Nono Corso di Formazione interdottorale di Diritto e Procedura Penale
"Giuliano Vassalli" per Dottorandi e Dottori di ricerca

Nuove frontiere tecnologiche e sistema penale

Sicurezza informatica, strumenti di repressione e tecniche di prevenzione

Siracusa, 29, 30 novembre, 1 dicembre 2018

La nona edizione del *Corso di Formazione interdottorale di Diritto e Procedura Penale "Giuliano Vassalli" per Dottorandi e Dottori di ricerca ricerca* è dedicata all'analisi del rapporto tra sistema penale e nuove tecnologie.

L'inarrestabile digitalizzazione di ogni forma di comunicazione e di interazione tra cittadini, attori economici, enti, istituzioni, rappresenta oggi un fattore di rischio notevole, in grado di comprimere i diritti e le libertà individuali. Il diritto penale è chiamato quindi a confrontarsi sempre più spesso con nuove forme e strumenti di aggressione, che rendono opportuno, a seconda dei casi, che le categorie dogmatiche tradizionali siano riadattate o che il legislatore intervenga a modificare il quadro normativo vigente. Analoghe esigenze si pongono sul versante processuale, atteso che l'evoluzione tecnologica continua a mettere a disposizione dell'accertamento penale (per qualunque tipo di reato) strumenti investigativi estremamente efficaci, ma altamente intrusivi della sfera di libertà individuale.

La tematica in oggetto pone, dunque, interrogativi di assoluta rilevanza nell'ambito penalistico e processualpenalistico.

Alcune questioni derivano dalla progressiva estensione di beni giuridici "tradizionali", che dà luogo, nella moderna società dell'informazione, a nuove esigenze di tutela e correlati diritti. Basti pensare al passaggio dal diritto all'immagine alla *digital identity*, dalla riservatezza alla *digital privacy*, dalla libertà d'informazione al *right to internet access*, dal domicilio fisico a spazi digitali o *cyberspace* di espansione della personalità dell'individuo.

Altre, ugualmente complesse, originano dai connotati peculiari del cyberspazio, privo di confini fisici e di limiti geografici (c.d. aterritorialità), atemporale e immateriale: fattori che forniscono formidabili strumenti, grazie anche alle opportunità di anonimato, per commettere o agevolare la commissione di reati.

Il contrasto alla criminalità informatica è reso inoltre particolarmente difficile dalla continua "metamorfosi" delle tecniche di attacco e delle modalità di offesa. Talune di esse sono realizzate mediante l'impiego di ritrovati tecnologici d'avanguardia, altre utilizzano le risorse ampiamente accessibili sul *web*, quali siti internet, *social network*, *forum* di discussione.

In entrambi i casi, i criminali informatici riescono a sfruttare appieno le potenzialità della rete sia come veicolo di informazione sia come luogo di scambio di beni e servizi.

Sul primo piano si pone il problema di bilanciare la libertà di espressione in rete con l'esigenza di salvaguardia di beni quali ad esempio l'ordine pubblico e la reputazione individuale. In tempi recenti il tema è tornato al centro del dibattito con riferimento alle attività di propaganda terroristica ed eversiva, ai "discorsi" di radicalizzazione e indottrinamento religioso o di incitamento all'odio.

Sul secondo piano si registra una preoccupante trasmigrazione di interi settori della criminalità economico-finanziaria verso lo spazio virtuale. Basti pensare al crescente utilizzo delle valute virtuali che apre le porte a nuove forme di riciclaggio totalmente digitale, all'allestimento di imponenti piattaforme di *e-commerce* per la vendita di beni intrinsecamente illeciti, che si affiancano al *phishing* e alle tradizionali frodi informatiche.

L'uso di strumenti digitali rappresenta anche la fonte di nuovi rischi per la *privacy* degli individui, che si concretizzano nella perdita di controllo sulla circolazione dei propri dati personali e in forme di captazione illecita degli stessi. Su questo fronte il Regolamento generale sulla protezione dei dati personali ed il c.d. "pacchetto privacy" europeo, anche grazie al ruolo propulsore della Corte di Giustizia, hanno aperto una nuova frontiera, imponendo al legislatore interno e agli

operatori del diritto in genere di confrontarsi con la trama normativa disegnata a livello eurounitario e la filosofia che ne è alla base.

Per garantire una adeguata protezione degli individui dai rischi provenienti dallo spazio virtuale, i più recenti interventi del legislatore dell'Unione valorizzano il momento della prevenzione e incentivano l'adozione di efficaci misure di protezione delle reti e dei sistemi informativi. L'esigenza di *compliance* e la previsione di misure organizzative a carico dei fornitori di servizi delineano, da un lato, nuove forme di responsabilità collettiva, dall'altro, ripropongono questioni relative all'opportunità di prevedere ipotesi di responsabilità per omesso controllo o di ricorrere all'utilizzo del meccanismo di cui all'art. 40, cpv., c.p..

Sul versante processuale, le nuove tecnologie non solo offrono innovativi strumenti o metodologie di indagine e, più in specifico, di ricerca della prova, ma influenzano anche in modo significativo l'acquisizione della *digital evidence* nel processo penale, soprattutto per l'"ambiente" in cui deve essere raccolta e le sue caratteristiche intrinseche (immaterialità, volatilità, promiscuità), dando luogo a complesse questioni. Tra queste, ad esempio, quelle in ordine alla conservazione dei dati di traffico, alla legittimità dell'impiego di certe tecniche di indagine e all'utilizzabilità dei risultati conseguiti, alla cooperazione giudiziaria e all'accesso transfrontaliero ai dati e/o alla *electronic evidence,* agli obblighi di collaborazione dei fornitori di servizi digitali con le autorità di *law enforcement*. Nella dinamica del processo si pongono inoltre interrogativi sul rispetto delle garanzie difensive dell'imputato, come è accaduto per la nuova disciplina delle intercettazioni mediante l'utilizzo di dispositivi mobili (c.d. captatore informatico), nonché rispetto alla tutela dei terzi coinvolti, anche indirettamente, nella varie forme di sorveglianza elettronica esistenti.

In questo scenario una punta avanzata dell'*iceberg* è rappresentata dalle implicazioni, in termini di configurazione di eventuali responsabilità e/o di tutela di diritti fondamentali del singolo, che l'utilizzo di algoritmi intelligenti o l'impiego di droni e auto ad alto contenuto tecnologico può comportare sul versante penale.

Le nuove frontiere tecnologiche sono dunque il motore del rapido cambiamento della società. Il sistema penale è oggi chiamato sempre più spesso e su diversi fronti a misurarsi con questi nuovi scenari, richiedendosi pertanto agli attori in esso coinvolti a diverso titolo di elaborare soluzioni e progettare nuovi assetti di disciplina.

***

Il corso si rivolge *in primis* a dottorandi e dottori di ricerca in discipline penalistiche (diritto e procedura penale, criminologia, ecc.). Stante l'interdisciplinarietà del tema prescelto, potranno partecipare anche i dottorandi e dottori di ricerca in ulteriori discipline giuridiche suscettibili di essere interessati al tema (diritto pubblico, diritto internazionale e dell'Unione europea, diritto comparato, filosofia del diritto, scienze politiche ecc.).

Per stimolare una partecipazione attiva, le sessioni sono articolate sulla base di una introduzione svolta da coordinatori e vedranno quindi l'intervento dei partecipanti che avranno fatto pervenire delle proposte di approfondimento di una delle tematiche attinenti all'area tematica di ciascuna sessione, secondo il sistema *call for papers*. Nel programma allegato, sono forniti a titolo solo esemplificativo alcuni spunti per possibili interventi. Il programma definitivo sarà predisposto una volta selezionati, ad opera del Comitato scientifico, i *papers* più rilevanti, che potranno indirizzarsi anche a profili del tema enucleato nelle diverse sessioni diversi da quelli proposti.

Le iscrizioni al corso dovranno pervenire entro il 21 ottobre 2018 tramite apposito *form* che sarà attivato sul sito **www.siracusainstitute.org**. I partecipanti interessati alla *call for papers* dovranno inviare entro tale data all'indirizzo **a.buonocore@siracusainstitute.org** :

- un breve *curriculum vitae* che includa i seguenti dati: università e docente di riferimento, eventuale data di conseguimento del titolo di dottore di ricerca;
- su file separato, il titolo dell'intervento proposto, corredato di un abstract di max. 5000 caratteri (spazi inclusi), da cui non sia possibile risalire all'identità dell'autore.

Le proposte più meritevoli saranno selezionate dal comitato scientifico per un intervento e l'ammissione sarà comunicata ai partecipanti selezionati entro il 28 ottobre 2018.

Al termine dei lavori i relatori saranno invitati a redigere un contributo scientifico sull'oggetto del loro intervento. I lavori saranno, previo superamento del relativo processo di valutazione e di selezione, oggetto di pubblicazione. Agli autori dei tre migliori contributi verrà inoltre data la possibilità di intervenire come relatori al Convegno annuale dell'AIDP, che avrà ad oggetto una tematica affine a quella del Corso interdottorale e si terrà nel mese di marzo del 2019 presso l'Università degli Studi di Teramo.

Le modalità di iscrizione e pagamento per la partecipazione al Corso verranno divulgate a breve.

Nuove frontiere tecnologiche e sistema penale

Sicurezza informatica, strumenti di repressione e tecniche di prevenzione

---

I AREA TEMATICA

IL DIRITTO PENALE NEL CYBERSPAZIO.

SPUNTI DI APPROFONDIMENTO:

- Definizione di cyber-criminality alla luce delle fonti internazionali ed europee
- Emersione di nuovi diritti della persona (diritto all'identità digitale e al controllo dei propri dati personali, diritto di accesso ad *Internet*, diritto all'oblio, libertà e sicurezza di aree informatiche o spazi virtuali di pertinenza dell'individuo) e connesse esigenze di tutela
- Desensibilizzazione soggettiva, moventi del crimine informatico e profilazione del cyber-criminale
- Commissione di reati *nel cyberspace o attraverso la rete* e problemi di giurisdizione
- L'individuazione del *locus commissi delicti* e i profili relativi alla legge penale nello spazio
- La sicurezza e la riservatezza informatica come beni giuridici e nuove esigenze di tutela nel contesto tecnologico
- Concorso di persone e reati associativi nel cyberspazio
- La confisca e le misure patrimoniali di contrasto al *cybercrime*
- Azione di contrasto al *cybercrime* nel diritto internazionale e dell'Unione Europea

II AREA TEMATICA

DIRITTO PENALE E LIBERTÀ DI ESPRESSIONE IN INTERNET

SPUNTI DI APPROFONDIMENTO:

- La diffamazione *on line*
- *Hate speech* e limiti alla libertà di espressione nello spazio virtuale
- Reati di opinione, apologia e istigazione a delinquere

- *Fake news* e profili di rilevanza penale
- Cyber-terrorismo e condotte di radicalizzazione e reclutamento
- Diffusione di riprese e registrazioni di carattere privato: profili di rilevanza penale

III AREA TEMATICA

FINANCIAL CYBERCRIME

SPUNTI DI APPROFONDIMENTO:

- La criminalità del profitto nell'era digitale: nuovi beni e nuove forme di aggressione
- Le strategie di contrasto a livello sovranazionale e eurounitario
- *Phishing*, frodi informatiche e frodi negli strumenti di pagamento
- Piattaforme di *e-commerce* illegale
- Dematerializzazione della moneta e nuove frontiere del riciclaggio
- L'utilizzo delle valute virtuali e la prestazione di servizi ad esse connessi
- Flussi di denaro sporco e strumenti di prevenzione
- *Cyber-organised crime* e *Organised-cybercrime*: le nuove frontiere del *financial-economic crime*

IV AREA TEMATICA

LA TUTELA PENALE DELLA PRIVACY NEL CYBERSPAZIO

SPUNTI DI APPROFONDIMENTO:

- Definizione di un nuovo (?) "*right to be let alone*" nel mutato contesto tecnologico
- Trattamento dei dati personali: beni giuridici e tecniche di tutela penale
- Le sanzioni previste per le violazioni della disciplina sul trattamento dei dati personali
- Rapporto tra illeciti penali e apparato sanzionatorio amministrativo
- La tutela della *privacy* nelle attività di contrasto alla criminalità
- La disciplina della *data retention*
- *Corporate liability* e *compliance*: responsabilità d'impresa nella protezione dei dati personali

V AREA TEMATICA

SICUREZZA INFORMATICA, *COMPLIANCE* E PREVENZIONE DEL RISCHIO DI REATO

SPUNTI DI APPROFONDIMENTO:

- Sicurezza cibernetica e posizioni di garanzia
- Posizioni di controllo e responsabilità dell'ISP
- Pirateria informatica, P2P *sharing* e responsabilità del *provider*
- La responsabilità degli enti dipendente da reato informatico
- Modelli gestionali, adozione di misure di sicurezza e esimenti di responsabilità
- Algoritmi predittivi e prevenzione del rischio di reato
- Intelligenza artificiale e forme di responsabilità per omesso impedimento di reati

VI AREA TEMATICA

NUOVE TECNOLOGIE E PROCESSO PENALE

SPUNTI DI APPROFONDIMENTO:

- Indagini ad alto contenuto tecnologico e tutela dei diritti fondamentali, fra strumenti investigativi e limiti al potere coercitivo dello Stato
- Prova digitale e processo penale
- Intercettazioni telematiche, utilizzo del c.d. captatore informatico e altre forme di sorveglianza elettronica
- Siti "civetta", agenti provocatori e operazioni sotto copertura
- Gli strumenti di cooperazione giudiziaria internazionale nel contrasto alla criminalità informatica
- Accesso transfrontaliero alla *electronic evidence*
- Il coordinamento investigativo a livello nazionale ed eurounitario
- La collaborazione fra i settori pubblico-privato e i rapporti con i *service providers*

Comitato scientifico:

Prof. Vincenzo Militello; Prof. Stefano Manacorda; Prof.ssa Gabriella di Paolo; Prof. Roberto Flor; Prof. Antonio Gullo; Prof. Vincenzo Mongillo; Prof. Nicola Pisani; Prof. Alessandro Spena; Prof. Francesco Zacchè.