**DIRITTO PENALE DELL’INFORMATICA**

**IUS 17 (a.a. 2018-2019)**

**36 h. (6 crediti)**

**Dr. Roberto Flor (coordinatore: 3 crediti)**

**Dr. Ivan Salvadori (3 crediti)**

**RISULTATI DI APPRENDIMENTO ATTESI**

L’insegnamento si propone di fornire le basi concettuali, metodologiche e culturali necessarie per analizzare il diritto penale dell’informatica e mira a far comprendere le categorie dei reati informatici e cibernetici, nonché le indagini ad alto contenuto tecnologico, sviluppando la capacità di utilizzare un linguaggio corretto ed adeguato per far acquisire allo studente le competenze giuridiche sia sul piano del diritto penale sostanziale che su quello del diritto penale processuale.
Il corso affronterà anche i nuovi fenomeni di illegalità in rete e connessi alle nuove tecnologie della comunicazione, in particolare sui social network, in Internet e nel cyberspace, quali ad esempio diffamazioni on-line, frodi, in specie nei servizi di on-line banking, phishing, identity theft, violazioni della privacy, violazioni del copyright, diffusione di pornografia infantile ed adescamento di minori in rete (child-grooming), cyber-terrorism e cyber-laundering, ecc. Verranno pertanto analizzate, partendo anche da casi concreti, le norme penali di recente emanazione o comunque applicabili a tali comportamenti illeciti, che vengono ricondotti alla criminalità informatica e più di recente al nuovo concetto di cybercrime.

Trattandosi di un settore di criminalità transnazionale e globale si terrà conto delle più importanti internazionali, in specie del Consiglio d'Europa (Convenzione Cybercrime e Convenzione di Lanzarote) e dell'Unione Europea (direttive contro gli attacchi informatici, sulla lotta alla pornografia infantile, sulla tutela della proprietà intellettuale, sul commercio elettronico e la tutela dei dati personali). Speciale attenzione verrà rivolta all'esame della possibile responsabilità penale degli Internet Service Providers, oggetto di molteplici pronunce sia della Cassazione che della Corte di Giustizia dell'Unione Europea (casi Google, Yahoo, Netlog, ecc.), nonché della esigenza di disciplinare la raccolta dei dati e delle prove elettroniche che stanno assumendo sempre maggior rilievo anche per l'accertamento e la prevenzione di qualsiasi reato, pur se non strettamente informatico.

Al termine dell’insegnamento lo studente dovrà dimostrare di essere in grado di correlare adeguatamente le norme di parte generale e della parte speciale del diritto penale, di inquadrare correttamente le singole fattispecie nel contesto di riferimento, anche sovranazionale, di risolvere casi pratici attinenti ai diversi reati studiati, individuandone gli elementi costitutivi e circostanziali, le regole d’imputazione, il possibile concorso, i beni giuridici tutelati.

**PROGRAMMA**

Il corso si snoderà nelle seguenti tre parti:

1. Esame delle principali disposizioni del codice penale italiano via via introdotte per contrastare i nuovi fenomeni criminosi, anche in attuazione di convenzioni internazionali e fonti dell'Unione Europea, in particolare: frodi informatiche, danneggiamenti informatici, falsi informatici, accessi abusivi, intercettazioni di comunicazioni telematiche, violazioni della corrispondenza informatica e telematica.

2. Reati previsti dalla legislazione in materia di privacy e di proprietà intellettuale.

3. Uso illecito di Internet: in particolare diffamazioni on-line, pornografia minorile, adescamento di minori, reati sui social network, responsabilità penale degli Internet Service Providers e dei bloggers.

**MODALITÀ DIDATTICHE**

Le modalità didattiche adottate sono distinte tra studenti frequentanti e non frequentanti in ragione dell’alto tasso di variabilità della normativa di riferimento e degli orientamenti giurisprudenziali, anche delle Corti superiori.

Con riguardo agli studenti frequentanti, le modalità didattiche consistono in lezioni frontali dedicate alla trasmissione delle nozioni basilari, delle categorie-chiave e degli strumenti applicativi fondamentali; a ciò si aggiungono le esercitazioni con il supporto di pronunce giurisprudenziali particolarmente significative. Inoltre, anche grazie alla piattaforma e-learning di Ateneo, vengono proposte specifiche letture di aggiornamento e recenti pronunce giurisprudenziali. Durante tutto l’anno accademico, inoltre, lo studente potrà usufruire dell’orario di ricevimento dei docenti, negli orari indicati sulle pagine web del dipartimento.

Con riguardo agli studenti non frequentanti, le modalità didattiche consistono in un supporto del docente ad uno studio aggiornato disponibili anche mediante avvisi appositamente dedicati. Previa registrazione nel portale del dipartimento, anche lo studente non frequentante potrà usufruire della piattaforma e-learning.

**TESI CONSIGLIATI**

CADOPPI A., CANESTRARI S., MANNA A., PAPA M., Cybercrime, Utet, Torino, 2018

**MATERIALI DIDATTICI**

I materiali didattici, le *slides* delle lezioni, le indicazioni bibliografiche, ed i contributi dottrinali e giurisprudenziali utilizzati dai docenti durante il corso saranno accessibili, previa registrazione, sulla piattaforma *e-learning* di Ateneo.

Si raccomanda in ogni caso di consultare costantemente, sia lezione che nello studio individuale, il codice penale, nella edizione più recente disponibile, vista la molteplicità di riforme.

**MODALITÀ D’ESAME**

L’esame si svolge in forma orale. I frequentanti che vogliano approfondire singole tematiche concordate con i docenti durante il corso o nelle eventuali esercitazioni potranno presentare brevi tesine in sostituzione di parti del programma.
La prova orale consiste in un colloquio teso a verificare:

* Il livello di raggiungimento e acquisizione delle conoscenze e delle abilità descritte in precedenza nella sezione “Obiettivi formativi”
* La capacità critica e valutativa degli istituti oggetto di studio
* La proprietà di linguaggio anche giuridico specialistico
* L’abilità di collegare in forma sistematica, ragionata e trasversale le conoscenze acquisite
* La capacità analitica e argomentativa e l’autonomia di giudizio, anche nella risoluzione di casi pratici

La valutazione finale è espressa in 30/30, per la sufficienza occorre ottenere almeno 18/30. Il candidato che dimostrerà un livello di approfondimento e di chiarezza tali da superare lo standard di preparazione espresso dal massimo dei punti potrà ambire ad ottenere la lode.