuridiche relative. **Applicazione delle conoscenze**

	Lo studente sarà in grado di utilizzare la conoscenza delle due discipline trattate durante le lezioni; sarà inoltre, in grado di analizzare alcune fattispecie concrete di incidenti di sicurezza sia ambito di cybersecurity che in quello della protezione dei dati, individuando i requisiti normativi applicabili sia in termini preventivi, come per esempio, i requisiti dalla data protezione *protection by design* e la *cybersecurity by design*. **Capacità di trarre conclusioni** Lo studente sarà in grado di individuare i soggetti passivi degli obblighi normativi: il titolare del trattamento, il contitolare del trattamento, i responsabili del trattamento, anche con riguardo all'organizzazione interna del soggetto con riferimento agli autorizzati e ai designati al trattamento dei dati. Per quanto concerne la cybersecurity, lo studente sarà in grado di comprende la rilevanza del rischio relativo all'impatto sulle reti ed ai sistemi informativi e la rilevanza di individuare le misure di sicurezza volte alla mitigazione del rischio connesso all'impatto sulle reti e i sistemi informativi con riguardo particolare al settore bancario e/o finanziario. **Abilità comunicative** Lo studente sarà in grado di descrivere e sostenere conversazioni su questioni di cybersecurity e in particolare su problematiche teorico-pratiche sulla protezione dei dati personali. **Capacità di apprendere** Lo studente al termine del Corso avrà conoscenza delle nozioni fondamentali necessarie per comprendere da una parte i rischi inerenti alle informazioni gestite con riguardo al rischio di impatto sulle infrastrutture critiche e connesse alle funzioni essenziali dello Stato e dall'altra, in termini di protezione dei dati, la tutela dei diritti e delle libertà fondamentali degli interessati che in concreto si atteggiano anche come diritto al controllo dei propri dati personali sia nella forma dei diritti di accesso, nel diritto all'esattezza dei dati, nel diritto all'integrità dei dati, alla portabilità degli stessi ed infine ad opporsi ai trattamenti dei propri dati quando questi trattamenti diventano illegittimi.
Organizzazione dell'insegnamento	Il corso è sviluppato attraverso le **lezioni preregistrate audio-video** che compongono, insieme a slide e dispense, i materiali di studio disponibili in piattaforma. In particolare, il Corso di Cybersecurity e protezione dei dati prevede 8 Crediti formativi. Il carico totale di studio per questo modulo di insegnamento è di circa 200 ore così suddivise in: **circa 160/180** ore per la visualizzazione e lo studio del materiale videoregistrato (20 Ore videoregistrate di Teoria e analisi di casi di studio presentate durante la lezione). **Circa 10/20 ore di Didattica Interattiva** nella forma di video-ricevimenti e messaggi tramite la piattaforma telematica. Si consiglia di distribuire lo studio della materia uniformemente in un periodo di 10 settimane dedicando tra le 15 alle 20 ore di studio a settimana
Contenuti del corso	**Modulo 1 – Parte sulla Cybersecurity** Tredici lezioni teorico pratiche videoregistrate e interattive per un impegno pari al 30% del totale di ore previste dall'insegnamento: Analisi dei concetti fondamentali sulla Cybersecurity e la protezione dei dati personali - Inquadramento storico della cybersecurity: dai conflitti del XX secolo alla *cyberwar* - Analisi del rischio in ambito cybersecurity e la rilevanza del settore bancario - Analisi degli elementi delle cybersecurity: il web, internet e la nozione di RID - La Cybersecurity nel contesto non giuridico e nel giuridico - la protezione dei dati - Schema di analisi in ambito protezione dei dati: i sei quesiti sulla protezione dei dati - aspetti strettamente connessi della cybersecurity - Lezione su Cybersecurity e protezione dei dati: il Cybersecurity Act, ENISA e ACN - Lezione su Cybersecurity e la protezione dei dati: pandemia e cybersecurity: rischi connessi alla pandemia e l'approccio proattivo - La cybersecurity e la protezione dei dati: il *contact tracing* (CT), aspetti di cybersecurity e protezione dei dati - Lezione su cybersecurity e protezione dei dati: analisi del quadro normativo sui servizi di pagamento: normativa tecnica e autenticazione forte - Analisi dei crimini informatici: frode informatica e aggravante della frode, accesso abusivo al sistema informatico - Analisi della violazione dei dati (incidenti di sicurezza in ambito protezione dei dati personali, c.d. *Data Breach*): presupposti e adempimenti connessi previsti dal GDPR - Lezione Cybersecurity e protezione dei dati: servizi: recepimento. NIS e Perimetro di sicurezza nazionale - Analisi legale dei crimini informatici: le frodi telematiche/informatiche e l'aggravante della frode informatica, l'accesso abusivo al sistema informatico – il d.lgs. 11/2010 sui servizi di pagamento e le responsabilità degli intermediari (Istituti di credito e prestatori di servizi di pagamento). **Modulo 2 – Parte sulla Protezione dei dati personali** Ventiquattro lezioni teorico pratiche videoregistrate e interattive per un impegno del 70% del totale di ore previste dall'insegnamento: Analisi del quadro normativo complessivo sulla protezione dei dati personali - Scopo e ambito applicativo della normativa sulla protezione dei dati personali -Principi applicabili sulla protezione dei dati personali: principi applicabili al trattamento dei dati - Principi di liceità sulla protezione dei dati personali - Analisi dei requisiti del consenso sulla protezione dei dati personali: articolo 7 del GDPR - Analisi delle garanzie del GDPR per il trattamento di categorie particolari dei dati personali - Seconda parte della lezione sulle garanzie previste dal GDPR in materia di trattamento di categorie particolari di dati personali - Garanzie in ambito di trattamento dei dati giudiziari - Lezione sul livello di sicurezza adeguato al rischio inerente al trattamento dei dati:

	valutazione del rischio e criterio di efficacia delle misure di sicurezza nel quadro delle responsabilità generali del trattamento dei dati personali - Il principi della data protezione *protection by design* e *by default* - le responsabilità generali del titolare del trattamento dei dati personali - nozione di rischio di pregiudizio sui diritti e libertà fondamentali in termini di gravità dell'evento - Analisi della autonoma titolarità del trattamento e le responsabilità generali dello stesso: i soggetti passivi degli obblighi previsti dal GDPR - L'accordo sulla protezione dei dati personali, il responsabile del trattamento, ambito applicativo, presupposti, distribuzione dei compiti e responsabilità – L'articolo 28 GDPR, analisi degli elementi del contratto sulla protezione dei dati personali (approfondimento sul ruolo del responsabile della trattamento dei dati) - Aspetti connessi alle responsabilità amministrativa solidali delle figure che occupano una posizione apicale - L'organizzazione sulla protezione dei dati all'interno del titolare del trattamento: distribuzione dei compiti e responsabilità tra gli autorizzati al trattamento e i designati al trattamento (art. 29 GDPR e art. 2 *quaterdecies* del Codice della Privacy) - L'esercizio dei diritti degli interessati: diritto di accesso ai dati e gamma dei diritti dell'interessato, dal diritto all'esattezza, all'integrità, all'aggiornamento, all'opposizione dei dati, alla portabilità dei dati – La tutela giurisdizionale nell'ambito della protezione dei dati personali: il risarcimento del danno e la violazione dei diritti e libertà fondamentali - Analisi critica della richiesta di risarcimento del danno da trattamento illecito dei dati, danni materiali e immateriali, il nesso causale - Analisi del consenso al trattamento: ambito applicativo e presupposti, cenni sul consenso del minore - Analisi del consenso al trattamento e del consenso del minore di età nella società dell'informazione - La prestazione del consenso del minore articolo 2 quinquies del codice della privacy - Analisi dei rischi e Valutazione di Impatto - Lezione sul Responsabile della protezione dei dati (Data Protection Officer - DPO) - Lezione sul Responsabile della protezione dei dati: analisi dell'obbligatorietà della designazione del DPO.
Materiali di studio	MATERIALI DIDATTICI A CURA DEL DOCENTE Il materiale didattico presente in piattaforma è suddiviso in due macroaree articolate rispettivamente in n. 13 moduli per la cybersecurity e in n. 24 moduli per la protezione dei dati personali. Essi ricoprono interamente il programma e ciascuno di essi contiene dispense, slide e videolezioni. Tale materiale contiene tutti gli elementi necessari per affrontare lo studio della materia. Testi consigliati: F. Di Resta, "P*rivacy, protezione dei dati e cybersecurity*", ed. Duepuntozero, 2021; I.Corradini e F. Di Resta, "C*ybersecurity, digital forensics e data protection*", ed. Themis, 2021.
Modalità di verifica dell'apprendimento	L'esame consisterà di norma nello svolgimento di una prova scritta e/o nel sostenimento di una orale (modalità di verifica che può essere svolta presso la sede centrale di Roma) tendente ad accertare le capacità di analisi, la proprietà di linguaggio e la capacità di rielaborazione dei concetti acquisiti. La prova scritta prevede domande a risposta multipla (di natura teorica e/o applicativa) che riguardano l'intero programma dell'insegnamento. Alle domande a risposta multipla relative ai contenuti del programma d'esame viene attribuito il valore congruo di punti per risposta corretta. In alternativa. La prova orale consiste in un colloquio teso ad accertare il livello di preparazione dello studente. Quest'ultimo normalmente si snoda in 3 domande (di natura teorica e/o applicativa) che riguardano l'intero programma dell'insegnamento. In ambedue le modalità d'esame, particolare attenzione nella valutazione delle risposte viene data alla capacità dello studente di rielaborare, applicare e presentare con proprietà di linguaggio il materiale presente in piattaforma.
Criteri per l'assegnazione dell'elaborato finale	L'assegnazione dell'**elaborato finale** avverrà sulla base di un colloquio con il docente in cui lo studente manifesterà i propri specifici **interessi** in relazione a qualche argomento che intende approfondire; non esistono **preclusioni** alla richiesta di assegnazione della tesi e non è prevista una **media particolare** per poterla richiedere.