PROGRAMMA DEL CORSO DI LABORATORIO TECNOLOGIE DIGITALI E CYBER SICUREZZA

SETTORE SCIENTIFICO

NN

CFU

6

ATTIVITÀ DI DIDATTICA INTERATTIVA (DI)

Le attività di Didattica Interattiva (TEL-DI) consistono, per ciascun CFU, in 2 ore erogate in modalità sincrona su piattaforma Class, svolte dal docente anche con il supporto del tutor disciplinare, e dedicate a una o più tra le seguenti tipologie di attività:

- sessioni live, in cui il docente guida attività applicative, stimolando la riflessione critica e il confronto diretto con gli studenti tramite domande in tempo reale e discussioni collaborative;
- webinar interattivi, arricchiti da sondaggi e domande dal vivo, per favorire il coinvolgimento attivo e la co-costruzione della conoscenza;
- lavori di gruppo e discussioni in tempo reale, organizzati attraverso strumenti collaborativi come le breakout rooms, per sviluppare strategie di problem solving e il lavoro in team;
- laboratori virtuali collettivi, in cui il docente guida esperimenti, attività pratiche o l'analisi di casi di studio, rendendo l'apprendimento un'esperienza concreta e partecipativa.

Tali attività potranno essere eventualmente supportate da strumenti asincroni di interazione come per esempio:

- forum;
- wiki;
- quiz;
- glossario.

Si prevede l'organizzazione di almeno due edizioni di didattica interattiva sincrona nel corso dell'anno accademico.

MODALITÀ DI VERIFICA DELL'APPRENDIMENTO

L’esame può essere sostenuto sia in forma scritta che in forma orale. L’esame orale consiste in un colloquio con la Commissione sui contenuti dell’insegnamento. L’esame in forma scritta consiste nello svolgimento di un test composto da 31 domande. Per ogni domanda lo studente deve scegliere una delle 4 possibili risposte. Solo una risposta è corretta e, in caso di risposte errate o mancanti, non sarà attribuita alcuna penalità. Rispondendo correttamente a tutte le 31 domande, si conseguirà la lode.

Oltre alla prova d’esame finale, il percorso prevede attività di didattica interattiva sincrona e prove intermedie che consentono alle studentesse e agli studenti di monitorare il proprio apprendimento, attraverso momenti di verifica progressiva e consolidamento delle conoscenze.

La partecipazione alle attività di didattica interattiva sincrona consente di maturare una premialità fino a 2 punti sul voto finale, attribuiti in funzione della qualità della partecipazione alle attività e dell’esito delle prove.

Per accedere alle prove intermedie è necessario aver seguito almeno il 50% di ogni ora di didattica interattiva.

Le prove intermedie possono consistere in un test di fine lezione o nella predisposizione di un elaborato. Le prove intermedie si considerano superate avendo risposto correttamente ad almeno l’80% delle domande di fine lezione. In caso di prove intermedie che prevedano la redazione di un elaborato, il superamento delle stesse ai fini della premialità sarà giudicata dal docente titolare dell’insegnamento.

I punti di premialità, previsti per le prove intermedie, sono sommati al voto finale d’esame solo se la prova d’esame è superata con un punteggio pari ad almeno 18/30 e possono contribuire al conseguimento della lode.

Le modalità d’esame descritte sono progettate per valutare il grado di comprensione delle nozioni teoriche e la capacità di applicazione delle stesse e consentiranno di valutare il livello di competenza e l’autonomia di giudizio maturati dalla studentessa e dallo studente. Le abilità di comunicazione e la capacità di apprendimento saranno valutate anche attraverso le interazioni dirette che avranno luogo durante la fruizione dell’insegnamento.

OBBLIGO DI FREQUENZA

A studentesse e studenti viene richiesto di partecipare ad almeno il 70% dell’attività di didattica erogativa (70% della TEL-DE).

TESTI CONSIGLIATI

I testi consigliati sono i seguenti:

Faini F. – Pietropaoli S., Scienza giuridica e tecnologie informatiche. Temi e problemi, 2° ed., Giappichelli, Torino, 2021;

Pietropaoli S., Informatica criminale. Diritto e sicurezza nell'era digitale. Aggiornata alla legge 90/2024 e alla direttiva NIS2, seconda edizione, Giappichelli, Torino, 2025.

I testi sono disponibili nella sezione “Biblioteca”.

OBIETTIVI FORMATIVI PER IL RAGGIUNGIMENTO DEI RISULTATI DI APPRENDIMENTO PREVISTI NELLA SCHEDA SUA

L’insegnamento è teso ad analizzare il rapporto tra diritto, tecnologie digitali e cyber sicurezza, gli aspetti giuridici e i profili legali dell’innovazione e della trasformazione digitale, l’impatto delle tecnologie digitali sui diversi aspetti relativi alla società e all’ordinamento giuridico, alla persona e ai suoi diritti, agli istituti e agli strumenti del giurista.

Nel corso sono affrontate tematiche significative dell’informatica giuridica, del diritto digitale, del diritto dell’informatica e delle nuove tecnologie e, in particolare, sono esaminate tecnologie digitali particolarmente rilevanti e profili giuridici della cybersecurity, avvalendosi dell’analisi di significativi casi di studio. In specifico, l’insegnamento si propone l’obiettivo di fornire conoscenze in merito al diritto della società digitale, alla luce dell’evoluzione normativa, giurisprudenziale e dottrinale, nazionale e sovranazionale. Il corso permette di acquisire conoscenze giuridiche e strumenti interpretativi in merito alla disciplina e alle problematiche relative all’utilizzo delle tecnologie digitali e ai profili della cyber sicurezza, attraverso lo studio delle fonti e degli aspetti maggiormente rilevanti sotto la lente giuridica. Al termine del corso di insegnamento, lo studente sarà in grado di raggiungere i seguenti risultati: acquisire le basi di una cultura informatico-giuridica, conoscere gli elementi fondamentali e i principali strumenti che caratterizzano il diritto digitale, comprendere e analizzare le implicazioni giuridiche, filosofiche, etiche e sociali delle tecnologie digitali e della cybersecurity, acquisendo consapevolezza in merito alle opportunità e ai rischi e in relazione alla necessità di bilanciamento tra interessi e diritti diversi; acquisire capacità di orientamento ed attitudine ad affrontare le principali questioni giuridiche della società tecnologica e gli aspetti filosofici, etici e giuridici relativi alle tecnologie digitali e alla cybersecurity; analizzare fattispecie concrete e risolvere problematiche specifiche, applicando le conoscenze e le capacità acquisite e adoperando un linguaggio tecnico-giuridico appropriato.

RISULTATI DI APPRENDIMENTO ATTESI

Conoscenza e capacità di comprensione
Lo studente acquisirà conoscenze in merito all’informatica giuridica e al diritto della società digitale, alla luce dell’evoluzione normativa, giurisprudenziale e dottrinale, nazionale e sovranazionale. Lo studente acquisirà conoscenze giuridiche e strumenti interpretativi in merito alla disciplina e alle problematiche relative all’utilizzo delle tecnologie digitali e ai profili giuridici della cybersecurity, attraverso lo studio delle fonti e degli aspetti maggiormente rilevanti sotto la lente giuridica.

Capacità di applicare conoscenza e comprensione
Al termine del corso, che si avvarrà anche dell’analisi di significativi casi di studio, lo studente acquisirà capacità di orientamento ed attitudine ad affrontare le principali questioni giuridiche della società tecnologica e gli aspetti filosofici, etici e giuridici della dimensione digitale. Lo studente sarà in grado di analizzare fattispecie concrete e risolvere problematiche specifiche relative al diritto digitale e all’informatica giuridica.

Autonomia di giudizio
Lo studente sarà capace di esaminare questioni, analizzare fattispecie e risolvere problematiche relative al diritto digitale e all’informatica giuridica, dimostrando capacità di ragionamento, analisi ed argomentazione, sviluppando spirito critico e mostrando abilità nel risolvere problemi concreti.

Abilità comunicative
Al termine del corso lo studente sarà capace di trattare in modo chiaro, corretto, pertinente ed esaustivo gli argomenti, le questioni e le problematiche relative al diritto digitale e all’informatica giuridica, adoperando il linguaggio tecnico-giuridico appropriato e mostrando capacità di orientarsi e di effettuare collegamenti concettuali.

Capacità di apprendimento
Lo studente acquisirà le basi di una cultura informatico-giuridica, conoscerà gli elementi fondamentali e i principali strumenti che caratterizzano il diritto digitale e sarà in grado di comprendere e analizzare le implicazioni giuridiche, filosofiche, etiche e sociali delle tecnologie digitali e della cybersecurity, acquisendo consapevolezza in merito alle opportunità e ai rischi e in relazione alla necessità di bilanciamento tra interessi e diritti diversi.

PROGRAMMA DIDATTICO: ELENCO VIDEOLEZIONI/MODULI

L'insegnamento è teso ad esaminare la relazione tra diritto, tecnologie digitali e cyber sicurezza e, in specifico, l'impatto delle tecnologie digitali sui diversi aspetti relativi alla società nel suo complesso, alla persona e ai suoi diritti, agli istituti e agli strumenti del giurista. Nel corso sono affrontate tematiche significative dell'informatica giuridica, del diritto digitale, del diritto dell'informatica e delle nuove tecnologie e, in specifico, sono esaminate tecnologie digitali particolarmente rilevanti e profili giuridici della cybersecurity, avvalendosi dell'analisi di significativi casi di studio. Le tematiche spaziano dall'umanesimo tecnologico alla tutela dei diritti digitali, dalla digital governance all'intelligenza artificiale, dalla cybersecurity alla cyberwar, dal complesso bilanciamento tra interessi ai difficili equilibri in tema responsabilità dell'Internet Service Provider, dall'informatica criminale all'informatica forense.

Il programma didattico è articolato in 30 lezioni suddivise in 7 moduli.

Il corso di insegnamento è interamente tenuto dalla Prof.ssa Fernanda Faini.

Elenco dei moduli e delle videolezioni:

Modulo 1. Umanesimo tecnologico: diritto e diritti digitali – Prof.ssa Fernanda Faini

1. L'evoluzione del diritto nell'era digitale: la regolazione della società tecnologica tra hard law e soft law
2. I regolamenti europei dedicati alle tecnologie digitali
3. La Dichiarazione europea sui diritti e i principi digitali per il decennio digitale
4. Il dato personale tra protezione giuridica e valorizzazione economica
5. La giurisprudenza sulla commerciabilità dei dati personali

Modulo 2. Digital governance e digital law: governare e regolare la dimensione digitale – Prof.ssa Fernanda Faini

6. I nomi a dominio: regolazione tecnica
7. I nomi a dominio: tutela giuridica
8. Il mondo digitale nella nuvola: il cloud computing
9. Società algoritmica, sovranità digitale e piattaforme digitali
10. Capitalismo della sorveglianza: Datagate, Cambridge Analytica e il caso Trump
11. Metaverso e metaversi

Modulo 3. Intelligenza artificiale: governo degli algoritmi e tutela dei diritti – Prof.ssa Fernanda Faini

12. La natura giuridica dell'algoritmo
13. Intelligenza artificiale e regolazione europea: l'Artificial Intelligence Act (regolamento UE 2024/1689)
14. Strategia italiana per l'intelligenza artificiale

15. Artificial intelligence, bias e discriminazione algoritmica
16. Intelligenza artificiale generativa: ChatGPT tra opportunità, rischi e “allucinazioni”

Modulo 4. Cybersecurity e cyberlaw: sicurezza e diritto nella società tecnologica – Prof.ssa Fernanda Faini

17. Sicurezza informatica: cyber risk e cybersecurity
18. Il framework giuridico europeo in materia di cybersecurity
19. Norme e strategie italiane sulla sicurezza informatica
20. La governance in materia di cybersecurity
21. Cyberwar e cyberweapons: la guerra cibernetica

Modulo 5. La responsabilità giuridica dell’Internet Service Provider – Prof.ssa Fernanda Faini

22. La responsabilità dell’Internet Service Provider
23. Provider passivo e attivo
24. La giurisprudenza sulla responsabilità del provider

Modulo 6. Informatica criminale: diritto penale e tecnologie informatiche – Prof.ssa Fernanda Faini

25. Elementi di diritto penale dell’informatica: cybersecurity e cybercrimes
26. I reati informatici nell’ordinamento giuridico italiano
27. Il phishing

Modulo 7. Informatica forense e prove digitali – Prof.ssa Fernanda Faini

28. Digital forensics e digital evidence
29. Quadro normativo in materia di informatica forense
30. Il caso Garlasco

ATTIVITÀ DI DIDATTICA EROGATIVA (DE)

Le attività di Didattica Erogativa consistono, per ciascun CFU, nell'erogazione di 5 videolezioni della durata di circa 30 minuti. A ciascuna lezione sono associati:

· una dispensa (PDF) di supporto alla videolezione oppure l’indicazione di capitoli o paragrafi di un e-book di riferimento, scelto dal docente tra quelli liberamente consultabili in piattaforma da studentesse e studenti;

· un questionario a risposta multipla per l’autoverifica dell’apprendimento.

AGENDA

1

Umanesimo tecnologico e diritto digitale

23/02

8.00-9.00 (1 ora)

2

Persona, identità e diritti digitali

23/02

9.00-10.00 (1 ora)

3

Nomi a dominio e cloud computing

23/02

10.00-11.00 (1 ora)

4

Metaversi

02/03

8.00-9.00 (1 ora)

5

Intelligenza artificiale: profili giuridici

02/03

9.00-10.00 (1 ora)

6

Intelligenza artificiale generativa: opportunità e rischi

02/03

10.00-11.00 (1 ora)

7

Cybersecurity e diritto europeo

09/03

8.00-9.00 (1 ora)

8

Cybersecurity e diritto nazionale

09/03

9.00-10.00 (1 ora)

9

Cyberwar

09/03

10.00-11.00 (1 ora)

10

Responsabilità giuridica dell’Internet Service Provider

16/03

8.00-9.00 (1 ora)

11

Informatica criminale

16/03

9.00-10.00 (1 ora)

12

Informatica forense e prova digitale

16/03

10.00-11.00 (1 ora)