

Università degli Studi di Firenze
Dipartimento di Scienze Giuridiche

Call for abstracts

Seminario dottorale

Sfide attuali e tendenze future del diritto processuale penale europeo
- III edizione -

26 Novembre 2026

È ormai noto come la trasformazione digitale della giustizia penale – sia a livello interno che sovranazionale – abbia ormai superato la fase della semplice sperimentazione. Tecnologie un tempo considerate eccezionali sono oggi parte integrante delle attività investigative, della raccolta e circolazione delle prove, della cooperazione giudiziaria e, sempre più spesso, dello stesso svolgimento del processo penale.

Si pensi, tra le altre, alle comunicazioni cifrate, all'acquisizione di dati conservati nei *cloud*, al riconoscimento facciale, ai sistemi biometrici, agli algoritmi di analisi e classificazione, ai più vari strumenti di intelligenza artificiale, alle videoconferenze. A ben vedere, tali tecnologie stanno modificando non soltanto come si indaga e come si giudica, ma impongono altresì una riflessione sulla portata di quelle categorie considerate “tradizionali” del diritto processuale penale: giurisdizione e territorialità, le nozioni di “perquisizione”, “sequestro” e “intercettazione”, il diritto alla prova, il contraddittorio, l'immediatezza, la presunzione di innocenza, la parità delle armi e il controllo giurisdizionale sull'attività investigativa.

Il 2026 rappresenta, sotto questo profilo, un anno particolarmente significativo. Dal 18 agosto 2026 trova applicazione il Regolamento (UE) 2023/1543 sugli ordini europei di produzione e di conservazione delle prove elettroniche, mentre il termine per il recepimento della complementare Direttiva (UE) 2023/1544 è scaduto il 18 febbraio dello stesso anno. Parallelamente, il Regolamento (UE) 2024/1689 sull'intelligenza artificiale (“AI Act”), divenuto in larga parte applicabile nel 2026 secondo un calendario progressivo, delinea un articolato sistema di divieti, limiti e garanzie destinato a incidere anche sull'impiego dell'intelligenza artificiale nell'attività di contrasto alla criminalità e nell'amministrazione della giustizia. Il Regolamento (UE) 2023/2844 e la Direttiva (UE) 2023/2843 accompagnano inoltre la progressiva digitalizzazione della cooperazione giudiziaria transfrontaliera, mentre il Regolamento (UE) 2024/982 (“Prüm II”) rinnova e amplia il quadro per la consultazione e lo scambio automatizzati di dati nell'ambito della cooperazione di polizia, includendo, tra l'altro, profili DNA, dati dattiloscopici e immagini del volto.

Questa evoluzione normativa si inserisce in un dialogo sempre più intenso con la giurisprudenza europea. La Corte di giustizia, dando origine alla ormai nota “*data retention saga*”, ha progressivamente definito i limiti alla conservazione e all'accesso ai dati delle comunicazioni elettroniche, da *Digital Rights Ireland* e *Tele2 Sverige* a *La Quadrature du Net*, *Prokuratuur*, *Commissioner of An Garda Síochána* e *SpaceNet*, fino alla più recente *La Quadrature du Net II*, che ha ulteriormente precisato le condizioni per la conservazione e l'accesso agli indirizzi IP. Una giurisprudenza che, peraltro, continua a svilupparsi, come mostrano le più recenti questioni ancora pendenti dinanzi alla Corte. Su un diverso ma contiguo versante, la sentenza della Grande Sezione in *M.N. (EncroChat)*, C-670/22, ha affrontato questioni centrali relative alla circolazione transfrontaliera di prove digitali già raccolte, ai presupposti per l'emissione di un Ordine europeo di indagine diretto alla loro trasmissione e alle garanzie di controllo giurisdizionale e di effettivo contraddittorio connesse al loro utilizzo nel procedimento penale.

Sul versante della Convenzione europea dei diritti dell'uomo (CEDU), il rapporto tra tecnologia e potere investigativo investe ormai tanto l'articolo 8 quanto le garanzie processuali dell'articolo 6. Si pensi, ad esempio, alla giurisprudenza sulla *mass surveillance* – tra cui *Big Brother Watch and Others v. United Kingdom* e *Centrum för Rättvisa v. Sweden* – che ha progressivamente elaborato (o, quantomeno, tentato di elaborare) requisiti più stringenti per i

sistemi di intercettazione e trattamento su larga scala dei dati personali. In *Glukhin v. Russia* la Corte EDU si è confrontata direttamente con l'impiego del riconoscimento facciale; in *Podchasov v. Russia*, con gli obblighi di conservazione, accesso e decrittazione delle comunicazioni cifrate. La Grande Camera in *Yüksel Yalçınkaya v. Türkiye* ha, inoltre, mostrato come l'utilizzo processuale di dati provenienti da applicativi digitali (*ByLock*) possa incidere tanto sull'accertamento individualizzato della responsabilità penale quanto sulla possibilità per la difesa di conoscere e contestare efficacemente la prova elettronica; principi successivamente ribaditi, tra l'altro, in *Demirhan and Others v. Türkiye*. Più di recente, *Minteb v. France* ha portato all'attenzione della Corte la questione della responsabilità penale derivante dal rifiuto di comunicare alle autorità i codici di accesso a dispositivi digitali.

Il seminario intende interrogarsi su questa trasformazione muovendo da una domanda di fondo: *in che modo l'innovazione tecnologica sta modificando l'architettura delle garanzie del processo penale?* La maggiore capacità tecnologica delle autorità investigative può tradursi in maggiore efficacia, ma rende al tempo stesso più complessa l'identificazione del momento in cui interviene un'ingerenza nei diritti fondamentali, dell'autorità che ne è responsabile ed, infine, dell'autorità giudiziaria chiamato a controllarla. L'automazione pone inoltre nuovi problemi di trasparenza e contestabilità: come può la difesa contestare un risultato prodotto da un sistema algoritmico? Quali informazioni devono essere accessibili per garantire un contraddittorio effettivo? E come cambiano queste domande quando dati, algoritmi, infrastrutture e fornitori di servizi sono distribuiti fra diverse giurisdizioni?

Sono pertanto particolarmente incoraggiati contributi riguardanti, tra gli altri, i seguenti temi:

- intelligenza artificiale e procedimento penale;
- riconoscimento facciale e tecnologie biometriche;
- prova elettronica e *digital forensics*, con particolare attenzione ad autenticità, integrità, affidabilità, catena di custodia, accessibilità alla difesa e utilizzabilità processuale di grandi quantità di dati digitali;
- *e-Evidence*, Ordine europeo di indagine e circolazione transfrontaliera della prova;
- comunicazioni cifrate, hacking investigativo e piattaforme criptate, incluse le questioni emerse nei procedimenti *EncroChat*, *Sky ECC* e analoghe operazioni investigative transnazionali;
- data retention, accesso ai metadati e sorveglianza digitale, nel dialogo tra articoli 7 e 8 della Carta, articolo 8 CEDU e giurisprudenza delle Corti di Lussemburgo e Strasburgo;
- digitalizzazione della cooperazione giudiziaria in materia penale, incluso l'impatto delle nuove tecnologie sui principi di immediatezza, oralità, pubblicità e partecipazione effettiva;
- nuove frontiere della prova tecnologica, incluse prove generate o elaborate mediante AI, deepfakes, sistemi automatizzati di trascrizione o traduzione.

Organizzazione dell'evento e modalità di partecipazione

La Cattedra di Diritto processuale penale del Dipartimento di Scienze Giuridiche dell'Università degli Studi di Firenze (prof.ssa Paola Felicioni) promuove una *call for abstracts* in vista di una giornata di studi dedicata alle **giovani studiose e ai giovani studiosi di diritto processuale penale europeo (dottorande e dottorandi, assegniste e assegnisti di ricerca, dottoresse e dottori di ricerca da non più di due anni)**.

Gli *abstracts* selezionati saranno presentati e discussi nell'ambito di una giornata di studi, che si terrà il 26 novembre 2026 presso la Scuola di Giurisprudenza dell'Università di Firenze.

Coloro i quali intendano prender parte al dibattito potranno inviare, **entro e non oltre il 24 ottobre 2026**, un abstract del proprio contributo, di lunghezza compresa tra le 300 e le 500 parole, al seguente indirizzo e-mail: seminariodottorale.unifi@gmail.com, indicando altresì il proprio nome, la propria qualifica completa, l'università di affiliazione e la propria mail istituzionale.

L'esito favorevole della selezione verrà comunicato **entro il 31 ottobre 2026**. In base al contenuto dei contributi ricevuti, ne sarà valutata la pubblicazione con modalità da comunicare in seguito.