La crisi della giurisdizione penale nella società digitalizzata.

Sfide, ostacoli, nuovi modelli di investigazione e di cooperazione giudiziaria

Corso dedicato a Vittorio Occorsio

Cod.: FPFP25030

Sede e data: Firenze, auditorium del Palazzo di Giustizia - 27 ottobre 2025 (apertura lavori ore 15.00) – 29 ottobre 2025 (chiusura lavori ore 13.00)

Responsabili del corso: Dott. Fabio Di Vizio, Prof. Stefano Dorigo, Avv. Federico Vianelli**,** componenti del Comitato direttivo della Scuola superiore della magistratura

Esperto formatore: Dott. Mario Palazzi – Procuratore della Repubblica di Viterbo

***

Presentazione

Nell'esercizio quotidiano della giurisdizione ci si trova ad affrontare diverse tipologie di delitti e a dover utilizzare metodologie di indagine che siano in grado di affrontare le questioni che esse pongono. L'incessante progresso tecnologico e la diffusione crescente delle interazioni umane sulla rete stanno, tuttavia, avendo un impatto talmente dirompente su varie forme di cyber-criminalità da richiedere che si affronti alla radice il tema dell'effettività della giurisdizione penale, quando costretta a operare in quello che viene definito Spazio o Ambiente Virtuale (SV), cioè in un intreccio di oggetti materiali (server, reti energetiche, cavi) e immateriali (programmi, connessioni, trasferimenti ecc.), che rendono possibile un rapidissimo trasferimento di informazioni, in un prossimo futuro senza tempi di latenza grazie all'utilizzo di tecnologie basate sul Quantum Computing.

L'esperienza ha portato a risultati molto importanti, anche sul piano della cooperazione internazionale, ma pone continue sfide e potenziali interferenze, se non conflitti, con altri poteri.

Innanzitutto, le pratiche di investigazione si sono adeguate ai nuovi strumenti. Molte indagini vedono ormai comunemente l'utilizzo di strumenti (come i sequestri sul web, anche di cripto-assets) sino a pochi anni fa di difficile attuazione; vi vanno poi espandendo le pratiche di utilizzo dell'IA nelle indagini: basti pensare all'elaborazione di grandi quantitativi di dati da parte della GdF per accertamenti in tema di riciclaggio e di reati finanziari. Anche il ricorso ai vari strumenti organizzativi, predisposti per facilitare le indagini transnazionali, è ormai usuale e i risultati crescono in maniera visibile: dalla costituzione di Joint Investigative Teams, all'utilizzo della intermediazione di organi quali Eurojust o Europol. Le recenti, importanti novità normative dell'Unione Europea si intrecciano con le possibilità offerte dalla Convenzione di Budapest e, ora, dalla Convenzione UN sul Cybercrime, che sarà aperta alla firma proprio nell'ottobre 2025. Ma la cyber-criminalità, intesa anche come insieme di reati comuni commessi attraverso la rete, pone una serie di ulteriori sfide collegate alla professionalità dei magistrati e alla organizzazione giudiziaria, avuto riguardo all'elevato contenuto tecnologico e quindi alla necessità di una formazione specifica dei magistrati requirenti e giudicanti, al livello sofisticato e spesso costoso delle indagini, alla necessità di governare numeri di notizie di reato in costante crescita esponenziale su questi fronti, a un approccio aperto alla cooperazione internazionale, alla

circolazione interna ed esterna ai singoli uffici di indirizzi interpretativi, prassi virtuose, tecniche investigative nuove.

*Su queste premesse, la **Scuola Superiore della Magistratura** e la **Fondazione Vittorio Occorsio** hanno progettato un corso durante il quale si svolgerà, innanzitutto, una ricognizione delle tipologie di reato che sono, per loro natura o per opportunità, commesse per il tramite di tecniche informatiche e di comunicazione avanzate. Si approfondirà, quindi, il tema degli strumenti di investigazione e di cooperazione, correlati alle diverse tipologie di reato. In questo contesto, particolare rilievo sarà dato all'evoluzione giurisprudenziale e ai temi ancora aperti, quali quello relativo alle piattaforme di comunicazione criptate in uso alla criminalità organizzata, in relazione alla qualificazione e utilizzabilità delle prove acquisite dall'estero, attraverso la decifrazione delle piattaforme, e ciò anche in relazione all'incessante e frenetico mutamento tecnologico delle piattaforme via via emerse e al possibile ricorso a strumenti di acquisizione più diretti e agili, ma apparentemente meno garantiti di quelli finora sperimentati.*

Se gli strumenti di indagine, di acquisizione e valutazione della prova e di cooperazione si vanno raffinando ed estendendo, resta tuttavia un'area nella quale l'esercizio della giurisdizione incontra liniti davvero significativi. Si tratta, peraltro, proprio dei casi in cui la minaccia derivante da tal genere di delitti è più grave per i cittadini e per la sicurezza nazionale. Si pensi agli attacchi informatici ai sistemi elettorali, alla base del funzionamento delle democrazie, o alle grandi infrastrutture critiche. Qui non si coglie solo il tema della attribuzione, fondamentale nel diritto pubblico internazionale per affermare la responsabilità degli Stati e legittimare le reazioni, ma in realtà anche quello dell'attualità del concetto fondante di sovranità, del quale la giurisdizione – affermata ed esercitata – costituisce storicamente una delle massime espressioni.

Allo Spazio virtuale non possono essere meccanicamente applicate le regolamentazioni previste dal diritto internazionale (IL) per le telecomunicazioni, l'Alto Mare o lo Spazio Esterno. Ognuna di queste entità contiene una parte della realtà sottesa allo Spazio virtuale, ma non è in grado di comprenderla interamente. Questa difficoltà costituisce attualmente l'oggetto del tentativo di giungere a una definizione di Spazio virtuale, presupposto di una regolamentazione condivisa; questa discussione è in corso nell'Open Ended Working Group (OEWG) delle Nazioni Unite. Da questo sforzo discenderà anche la possibilità di contribuire alla individuazione delle norme di diritto internazionale applicabili allo Spazio virtuale. Vi sono implicazioni di siffatte definizioni anche per ciò che concerne l'effettività della cooperazione giudiziaria e di polizia nello Spazio virtuale.

Nell'anno passato sono giunte a conclusione due iniziative fondamentali per l'esercizio della giurisdizione penale nei crimini informatici transnazionali che si avvalgono di tecnologie di IA. L'Unione Europea ha varato una serie di iniziative, volte a disciplinare la prova elettronica (la e-evidence), contribuendo così alla unificazione delle definizioni di base, presupposto di un'efficace cooperazione tra gli Stati e le loro A.G. Nello stesso tempo, la Convenzione delle Nazioni Unite sul Cybercrime, definitivamente adottata dall'Assemblea generale dell'Onu il 24/12/2024 e che sarà aperta alla firma nell'ottobre 2025, dunque in contemporanea al presente corso, prevede sia la tendenziale omogeneizzazione delle fattispecie, sia l'adozione di strumenti di cooperazione di polizia e giudiziaria, specificamente mirati ad affrontare le difficoltà della collaborazione quando i reati si dipanano in parte nello Spazio virtuale, tra i quali l'innovativo tool dei Corpi Investigativi Comuni, in linea con il Secondo Protocollo Addizionale alla Convenzione di Budapest. Vi è dunque innanzitutto la necessità di diffondere tra gli operatori la conoscenza delle nuove tematiche, dei nuovi strumenti e delle possibilità che essi offrono per un più efficace contrasto di forme criminali particolarmente aggressive. Il tutto anche attraverso il confronto con esperienze concrete nell'ambito dei programmati laboratori.

A ciò deve accompagnarsi la consapevolezza che non tutti i problemi sono stati risolti e che permangono ostacoli all'effettivo esercizio della giurisdizione, derivanti dagli intrecci tra tecnica e diritto, che sono caratteristici dell'ambiente virtuale, nonché da persistenti differenze tra ordinamenti nazionali, dalle criticità nella cooperazione internazionale e di polizia. Quale reazione è legittima, nel caso in cui l'attacco – dunque il delitto consumato nella giurisdizione nazionale – proviene da Stato che non ha sottoscritto le Convenzioni o non vi dà comunque esecuzione? Quali potranno legittimamente essere le forme di accertamento

autoritativo o di interruzione della condotta in atto che una giurisdizione potrà imporre alla sovranità di un altro Stato, quando questo non aderisce alle Convenzioni o non vi dà attuazione? Potrà, ad esempio, effettuarsi comunque il sequestro del contenuto di un server sito in Paese terzo non collaborativo? Dal punto di vista tecnico ciò è possibile. Lo è dal punto di vista del diritto internazionale e da quello del nostro diritto interno? Sono temi da tempo divenuti realtà, che si sperimentano già in procedimenti penali interni e in complesse pratiche di cooperazione giudiziaria e di polizia, supportate dalle competenti agenzie europee con il contributo di Paesi Terzi. Gli intrecci sin qui descritti sono stati al centro dell'approfondimento del diritto pubblico (IL) e umanitario internazionale (IHL). Il Manuale Tallinn, redatto dal Centro di Eccellenza della NATO, ha costruito su queste tematiche i potenziali sviluppi del IL, volto a disciplinare i conflitti che sempre di più si svolgeranno sulle reti informatiche.

Su questi temi saranno conclusivamente chiamati a discutere i relatori, magistrati, esperti ed attori del settore.

Metodologia: *relazioni frontali, tavola rotonda con fasi laboratoriali e dialogiche con i partecipanti*

Organizzazione: *Scuola Superiore della Magistratura e Fondazione Vittorio Occorsio*

Durata: *quattro sessioni*

Numero complessivo dei partecipanti e modalità di partecipazione: *Centoquaranta (ottanta in presenza e sessanta da remoto)*

Composizione della platea: *magistrati ordinari con funzioni penali*

Postergazioni: *nessuna*

Programma

Lunedì 27 ottobre 2025

1^ sessione: ***La giurisdizione penale alla prova della società digitalizzata: fattispecie e mezzi di prova***

ore 15,00 Presentazione del corso da parte dei responsabili della Scuola e dell'esperto formatore

ore 15,15 *L'evoluzione della legislazione penale sostanziale sul cybercrime nel quadro nazionale e internazionale*

Nicola SELVAGGI, Professore associato di diritto penale nell'Università Mediterranea di Reggio Calabria, Vice Capo Ufficio Legislativo Ministero della Giustizia

ore 15,45 *Presente e futuro della prova elettronica (dai "tabulati" al cloud, dalla cooperazione volontaria, dalla EU E-evidence Package)*

(dialogo a più voci)

Simona RAGAZZI, Giudice per le indagini preliminari - Tribunale di Catania

Silvia SIGNORATO, Professoressa associata di procedura penale presso l'Università di Padova

ore 16.45 *La giurisdizione penale nel rapporto con l'Intelligence e altri poteri statuali di contenimento di minacce cibernetiche: interferenza, concorrenza o armoniosa ripartizione di sfere?*

(dialogo a più voci)

Eugenio FUSCO, Procuratore Aggiunto presso il Tribunale di Milano

Alessandra GUIDI, Prefetto, Vice Direttore, Dipartimento delle informazioni per la sicurezza (DIS)

ore 17,30 Dibattito

ore 18,00 Sospensione dei lavori

***

Martedì 28 ottobre 2025

2^ sessione: L'evoluzione della cooperazione internazionale nello spazio virtuale

ore 9.15 *Le indagini in materia di cybercrime e l'utilizzo degli strumenti di cooperazione: esperienze a confronto*

(dialogo a più voci)

Eugenio ALBAMONTE, sostituto procuratore presso la Direzione Nazionale Antimafia ed Antiterrorismo

Ivano GABRIELLI, Direttore del Servizio Polizia Postale e per la Sicurezza Cibernetica

ore 10,00 *Le forme di cooperazione internazionale di polizia nelle indagini ed il ruolo di Eurojust ed Europol*

(dialogo a più voci)

Filippo SPIEZIA, membro nazionale di Eurojust

Gianluca GENTILE, già in forza alla polizia postale (CNAIPIC), italian Liaison Bureau di Europol

ore 10,45 Dibattito

ore 11,15 Pausa

ore 11,30 *La cooperazione giudiziaria multilaterale; la convenzione di Budapest e la convenzione delle NU sul cybercrime*

Concetta LOCURTO, magistrato, assistente di studio a tempo pieno di Giudice Costituzionale

ore 12.15 Dibattito

ore 13,00 Sospensione dei lavori

3^ sessione: quale spazio per la giurisdizione?

ore 14,00 *La effettività della enforcement jurisdiction nello spazio virtuale. La prospettiva del diritto internazionale pubblico evoluzione*

(dialogo a più voci)

Cedric RYNGAERT, Professore di diritto internazionale pubblico presso l'Università di Utrecht (Paesi Bassi)

Mark ZOETEKOUW, senior legal advisor on cybercrime - Dutch police

Liis VIHUL, Coeditrice del Manuale di Tallinn 3.0 e presidente del Cyber Law International, componente del NATO Cooperative Cyber Defence Centre of Excellence

ore 15,00 Dibattito

Laboratorio su esperienze

Ore 15,30 *1. La disinformazione sulla rete. Dal* deep fake *alle turbative dei processi elettorali in Europa (Il* leading case *"Romania 2024")*

Oreste POLLICINO, professore ordinario di Diritto Costituzionale Università degli Studi Luigi Bocconi di Milano

ore 16,15 Dibattito

ore 17,00 Sospensione dei lavori

***

Mercoledì 29 ottobre 2025

ore 9,15 **quarta sessione:**

2. Il 5° dominio: il ruolo della Difesa e le nuove regole del gioco, dalla competizione al conflitto.

Gianluca ZULINI, colonnello E.I., Capo Ufficio Operazioni Cyber, Comando per le operazioni in Rete (COR)

ore 10.00 *3. Azioni di intelligence difensive ed offensive: criticità e potenzialità (simulazione a cura dell'AISE)*

Carlo ZONTILLI, Generale di Divisione E.I., Vice Direttore dell'Agenzia informazioni e sicurezza esterna

ore 10,45 Dibattito

ore 11,00 Pausa

ore 10,45 **Tavola rotonda**

Le frontiere "mobili" della giurisdizione nazionale in risposta a operazioni cyber provenienti da altri Stati

moderatore:

Giovanni SALVI, già Procuratore generale presso la Corte di cassazione – Presidente del Comitato Scientifico FVO

Margherita CASSANO, già Primo Presidente Corte di Cassazione

Maurizio DE LUCIA, Procuratore della Repubblica presso il Tribunale di Palermo

Luca LUPARIA DONATI, Professore ordinario di diritto processuale penale presso l'Università degli Studi di Milano

Raffaele PICCIRILLO, sostituto procuratore presso la Corte di Cassazione

ore 12,30 Dibattito

ore 13,00 Chiusura dei lavori