LUISS

Corso di laurea in Giurisprudenza

Cattedra Diritto Processuale Penale

La prova digitale in una prospettiva nazionale e sovranazionale, il ruolo dei service provider, la tutela della privacy e del diritto di difesa

Prof. Alberto Macchia

RELATORE

Prof. Filippo Dinacci

CORRELATORE

David Sonnino - Matr. 166083

CANDIDATO

Anno Accademico 2024/2025

Indice

Introduzione

La prova, al centro del processo penale, è il punto di contatto tra la realtà giuridica procedurale e quella fattuale. L'evoluzione della realtà contemporanea è stata accompagnata da significative trasformazioni sia nel ruolo delle prove sia nelle regole che ne disciplinano l'ammissibilità. La rivoluzione che il diritto delle prove penali sta attualmente affrontando è la crescente digitalizzazione delle pratiche investigative;[1] l'impatto della tecnologia sul diritto processuale penale è, infatti, duplice. Consente, da un lato, nuove forme di attività criminale attraverso le moderne telecomunicazioni e fornisce al contempo potenti strumenti per le indagini e la repressione dei reati.[2] Le moderne tecniche investigative possono, dunque, consentire un'ampia sorveglianza dell'imputato.[3]

L'uso di prove digitali nei procedimenti penali comporta nuove sfide per l'effettivo esercizio del diritto di difesa e per la tutela della privacy, richiedendo un adeguamento delle garanzie processuali tradizionali e lo sviluppo di strumenti di controllo giurisdizionale capaci di bilanciare l'efficacia investigativa con la protezione dei diritti fondamentali.

Un'altra sfida importante è rappresentata dalla natura immateriale delle prove digitali. Il carattere della intangibilità tende a erodere il tradizionale principio di territorialità, rendendo cruciale la collaborazione giudiziaria tra stati. A differenza delle prove fisiche, infatti, i dati digitali possono essere archiviati, consultati o trasmessi in più giurisdizioni in un lasso di tempo limitato. Per affrontare questo problema, sia il Consiglio d'Europa che l'UE hanno sviluppato strumenti legali che facilitano la cooperazione giudiziaria. Nel 2001, il Consiglio d'Europa ha elaborato la Convenzione di Budapest, considerata lo strumento di

1 SIRIUS Project (Eurojust and Europol), *EU Electronic Evidence Situation Report 2024* (November 2024).
2 M. Simonato, *'Defence Rights and the Use of IT in Criminal Procedure'* in *International Journal of Penal Law,*2019, 1/85, 264.
3 E. Busillo, '*Conservazione e produzione della prova digitale nella nuova disciplina europea: il potenziale disallineamento con i principi espressi dalla giurisprudenza di settore'* in *Freedom, Security & Justice: European Legal Studies*, 2023, 3, 27.

più ampia portata nella lotta globale contro la criminalità informatica.[4] Entrambe le organizzazioni regionali si sono concentrate nel fornire agli Stati membri adeguati strumenti di collaborazione internazionale e di disciplina procedurale nella raccolta della prova digitale.[5] A ciò si aggiunge il crescente ruolo dei service provider, ormai divenuti attori centrali non solo nel mercato digitale, ma anche nei meccanismi di cooperazione giudiziaria, in quanto custodi privilegiati di informazioni essenziali per l'accertamento dei reati.[6] Il panorama europeo di disciplina della prova digitale ha profonde ricadute sul diritto nazionale.[7]

Quest'ultimo risente della scarsa tipizzazione normativa dei fenomeni informatici e si confronta con il rischio di apparire inadeguato di fronte alle sfide poste dalla crescente internazionalizzazione e digitalizzazione della procedura penale. Un delicato intreccio di giurisprudenza e di legislazione, sia nazionale che sovranazionale, sta definendo le caratteristiche e l'evoluzione normativa di un istituto destinato ad assumere un ruolo di crescente centralità nel processo penale: la prova digitale. Il quadro normativo attuale della prova digitale richiede un'analisi compiuta che tenga conto della dimensione internazionale del diritto processuale penale, del conseguente rispetto degli obblighi internazionali da parte degli Stati membri e del delicato equilibrio tra esigenze investigative di tutela della privacy e del contraddittorio per l'accusato.[8]

4 Convenzione del Consiglio d'Europa sulla criminalità informatica, adottata a Budapest il 23 novembre 2001
5 J. Clough, *A World of Difference: The Budapest Convention of Cybercrime and the Challenges of Harmonisation* in *Monash University Law Review* 2014, 40, 698, 699.
6 V. Mitsilegas, The privatisation of mutual trust in Europe's area of criminal justice: The case of e-evidence in Maastricht Journal of European and Comparative Law 2018, 25/3 , 263.
7 Orlando C., 'Mutua ammissibilità della prova tra gli Stati membri dell'Unione europea ed e-evidence: riflessioni a margine della Proposta di Direttiva dello European Law Institute' in Sistema Penale, 2023, 11, 117.
8 M. Galič, *'Defence Rights in the Context of Huge Data Sets and Big Data Forensic Tools in Criminal Proceedings'* in *J. Boom Strafblad,* 2021, 2/22, 41, 43.

Capitolo 1 Definizione di prova digitale

1.1 Inquadramento generale

1.1.1 Le caratteristiche della prova digitale

Il codice di procedura penale e la Convenzione di Budapest non definiscono il concetto di prova digitale. L'art. 1 della Convenzione è, infatti, dedicato alle definizioni, e fornisce una distinzione tra i diversi tipi di dati rilevanti per le indagini sulla criminalità informatica. Queste definizioni non devono essere copiate alla lettera dal legislatore nazionale, ma devono essere implementate secondo i principi del trattato. In particolare, l'art. 1 distingue tra dati relativi agli abbonati, dati di traffico e dati di contenuto. I primi riguardano l'identificazione dell'utente di un servizio, i secondi descrivono le modalità di trasmissione delle comunicazioni su una rete, come indirizzi IP, tempi e durata, mentre i dati di contenuto coincidono con le informazioni effettivamente scambiate, quali il testo di un'e-mail, le immagini condivise in una chat o i file scaricati da un server.[9]

Questa differenziazione è fondamentale ai fini applicativi ed investigativi, in quanto determina il modo in cui i dati devono essere raccolti, conservati e analizzati nel contesto delle investigazioni informatiche. A maggior ragione, la classificazione è riprodotta dal Regolamento E-evidence, che garantisce diversi livelli di protezione a seconda del tipo di dati, bilanciando le esigenze investigative e il diritto alla privacy.[10]

In ambito accademico sono state elaborate due teorie per definire la prova digitale. Secondo un primo orientamento, essa viene descritta in termini puramente tassonomici, ma tale approccio risulta problematico poiché ancorato alla multiforme natura dei dati digitali, difficili da classificare. In questa prospettiva, la prova digitale è stata contrapposta a quella analogica, con la quale differisce soprattutto per l'incorporazione: essa, infatti, è smaterializzata ed

9 Rapporto esplicativo alla Convenzione sulla criminalità informatica, 3.
10 Regolamento E-Evidence Art. 3.

esiste indipendentemente dal supporto materiale che la veicola, vivendo nell'etere[11]. Ciò comporta notevoli difficoltà per il giurista quali la facile modificabilità del file, un maggior rischio di alterazione e la necessità di salvaguardare l'autenticità della prova.[12]

Secondo un'impostazione complementare, la prova digitale può essere intesa anche in senso funzionale, prescindendo dalla disciplina giuridica che la regola, e ponendo invece l'accento sul suo scopo e sulle modalità con cui opera. In quest'ottica, essa è definita come "qualsiasi informazione o dato che possa avere rilevanza per l'indagine" e, più precisamente, comprenderebbe le informazioni o i dati memorizzati, ricevuti o trasmessi da un dispositivo elettronico. I dati informatici rilevanti a fini probatori vengono acquisiti, nella pratica, mediante la confisca del dispositivo e l'estrazione del contenuto del computer. Le evidenze digitali si caratterizzano per tre elementi distintivi: l'invasività rispetto ai diritti fondamentali, la dimensione transnazionale derivante dalla localizzazione dei dati presso fornitori di servizi privati, e l'elevato grado di complessità tecnica connesso alla loro natura immateriale.[13]

1.1.2 Il rapporto con i diritti fondamentali

Una ricca giurisprudenza sia della CGUE sia della Corte EDU mostra la tensione tra i diritti alla privacy e alla difesa e l'uso di strumenti investigativi avanzati, come l'accesso ai telefoni cellulari. Gli Stati perseguono l'obiettivo di combattere il crimine attraverso il controllo delle telecomunicazioni e l'accesso ai dati personali, essi devono adeguarsi al progresso tecnologico degli attori criminali per garantire un'efficace applicazione della legge penale.[14] Tuttavia, questo potere deve essere limitato sulla base della proporzionalità per evitare abusi.[15]

---

11 P. Tonini e C. Conti, *Il diritto delle prove penali*, Giuffrè, Milano 2014.
12 A. Scalas, *I confini mobili della digital evidence: una necessaria tassonomia per la tutela delle garanzie* in *Archivio Penale*, 2023, 2 2.
13 Busillo, op. cit., p.29.
14 O. Murro., *Lo smartphone come fonte di prova. Dal sequestro del dispositivo all'analisi dei dati,* Cedam, Padova 2024.
15 N. Faiola, *Data retention ed accesso ai dati per scopi securitari: condizioni e limiti alla luce della giurisprudenza della Corte di giustizia dell'Unione europea*, in *Il diritto dell'Unione europea*, 2023, 1, 77.

Le sentenze della "saga della *data retention*"[16] hanno sottolineato l''acceso ai dati informatici può rivelare aspetti altamente sensibili della vita privata delle persone, comprese le abitudini quotidiane, i luoghi di residenza o di viaggio, le attività personali, le relazioni sociali e gli ambienti frequentai regolarmente.[17] Anche l'accesso a una quantità limitata di dati o per un breve periodo di tempo può essere in grado di fornire informazioni precise sulla sfera più intima di un utente di un mezzo di comunicazione elettronica.

La gravità della limitazione dei diritti fondamentali è un fattore importante che deve essere preso in considerazione quando si valuta la proporzionalità di una misura investigativa. Maggiore è il grado di intrusione nei diritti fondamentali, più forti ed efficaci devono essere le garanzie. Nel caso *Landeck*, la CGUE ha affermato che l'accesso ai dati di un telefono cellulare deve essere considerato particolarmente grave, considerando la natura e la sensibilità dei dati.[18] Questi dati possono arrivare a essere dati personali, rivelando origini razziali o etniche, opinioni politiche e convinzioni religiose o filosofiche, giustificando la protezione speciale dell'art. 10 della direttiva E-privacy.[19] Tuttavia, va osservato che, qualora i dati risultino essenziali per accertare la responsabilità penale dell'individuo in relazione a crimini gravi, l'intrusività della misura può trovare giustificazione nel rischio di impunità che deriverebbe dall'eventuale mancata considerazione di tali informazioni.

Quantità crescenti di dati elettronici, tecniche investigative opache, e la mancata *disclosure* tempestiva di informazioni digitali rendono spesso illusorio anche il diritto della difesa a partecipare effettivamente al processo di formazione della

16 Corte di Giustizia Cause riunite C-293/12 e C-594/12, *Digital Rights Ireland Ltd contro Minister for Communications, Marine and Natural Resources e altri* in curia.europa.eu; Corte di Giustizia, Cause riunite C-511/18, C-512/18 e C-520/18 *La Quadrature du Net e altri c. Premier Ministre e altri*, ECLI:EU:C:2020:791 in curia.europa.eu.
17 Corte di Giustizia, Cause riunite C-511/18, C-512/18 e C-520/18 *La Quadrature du Net e altri c. Premier Ministre e altri*, ECLI:EU:C:2020:791 in curia.europa.eu
18 Corte di Giustizia, causa C-548/21, C G v. *Bezirkshauptmannschaft Landeck* ECLI:EU:C:2024:830 in curia.europa.eu, para 95.
19 Ibid., para 93.

prova accentuando il rischio di uno squilibrio strutturale tra accusa e difesa e mettendo in discussione la stessa effettività del principio del contraddittorio.

Come si vedrà nel corso dell'ultimo capitolo, in cui saranno approfondite le sfide alla protezione dei diritti alla privacy e alla difesa nell'epoca digitale, il principio della tutela giurisdizionale effettiva svolge un ruolo fondamentale nella salvaguardia dei diritti fondamentali, contribuendo a limitare l'impatto delle misure investigative invasive.[20]

1.1.3 Principio di territorialità e prova digitale

Nel contesto digitale il principio di territorialità, che attribuisce la giurisdizione allo Stato in cui viene commesso il reato diventa un ostacolo all'azione penale. Le chat criptate scambiate sulle piattaforme di messaggistica sono una delle categorie più rilevanti di prove digitali. I service provider sono i luoghi fisici in cui vengono archiviate le chat, presso gli uffici dei social network. Tali soggetti sono aziende private spesso situate in stati diversi da quello in cui avviene il processo, il che comporta maggiori difficoltà pratiche nella raccolta delle prove. A volte, nemmeno il service provider conosce l'esatta posizione dei dati, provocando un'incertezza ancor maggiore.[21] Nel caso di reati informatici è ben più difficile accertare dove si sia perpetrata la condotta poiché spesso gli effetti si producono in stati diversi.

Ad un primo esame, le prove digitali sollevano problemi giurisdizionali. L'ubiquità del *cloud computing* porta a due effetti diversi: conflitti giurisdizionali e la necessità di una cooperazione internazionale, anche in indagini penali che a prima vista parrebbero esclusivamente nazionali.[22] L'accesso ai dati è un vero e proprio ambito di tensione giurisdizionale in cui diverse entità sovrane potrebbero potenzialmente esercitare la propria competenza.[23] Come dimostrato

20 O. Murro, op. cit., p.216.
21 H. Abraha*, Law enforcement access to electronic evidence across borders: mapping policy approaches and emerging reform initiatives*, in *International Law of Information Technology*, 2021, 29, 118, 121.
22 I. Zerbes*, Legal Issues of Transnational Exchange of Electronic Evidence in Criminal Proceedings*, *European Criminal Law. Review*.,2015, 5, 304, 306.
23 Abraha, op. cit., p.14.

da diversi casi quali ad esempio *Microsoft c. Belgio*, queste tensioni si riflettono in un corpus giurisprudenziale ben sviluppato in cui entrano in gioco interessi contrapposti.[24] Lo Stato territoriale in cui si trovano i dati cerca di salvaguardare le proprie prerogative sovrane; lo Stato che esercita l'azione penale fa valere il proprio interesse a garantire la sicurezza pubblica e a far rispettare il diritto penale; l'individuo interessato rivendica il diritto alla privacy e alla protezione dei dati; mentre il fornitore di servizi mira a preservare la propria autonomia imprenditoriale e a evitare indebite interferenze.[25]

Come già accennato, sia il Consiglio d'Europa che l'Unione Europea hanno saputo riconoscere tempestivamente la portata rivoluzionaria della prova digitale, emanando strumenti legislativi che facilitano l'ingresso di questo tipo di prova nei procedimenti penali e obbligano gli Stati membri a rispettare regole minime. I legislatori sono intervenuti in questo settore, consapevoli della tensione intrinseca tra la prova digitale e la tutela dei diritti fondamentali. La Direttiva OEI e la Convenzione di Budapest sono strumenti legislativi complementari che costituiscono un approccio unificato, ma insufficiente, per affrontare le sfide della prova digitale. Mentre la Convenzione prevede l'armonizzazione degli aspetti legali e sostanziali della criminalità informatica, la Direttiva OEI fornisce agli Stati membri dell'Unione Europea uno strumento efficiente e rapido per la raccolta delle prove.[26]

L'introduzione dell'OEI può essere attribuita alle inefficienze del tradizionale quadro di mutua assistenza giudiziaria. Il suo ampio utilizzo deriva dal fatto che ha ampiamente sostituito la mutua assistenza legale come strumento principale per la raccolta di prove transfrontaliere all'interno dell'UE. Nel campo delle prove digitali, le carenze degli strumenti classici della mutua assistenza legale si

24 P. De Hert, *The Microsoft Ireland case and the cyberspace sovereignty trilemma: Post-territorial technologies and companies question territorial state sovereignty and regulatory state monopolies* in *Brussels Privacy Hub Working Paper* 2018, 4/11.
25 A.M. Osula, *Transborder access and territorial sovereignty* in *Computer law and Security Rev*iew, 2021, 29/118, 719, 725.
26 S. Depauw*, Electronic Evidence in Criminal Matters: How about E-Evidence Instruments 2.0*, *Europeam Criminal Law Review.,* 2020, 8, 62, 71.

fanno sentire ancora di più, infatti, essi sono concepiti per un tipo di prova più tradizionale. Il quadro normativo è stato di recente arricchito dalla emanazione del Regolamento E-evidence sull'OEP e OEC. Questi ultimi sono strumenti giuridici che consentono alle autorità giudiziarie di uno Stato membro di richiedere direttamente, in modo rapido ed efficace, la produzione o conservazione di prove digitali da fornitori di servizi situati in un altro Stato membro, senza necessità di ricorrere ai tradizionali strumenti di cooperazione giudiziaria.[27]

In un'ottica comparativa, le istituzioni europee si sono mosse in modo coerente rispetto al legislatore statunitense, il quale ha elaborato il CLOUD Act. Lo strumento normativo determina la possibilità per gli u.s.a. di stipulare trattati che facilitano la cooperazione internazionale in materia di raccolta della prova digitale presso service provider.[28] Questa norma contiene forme di protezioni ingenti nei confronti dei dati appartenenti ai cittadini americani, e rappresenta la volontà dello stato in cui la maggior parte dei service provider rilevanti risiedono di influenzare la politica globale di raccolta della prova digitale nei procedimenti penali. Finora solo l'Australia e Il Regno Unito hanno concluso questo tipo di trattati. Per quanto riguarda i rapporti con l'Europa, persistono importanti divergenze in tema di protezione dei dati personali. Il GDPR, infatti, fornisce una protezione elevata e non comparabile rispetto alle analoghe legislazioni statunitensi, il che complica l'efficientamento della cooperazione efficiente in materia di raccolta della prova.[29]

---

27 S.Tosza, '*All Evidence is Equal, but Electronic Evidence is More Equal than Any Other: The Relationship between the European Investigation Order and the Admissibility of Evidence in Criminal Proceedings'* in *New Journal of European Criminal L*aw, 2020, 11/2, 161.
28 U.S. Department of Justice, CLOUD Act Resources, disponibile su https://www.justice.gov/criminal/cloud-act-resources accesso 9 luglio 2025.
29 Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali e alla libera circolazione di tali dati; Calderini B., *Cloud Act: la norma USA che fa a pugni con la privacy europea, i nodi* in Agenda digitalE https://www.agendadigitale.eu/sicurezza/privacy/cloud-act-la-norma-usa-che-fa-a-pugni-con-la-privacy-europea-i-nodi/, accesso 9 luglio 2025.

La tendenza generale, constata dalla legislazione globale,[30] in tema di prova elettronica e confermata dal recentissimo Regolamento e-evidence dell'UE è la "privatizzazione" dei meccanismi di ricerca della prova in questa area del diritto procedurale penale. L'importanza di soggetti privati, spesso particolarmente strutturati, quali detentori di informazioni vitali per la repressione dei reati e il mantenimento della sicurezza pubblica, ha imposto ai legislatori di tutto il mondo di elaborare strumenti avanzati di collaborazione che coinvolgano anche imprese private.[31] L'OEP e l'OEC sono il passaggio più recente di una procedura penale più dinamica e adattabile al contesto economico moderno. A riprova di ciò, lo scopo perseguito dal regolamento è quello di consentire alle pubbliche accuse degli Stati membri di ingiungere direttamente soggetti che prestino servizi nell'UE di fornire o di mantenere prove elettroniche che siano nella loro disponibilità. I prestatori di servizi sono identificati nelle persone fisiche o giuridiche, attive nell'Unione, che si occupino di comunicazioni elettroniche, servizi della società dell'informazione (quali social network, mercati online, servizi di hosting) e servizi di nomi di dominio Internet e di numerazione IP.[32]

1.1.4 Il ruolo delle best practices nella gestione delle sfide tecnologiche della prova digitale

L'alto livello di sofisticazione tecnologica rappresenta un problema per la raccolta, la conservazione e la successiva ammissibilità della prova digitale nel procedimento penale. Nella disciplina e nella regolamentazione della prova digitale, il diritto e la tecnica si incontrano, e il giurista è chiamato a fornire soluzioni che garantiscano i diritti fondamentali in un contesto innovativo. Le principali insidie che derivano dalla natura tecnica della prova digitale sono la modificabilità e la promiscuità del dato informatico. L'assenza di incorporazione

30 Convenzione sulla criminalità informatica, aperta alla firma il 23 novembre 2001, ETS n. 185; U.S. Department of Justice, CLOUD Act Resources, disponibile su https://www.justice.gov/criminal/cloud-act-resources accesso 9 luglio 2025.
31 A. Rosanò, *La "privatizzazione" nello spazio di libertà, sicurezza e giustizia: tre esempi* in *Rivista di diritto europeo* 2020, 1.
32 Ibid.

in un supporto materiale comporta un più elevato coefficiente di alterabilità della prova digitale rispetto a quella analogica.[33]

Il rischio più avvertito è la possibile mancanza di coincidenza tra il dato così come è stato raccolto e ciò che viene effettivamente introdotto nel processo penale. I dati informatici vengono di norma raccolti in masse imponenti e senza un'accurata selezione. La caratteristica della promiscuità rende complessa l'individuazione, l'estrazione e la selezione del dato rilevante ai fini probatori, accrescendo il rischio che informazioni non pertinenti o addirittura pregiudizievoli per l'imputato vengano acquisite o valutate nel processo penale.[34]

In tale contesto, la prova digitale è stata a lungo regolata esclusivamente dalle best practice delle procure. La *digital forensics*, cioè l'insieme di tecniche volte alla raccolta e conservazione delle prove penali digitali hanno subito un'evoluzione significativa ed una crescente standardizzazione tra diversi stati.[35] L'elaborazione di tali procedure deve essere vista con favore in quanto consente una sufficiente elasticità e adattabilità rispetto al progresso tecnologico. Gli insiemi di dati di grandi dimensioni richiedono una solida infrastruttura tecnologica e procedure standardizzate per garantirne la corretta gestione; tali strutture sono spesso carenti.[36]

Inoltre, problemi come l'incompletezza, l'incoerenza o l'imprecisione dei dati possono portare ad analisi errate e, in ultima analisi, a risultati ingiusti. Nel contesto delle prove digitali, queste carenze possono avere conseguenze particolarmente gravi, in quanto possono compromettere sia l'ammissibilità che il valore probatorio delle prove presentate.[37] Tali pericoli sono accentuati in casi

33 P. Tonini C. Conti, *Diritto delle Prove penali*, p. 153.
34 R. Stoykova, *The right to a fair trial as a conceptual framework for digital evidence rules in criminal investigations* in *Computer Law and Security Rev*iew 2023, 49.
35 M. Caianiello e A. Camon, *Digital Forensic Evidence Towards Common European Standards in Antifraud Administrative and Criminal Investigation,* Wolters Kluwer, Milano, 2021, 241.
36 Ibid., 43.
37 Ibid., 246.

di investigazioni digitali che coinvolgono più stati. Un'indagine transfrontaliera può incontrare sfide scoraggianti. La durata del procedimento può essere influenzata dalla mancanza di coordinamento nel perseguimento dei reati. Indagini non coordinate tra i diversi Stati possono comportare una perdita di tempo e di risorse. La difficile comunicazione tra le varie autorità giudiziarie può portare a una insufficiente divisione del lavoro e alla conseguente duplicazione delle indagini. La complessità delle prove digitali deriva anche dalla limitata comprensione dei vari quadri giuridici e degli strumenti di cooperazione internazionale. La situazione è ulteriormente aggravata dalla mancanza di veri e propri standard comuni per la conservazione delle prove digitali.

A tal fine, Eurojust, Europol e l'istituzione di squadre investigative comuni possono costituire un rimedio efficace alla mancanza di scambio di informazioni in casi transfrontalieri. Sebbene l'OEI rappresenti lo strumento giuridico principale per la cooperazione giudiziaria nella raccolta delle prove, questi meccanismi complementari evidenziano che la cooperazione può essere realizzata attraverso vari canali. La missione principale di Eurojust è quella di migliorare il coordinamento e la cooperazione tra le autorità giudiziarie dei diversi Stati membri. Svolge un ruolo centrale nel facilitare le indagini transfrontaliere, il che lo rende particolarmente adatto ad affrontare le sfide derivanti da quadri giuridici frammentati e canali di comunicazione limitati.[38]

Non solo, le agenzie europee per la collaborazione giudiziaria in ambito penale forniscono importanti spunti anche per la formazione di *best practice* condivise da parte delle procure degli stati membri, favorendo sia l'adeguatezza tecnica delle pratiche sia il rispetto degli standard di protezione dei diritti fondamentali conformemente alla Carta di Nizza. Sia il report contro il Cybercrime di Eurojust sia il Sirius report sulla prova digitale, redatto in collaborazione tra Eurjust e Europol, forniscono importanti spunti per il legislatore e per le autorità

38 SIRIUS Project (Eurojust and Europol), EU Electronic Evidence Situation Report (November 2024), 38.

giudiziarie al fine di comprendere in modo significativo le migliori opzioni normative e i risvolti pratici dell'utilizzo di prove digitali.[39]

Secondo il report di Eurojust, L'uso della crittografia complica le indagini, l'aumento della riservatezza e della privacy ha il prezzo di rendere inefficienti le indagini tradizionali. Oggi la crittografia è ampiamente utilizzata dai criminali per nascondere il traffico illecito. Un chiaro esempio di questa tendenza è l'uso delle criptovalute nelle transazioni sospette. Le criptovalute rendono molto più difficile "seguire il denaro" derivante da attività criminali, aumentando le possibilità di riciclarlo. Un'altra sfida importante è rappresentata dall'accesso a grandi volumi di dati e dalla loro successiva conservazione. A causa della sua natura tecnica, l'inclusione di prove digitali allunga la durata dei procedimenti penali e può causare la perdita o l'alterazione dei dati. Le migliori prassi per l'uso delle prove digitali dovrebbero includere metodi di conservazione e ricerca appropriati che favoriscano l'interpretazione appropriata dei dati nel rispetto della privacy e della protezione dei dati.[40]

Il caso *EncroChat* rappresenta un modello di efficace cooperazione giudiziaria transfrontaliera e di buone prassi nella lotta alla criminalità informatica. Condotta congiuntamente dalle autorità francesi e olandesi e coordinata con l'assistenza di Eurojust, l'operazione ha dimostrato il valore del coinvolgimento precoce degli attori giudiziari e della creazione di una squadra investigativa comune nella gestione di complesse indagini transnazionali.[41] Eurojust ha svolto un ruolo fondamentale nel facilitare le riunioni di coordinamento, che hanno consentito arresti e perquisizioni simultanei e lo scambio reciproco di informazioni. Il caso ha anche sottolineato l'importanza di garantire un'efficace tutela giudiziaria nel contesto di misure investigative intrusive.[42] Per quanto riguarda l'intercettazione di comunicazioni criptate, l'operazione ha evidenziato

39 Eurojust cybercrime report (27), 6.
40 M. Caianello e A. Camon, op. cit, p 179.
41Corte di giustizia, causa C-670/22, *Encrochat*, ECLI:EU:C:2024:385 in curia.europa.eu; Whal., ECJ Ruled in EncroChat Case, in eucrim, 7 marzo 2024, disponibile in https://eucrim.eu/news/ecj-ruled-in-encrochat-case/, ultimo accesso 17 marzo 2025.
42 Eurjust Cybercrime report (n.27), 10.

la necessità di un approccio equilibrato tra l'efficienza investigativa e la salvaguardia dei diritti fondamentali, come verrà ulteriormente spiegato nei capitoli successivi.[43]

43 J.Oerlemans *Legal Aspects of the EncroChat Operation: A Human Rights Perspective,* in *European Journal of Crime, Criminal law and. Criminal Justice*, 2020, 30, 309, 313.

Capitolo 2 La prospettiva sovranazionale

2.1 Raccolta della prova digitale e cooperazione internazionale

Considerata la natura immateriale e transnazionale della prova digitale, il Consiglio d'Europa e l'UE rivestono un ruolo centrale nell'elaborazione di regole comuni per la sua raccolta, adattando la disciplina normativa affinché possa rispondere alle sfide poste al principio di territorialità. Le linee direttrici della disciplina normativa sono il superamento della *silver platter doctrine* e del *forum shopping* in un'ottica di rispetto dei diritti fondamentali dell'uomo e certezza giuridica. Originariamente sviluppata nel contesto statunitense, la *silver platter doctrine* consentiva alle autorità federali di utilizzare prove ottenute illegalmente da autorità statali, purché queste ultime non fossero soggette agli stessi vincoli costituzionali. Applicata in ambito europeo, questa logica si traduce nel rischio che le autorità di uno Stato membro possano utilizzare prove raccolte all'estero in violazione di garanzie fondamentali, sfruttando il fatto che il paese di esecuzione non applichi le stesse garanzie procedurali.

L'approccio congiunto rispetto alla repressione dei reati serve ad evitare la creazione dei c.d *safe hevens*, nei quali le autorità giudiziarie potrebbero acquisire prove digitali in condizioni di minore tutela dei diritti fondamentali, per poi trasferirle e utilizzarle nei procedimenti penali di altri Stati membri.[44] L'assenza di standard comuni nella raccolta della prova digitale crea il rischio di forum shopping, ovvero la possibilità per le autorità inquirenti di selezionare lo Stato membro più "tollerante" dal punto di vista probatorio per acquisire *digital evidence*.[45] Mentre la disciplina della Convenzione di Budapest si è concentrata sulla armonizzazione delle misure sostanziali e procedurali per combattere il cybercrime, l'UE ha elaborato avanzati strumenti di collaborazione giudiziaria in materia penale quali l'OEI e l'OEP. l'OEI rappresenta un importante strumento normativo che consente a un'autorità giudiziaria di uno Stato membro

44 M. van Wijk, *Cross-border Evidence Gathering: Equality of Arms within the EU?*, Eleven International Publishing, L'Aia, 2017, 53.
45 A. Klip, European Criminal Law: An Integrative Approach, Intersentia, Anversa, 2021.

di disporre l'esecuzione di atti di indagine in un altro Stato membro.[46] Per i motivi che si andranno ad approfondire nei seguenti paragrafi l'EIO è uno strumento fortemente innovativo e più efficiente rispetto ai tradizionali strumenti di collaborazione in materia penale tra stati diversi quali ad esempio la Convenzione di mutua assistenza giudiziaria del 1959 elaborata dal Consiglio d'Europa.[47] La Convenzione di mutua assistenza legale del Consiglio d'Europa rappresenta il modello tradizionale di cooperazione giudiziaria, tuttora rilevante nei rapporti con Stati terzi.

La legislazione del Consiglio d'Europa si è successivamente evoluta con la Convenzione di Budapest del 2001 sulla criminalità informatica, che ha rappresentato il primo strumento internazionale vincolante volto a disciplinare sia la repressione dei reati informatici sia la cooperazione transnazionale in materia di prove digitali. Tale quadro è stato ulteriormente rafforzato con l'adozione del Secondo Protocollo addizionale del 2022, il quale introduce disposizioni specifiche per facilitare l'accesso diretto ai dati da parte delle autorità competenti, rafforzare le garanzie procedurali e migliorare i meccanismi di cooperazione rapida, anche attraverso canali diretti con i fornitori di servizi e procedure più snelle di mutua assistenza.[48]

A differenza dell'OEI che viene utilizzato per qualsivoglia tipo di prova, l'OEP rappresenta uno strumento legislativo ritagliato sulle caratteristiche della prova digitale, poiché consente all'autorità giudiziaria di rivolgersi direttamente al service provider ed ha tempi di emissione ed esecuzione marcatamente più brevi. L'Ordine Europeo di Produzione è una misura giuridica vincolante emessa da un'autorità giudiziaria o competente di uno Stato membro dell'Unione europea che impone a un fornitore di servizi stabilito o rappresentato in un altro Stato membro di fornire dati elettronici specifici in un termine breve e definito,

46 H. Satzger, *International and European Criminal Law*, C.H. Beck, Monaco, 2021, 123.
47 Convenzione europea di assistenza giudiziaria in materia penale, firmata a Strasburgo il 20 aprile 1959, ETS n. 030.
48 Clough, op. cit., p.700.

affinché possano essere utilizzati come prova in un procedimento penale o per l'esecuzione di una decisione giudiziaria.

Il quadro normativo comunitario è stato arricchito dall'istituzione della Procura europea che sta contribuendo a facilitare lo scambio e la circolazione della prova digitale grazie al coordinamento centralizzato delle indagini e all'impiego di canali diretti tra i procuratori europei delegati.

2.1.1 Gli strumenti tradizionali di mutua assistenza legale e la Convenzione del 1959

La globalizzazione delle attività criminali e la mancanza di giurisdizione su atti coercitivi volti ad ottenere prove in uno stato diverso da quello di appartenenza ha portato gli Stati di tutto il mondo ad accordarsi circa modalità di condivisione della prova. Nei trattati di mutua assistenza legale troviamo diverse disposizioni volte alla collaborazione tra la polizia giudiziaria di diversi stati e le autorità giudiziarie com l'inseguimento transfrontaliero, la sorveglianza transfrontaliera, scambio di informazioni e la raccolta di prove. Questi trattati contengono spesso disposizioni volte a consentire che uno Stato compie un'azione o misura investigativa volta alla raccolta di prove al fine di condurre indagini, procedere penalmente, celebrare un processo o eseguire una sanzione in un altro Stato. Un chiaro esempio di strumento tradizionale di mutua assistenza legale è la Convenzione di mutua assistenza giudiziaria del 1959.[49]

La rogatoria internazionale (dal francese *commissions rogatoires*) costituisce uno strumento di cooperazione giudiziaria tra Stati, volto a ottenere o trasmettere atti processuali, comprese, ad esempio, le prove digitali, quando un procedimento penale pendente in uno Stato richieda lo svolgimento di attività istruttorie nel territorio di un altro Stato. L'esecuzione di una rogatoria segue una procedura bifasica, che prevede un primo vaglio di tipo politico da parte del Ministero della giustizia, seguito da un provvedimento di exequatur dell'autorità

49 C.M. Paolucci, Cooperazione giudiziaria e di polizia in materia penale UTET Giuridica, Milano, 2007.

giudiziaria. La rogatoria può essere richiesta per tutti i crimini che siano nella giurisdizione dello stato territoriale, per alcuni atti di investigazione è richiesto che sia presente il requisito della doppia criminalità, e cioè che si stia perseguendo un crimine che è tale sia nello stato richiedente sia in quello richiesto.[50]

In alcuni casi tassativi è prevista la possibilità di rifiutarsi di collaborare: in caso di perseguimento di reati politici o fiscali, quando l'assistenza è pregiudizievole per la sovranità, la sicurezza, l'ordine pubblico o altri interessi essenziali dello Stato richiesto, se gli Stati hanno aggiunto motivi di rifiuto tramite riserve all'art. 2 della Convenzione (ad esempio il *ne bis in idem* o perseguimento nello Stato richiesto) e in caso di mancato rispetto dei diritti fondamentali previsti dalla CEDU. L'assistenza giudiziaria segue, in linea di principio, la *lex loci* secondo l'art. 3 della Convenzione 1959; tuttavia, ai sensi dell'art. 8 del Secondo Protocollo addizionale, può essere adottata una forma ibrida, che consente di rispettare le formalità e le procedure indicate dallo Stato richiedente, purché queste non violino i principi fondamentali dell'ordinamento dello Stato richiesto.[51]

2.1.2 La convenzione di Budapest

La promulgazione della Convenzione di Budapest ha segnato un rilevante progresso nella disciplina della raccolta transnazionale della prova digitale, introducendo strumenti di cooperazione più adeguati. Nell'era contemporanea e nel prossimo futuro, la prova digitale è essenziale per l'attribuzione della responsabilità penale sia per i reati informatici in senso stretto sia per i reati comuni commessi via internet. reati informatici sono quelli inseriti nell'elenco

50 G. Papucharova, *The Request for Mutual Assistance and the European Investigation Order – Is the Modern Legal Assistance Instrument Better than its Predecessor* in *International Conference Knowledge-Based Organization* 2020, 26/2, 211.
51 Consiglio d'Europa, Relazione esplicativa alla Convenzione europea di assistenza giudiziaria in materia penale (Aprile 1959).

minimo e facoltativo della Convenzione di Budapest, in cui l'uso del sistema informatico è intrinseco ed essenziale per la commissione del reato.[52]

La Convenzione mira principalmente a: armonizzare gli elementi del diritto penale sostanziale interno relativi ai reati e alle disposizioni connesse nell'ambito della criminalità informatica; prevedere poteri di diritto penale processuale interno necessari per l'indagine e il perseguimento di tali reati, così come di altri reati commessi mediante un sistema informatico o per i quali le prove siano in forma elettronica; istituire un regime rapido ed efficace di cooperazione internazionale. Gli obiettivi perseguiti dalla Convenzione di Budapest trovano attuazione in modo sistematico all'interno del testo convenzionale, poiché a ciascuna finalità individuata corrisponde una specifica parte normativa: dalle disposizioni sostanziali volte all'incriminazione delle condotte tipiche di criminalità informatica, a quelle procedurali concernenti i poteri di indagine e acquisizione della prova digitale, fino alle clausole di cooperazione internazionale che mirano a garantire l'efficacia transfrontaliera delle indagini e dei procedimenti penali.[53]

Ai fini della presente tesi, si farà riferimento alla Convenzione di Budapest come strumento fondamentale per l'armonizzazione del diritto penale processuale, e quindi al Capitolo 2 della stessa. Il diritto penale sostanziale della Convenzione di Budapest non è rilevante ai fini della presente tesi in quanto la prova digitale può servire per l'accertamento sia di crimini informatici sia tradizionali. Nonostante nell'ambito degli stati membri dell'UE la collaborazione internazionale sia favorita dalla Direttiva OEI e dal Regolamento E-evidence, si prenderà in considerazione brevemente il secondo protocollo addizionale della Convenzione.

Come già accennato nel precedente capitolo la Convenzione di Budapest è stata recepita attraverso la l. 18 Marzo 2008, n. 48. Tale norma ha modificato il codice

52 Consiglio d'Europa, Rapporto esplicativo alla Convenzione sulla criminalità informatica (23 novembre 2001), 7.
53 Rapporto esplicativo alla Convenzione sulla criminalità informatica.

di procedura penale e si configura come un tentativo di conformare il diritto interno al progresso tecnologico dettato dal sempre crescente utilizzo di nuove forme di comunicazione informatica in ambito criminale. La Convenzione adatta le tradizionali misure procedurali, come la perquisizione e il sequestro, al nuovo scenario tecnologico. Inoltre, nuove misure, quali ad esempio la conservazione rapida dei dati, sono state elaborate al fine di garantire che le misure tradizionali di raccolta restino efficaci in un ambiente caratterizzato da notevole volatilità. Poiché i dati informatici non sono sempre statici, ma possono essere in transito nel processo di comunicazione, anche altre procedure tradizionali di raccolta, come la raccolta in tempo reale dei dati di traffico e l'intercettazione dei contenuti, sono state adattate per consentire la raccolta di dati elettronici in corso di comunicazione.[54]

L'area di competenza della Convenzione è definita in ampio tale da comprendere indagini o procedimenti penali riguardanti l'accertamento di reati previsti dalla Convenzione, altri reati penali commessi mediante un sistema informatico, nonché alla raccolta di prove in forma elettronica relative a un reato. Ciò garantisce che, fatte salve le eccezioni contenute nella Convenzione, le prove in forma elettronica relative a qualsiasi reato possano essere ottenute o raccolte mediante tali poteri e procedure. Tali procedure devono essere conformi rispetto ai diritti umani e le libertà applicabili sulla base del diritto nazionale di ciascuna Parte contraente. Poiché la Convenzione si applica a Parti appartenenti a sistemi giuridici e culture differenti, non è possibile specificare in dettaglio le condizioni e le garanzie applicabili a ciascun potere investigativo o procedura.[55] La Convenzione sancisce l'applicazione del principio di preservazione alle prove digitali. Secondo cui devono essere protette da qualsiasi evento che possa causarne il cambiamento o il deterioramento della qualità o della condizione attuale. A tale scopo, le Parti contraenti possono

54 G. Corasaniti, *Cybercrime. Le nuove frontiere della responsabilità penale e della prova digitale*, Giuffrè, Milano, 2022.
55 Rapporto esplicativo alla Convenzione sulla criminalità informatica.

emanare ordini di produzione rivolti ai service provider e volti ad ottenere la conservazione di dati.

La Convenzione prevede un'ampia gamma di mezzi di ricerca della prova che possono essere impiegati nel corso di investigazioni digitali. Gli istituti tradizionali del sequestro e della perquisizione sono modellati in modo tale da garantire un'efficace acquisizione e tutela della prova digitale. Tali atti coercitivi espressione della potestà pubblica comprendono: il sequestro o la protezione equivalente di un sistema informatico, di sue parti o di supporti di memorizzazione; la creazione e conservazione di copie dei dati informatici pertinenti; il mantenimento dell'integrità dei dati memorizzati; nonché la possibilità di rendere inaccessibili o rimuovere i dati stessi dal sistema informatico oggetto di ricerca.[56] La Convenzione prevede anche misure di raccolta in tempo reale di dati di traffico e di intercettazione di dati di contenuto. Per mezzo delle prime le autorità giudiziarie possono identificare gli autori di un reato attraverso l'identificazione di indirizzi ip durante l'utilizzo di servizi informatici. Le autorità possono archiviare, raccogliere e obbligare i service provider a fornire tale tipologia di dati. La misura dell'intercettazione di dati di contenuto è accompagnata da salvaguardie maggiori vista la maggiore intrusività della misura. I dati di contenuto non determinano solo l'identificazione del reo ma anche l'apprensione di informazioni rilevanti incluse nelle telecomunicazioni.

2.1.3 Il secondo protocollo addizionale della convenzione di Budapest

Data l'immaterialità e transnazionalità, la collaborazione internazionale in materia di prova digitale rappresenta un passo essenziale verso una risposta globale nei confronti della criminalità informatica. Il Consiglio d'Europa, sulla base delle conclusioni pubblicate dal *Cloud Evidence Group* del Comitato della Convenzione di Budapest, ha constato l'inefficienza dei tradizionali strumenti di mutua assistenza legale, nonché la possibilità di migliorare i meccanismi previsti

56 S. De Flammineis*, Le sfide della prova digitale: sequestri, chat, processo penale telematico e intelligenza artificiale*, Sistema penale, 2024.

dalla Convenzione di Budapest e si è adoperato per la predisposizione di strumenti più efficienti. L'inadeguatezza dei precedenti atti normativi è mostrata anche dal ricorso alla c.d. *voluntary disclosure*, le giurisdizioni nazionali hanno iniziato a bypassare le forme tradizionali di cooperazione previste dalla Convenzione, rivolgendosi direttamente ai fornitori di servizi per la raccolta delle informazioni. Ne consegue una carenza di legalità nelle attività investigative e un'ampia discrezionalità riconosciuta a soggetti privati, i quali operano secondo logiche di mercato.[57]

Allo scopo di favorire la cooperazione rafforzata nell'ambito della raccolta della prova digitale, nel 2022, il Consiglio d'Europa ha adottato il secondo protocollo addizionale alla Convenzione di Budapest.[58] Esso costituisce uno strumento ulteriore ed accessorio alla Convenzione, e un *continuum* rispetto alle finalità della stessa e mira a favorire la circolazione delle prove e l'interazione coi service provider. In questo senso, è opportuno notare che il protocollo addizionale ha caratteristiche affini con il Regolamento E-evidence emanato da parte dell'UE.

Il protocollo istituisce all'art. 6 e 7 una procedura che consente la cooperazione diretta tra le autorità di una Parte e un fornitore di servizi situato nel territorio di un'altra Parte, al fine di ottenere informazioni sugli abbonati. L'obbiettivo esplicito è di superare le lentezze e le inefficienze delle procedure tradizionali di mutua assistenza, rendendo più celere l'accesso a una tipologia di dati, le informazioni sugli abbonati, che spesso costituiscono il punto di partenza per lo sviluppo delle indagini penali, soprattutto nei contesti digitali. Qualora l'*internet provider* non risponda nei termini o rifiuti di fornire i dati, la Parte richiedente può emettere un'ordinanza da presentare a un'altra Parte, affinché quest'ultima

57 M. Buccarella*, Il secondo Protocollo addizionale alla Convenzione di Budapest sulla criminalità informatica: cooperazione rafforzata e disclosure delle prove elettroniche* in *Quaderni AISDUE*, 2022, 1.
58 Secondo Protocollo addizionale alla Convenzione sulla criminalità informatica sulla cooperazione rafforzata e la divulgazione delle prove elettroniche, aperto alla firma il 12 maggio 2022, CETS n. 224.

possa obbligare un fornitore di servizi nel proprio territorio a fornire informazioni sugli abbonati o dati relativi al traffico.

Viene così introdotto un meccanismo che integra le disposizioni sull'assistenza reciproca previste dalla Convenzione. Esso è concepito per essere più snello rispetto alle attuali procedure di assistenza reciproca, poiché richiede alla Parte richiedente di fornire un numero più limitato di informazioni e consente un accesso più rapido ai dati attraverso un canale diretto verso i *service provider*.[59] L'idea di fondo è chiara: senza una procedura più agile, gli Stati rischiano di vedere frustrati i propri sforzi investigativi. Le procedure classiche erano pensate per un contesto "analogico", fatto di rogatorie cartacee e tempi lunghi; oggi, invece, serve un modello che tenga conto della volatilità delle prove digitali e dell'urgenza di agire in tempo reale. Il meccanismo di cooperazione è rafforzato dall'esistenza di procedure d'emergenza che sono caratterizzate da ancor più speditezza ed efficienza al fine di ottenere una comunicazione accelerata dei dati rilevanti.[60]

Questo meccanismo si aggiunge, senza pregiudicarli, agli altri strumenti di assistenza reciproca previsti dalla Convenzione o da altri accordi multilaterali o bilaterali, ai quali ciascuna Parte può continuare a fare ricorso. Quando, come spesso accade, si intendono ottenere contemporaneamente informazioni sugli abbonati, dati relativi al traffico e contenuti memorizzati, può risultare più efficiente richiedere tutte e tre le tipologie di dati riferite al medesimo account mediante un'unica richiesta tradizionale di assistenza giudiziaria, piuttosto che ricorrere, per alcune categorie di dati, al meccanismo previsto dal presente art. e, per le altre, a una distinta procedura di assistenza reciproca.[61]

---

59 Consiglio d'Europa, Rapporto esplicativo al Secondo Protocollo addizionale alla Convenzione sulla criminalità informatica sulla cooperazione rafforzata e la divulgazione delle prove elettroniche, CETS n. 224, Strasburgo, 12 maggio 2022.
60 S. Aterno, *La Convenzione di Budapest del 2001 e la L. n. 148/2008* in Cadoppi A., *Cybercrime*, Utet Giuridica, Torino, 2023, 1578.
61Ibid.

Dando attuazione all'art. 13 della Convenzione che stabilisce che ciascuna Parte rispetti le condizioni e le garanzie previste dal proprio diritto interno, nonché il rispetto dei diritti umani, l'art. 14 stabilisce la protezione dei dati personali sul modello comunitario. Siamo in presenza di una norma che usa come modello la legislazione europea e che allarga agli stati sottoscrittori della protocollo addizionale estranei alle logiche del diritto europeo, garanzie già previste nel GDPR quali la limitazione delle finalità, individuazione di una base giuridica, qualità dei dati e previsione di regimi "speciali" per alcune particolari categorie, obblighi gravanti sui titolari del trattamento, diritti dei soggetti ai quali i dati si riferiscono e il controllo indipendente secondo il diritto alla revisione giudiziale.[62]

2.1.4 L'ordine europeo d'indagine

Nell'ambito della legislazione comunitaria, lo sviluppo dello Spazio di Libertà, Sicurezza e Giustizia è caratterizzato dall'intenzione del legislatore europeo di applicare i principi stabiliti nell'ambito del precedente primo pilastro, riguardante la politica economica e monetaria, alla cooperazione giudiziaria in materia penale. In base al principio del mutuo riconoscimento, le decisioni giudiziarie, come le persone, i beni, i servizi e i capitali, dovrebbero circolare liberamente tra gli Stati membri. La fiducia reciproca è una pietra miliare del mutuo riconoscimento.[63] Il riconoscimento reciproco delle decisioni giudiziarie è possibile perché gli Stati membri accettano l'esistenza di un elevato grado di omogeneità nella tutela dei diritti umani. La cooperazione giudiziaria in materia penale implica una accettazione delle differenze e una presunzione di rispetto del diritto dell'UE e dei diritti fondamentali nei diversi Stati membri. Quello della fiducia reciproca non è, tuttavia, un principio assoluto, ma una presunzione

62 G. Ruotolo*, La disciplina dell'e-evidence e la cooperazione rafforzata nel secondo Protocollo addizionale alla Convenzione di Budapest* in *Diritto penale e processo*, 2022, 8, 1026.
63 Corte di giustizia dell'Unione europea, parere 2/13, *Adesione dell'UE alla CEDU*, ECLI:EU:C:2014:2454, ECR I-0000 curia.europa.eu.

relativa che può essere messa in discussione in presenza di una grave minaccia alla tutela dei diritti fondamentali.[64]

Il mutuo riconoscimento e la fiducia reciproca costituiscono le basi su cui è stata istituita la Direttiva OEI. L'OEI è il più importante strumento giuridico dell'UE attualmente a disposizione delle autorità giudiziarie per la raccolta di prove in altri Stati membri. L'adozione di questo strumento giuridico ha notevolmente accelerato e snellito la raccolta delle prove rispetto ai tradizionali accordi di mutua assistenza legale.[65] L'ottimizzazione della raccolta e dello scambio di prove tra Stati diversi nelle indagini transnazionali è in gran parte dovuta alle semplificazioni procedurali introdotte dalla Direttiva. In primo luogo, è stato eliminato il passaggio intermedio del controllo politico: l'emissione e l'esecuzione dell'OEI coinvolgono solo le autorità giudiziarie. In secondo luogo, il controllo giurisdizionale dell'OEI è stato limitato a specifici motivi di rifiuto, migliorando così l'efficienza del processo.[66]

Questo risultato è possibile solo grazie all'elevato grado di cooperazione e fiducia reciproca tra gli Stati membri. La fase obbligatoria di verifica del rispetto dei diritti fondamentali è più formalistica e meno approfondita rispetto ad altri strumenti di cooperazione internazionale.[67] Ciononostante, l'esistenza della fiducia reciproca non può giustificare l'esistenza di un cieco affidamento circa il rispetto dei diritti fondamentali, in particolare nel campo del diritto penale, dove il rischio di violazione delle prerogative dell'imputato nelle indagini transnazionali è significativo. A tal fine, la Direttiva OEI contiene diverse disposizioni volte a salvaguardare i diritti dell'imputato, impedendo che

64 Corte di giustizia dell'Unione europea, C-852/19, *Gavanozov II*, ECLI:EU:C:2021:422 curia.europa.eu.
65 A. Mosna, *Judicial Protection in EU Cross-Border Evidence-Gathering: The EIO as a Case Study*, in *European Criminal Law Review*, 2024,14, 2, 148, 152.
66 Mosna, op. cit., p.155.
67 M. Daniele, *Ricerca e formazione della prova,* in Roberto E Kostoris, *Manuale di procedura penale europea*, Giappichelli, Torino, 2019, 518.

l'autonomia procedurale degli Stati membri crei lacune nella protezione giurisdizionale.[68]

Le Convenzioni di mutua assistenza legale e la Direttiva OEI adottano regole di diritto processuale che devono essere seguite durante la raccolta di prove transnazionali. Queste due regole sono la *lex loci* e la *lex fori*. Secondo la *lex loci*, le prove devono essere raccolte secondo la legge dello Stato richiesto. Applicato alle prove digitali, ciò significa che le misure investigative saranno eseguite seguendo la procedura penale dello Stato in cui i dati sono conservati.[69] Al contrario, la *lex fori* stabilisce che le prove devono essere raccolte secondo la legge dello Stato che esercita l'azione penale.[70] La logica è quella di evitare l'inammissibilità delle prove raccogliendole in conformità alla legge dello Stato in cui saranno utilizzate in tribunale.[71] La Direttiva OEI mitiga l'uso della *lex loci* affermando che l'autorità di esecuzione deve adempiere alle formalità richieste dall'autorità di emissione, salvo che tali formalità violino i principi fondamentali dell'ordinamento giuridico dello Stato di esecuzione.

La Direttiva OEI non include norme sull'ammissibilità delle prove o regole di esclusione probatoria. Il legislatore europeo, attraverso l'introduzione di una *lex loci* temperata, non ha affermato un regime omogeneo della materia che è ancora governata dall'incertezza.[72] In assenza di un approccio normativo uniforme degli Stati membri in materia di raccolta e conseguente ammissibilità delle prove in tribunale e a causa dell'elevato livello di sofisticazione tecnologica delle prove digitali, le "best practice" delle autorità giudiziarie svolgono un ruolo cruciale nel definire l'ambito appropriato delle indagini nel campo delle prove digitali transnazionali.[73]

---

68 O. Calavita, *L'Ordine europeo di indagine penale. Presente e futuro della cooperazione probatoria nell'Unione europea* Wolters Kluwer, Milano, 2023.
69 M. Daniele, *Ricerca e formazione della prova*, p.520.
70 Savignano N., *La tutela dei diritti fondamentali nella raccolta transnazionale della prova penale tra gli Stati membri dell'Unione europea*, Tesi PhD, Università degli Studi di Napoli Federico II, 2019.
71 O. Calavita, *L'Ordine europeo di indagine penale,* p.257.
72 N. Savignano, op. cit., p.207.
73 O. Calavita, *L'Ordine europeo di indagine penale,* p.260.

Lo Stato di emissione, quello in cui le prove saranno utilizzate in giudizio, può contribuire a decidere le formalità e le procedure per lo svolgimento dell'indagine, come consentito dall'art. 9(2) della Direttiva OEI. Ciò garantisce che le regole utilizzate per raccogliere le prove corrispondano a quelle usate per ammetterle in giudizio. Se le prove sono raccolte all'estero in modo conforme agli standard giuridici dello Stato di emissione, in particolare per quanto riguarda la protezione dei diritti individuali, sarà più probabile che esse siano accettate dal giudice del processo senza complicazioni.[74]

L'art. 6 della direttiva OEI stabilisce le condizioni per l'emissione di un OEI: l'atto d'indagine deve essere necessario e proporzionato e deve essere quello che avrebbe dovuto essere disposto in un caso nazionale analogo. Queste condizioni rafforzano lo stato di diritto nella cooperazione transfrontaliera e riconoscono la necessità di un riconoscimento reciproco delle differenze e nel rispetto dei diritti fondamentali.[75] L'art. 6 è strettamente collegato all'art. 14 della direttiva 2014/41/UE, che obbliga gli Stati membri a fornire rimedi giuridici, alle misure investigative ottenute attraverso l'emanazione dell'OEI, equivalenti a rispetto quelli disponibili in un caso nazionale analogo. Questa disposizione sostiene l'applicazione del principio di equivalenza tra i rimedi giuridici nazionali e i rimedi giuridici disponibili nel contesto di indagini transfrontaliere. Le misure non solo devono essere conformi alla *lex fori* e alle norme sui diritti fondamentali, ma devono anche essere impugnabili.[76]

Nel caso Gavanozov II, la CGUE ha riconosciuto che una violazione del principio di tutela giurisdizionale effettiva può essere una base legittima per il rifiuto di emettere un OEI. La Corte ha stabilito che gli articoli 14 e 6 della direttiva OEI obbligano gli Stati membri a garantire alle persone sottoposte a misure investigative l'accesso a mezzi di ricorso equivalenti a quelli disponibili in casi analoghi a livello nazionale. L'assenza di un tale rimedio nello Stato

74 Depauw, op cit, p.23
75 Satzger, op. cit, p.117.
76 A. de Vries, *Evidence and Transnational Punitive Enforcement Proceedings in the European Union*, Intersentia, Anversa, 2024.

membro emittente costituisce una violazione dell'art. 47 della Carta di Nizza e preclude l'emissione di un OEI. È importante notare che la Corte ha riconosciuto la natura non assoluta della fiducia reciproca tra gli Stati membri, definendola una presunzione confutabile, che può essere invertita nei casi in cui vi sia una minaccia sostanziale ai diritti fondamentali. Di conseguenza, la Corte ha stabilito che nei casi in cui il diritto a un rimedio effettivo non è rispettato, il principio del riconoscimento reciproco deve essere superato e l'esecuzione dell'OEI deve essere negata.[77]

In *Dzivev*, la CGUE ha esaminato se prove raccolte tramite un OEI emesso da un giudice non competente secondo il diritto nazionale possano essere comunque utilizzate in giudizio, in nome della tutela degli interessi finanziari dell'UE in modo conforme all'art. 325 TFUE. La validità dell'OEI dipende anche dal rispetto del diritto nazionale, soprattutto in relazione alla competenza dell'autorità emittente. L'efficacia del procedimento penale transfrontaliero non può giustificare una violazione delle regole fondamentali nazionali sulla formazione della prova. L'art. 6 della Direttiva OEI richiede che l'ordine sia emesso da un'autorità competente secondo il diritto nazionale. Un OEI emesso da un'autorità incompetente secondo la legge nazionale non produce effetti validi e le prove raccolte possono essere escluse. Il principio del mutuo riconoscimento ha dei limiti, soprattutto quando si scontra con garanzie fondamentali come il diritto a un equo processo e la legalità dell'istruttoria penale.[78]

Il successivo caso *EncroChat* rappresenta un esempio emblematico dell'importanza di un'efficace tutela giudiziaria nella raccolta transfrontaliera di prove digitali. Come *Gavanozov II* e *Dzivev*, questo caso sottolinea la necessità di rispettare le condizioni stabilite dagli articoli 6 e 14 della direttiva OEI. Tuttavia, la Corte è andata oltre la questione dell'emissione, riconoscendo la possibilità di escludere le prove già in possesso dell'autorità giudiziaria. Infatti,

77 Corte di Giustizia, Causa C-852/19 *Gavanozov II*, ECLI:EU:C:2021:422 in curia.europa.eu.
78 Corte di Giustizia, Causa C 310/16, *Dzivev e altri* ECLI:EU:C: 2019:21 in curia.europa.eu.

l'art. 14, paragrafo 7, dell'OEI stabilisce che lo Stato di emissione deve prendere in considerazione qualsiasi ricorso riuscito al riconoscimento o all'esecuzione di un OEI in base al proprio diritto nazionale. Fatte salve le procedure nazionali, gli Stati membri devono garantire il rispetto dei diritti della difesa e l'equità del procedimento nella valutazione delle prove ottenute tramite l'OEI.[79]

Nonostante la dimostrata efficienza per quanto concerne le prove tradizionali, l'OEI si è dimostrato meno adatto alle sfide poste dalla prova digitale. I termini previsti per l'esecuzione di un OEI, di norma 30 giorni per decidere e 90 giorni per eseguire, risultano inadeguati rispetto al carattere volatile ed effimero di molti dati digitali ritardi nell'acquisizione possono comportare la perdita irreversibile della prova o una significativa riduzione del suo valore probatorio. L'OEI si basa su un modello tradizionale di giurisdizione territoriale in materia di esecuzione, che presuppone un chiaro collegamento geografico tra la prova e uno specifico Stato. Tuttavia, le prove digitali superano frequentemente i confini nazionali, essendo spesso conservate in cloud o su server situati in più giurisdizioni. L'efficacia dell'OEI in materia di prove elettroniche dipende in larga misura dalla cooperazione dei fornitori di servizi privati, spesso ubicati al di fuori dell'Unione europea. Tale dipendenza comporta criticità sia in termini di tempistiche che di certezza nell'acquisizione della prova, aggravate dall'assenza di un quadro normativo armonizzato a livello internazionale che disciplini gli obblighi dei fornitori a collaborare.[80]

2.1.5 Regolamento E-evidence

Sulla base delle difficoltà pragmatiche incontrate dalle autorità giudiziarie nella raccolta della prova digitale, la Commissione europea ha proposto l'istituzione di uno strumento legislativo ad hoc che fosse utilizzabile solo per le prove

79 Corte di Giustizia, Cause riunite C-511/18, C-512/18 e C-520/18 *La Quadrature du Net e altri c. Premier Ministre e altri*, ECLI:EU:C:2020:791 in curia.europa.eu; A. Kanakakis, *The EncroChat Judgment (Case C-670/22, MN): CJEU Steering a Bold Course through the Symplegades of Evidence Admissibility* in *Blog UKAEL* https://ukael.org/2024/07/01/the-encrochat-judgment-case-c-670-22-mn-cjeu-steering-a-bold-course-through-the-symplegades-of-evidence-admissibility, accesso 2 Giugno 2025.
80 S. Tosza, *All Evidence is Equal, but Electronic Evidence is More Equal than Any Other,* p.181.

digitali. Tale proposta del 2018 è diventata il regolamento nel 2023, dopo una vacatio legis di 3 anni, il regolamento diverrà effettivo e avrà applicazione obbligatoria in tutti gli stati membri a partire dal 2026. Il Regolamento E-evidence prevede due diversi istituti l'ordine europeo di produzione (OEP) e l'ordine europeo di conservazione (OEC). Il primo consiste in una decisione vincolante adottata da un'autorità competente che impone a un fornitore di servizi l'obbligo di fornir prove elettroniche specificate. Il secondo è un ordine vincolante adottato da un'autorità competente che impone a un fornitore di servizi l'obbligo di conservare determinati dati per un periodo di tempo limitato, in attesa dell'emissione di un successivo ordine di produzione. L'OEC opera quindi in ottica prodromica rispetto all'ordine di produzione ed è finalizzato ad una successiva emanazione di quest'ultimo.[81]

Per tali ragioni l'OEC è meno intrusivo rispetto ai diritti fondamentali e di conseguenza ha requisiti meno stringenti. Diversamente dall'OEI, entrambi gli strumenti adottano una logica diretta, indirizzandosi direttamente al service provider localizzato in un altro Stato membro, evitando così di dover transitare attraverso le autorità centrali con meccanismi di cooperazione giudiziaria tradizionali. Tuttavia, l'obiettivo di semplificare e accelerare il processo di acquisizione delle prove digitali avviene a costo di evitare l'autorizzazione da parte dello stato di esecuzione.[82]

Entrambi gli strumenti si rivolgono a dati degli abbonati, di traffico, e di contenuto, con diversi presupposti per la emanazione dell'ordine.[83] Per i primi, l'autorizzazione può provenire da un giudice, da un pubblico ministero o da un'altra autorità pubblica competente e può riguardare qualsiasi reato, anche

81 Regolamento E-evidence.
82 O. Calavita., *La proposta di regolamento sugli ordini di produzione e conservazione europei: Commissione, Consiglio e Parlamento a confronto* in La legislazione penale *http://www.lalegislazionepenale.eu/la-proposta-di-regolamento-sugli-ordini-di-produzione-e-conservazione-europei-commissione-consiglio-e-parlamento-a-confronto-oscar-calavita/* acesso 1 Giugno 2025.
83 D. Zapf e D. Malaga, *EU breaks down digital borders: New e-Evidence rules facilitate cross-border investigations* in White and Case Publications https://www.whitecase.com/insight-alert/eu-breaks-down-digital-borders-new-e-evidence-rules-facilitate-cross-border?utm_source=chatgpt.com, accesso 26/08/2025.

crimini bagatellari. Al contrario, l'accesso alla seconda e terza categoria di dati comporta un'intrusione significativa nei diritti fondamentali, ed è limitato alla persecuzione di reati puniti con una pena detentiva pari o superiore a tre anni, oppure un reato incluso nell'elenco delle fattispecie previste. In aggiunta, il regolamento stabilisce in questo caso come idoneo il solo intervento di un soggetto imparziale e indipendente, quale un organo giudicante.[84]

Similarmente all'OEI, sia l'OEP che L'OEC richiedono che l'emissione sia necessaria e proporzionata. La necessità delle misure deve essere valutata in relazione agli obiettivi di una società democratica, come la sicurezza pubblica, la prevenzione dei reati o la protezione dei diritti altrui conformemente all'art. 8(2) della CEDU. Tale valutazione implica l'esistenza di un bisogno sociale imperioso, tenendo conto del margine di apprezzamento riconosciuto alle autorità nazionali. La proporzionalità richiede invece un bilanciamento tra interessi pubblici e privati, secondo un test articolato in tre fasi: la verifica dell'idoneità dello strumento rispetto allo scopo perseguito; la valutazione della stretta necessità, preferendo misure meno lesive dei diritti fondamentali e il controllo di proporzionalità in senso stretto, basato sul confronto tra i vantaggi della misura e i suoi effetti negativi sui diritti.[85]

Per quanto concerne la procedura di emissione, il regolamento prevede due diverse possibilità: una procedura ordinaria e una procedura d'emergenza. La procedura ordinaria si applica in assenza di esigenze di particolare urgenza, in questo caso l'autorità giudiziaria competente emette l'ordine e lo trasmette direttamente al prestatore di servizi stabilito in un altro Stato membro. Il prestatore di servizi dispone di un termine ordinario di dieci giorni per rispondere e fornire i dati richiesti. Al contrario la procedura d'emergenza o coatta si applica nei casi in cui è necessario ottenere celermente prove elettroniche al fine di

84 S. Tosza, *All Evidence is Equal, but Electronic Evidence is More Equal than Any Other*, 187.
85 R. Pezzuto, *Accesso Transnazionale alla Prova Elettronica mel Procedimento Penale: la Nuova Iniziativa Legislativa della Commissione Europea al Vaglio del Consiglio dell'Unione* in *Diritto Penale Contemporaneo* 2019,1, 57, 82.

prevenire un grave rischio per la vita o per l'integrità fisica di una persona, oppure prevenire la commissione di un reato grave. L'ordine deve contenere una motivazione specifica che giustifichi l'urgenza e Il prestatore di servizi ha un termine ridotto di sei ore per eseguire l'ordine e fornire i dati. Restano comunque ferme le tutele dei diritti fondamentali e la possibilità di controllo successivo.[86]

Un aspetto particolarmente delicato disciplinato dal Regolamento E-evidence riguarda la possibilità di conflitto tra l'esecuzione dell'OEP e i diritti o interessi fondamentali di uno Stato terzo. L'art. 17 del Regolamento introduce una procedura articolata volta a contemperare le esigenze della cooperazione giudiziaria in materia penale nel rispetto della sovranità di Stati terzi e dei diritti individuali. Il Regolamento E-evidence attribuisce un ruolo importante ai service provider in un'ottica di controllo decentralizzato del rispetto dei diritti fondamentali dell'accusato, ma anche per garantire che l'attività di impresa possa svolgersi senza indebite pressioni o interferenze esterne.[87]

A fronte della segnalazione da parte del service provider, l'autorità emittente è tenuta a procedere a un primo riesame dell'ordine, valutando le ragioni addotte dal provider nonché eventuali osservazioni dello Stato di esecuzione. Qualora ritenga l'obiezione fondata, l'autorità può procedere al ritiro dell'ordine; in caso contrario, deve sottoporre la questione al vaglio del giudice competente nello Stato di emissione.[89] A questo punto, il giudice effettua una duplice valutazione. In primo luogo, verifica l'effettiva sussistenza di un conflitto con la normativa del paese terzo. Qualora tale conflitto venga escluso, l'ordine viene confermato e il provider sarà tenuto a darvi esecuzione. In caso contrario, il giudice procede ad una valutazione ulteriore, volta a stabilire se, pur in presenza del conflitto,

86 A. Juszczak, *The Use of Electronic Evidence in the European Area of Freedom, Security, and Justice: An Introduction to the New EU Package on E-evidence* in *Eurcrim* 2023,2, 183, 187.
87 D. Feiler, *New EU Regulation on Digital Evidence Opens Up Risk of Data Misuse* in *Connect on Tech by Backer Mckenzie* https://connectontech.bakermckenzie.com/new-eu-regulation-on-digital-evidence-opens-up-risk-of-data-misuse, accesso 1 luglio 2025
88 O. Calavita, *La proposta di regolamento sugli ordini di produzione e conservazione europei,* p.32.
89 N. Visco Comandini, *La Prova Digitale nel Procedimento Penale: profili critici e prospettive future tra confini europei e nazionali*, Tesi di laurea, Luiss Guido Carli, 2023.

l'interesse pubblico sotteso all'ordine giustifichi comunque il suo mantenimento. Il giudice può richiedere informazioni aggiuntive alle autorità del paese terzo interessato, al fine di adottare una decisione pienamente informata.[90]

Al termine di tale procedimento, il giudice decide se confermare l'ordine oppure revocarlo, determinando così il suo ritiro da parte dell'autorità emittente, bilanciando le esigenze dell'efficienza investigativa con il rispetto degli ordinamenti esterni e dei diritti fondamentali. Esso si inserisce adeguatamente nel complesso di garanzie procedurali fornite dal Regolamento e rappresenta un tentativo di soluzione della tensione tra esigenze di celerità nella raccolta della prova digitale e la tutela di principi fondamentali dell'ordinamento europeo.

2.1.6 La procura europea

L'istituzione della procura europea sulla base del Regolamento 2017/1939 ha importanze ricadute sul piano della prova digitale. L'EPPO è un organismo indipendente e sovranazionale incaricato di indagare, esercitare l'azione penale e rinviare a giudizio gli autori di reati che ledono gli interessi finanziari dell'Unione europea (come frodi, corruzione, appropriazione indebita di fondi europei, evasione dell'IVA transfrontaliera superiore a 10 milioni di euro). Opera in modo decentrato, tramite procuratori europei delegati nei singoli Stati membri partecipanti, attualmente 22, ma è coordinata da un livello centrale con poteri direttivi.[94]

La rilevanza della Procura europea emerge in particolare dalla sua natura transnazionale: essa si troverà frequentemente a dover fronteggiare le criticità

90 V. Franssen, *The European Commission's E-evidence Proposal: Toward an EU-wide Obligation for Service Providers to Cooperate with Law Enforcement?* In *European Law Blog* https://europeanlawblog.eu/2018/10/12/the-european-commissions-e-evidence-proposal-toward-an-eu-wide-obligation-for-service-providers-to-cooperate-with-law-enforcement/> ultimo, accesso 29 Giugno 2025.
91 O. Calavita, *La proposta di regolamento sugli ordini di produzione e conservazione europei,* p.36.
92D. Feiler., op. cit., p.5.
93 V. Franssen, op. cit., p.4.
94 Regolamento (UE) 2017/1939 del Consiglio, del 12 ottobre 2017, che attua una cooperazione rafforzata sull'istituzione della Procura europea («EPPO») [2017] GU L283/1

legata all'acquisizione e alla gestione della prova digitale, disponendo tuttavia degli strumenti normativi e operativi necessari per garantire un efficace coordinamento delle indagini a livello sovranazionale. All'istituzione della procura seguirà l'elaborazione e consolidamento di prassi armonizzate in materia di ammissibilità e attendibilità della prova digitale, costituendo un banco di prova per l'effettiva armonizzazione delle garanzie procedurali a livello UE. I procuratori europei delegati agiscono come pubblici ministeri nazionali ma possono contare sul supporto di una struttura centralizzata, utilizzando strumenti digitali comuni per la raccolta e gestione delle prove, nel rispetto del diritto dell'UE. L'EPPO è tenuto a rispettare e applicare in modo uniforme i principi europei, inclusi quelli sul diritto al contraddittorio e sulla tutela dei dati personali, spesso rilevanti nell'acquisizione e nell'uso di prove digitali.[95]

In caso di indagini transfrontaliere, l'assenza di criteri chiari per il tribunale competente favorisce il forum shopping e mina la prevedibilità. L'EPPO ha discrezionalità nel cambiare il forum investigativo e di giudizio, il che può influire negativamente sul diritto dell'imputato a un giudice naturale precostituito per legge. Il Regolamento EPPO rimanda alla normativa UE sui diritti procedurali, ma la sua applicazione è lasciata ai diritti nazionali, infatti, manca una normativa uniforme sul regime probatorio, sulla legalità delle misure coercitive e sull'ammissibilità delle prove il controllo giurisdizionale della CGUE è particolarmente limitato.[96] Tutte queste sfide poste dall'istituzione della procura sono ancor più sentite con riguardo alla prova digitale. La prova digitale è altamente sensibile al tema della legalità e ammissibilità, gli ordinamenti nazionali hanno regole diverse su come acquisire, conservare e utilizzare le prove, anche attraverso misure coercitive. La discrezionalità dell'EPPO nella scelta del foro può far sì che un'indagine possa essere indirizzata verso lo Stato

95 K. Ligeti, *The European Public Prosecutor's Office at Launch: Adapting National Systems, Transforming EU Criminal Law*, Hart Publishing, Oxford, 2022, 457.
96 V. Mitsilegas, *'European prosecution between cooperation and integration: The European Public Prosecutor's Office and the rule of law'* in *Maastricht Journal of European and Comparative Law*, 2021, 28, 2, 245.

con il regime probatorio più favorevole all'accusa, aggirando così regole di garanzia più stringenti.

Considerato l'aumento delle indagini condotte dall'EPPO, nelle quali i dati informatici risultano necessari per dimostrare la commissione di un reato, identificare gli autori e rintracciare i proventi illeciti, l'EPPO è tenuta ad applicare i quadri giuridici, le norme, le procedure e le reti di cooperazione di cui dispone. In caso contrario, non sarebbe in grado di raccogliere efficacemente tali dati informatici e di trasformarli in prove utilizzabili in giudizio. Gli strumenti giuridici applicabili alla gestione della prova elettronica da parte dell'EPPO variano in base al luogo in cui si trovano i dati. Nella maggior parte dei casi, le richieste transfrontaliere di prove elettroniche comportano il trasferimento iniziale di dati personali operativi da parte dell'EPPO verso autorità o soggetti privati situati al di fuori dell'Unione europea. Di conseguenza, la tutela dei dati personali deve essere oggetto di attenta considerazione, e il procuratore europeo delegato deve giustificare il trasferimento dei dati verso Paesi terzi in conformità con le norme sulla protezione dei dati previste dal Regolamento EPPO, ricorrendo a diversi strumenti giuridici.[97]

2.2 Ammissibilità della prova digitale alla luce della giurisprudenza europea

2.2.1 Premessa: l'assenza di regole comuni europee

Sebbene l'art. 82(2) TFUE includa l'ammissibilità reciproca delle prove tra le aree del diritto processuale penale che possono essere oggetto di armonizzazione, il legislatore dell'UE non è ancora intervenuto in questo ambito. Mentre alcuni aspetti fondamentali del procedimento penale, come i diritti delle vittime e della difesa,[98] sono stati in una certa misura armonizzati attraverso diversi strumenti giuridici, il legislatore ha evitato di fornire indicazioni specifiche sull'ammissibilità delle prove. La ragione più importante alla base

97 A. Frunza-Nicolescu, *Electronic Evidence Collection in Cases of the European Public Prosecutor's Office. Legal Framework*, Procedures, and Specifics' in *eucrim*, 2023, 2, 210.
98 Direttiva (UE) 2016/343 del Parlamento europeo e del Consiglio del 9 marzo 2016, sul rafforzamento di alcuni aspetti della presunzione di innocenza e del diritto di presenziare al processo nei procedimenti penali, in GUUE, L 65 del 11 marzo 2016.

della mancanza di armonizzazione risiede nella sensibilità della questione in termini di sovranità nazionale. La Direttiva OEI non fa eccezione, in quanto manca di disposizioni dedicate all'ammissibilità della prova. Pertanto, l'ammissibilità della prova è ancora considerata un grande tabù nell'ambito del diritto penale europeo.[99]

In dottrina è emersa una sempre crescente richiesta di armonizzazione della materia, la quale rappresenta una priorità sempre più urgente;[100] infatti, in assenza di standard comuni sull'ammissibilità, la fiducia reciproca tra le autorità giudiziarie risulta compromessa. Gli Stati esecutori potrebbero essere riluttanti ad agire su un OEI se non possono essere certi che la prova sarà utilizzata in modo equo o legittimo. Regole nazionali divergenti possono quindi ostacolare il regolare funzionamento degli strumenti di reciproco riconoscimento.[101] Un diritto probatorio che varia ampiamente tra gli Stati membri genera inefficienze e il rischio che le prove vengano escluse nello Stato del foro. Inoltre, l'armonizzazione contribuisce a garantire che i diritti dell'imputato, in particolare il diritto a un equo processo ai sensi dell'art. 47 della Carta dei diritti fondamentali dell'UE e dell'art. 6 della CEDU, siano protetti in modo uniforme nell'UE. Ciò evita scenari in cui prove raccolte in uno Stato membro in violazione delle garanzie procedurali vengano ammesse in un altro Stato.[102]

La disposizione vincolante più ampia ed esplicita in materia di prova è l'art. 37 del Regolamento EPPO.[103] Tuttavia, tale disposizione non contiene una clausola di esclusione o di ammissibilità della prova; essa prevede soltanto una clausola

99 J. Vervaele, *Mutuo riconoscimento, fiducia reciproca e standard probatori nel diritto penale europeo: la via della Corte di giustizia europea*, in Illuminati G. *Prova penale e Unione europea*, Bononia University Press, Bologna, 2009,195
100 L. Bachmaier Winter, *Mutual Admissibility of Evidence and Electronic Evidence in the EU: A New Try for European Minimum Rules in Criminal Proceedings?* in *eucrim* 2022,3, 117.
101 J. Vervaele, *Mutuo riconoscimento, fiducia reciproca e standard probatori nel diritto penale europeo*, 197.
102 K. Ligeti, *Admissibility of Evidence in Criminal Proceedings in the EU* in *eucrim*, 2020, 3, 201.
103 Regolamento (UE) 2017/1939 del Consiglio del 12 ottobre 2017, che attua una cooperazione rafforzata sull'istituzione della Procura europea (EPPO), in GUUE, L 283 del 31 ottobre 2017.

di non discriminazione per le prove raccolte all'estero. Ai sensi dell'art. 37(1) del Regolamento EPPO, la prova non dovrebbe essere esclusa unicamente per il fatto di essere stata raccolta in un altro Stato membro. Questa disposizione non armonizza le regole nazionali sull'ammissibilità della prova; piuttosto, mira a impedire che i procedimenti penali nazionali siano isolati rispetto alla prova transfrontaliera, un obiettivo già perseguito dagli strumenti tradizionali di cooperazione giudiziaria. Inoltre, l'art. 37(2) afferma che il Regolamento non incide sul potere del giudice nazionale di valutare la prova. Tuttavia, ciò non esclude che le regole nazionali sulla valutazione della prova possano essere interpretate in conformità con il diritto primario dell'UE, come costantemente affermato dalla CGUE.[104]

Un'ampia gamma di strumenti non vincolanti ha affrontato l'urgente necessità di completare l'armonizzazione di questo ambito. La stessa Commissione europea ha esplorato la possibilità di armonizzarne la disciplina nel Libro Verde,[105] essa ha individuato come uno degli obiettivi principali per la costruzione di uno Spazio di Libertà, Sicurezza e Giustizia, la riduzione delle differenze tra gli Stati membri nel campo del diritto probatorio, al fine di facilitare la cooperazione giudiziaria. Sulla base di tale Libro Verde, l'Istituto di Diritto Europeo ha proposto una direttiva sull'ammissibilità reciproca della prova.[106] Gli Stati membri dovrebbero garantire che la prova ottenuta in conformità con la *lex loci* sia ammissibile nel procedimento penale dello Stato del foro, salvo che essa violi principi costituzionali fondamentali dello stesso. La proposta distingue poi tra inammissibilità assoluta e non assoluta, in base alla gravità delle violazioni.[107]

104 D. Brodowsky, *The European Public Prosecutor's Office: A Commentary*, Oxford University Press, Oxford, 2022.
105 Commissione europea, Libro verde sull'acquisizione e l'ammissibilità della prova in materia penale tra Stati membri, COM (2009) 624 def., 11 novembre 2009.
106 European Law Institute, Proposta per l'armonizzazione della prova nel procedimento penale, marzo 2023, artt. 5–8.
107 A. Martínez Santos, *Admisibilidad mutua de prueba penal transfronteriza en la Unión Europea: La Propuesta de Directiva del European Law Institute*, in *Revista General de Derecho Procesal*, 2023, 61, 51, 64.

La proposta di direttiva include disposizioni specifiche sull'ammissibilità della prova digitale. La prova digitale dovrebbe rispettare i principi di autenticità e completezza, preservando così l'integrità della catena di custodia. L'art. 8 richiede agli Stati membri di garantire il rispetto di standard specifici volti a tutelare la sicurezza dei dati relativi alla prova elettronica. Garantire la sicurezza dei dati durante la conservazione e la trasmissione di tali prove, mediante standard e sistemi riconosciuti, riveste un ruolo cruciale per preservarne l'affidabilità e, conseguentemente, il valore probatorio.[108]

La proposta stabilisce regole generali e principi ragionevoli che possono costituire una solida base per l'armonizzazione dei sistemi giuridici nazionali. Allo stesso tempo, tali regole non sembrano imporre vincoli eccessivamente rigidi che possano compromettere le tradizioni costituzionali degli Stati membri. Sotto questo profilo, la proposta raggiunge un giusto equilibrio tra l'esigenza di uniformità a livello europeo e la salvaguardia delle specificità giuridiche nazionali.[109] La scelta di disciplinare i casi più chiari, cioè quelli in cui la violazione del principio del contraddittorio cosi come inteso all'art. 47 della CDFUE è palese, lasciando spazio ai legislatori nazionali per andare oltre le regole minime, è considerata apprezzabile da parte della dottrina.[110] Questo approccio rispetta il principio di sussidiarietà e consente agli Stati membri di adottare misure più dettagliate o più protettive in linea con le proprie tradizioni giuridiche.

In assenza di norme comuni minime, come già più volte affermato dalla CGUE l'ammissibilità della prova è disciplinata dagli Stati membri secondo l'autonomia procedurale nazionale. Gli Stati membri dell'UE possono essere suddivisi in diverse categorie di approccio, in base alla differente ratio che governa il settore.

---

108 C. Orlando*, Mutua ammissibilità della prova tra gli Stati membri dell'Unione europea ed e-evidence: riflessioni a margine della Proposta di Direttiva dello European Law Institute* in *Sistema Penale*, 2023, 11, 19, 24.
109 A. Martinez Santos, op. cit., p.66.
110 Panzavolta M., *Streamlining the Exclusion of Illegally Obtained Evidence in Criminal Justice, progetto Defence Rights in Evidentiary Procedures*, Progetto Giustizia Commissione europea, Bruxelles, 2021, 62; Bohlander M., *Principles of German Criminal Law*, Hart Publishing, Oxford, 2009, 163.

Secondo la “teoria dell’albero avvelenato”, alcuni Stati, come Italia e Francia, fondano l’esclusione della prova sulla violazione dei diritti fondamentali nel corso del procedimento. L’albero è l’atto illecito compiuto dalle autorità di polizia o giudiziarie, mentre il frutto è la prova inutilizzabile.[111] Stati come la Germania adottano invece l'approccio della c.d. integrità giudiziaria. L’esclusione della prova si applica solo in caso di gravi violazioni da parte delle autorità, tenendo conto del rischio di compromettere la reputazione del sistema giudiziario e dell’interesse a garantire che i reati non rimangano impuniti.[112]

La tendenza generale nei diversi sistemi giuridici è quella di classificare l'inammissibilità della prova lungo un continuum, che va dalle semplici irregolarità procedurali fino alla nullità assoluta. Accanto alle norme sull'inammissibilità, è opportuno considerare anche quelle disposizioni procedurali che impongono al giudice di tener conto di determinati fatti nella valutazione della colpevolezza dell'imputato. Ad esempio, nel diritto tedesco, il principio di proporzionalità svolge un ruolo chiave nel determinare le conseguenze delle violazioni procedurali. In particolare, l'inammissibilità della prova non è automatica; essa dipende da un bilanciamento che considera la gravità della violazione procedurale e il suo impatto sui diritti fondamentali.[113]

Sussistono divergenze significative tra i sistemi giuridici degli Stati membri; tuttavia, l’uso legittimo ed equo della prova è costantemente collegato al rispetto del diritto a un equo processo, come sancito dagli articoli 47 e 48 della Carta dei diritti fondamentali dell'UE e dall'art. 6 della CEDU. In relazione all'ammissibilità della prova digitale, la CGUE ha riconosciuto tale collegamento

111 P.Tonini e C. Carlotta, *Manuale di Procedura Penale*, Giuffrè Francis Lefebvre, Milano 2024.
112 Panzavolta M., *Streamlining the Exclusion of Illegally Obtained Evidence in Criminal Justice, progetto Defence Rights in Evidentiary Procedures*, Progetto Giustizia Commissione europea, Bruxelles, 2021, 62; Bohlander M., *Principles of German Criminal Law*, Hart Publishing, Oxford, 2009, 163.
113 S. Gless and T. Richter, *Do Exclusionary Rules Ensure a Fair Trial? A Comparative analysis*, Springer, Cham, 2019.

tutelando un aspetto specifico del diritto a un equo processo, ossia il principio della parità delle armi.

In assenza di una disciplina comune e univoca, è interessante osservare la diversità di approcci adottati dalla giurisprudenza delle corti sovranazionali, in particolare della Corte EDU e della CGUE, in materia di ammissibilità della prova digitale. Merita attenzione, inoltre, la proposta di direttiva elaborata dall'*European Law Institute*, volta a promuovere un processo di armonizzazione in questo settore.

2.2.2 L'approccio della Corte europea dei diritti dell'uomo

La CEDU non include alcuna disposizione esplicita che disciplini l'ammissibilità della prova. Come ripetutamente affermato dalla giurisprudenza della Corte EDU, l'ammissibilità della prova ricade nell'ambito di competenza dei tribunali nazionali.[114] Questo punto di partenza è in linea con l'approccio adottato dalla CGUE, che considera anch'essa la disciplina dell'ammissibilità della prova come una questione di competenza degli Stati membri. Nella sua valutazione, la Corte EDU esamina il procedimento penale nel suo complesso, dalle fasi iniziali fino alla sentenza finale. Una singola irregolarità procedurale non è sufficiente a costituire una violazione dell'art. 6; è necessario dimostrare che l'irregolarità, considerata alla luce dell'intero processo, abbia reso il procedimento iniquo.[115] Tali irregolarità comprendono l'uso di prove ottenute in violazione dei diritti fondamentali, come tramite tortura o sorveglianza estesa.[116]

La Corte EDU aderisce alla dottrina della "quarta istanza", secondo cui essa non si considera una corte d'appello finale, né è suo compito valutare errori di fatto o di diritto commessi dai tribunali nazionali. Questa dottrina limita la competenza della Corte a esaminare potenziali violazioni dello stato di diritto ed

114 Corte EDU, *Schenk c. Svizzera*, ricorso n. 10862/84 (12 luglio 1988) in hudoc.echr.coe.int
115 Corte EDU, *Budak c. Turchia*, ricorso n. 69762/12 (24 settembre 2012), para 70 in hudoc.echr.coe.int.
116 Corte EDU, *Jalloh c. Germania*, ricorso n. 54810/00 (11 luglio 2006) in hudoc.echr.coe.int; Corte EDU*, Bykov c. Russia*, ricorso n. 4378/02 (10 marzo 2009) in hudoc.echr.coe.int.

è fondata sul principio di sussidiarietà. Di conseguenza, il semplice inserimento di prove ottenute illegalmente non rende iniquo l'intero procedimento. Questo approccio restrittivo suggerisce che solo una violazione particolarmente grave possa compromettere l'equità complessiva del procedimento penale. Talvolta, questioni relative al diritto della prova possono giocare un ruolo centrale nel procedimento penale e risultare cruciali nella valutazione dell'equità complessiva del processo ai sensi dell'art. 6 della CEDU.[117]

Tuttavia, la soglia particolarmente elevata fissata dalla Corte nell'interpretazione dell'art. 6 CEDU presenta alcune criticità, come sottolineato anche dalla dottrina e da parte degli stessi giudici della Corte. Secondo *Samartzis*, Il principale limite dell'approccio che valuta il procedimento nel suo complesso consiste nel rischio che la Corte rilevi una violazione del diritto a un giusto processo solo quando sia convinta dell'innocenza dell'imputato. La Corte potrebbe erroneamente equiparare l'equità complessiva del procedimento con l'esito del processo minando il principio di un giusto processo e limitando la portata della disposizione solo alle situazioni in cui l'imputato non è colpevole. La Corte, in definitiva, privilegia il controllo della criminalità e il rispetto dei sistemi giuridici nazionali rispetto alla protezione effettiva del diritto a un giusto processo.[118]

I limiti riguardo alla concezione dell'equità del procedimento nel suo complesso sono stati sollevati non solo dalla dottrina, ma anche da giudici della Corte EDU in opinioni dissenzienti.[119] Vale la pena citare l'opinione dissenziente di alcuni di questi giudici che hanno sostenuto un approccio più rigoroso all'esclusione della prova. In tal senso, il giudice *Pinto de Albuquerque* ha dichiarato che l'esistenza di regole di esclusione rappresenta l'unico modo per creare un effetto deterrente rispetto alla violazione della CEDU. Il potere di sanzionare la

117 Ibid.
118 A. Samartzis, *Weighing Overall Fairness: A Critique of Balancing under the Criminal Limb of Article 6 of the European Convention on Human Rights*, in *Human Rights Law Review*, 2021, 21, 409, 418.
119 K. Zajac, *The Admissibility of Tainted Evidence in Criminal Proceedings as a Rule of Law Issue Under the ECHR*, in *Criminal Law Forum*, 2025, 36, 33, 57.

violazione del diritto alla difesa sancito dalla CEDU, tramite l'inammissibilità, dovrebbe ricadere nell'ambito di valutazione della Corte.[120]

La forte esigenza di protezione del diritto al contraddittorio, di commentare efficacemente la raccolta e l'ammissibilità della prova, è stata sostenuta in casi come *Einarsson c. Islanda* e *Khan c. Regno Unito*.[121] Riguardo alla prova digitale, il giudice *Pavli* ha affermato che la limitazione dei diritti della difesa sanciti nella CEDU dovrebbe essere limitata a quanto strettamente necessario. Pertanto, l'accusa ha l'obbligo di divulgare tutte le prove rilevanti per garantire il rispetto del principio della parità delle armi.[122] Il mancato rispetto di tale obbligo aggrava la disparità di mezzi tra le parti e compromette l'equità del procedimento ai sensi dell'art. 6 della CEDU, in un ambito in cui l'accusa gode già di vantaggi tecnologici e informativi. Il rischio di una protezione inefficace dell'art. 6 della CEDU si traduce in un indebolimento del ruolo normativo della Corte nella definizione delle garanzie procedurali in un contesto sempre più complesso come quello dell'era digitale.[123]

Come ha affermato il giudice *Locauides*, "Non posso accettare che un processo possa essere equo, come richiesto dall'art. 6, se la colpevolezza di una persona per qualsiasi reato è stabilita tramite prove ottenute in violazione dei diritti umani garantiti dalla Convenzione."[124] In contrasto con la vaghezza e l'ambiguità spesso associate alla nozione di equità, il giudice sostiene la necessità di una regola chiara di esclusione, affermando che l'art. 6 deve offrire una protezione concreta dei diritti fondamentali e non semplici garanzie teoriche o illusorie. La regola di esclusione è nuovamente considerata come la garanzia più appropriata contro l'abuso del potere statale nei confronti dell'imputato, indipendentemente

120 Corte EDU, Murtazaliyeva c. Russia, ric. n. 36658/05, Grande Camera (18 dicembre 2018) in hudoc.echr.coe.int.
121 Corte EDU, *Khan c. Regno Unito*, ricorso n. 35394/97 (12 maggio 2000) in hudoc.echr.coe.int; Corte EDU, *Sigurður Einarsson e altri c. Islanda*, ricorso n. 39757/15 (4 giugno 2019) in hudoc.echr.coe.int.
122 Corte EDU, *Sigurður Einarsson e altri c. Islanda (opinione dissenziente del giudice Pavli*), (4 giugno 2019), para 24 in hudoc.echr.coe.int.
123 Ibid.
124 Corte EDU, *Khan c. Regno Unito (opinione dissenziente del giudice Loucaides),* ricorso n. 35394/97 (12 maggio 2000) in hudoc.echr.coe.int.

dalla sua colpevolezza o innocenza. Come afferma opportunamente l'opinione dissenziente, "Violando la legge per applicarla, si cade in una contraddizione in termini e in una proposizione assurda." Il giudice Spielmann, nella sua opinione dissenziente nel caso *Bykov c. Russia,* sostiene in modo simile una regola automatica di esclusione nei casi in cui prove ottenute illegalmente abbiano influenzato in modo significativo l'esito del procedimento e non siano state sottoposte a un contraddittorio. Egli evidenzia l'incoerenza dell'accettare tali prove in un quadro che pretende di tutelare il diritto a un giusto processo.

2.2.3 La Corte di Giustizia e la regola europea di esclusione della prova

Analogamente rispetto alla CEDU il diritto europeo non conosce regole generali di ammissibilità della prova poiché il legislatore dell'Unione europea si è costantemente astenuto dall'armonizzare le norme sulle prove in materia penale, la CGUE ha ritenuto che, come regola generale, spetti agli Stati membri regolare questo settore.[125] Allo stesso tempo però la CGUE ha più volte affermato delle eccezioni a questa regola generale stabilendo l'obbligo per i giudici nazionali di "ignorare informazioni e prove se l'imputato non è in condizione di commentare efficacemente tali informazioni e tali prove, e tali informazioni e prove sono suscettibili di avere un'influenza preponderante sull'accertamento dei fatti". Come sostenuto dalla CGUE, l'ammissibilità delle prove è di competenza del diritto nazionale, una posizione condivisa anche dalla Corte EDU. La Corte di Strasburgo è sempre stata riluttante a richiedere l'esclusione di prove ottenute illegalmente, concentrandosi invece sull'equità del procedimento nel suo complesso.[126]

Il legislatore europeo ha, quindi, elaborato gli strumenti giuridici dell'OEI e l'OEP per migliorare l'efficienza della condivisione delle prove tra gli Stati membri. Questi stessi strumenti contengono alcune disposizioni dedicate alla

125 Corte EDU, *Bykov c. Russia (opinione dissenziente del giudice Spielmann*), ricorso n. 4378/02, § 6 (10 marzo 2009) in hudoc.echr.coe.int.
126 M. Panzavolta, *Exclusion of Evidence in Times of Mass Surveillance: In Search of a Principled Approach to Exclusion of Illegally Obtained Evidence in Criminal Cases in the European Union* in *Internationanal Journal of Proof and evidence*, 2022, 26/3, 199, 202.

tutela dei diritti della difesa nel contesto della raccolta delle prove, in modo equivalente nei diversi ordinamenti giuridici. La CGUE ha adottato un approccio garantista nei confronti di tali disposizioni, interpretandole in modo protettivo per salvaguardare i diritti dell'imputato. La mancanza di regole minime comuni sull'ammissibilità delle prove digitali induce la Corte a elaborare norme in questo settore del diritto penale processuale.

L'art. 14(7) della Direttiva OEI consente questa interpretazione poiché afferma che lo Stato di emissione deve agire secondo il principio del giusto processo nel valutare prove ottenute tramite un OEI.[127] In casi di applicazione del diritto europeo alla materia penale il giudice nazionale è tenuto a seguire i principi stabiliti dalla CGUE, in virtù del principio del primato e dell'effetto diretto del diritto UE. Nonostante l'ammissibilità delle prove sia ancora disciplinata dal diritto nazionale, l'autonomia procedurale degli Stati membri è limitata da due principi e, cioè l'efficacia e l'equivalenza. Le norme nazionali sull'ammissibilità non possono essere meno favorevoli di quelle che regolano ricorsi analoghi a livello nazionale, e non possono rendere impossibile nella pratica o eccessivamente difficile l'esercizio dei diritti conferiti dal diritto dell'UE. Tra i fondamenti costituzionali del diritto europeo, il principio dell'effettiva tutela giurisdizionale svolge un ruolo predominante nei casi di prove penali transfrontaliere che restringono la portata applicativa di alcuni diritti fondamentali.[128]

Nel caso *WebMindLicenses*, la Corte ha applicato un ragionamento simile con riguardo al procedimento amministrativo in materia di IVA, affermando che prove raccolte in procedimenti amministrativi non possono essere ammesse in procedimenti penali laddove l'imputato non sia stato in condizione di esercitare

127 A. Sachoulidou, *The Court of Justice in Staatsanwaltschaft Berlin v M.N. (EncroChat): From Cross-Border, Data-Driven Police Investigations to Evidence Admissibility* in *Maastricht Journal of European and Comparative Law*, 2023, 31/4, 517.
128 S. Prechal., *Effective Judicial Protection: Some Recent Developments- Moving to the Essence* in *Review of European Admininistartive. Law*., 2020, 3, 175, 178.

i propri diritti di difesa nella fase iniziale della raccolta delle prove.[129] Il diritto di difesa trova una fondamentale espressione nella possibilità di commentare e contestare le prove presentate. In breve, la regola europea di esclusione della prova è un'interpretazione costituzionalmente orientata della legislazione secondaria dell'UE composta da due elementi diversi: l'incapacità di discutere la prova adeguatamente e l'elevato valore probatorio della prova.[130]

Il giudice nazionale deve considerare le tradizioni giuridiche nazionali relative al diritto di presentare prove, la natura della prova in questione, e i principi fondamentali del diritto dell'UE nell'interpretare la legislazione secondaria dell'UE. Nei casi che coinvolgono prove digitali, la proporzionalità tra le misure investigative e la protezione dei diritti fondamentali dovrebbe essere considerata come un fattore decisivo che può portare all'inammissibilità della prova.[131]

Nella valutazione della Corte è assente una distinzione tra l'inammissibilità della prova e la considerazione delle violazioni dei diritti solo come fattore nella valutazione del valore probatorio. La prima comporta l'esclusione totale della prova dal procedimento, mentre la seconda consente l'ammissione della prova, ma ne riduce potenzialmente il peso o la credibilità nella valutazione complessiva. L'inammissibilità della prova è una conseguenza molto più radicale, in quanto impedisce alla prova di entrare nel procedimento. Al contrario, quando una violazione dei diritti è considerata soltanto nella valutazione della prova, essa può determinare una minore valore probatorio, ma non comporta l'esclusione della stessa.[132] La proposta di Direttiva ELI disciplina sia casi di esclusione sia di mera valutazione da parte del giudice, identificando

129 Corte di giustizia, causa C-419/14, *WebMindLicenses*, ECLI:EU:C:2015:832. curia.europa.eu; M. Luchtman, *Pertinent Issues of Punitive Enforcement in a Composite Legal Order*, in M. Luchtman, K.Ligeti e J.Vervaele, *EU Enforcement Authorities: Punitive Law Enforcement in a Composite Legal Order*, Hart Publishing Oxford, 2023, 273, 279.
130 M. Panzavolta, *Exclusion of Evidence in Times of Mass Surveillance: In Search of a Principled Approach to Exclusion of Illegally Obtained Evidence* in *The International Journal of Evidence and Proof*, 2022, 26/3, 199.
131 Simonato, op cit., p.39.
132 K. Ligeti., *Admissibility of Evidence in Criminal Proceedings,* p.204

la soglia di gravità richiesta per giustificare la sanzione più appropriata.[133] L'esclusione assoluta della prova può essere effetto della violazione del diritto ad un giusto processo, oppure del divieto di tortura o di trattamenti inumani e degradanti.[134] Tali casi di esclusione sono selezionati tramite un'analisi approfondita della giurisprudenza della CGUE e della Corte EDU.

Al fine di garantire il rispetto dei principi fondamentali del diritto penale europeo, la CGUE ha fornito un'interpretazione costituzionalmente orientata del diritto secondario dell'UE, che conduce all'inammissibilità della prova in casi di gravi violazioni del principio della parità delle armi. Tale interpretazione è supportata dalla visione secondo cui l'esclusione costituisce la sanzione più ovvia ed efficace per violazioni sostanziali dei diritti probatori. Ciononostante, dato l'attuale stato di frammentazione, un intervento di armonizzazione in questo settore rimane indispensabile, secondo la dottrina per assicurare coerenza e la salvaguardia effettiva dei diritti fondamentali negli Stati membri.[135]

Come è stato ampiamente riconosciuto, la CGUE sostiene un approccio peculiare all'esclusione della prova. Decisioni come *La Quadrature du Net I* e *Prokuratuur* hanno affermato l'esistenza di un'eccezione alla regola generale dell'autonomia procedurale degli Stati membri riguardo all'ammissibilità della prova. L'eccezione si basa sul principio di effettività ed equivalenze del diritto dell'UE. Secondo la giurisprudenza della Corte, solo violazioni sostanziali del principio del contraddittorio dovrebbero portare il giudice nazionale a ignorare la prova ottenuta.[136] La violazione dovrebbe soddisfare due requisiti differenti: l'incapacità di discutere adeguatamente la prova e l'elevato valore probatorio della prova.

---

133 European Law Institute, Proposal for a Directive on the Admissibility of Electronic Evidence in Criminal Proceedings in the European Union, 2023, disponibile su: https://www.europeanlawinstitute.eu/projects-publications/completed-projects-old/admissibility-of-evidence/.
134 M. Daniele., *Scope of Judicial Review in the Executing State in EIO Proceedings*, *in European Criminal Law Review*, 2024, 14/2, 177.
135 K. Ligeti, *Admissibility of Evidence in Criminal Proceedings in the EU,* p.209.
136 Corte di Giustizia, Cause riunite C-511/18, C-512/18 e C-520/18 *La Quadrature du Net e altri c. Premier Ministre e altri*, ECLI:EU:C:2020:791. in curia.europa.eu.

Il caso *EncroChat* ha stabilito che i giudici devono escludere la prova quando il principio del contraddittorio è violato nei procedimenti penali transfrontalieri che coinvolgono prove digitali.[137] la Corte abbia stabilito che l'imputato deve poter contestare le prove della controparte dinanzi a un'autorità indipendente e imparziale e abbia definito le caratteristiche di tale controllo, non ha chiarito le conseguenze giuridiche dell'uso di prove ottenute illegalmente.[138] L'assenza di un'armonizzazione generale dell'ammissibilità della prova a livello dell'UE non impedisce alla CGUE di interpretare il diritto secondario dell'UE alla luce del principio della tutela giurisdizionale effettiva, né di imporre l'esclusione della prova ottenuta illegalmente come sanzione più appropriata.[139] Nell'ipotesi in cui l'esclusione si configuri quale rimedio sanzionatorio più coerente ed effettivo, la Corte di giustizia non può esimersi dal farne applicazione nei casi di violazioni manifeste dei diritti fondamentali, essendo tale misura lo strumento più idoneo a garantire l'effettività della tutela giurisdizionale e a preservare l'integrità dell'ordinamento dell'Unione.

2.2.4 Un confronto tra l'approccio delle tue corti: l'avanzamento nella protezione del diritto di difesa della Corte di Giustizia

La CGUE sembra non condividere integralmente la dottrina dell'equità del procedimento nel suo complesso sviluppata dalla Corte EDU. Sebbene entrambe le Corti mostrino una deferenza formalistica verso i tribunali nazionali riguardo all'ammissibilità della prova, la CGUE ha adottato un approccio più deciso, mostrando la propria disponibilità a superare l'autonomia probatoria nazionale nei casi di gravi violazioni dei diritti fondamentali. A differenza della Corte EDU, la Corte di giustizia, attraverso la sua interpretazione dell'art. 47 della Carta dei diritti fondamentali e del principio della tutela giurisdizionale effettiva,

137 Ibid. para 130-131.
138 G. Lasagni, *Admissibility of Evidence in Criminal Proceedings: Lessons and Problems from the Data Retention Saga* in Bachmaier L. Winter e Salimi F., *Admissibility of Evidence in EU Cross-Border Criminal Proceedings: Electronic Evidence, Efficiency and Fair Trial Rights*, Springer, Berlino, 2023, 49, 55.
139 A. Mosna, *Judicial protection in EU cross-border evidence gathering: the EIO as a case study.* In *European Criminal Law Review*, 2022, 14/2, 148, 156.

ha adottato una concezione dell'equità più ampia di quella sviluppata nell'ambito dell'art. 6 della CEDU.[140]

La CGUE sostiene un'interpretazione della legislazione secondaria dell'UE che rafforza l'uguaglianza procedurale e garantisce il rispetto dei diritti fondamentali dell'imputato, anche attraverso l'applicazione della regola di esclusione laddove appropriato. La Corte ha dimostrato una maggiore sensibilità rispetto alla natura intrusiva delle misure investigative digitali e al rischio che tali strumenti possano compromettere in modo sproporzionato i diritti della difesa se non accompagnati da adeguate garanzie procedurali.

Nel caso *EncroChat*, la Corte di giustizia si è discostata dalle decisioni di due corti supreme nazionali, riconoscendo la possibilità di escludere la prova. Tuttavia, il contributo della Corte EDU non deve essere trascurato, poiché continua a svolgere un ruolo rilevante nel definire gli standard europei in materia di ammissibilità della prova digitale. La giurisprudenza della Corte di giustizia offre indicazioni limitate sugli standard probatori applicabili, che possono essere integrate dalla giurisprudenza della Corte EDU. Nei casi che coinvolgono la prova digitale, la Corte EDU ha sostenuto la necessità di valutare la qualità e l'integrità della prova, nonché la possibilità che essa venga esclusa.[141]

L'analisi comparata rivela differenze sostanziali di approccio tra la CGUE e la Corte EDU riguardo all'ammissibilità della prova digitale. Sebbene entrambe le Corti formalmente deferiscano alle regole nazionali, la Corte EDU adotta un approccio olistico basato sull'equità complessiva del procedimento, spesso risultando insufficiente nella protezione dei diritti della difesa e della privacy dell'imputato. D'altra parte, la CGUE è sempre più incline a imporre conseguenze di esclusione per gravi violazioni del diritto a una tutela giurisdizionale effettiva. La giurisprudenza della Corte EDU rimane una fonte essenziale di supporto interpretativo, in particolare per quanto riguarda la

140 A, Sachoulidou, *'The Court of Justice in Staatsanwaltschaft Berlin v M.N. (EncroChat),* p.517.
141 M. Panzavolta, *Exclusion of Evidence in Times of Mass Surveillance*, p.69.

valutazione degli standard probatori. In assenza di regole armonizzate a livello UE, l'interazione tra le due Corti è fondamentale per definire la protezione dei diritti fondamentali in un ambito complesso e poco regolato quale quello della prova digitale.

2.2.5 La possibile armonizzazione normativa sulla prova digitale

L'armonizzazione mirata delle disposizioni relative alle sole prove digitali è stata riconosciuta in dottrina come un passo necessario per il legislatore europeo. Gli Stati membri potrebbero essere più propensi a raggiungere un consenso sull'armonizzazione specifica della prova digitale, piuttosto che perseguire una completa armonizzazione delle norme probatorie. L'esigenza pratica di efficienza, unita alla natura tecnica della prova digitale, che è lontana dalle aree più ideologicamente sensibili del diritto penale, possono essere incentivi chiave per l'armonizzazione. Inoltre, un'armonizzazione mirata delle prove digitali appare più fattibile e urgente, data la natura transfrontaliera dei dati digitali e l'enorme volume di informazioni che possono essere coinvolte nelle indagini penali.[142]

Secondo *Bachmaier* molti Stati membri non dispongono ancora di una legislazione completa e aggiornata sulle prove digitali.[143] Un intervento a livello europeo non solo faciliterebbe la cooperazione transfrontaliera, ma sosterrebbe anche lo sviluppo giuridico interno dei sistemi nazionali.[144] Da una prospettiva nazionale, il processo di armonizzazione potrebbe anche modernizzare i quadri giuridici nazionali che rimangono frammentati o obsoleti in materia di prove digitali.[145]

Le sfide dell'armonizzazione possono essere affrontate attingendo alla giurisprudenza della CGUE e alla proposta di direttiva dell'*European Law Institute.* Sebbene l'armonizzazione rimanga un obiettivo difficile, soprattutto

142 L. Bachmaier, *Mutual Admissibility of Evidence and Electronic Evidence in the EU: A New Try for European Minimum Rules in Criminal Proceedings?* in *eucrim* 2022,3, 117.
143 Ibid, 227.
144 ELI porposta di direttiva per l'armonizzazione della prova penale.
145 G. Lasagni, op. cit., p.65.

alla luce degli approcci divergenti illustrati nella precedente sezione, non è irraggiungibile. I sistemi di giustizia penale degli Stati membri mostrano un impegno comune nel sanzionare le più gravi violazioni dello Stato di diritto nei procedimenti penali, come l'uso della tortura o l'assenza di contraddittorio.[146]

L'applicazione di norme costituzionali europee, come l'art. 47 CDFUE, a procedimenti penali transnazionali, obbliga gli Stati membri a sviluppare una comprensione condivisa dei principi sottostanti e delle risposte appropriate alla loro violazione. L'interpretazione della CGUE sta gradualmente ampliando i confini del diritto dell'UE nel campo dell'ammissibilità delle prove, come ha fatto in precedenza in altre aree del diritto europeo. Tuttavia, come affermato da *Ligeti*,[147] l'intervento giudiziario da solo è insufficiente e rimane incompleto nell'affrontare le complesse sfide in questo campo, ed è indispensabile un intervento legislativo. La creazione di un quadro giuridico coerente a livello europeo in materia di prove digitali garantisce l'interoperabilità delle procedure penali nazionali e facilita la cooperazione giudiziaria tra gli Stati membri.[148]

Per quanto riguarda l'elaborazione di una direttiva europea volta a stabilire norme minime sulla prova digitale, la proposta dell'ELI fornisce utili indicazioni, essa contiene una definizione omogenea di prova digitale, norme minime relative agli standard procedurali per l'accesso e la raccolta e norme che disciplinino l'ammissibilità delle prove alla luce dei diritti fondamentali dell'UE. Inoltre, la proposta di direttiva garantisce la coerenza del quadro legislativo relativo agli strumenti per la raccolta transnazionale delle prove, come l'OEI e l'OEP, e assicurare il rispetto delle tutele della privacy, in particolare quelle sancite dalla direttiva sull'applicazione della legge.[149]

146 G. Illuminati, *Prova penale e Unione europea*, Bononia University Press, 2009, Bologna, 206
147 K. Ligeti, *Admissibility of Evidence in Criminal Proceedings in the EU*, p.208.
148 Ibid.
149 Martínez Santos A., op. cit., p.64.

Capitolo 3 La prospettiva nazionale

3.1 Raccolta della prova digitale

3.1.1 Mezzi di ricerca della prova informatici e best practice

L'entrata in vigore della legge 18 marzo 2008, n. 48, in ratifica ed esecuzione della Convenzione di Budapest, ha determinato l'adeguamento di alcune disposizioni procedurali al progresso tecnologico. La novella legislativa del 2008 ha inciso direttamente su disposizioni contenute nei libri III e IV del codice di procedura penale, nonché sull'art. 132 del Codice in materia di protezione dei dati personali.[150] Quindi, le modifiche più consistenti hanno interessato sia i tradizionali mezzi di ricerca della prova quali l'ispezione, la perquisizione e il sequestro sia la disciplina della conservazione dei dati.

L'innovazione più significativa di cui l'ordinamento penale è stato investito è l'ingresso nel procedimento della cosiddetta *computer forensics*, che guida la metodologia investigativa e il rispetto delle garanzie procedurali.[151] Ciò che prima era regolato esclusivamente da prassi investigative e da una metodologia mutuata dalla polizia anglosassone, diventa norma vincolante e soggetta all'interpretazione da parte degli operatori principali del processo penale.[152]

La procedura di raccolta della prova digitale segue tre passaggi fondamentali e, cioè, l'individuazione, l'acquisizione e la conservazione del dato digitale. Nel corso della procedura, il dato informatico rilevante ai fini dell'attribuzione della responsabilità penale è soggetto ai principi del c.2 dell'art 244. La polizia giudiziaria deve garantirne la conservazione attraverso l'utilizzo di hardware e software appropriati, in modo tale da adottare "misure tecniche dirette ad assicurare la conservazione dei dati originali ed impedirne l'alterazione". Le *best practice* rappresentano una forma di eterointegrazione della norma penale con

150 Decreto del Presidente della Repubblica 22 settembre 1988, n. 447, Codice di procedura penale; Decreto legislativo 30 giugno 2003, n. 196, Codice in materia di protezione dei dati personali.
151 Corasaniti, op. cit., p.195.
152 Corasaniti, op. cit., p.199.

fonti secondarie. Esse sono prassi operative considerate ottimali all'interno di un determinato settore professionale o tecnologico e possono derivare da linee guida di enti tecnici, raccomandazioni internazionali, standard di settore o dalla prassi consolidata. La norma penale necessita, in taluni casi, di essere etero integrata al fine di garantire la sua conformità rispetto a un progresso tecnologico sempre più rapido. L'aggiornamento continuo della norma incriminatrice ogniqualvolta essa risulti inadeguata rispetto alle nuove realtà operative comporterebbe, infatti, uno sforzo legislativo eccessivo e difficilmente sostenibile.

Il ricorso alle *best practice*, laddove previsto dalle norme del codice di procedura penale, consiste nella etero-integrazione da parte di fonti secondarie, che devono però essere sufficientemente autorevoli. Tra queste, particolare rilevanza assumono le *best practice* elaborate dalla Guardia di Finanza. La Guardia di Finanza ha sviluppato nel tempo una serie di prassi consolidate nella gestione della prova digitale, soprattutto in ambito di reati economico-finanziari, frodi fiscali e criminalità informatica. La guardia di finanza addestra personale specializzato ovvero I Gruppi Anticrimine Tecnologico (GAT) che dispongono di unità con competenze tecniche avanzate, formate su protocolli di acquisizione, cifratura e analisi forense, e sono soggetti ad una formazione continua su queste tematiche.[153]

Per quanto concerne la fase delle indagini preliminari, parte della dottrina più avvertita ha evidenziato come il bilanciamento tra le esigenze investigative e le garanzie difensive debba realizzarsi attraverso forme di contraddittorio tecnico graduato. In tale prospettiva, l'intervento del difensore anche nella fase predibattimentale, pur in presenza di atti a sorpresa, risponde all'esigenza di evitare sia l'assenza totale di contraddittorio, particolarmente rischiosa data la complessità tecnica della prova digitale, sia un suo utilizzo distorto attraverso il

153 Comando generale della Guardia di Finanza, III Reparto Operazioni – Ufficio Tutela Entrate, Manuale operativo in materia di contrasto all'evasione e alle frodi fiscali (Circolare n. 1/2018), Vol. II, online at gdf.gov.it

preavviso all'indagato, che potrebbe compromettere l'efficacia delle indagini. Non può infatti escludersi che la disponibilità materiale dei dati da parte dell'indagato consenta una loro alterazione o cancellazione, con conseguenti effetti pregiudizievoli per l'affidabilità del risultato probatorio.[154]

Gli accorgimenti tecnici, sulla scorta di quanto esplicitato dalla Guardia di Finanza, sono particolarmente rilevanti, e devono essere visti con favore, nel terreno delle *digital evidence* in cui il contraddittorio si forma per lo più *ex post* nella fase dibattimentale, sulle operazioni di indagine informatica precedentemente svolte dalla polizia giudiziaria. La contestazione da parte della difesa circa la correttezza della raccolta e utilizzo della prova avverrà sulla base di una duplice analisi. In primo luogo, la difesa può verificare se l'espletamento delle indagini digitali ha seguito la metodologia ideale per il caso concreto, valutata in termini di minore probabilità di alterazione del dato digitale. In secondo luogo, è necessario analizzare se la metodologia ideale è stata nella pratica seguita in modo conforme.[155]

Nella fase finale dell'analisi dibattimentale, che può svolgersi anche mediante il ricorso a periti tecnici nominati dal giudice o dalle parti, si procede all'elaborazione critica dei dati digitali, alla ricostruzione dei nessi logici tra essi e alla formulazione di una sintesi esplicativa. Tale sintesi ha la funzione di fornire al giudice, nella sua qualità di custode della realtà processuale e di intermediario tra il sapere specialistico e il piano decisionale, gli strumenti conoscitivi necessari per valutare l'affidabilità e la rilevanza probatoria del materiale informatico acquisito.[156]

Tali modalità operative vanno dalla semplice predisposizione di una copia del file, per evitarne la modificazione, alla più sofisticata redazione di un verbale di

154 M. Daniele, *La prova digitale nel processo penale* in *Rivista di diritto processuale penale*, 2021, 2, 283, 297.
155 F. M. Molinari., *Le attività investigative inerenti alla prova di natura digitale* in Cassazione penale 2013, 3, 1259, 1265.
156 Colaiocco, op. cit., p.8.

tutte le operazioni svolte attraverso captatore informatico.[157] Nello specifico, la copia del file rappresenta uno snodo importante per tutta l'attività di acquisizione digitale, e avviene mediante la tecnica della *bitstream image*, che consente di ottenere una copia forense esatta e integrale del supporto informatico. Si tratta di una duplicazione bit per bit del contenuto, che include non solo i file attivi, ma anche lo spazio non allocato, i file cancellati e i metadati, assicurando così la completezza dei contenuti acquisiti. Il codice *hash* è lo strumento di controllo dell'integrità del dato. Si tratta di una stringa alfanumerica generata attraverso una funzione matematica che rappresenta in modo univoco il contenuto di una copia forense; anche una minima modifica nel contenuto produce un *hash* completamente diverso.[158]

L'attività investigativa è orientata non soltanto all'acquisizione del dato, ma anche, e in misura prevalente, al supporto informatico in cui esso è conservato. È difficile concepire la prova digitale come un elemento isolato: risulta invece necessario considerare l'intero blocco di informazioni generati dagli individui, che costituiscono il contesto digitale nel quale il singolo elemento probatorio acquista significato e valore. La rielaborazione dei mezzi di ricerca della prova canonici deriva pure dall'esigenza di garantire rigore e standardizzazione delle procedure, in uno scenario caratterizzato da complessità tecnica e potenziale disordine interpretativo.[159] Il legislatore ha preferito una disciplina elastica, sempre ispirata alle *best practice* investigative, in cui l'impiego di strumenti forensi avanzati assicura l'integrità, la tracciabilità e l'utilizzabilità processuale della prova digitale.

Preliminarmente rispetto alla trattazione dei singoli mezzi di ricerca della prova, è opportuno dare conto dell'esistenza di un vivo contrasto tra dottrina e giurisprudenza con riguardo alla classificazione della raccolta della prova digitale quale forma di accertamento tecnico ripetibile o irripetibile. La

157 O. Murro, *Lo smartphone come fonte di prova*, p.255.
158 M. Torre, *La ricerca della prova digitale: le perquisizioni online nel contesto del processo penale telematico*, Tesi PhD, Università di Firenze, 2025, 40-41.
159 Ibid., 51.

distinzione non è priva di rilievi applicativi in quanto comporta l'applicazione degli art. 359 o 360 c.p.p. che provvedono un diverso regime probatorio e delle garanzie processuali per la difesa dell'imputato.[160]

3.1.2 La prova digitale come accertamento tecnico irripetibile

L'accertamento tecnico rappresenta un'attività a carattere scientifico finalizzata all'acquisizione della prova ad opera dei consulenti, rivestendo un ruolo essenziale in ambiti caratterizzati da particolare complessità metodologica, come nel caso della prova digitale. La ripetibilità dell'accertamento consiste nella possibilità che sia possibile svolgere più di una volta l'accertamento in modo tale da consentire la rinnovazione durante l'istruttoria dibattimentale. Secondo la giurisprudenza, il fatto che, secondo la tecnica della *bitstream image*, sia la copia del dato informatico ad essere analizzata da parte della polizia giudiziaria, è sufficiente a dimostrare la possibilità di reiterare l'azione investigativa. L'attività di formazione di copia o duplicato di un documento informatico non richiede una valutazione critica, così che può essere classificata come rilievo e non accertamento.[161] Come conseguenza non saranno applicabili le salvaguardie del contraddittorio anticipato, quali l'esecuzione delle misure da parte del pubblico ministero e la notifica al difensore.[162]

Secondo la dottrina, la maggioranza delle operazioni di informatica forense dovrebbero essere classificate come non ripetibili.[163] Tale statuizione deriva dalla considerazione della particolare vulnerabilità dei dati digitali alla manipolazione e dell'esigenza di assicurare adeguate garanzie di contraddittorio

160 F. Giunchedi, *Gli accertamenti tecnici irripetibili: tra prassi devianti e recupero della legalità*, UTET Giuridica, Torino 2009.
161 C. Parodi *Indagini informatiche e acquisizione dei file: accertamento o rilievo*? in *Ius Penale*giuffreflit.eu1.proxy.openathens.net/dettaglio/8354475/Documento?ticket=AQIC5wM2LY4Sfcx0bFbxB3jWNurXNhsO1952GD7RvoARGEc.%2aAAJTSQACMDMAAlNLABMyNjc3MzE4ODE4MTMTYxNDkyMjkxAAJTMQACMDI.%, accesso 10/07/2025.
162 Cass. Pen., Sez. II, 16 giugno 2015, n. 24998 in onelegale.wolterskluwer.it.
163 L. Luparia e G. Ziccardi, *Investigazione penale e tecnologia informatica*, Giuffre, Milano, 2009.

già nella fase investigativa. La configurazione come accertamento tecnico consentirebbe di avere una cristallizzazione del dato informatico.[164]

Altra parte della dottrina sostiene che probabilmente una rigida e generica classificazione della acquisizione della prova digitale come accertamento o rilievo è inutile e deleteria, in considerazione della molteplicità delle modalità operative attraverso le quali l'autorità investigativa può interagire con l'informatica forense. È preferibile quindi una analisi caso per caso e sulla base delle più rilevanti *best practice* per definire la disciplina applicabile e le conseguenti garanzie difensive discendenti dalla stessa.[165]

3.1.3 Ispezione informatica

In linea generale, l'ispezione tradizionale rappresenta un mezzo di ricerca della prova attraverso il quale l'investigatore osserva direttamente, e con particolare attenzione, persone, cose o luoghi. Etimologicamente derivata dal latino *inspicere*, l'espressione rimanda all'azione di guardare dentro, ovvero l'atto di analizzare dall'interno qualcosa. Essa si caratterizza per essere effettuata mediante la sola percezione visiva e si distingue dalla perquisizione per l'assenza di un intervento fisico attivo.[166]

Ne consegue che questa attività investigativa comporta un impatto modificativo minore sulla scena *criminis*, in quanto limitata alla mera percezione della realtà esteriore, senza alterazioni materiali del contesto osservato.[167] A seguito della percezione, l'*inspiciens* è tenuto alla descrizione e registrazione di quanto osservato grazie alla attività di verbalizzazione. Disciplinata dall'art. 244, c.1 c.p.p. l'ispezione rappresenta lo strumento idoneo ad accertare su persone, cose o luoghi, "tracce" o "altri effetti materiali del reato".[168] È stato argomentato dalla dottrina pressoché unanime che la tradizionale dicotomia tra ispezione e

164 A.E. Ricci, *Digital evidence e irripetibilità delle operazioni acquisitive*, in Diritto penale e procedura., 2010, 33.
165 M. Pittirruti, *Digital evidence e procedimento penale*, Giappichelli, Torino 2017
166 P. Conti e C. Conti, *Diritto delle prove penali,* p.187
167 Ibid.
168 P. Cordero, *Procedura penale*, Giuffrè, Milano, 2019.

perquisizione ha meno significato in tema di investigazioni digitali. Un'attenta lettura del disposto dell'art. 244, c.2 c.p.p, suggerisce una sovrapposizione quasi totale dei due istituti. La constatazione pragmatica da cui discende l'equiparazione tra ispezione e perquisizione informatiche è la difficoltà nell'attribuzione di un divergente coefficiente di invasività delle attività investigative nel digitale.[169]

3.1.4 La perquisizione informatica

Per comprendere appieno il ruolo preminente assunto dalla perquisizione rispetto all'ispezione in ambito informatico, è necessario esaminarne più da vicino la disciplina. Tradizionalmente, la perquisizione (dal lartino *perquiere*) è un mezzo di ricerca della prova volto alla ricerca materiale del corpo del reato o delle cose ad esso pertinenti, eseguita su luoghi o persone e finalizzata all'apprensione della *res* o all'arresto del reo.[170]

La perquisizione implica un impegno manuale da parte del soggetto inquirente e determina una maggiore intrusività rispetto alla semplice ispezione,[171] per dispiegare la sua efficacia deve essere "a sorpresa" e per tale ragione è atto urgente e riservato, essa può essere performata in casi tassativi tutti accumunati da requisito del fondato motivo che attraverso questa attività investigativa si possano raggiungere gli obbiettivi prefissati dall'art. 247 c.p.p.

L'indagato deve essere informato della facoltà di nominare un avvocato, il quale può assistere alla perquisizione in funzione di garanzia difensiva. Della perquisizione deve essere redatto verbale, in tal modo si garantisce la documentazione dell'operazione.

Il fondato motivo viene interpretato dalla dottrina processual-penalistica come l'esistenza di veri e propri indizi riguardo a una concreta ipotesi criminosa, l'indicazione dello stesso risulta essere condizione di validità del

169 P. Felicioni, *le ispezioni e perquisizioni di dati e sistemi* in A. Cadoppi, *Cybercrime*, Utet Giuridica, Torino, 2023, 1599.
170 P. Felicioni, *Le ispezioni e le perquisizioni*, Giuffrè, Milano, 2004, 96.
171 Ibid.

provvedimento,[172] tuttavia, la necessaria specificazione delle ipotesi criminose in relazione alle quali si procede non comporta l'onere di indicare gli indizi di colpevolezza.[173]

In assenza del requisito del fondato motivo la perquisizione si tradurrebbe in un mezzo per la ricerca di notizie di reato, come tale inammissibile perché lesivo della libertà individuale tutelata dagli art. 13 e 14 della costituzione.[174] In particolari casi di urgenza o in flagranza di reato l'ingerenza dei diritti fondamentali è dimostrata dalla sopracitata protezione costituzionale, la quale ha determinato obblighi particolarmente significativi per il legislatore e per i giudici attraverso una doppia riserva di legge e di giurisdizione per il compimento di atti limitativi della libertà personale e domiciliare. Interessante notare che l'art. 68 della costituzione impedisce che i parlamentari possano essere soggetti a perquisizione senza l'approvazione della camera di appartenenza.[175]

In ottemperanza al dettato costituzionale, il c.p.p. impone che la perquisizione avvenga nei casi e nei modi previsti dalla legge in forza di decreto motivato da parte dell'autorità giudiziaria. Tuttavia, in particolari situazioni di urgenza o in flagranza di reato la polizia giudiziaria può procedere a perquisizione in assenza del decreto motivato da parte del pubblico ministero, In tali casi, deve informare immediatamente il pubblico ministero e redigere verbale, trasmettendolo al pubblico ministero per la convalida.[176]

La disciplina italiana della perquisizione e l'applicazione della stessa da parte delle autorità è incline a determinare una restrizione della portata dell'art. 8

172 Cass., sez. V, 15 dicembre 1994, n. 5153/95 in onelegale.wolterskluwer.it.
173 Cass., sez. III, 14 dicembre 2007, n. 6465 in onelegale.wolterskluwer.it.
174 S. Palla, *Art. 247* in Spangher G., *il codice di procedura penale: annotato con la giurisprudenza*, Giuffe, Milano, 2024.
175 M. Bargis, voce *Perquisizione* in *Digesto delle discipline penalistiche vol IX*, Utet, Torino 1997, 278.
176 P. Balducci., voce *Perquisizione* in *Enciclopedia del diritto vol XXXIII*, Giappichelli, Torino, 2000.

CEDU dedicato alla protezione della vita privata.[177] La Corte EDU ha affermato che, "in assenza di un controllo giurisdizionale preventivo o di un controllo effettivo a posteriori della misura adottata, le garanzie della legislazione italiana non sono state sufficienti per evitare abusi da parte delle autorità incaricate dell'indagine penale"[178]. Sebbene la misura fosse formalmente prevista dal codice di procedura penale, "il diritto interno non ha offerto al ricorrente sufficienti garanzie contro gli abusi o l'arbitrarietà prima o dopo la perquisizione".[179] Di conseguenza, il ricorrente non ha beneficiato di un controllo effettivo, come richiesto da uno Stato di diritto in una società democratica. La Corte ha quindi concluso che l'ingerenza nel diritto al rispetto del domicilio non era prevista dalla legge ai sensi dell'art. 8 della Convenzione. A fondamento della decisione, la Corte ha ribadito che la perquisizione costituisce un'interferenza delle autorità pubbliche nella vita privata del ricorrente. Tale interferenza, per essere compatibile con l'art. 8 CEDU, deve essere prevista dalla legge e necessaria in una società democratica.[180]

L'art. 8 della l. 18 Marzo 2008, n. 48 ha aggiunto all'art 247 un nuovo comma che corrisponde alla modalità informatica attraverso la quale la perquisizione può essere posta in essere. Secondo quanto previsto dal comma 1-bis dell'art. 247 c.p.p. "quando vi è fondato motivo di ritenere che dati, informazioni, programmi informatici o tracce comunque pertinenti al reato si trovino in un sistema informatico o telematico, ancorché protetto da misure di sicurezza, ne è disposta la perquisizione, adottando misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione".

La penetrazione nel sistema informatico implica per sua definizione quasi sempre un *quid pluris* rispetto alla mera attività di scrutamento tipica

177 Corte Edu,Brazzi c. Italia, ricorso n. 57278/11, (27 settembre 2018) in hudoc.echr.coe.int, para 51.
178 Ibid, para 52
179 Ibid., para 56.
180 D. Cardamone, *La sentenza della CEDU, Brazzi c. Italia: sono arbitrarie le perquisizioni disposte dall'autorità giudiziaria*" in *Questioni di Giustizia*
https://www.questionegiustizia.it/art./la-sentenza-della-cedu-brazzi-c-italia-sono-arbitrarie-le-perquisizioni-disposte-dall-autorita-giudiziaria-_15-01-2019.php accesso 23 giugno 2025.

dell'ispezione tradizionale. Ad esempio, è difficile immaginare un'attività di accesso in tempo reale a dati informatici contenuti in uno smartphone senza il rischio di provocare una modificazione digitale dei contenuti.

Nell'incertezza della scelta del mezzo di prova più adeguato tra perquisizione e inspezione la dottrina ha suggerito un approccio garantista delle prerogative dell'indagato che restringe il campo applicativo dell'ispezione a quei soli casi in cui l'intrusione non è importante e il potenziale di alterazione del file è ridotto. Si può ipotizzare l'utilizzo di questo mezzo di ricerca della prova per rilievi esterni circa lo stato di sistemi informatici o telematici.[181] La diversa penetrazione nella sfera privata del soggetto privato si riflette anche in un diverso esito che caratterizza i due mezzi di ricerca della prova, mentre la perquisizione è finalizzata al sequestro del dato informato, l'ispezione sarebbe limitata alla copia del contenuto.[182]

Viste le maggiori garanzie difensive, le quali sono disciplinate dagli 247 s.s. c.p.p., nonché dagli artt. 352, 356, 365, 369 c.p.p. e 114 disp. att. del c.p.p.,[183]. e la maggiore adattabilità al contesto informatico, a seguito di una valutazione caso per caso, lo strumento dovrà essere preferito rispetto all'ispezione informatica. Minimo comune determinatore dei due mezzi di ricerca della prova è l'obbligo di conservazione e non alterazione del dato digitale in capo all'autorità giudiziaria, e il rimando alle best practice per determinare la migliore modalità pratica di raccolta, tenendo in considerazione la rapida evoluzione del progresso tecnologico.[184] La perquisizione si compone di due fasi, una prima preview nella quale si visualizza il sistema informatico (Cartelle, files, fotografie o altri documenti informatici), per poi passare alla fase di ricerca vera e propria.

181 G. Corasaniti, op. cit., p.206.
182 P. Felicioni, *le ispezioni e perquisizioni di dati e sistemi*, p.1601-1602.
183 R. Valli, *La perquisizione informatica e la perquisizione da remoto'*in *IUS Diritto Processuale Penale* https://ius.giuffrefl.it/dettaglio/6618776/la-perquisizione-informatica-e-la-perquisizione-da-remoto, acesso 23 Giugno 2025.
184 G. Braghò, *'L'ispezione e la perquisizione di dati, informazioni e programmi informatici'* in Luparia G.P., *Criminalità informatica*, Giappichelli, Torino, 2022.

Anche nell'ambito digitale, la perquisizione si configura, nell'ottica processual-penalistica, come un atto di ricerca probatoria che trova la sua principale finalità nell'individuazione di cose pertinenti al reato suscettibili di sequestro. In particolare, essa non costituisce un atto autonomo e fine a sé stesso, ma è normalmente orientata a rendere possibile il successivo vincolo reale su beni o dati rilevanti ai fini dell'accertamento penale.[185] Ne deriva che il rapporto tra perquisizione e sequestro assume carattere funzionale, giacché l'una opera prevalentemente quale strumento preliminare all'attuazione dell'altro.

3.1.5 Il sequestro di dati informatici presso i fornitori di servizi informatici

Di norma, a seguito della perquisizione, la polizia giudiziaria procede al sequestro probatorio del corpo del reato o delle cose a questo pertinenti. Tale sequestro comporta l'instaurazione, nei confronti della res, di un vincolo di indisponibilità. Il codice di procedura penale disciplina il sequestro della corrispondenza presso uffici postali o servizi telematici all'art. 254, disposizione che si è tuttavia rivelata inadeguata rispetto al sequestro di file informatici. La legge di ratifica ha pertanto introdotto l'art. 254-bis c.p.p., conformando la disciplina agli altri strumenti di ricerca della prova digitale i principi contenuti al c.2 dell'art.244 c.p.p. Ai sensi dell'art. 254-bis, il sequestro di dati informatici ha ad oggetto la copia del file, che costituisce il vero oggetto del vincolo; ne consegue che l'indagato può conservare il possesso dell'hardware in cui il file è contenuto.[186]

La norma è diretta nei confronti della medesima categoria di soggetti del Regolamento E-evidence cioè ai soli fornitori di servizi informatici e di telecomunicazioni. Ne deriva che, ad altri soggetti quali aziende private di diversa natura e pubbliche amministrazioni si applicheranno le norme comuni. Lo strumento normativo è stato utilizzato da parte delle procure i termini più brevi della *data retention* o della conservazione di dati digitali. Tuttavia, la Corte

185 L. Parlato, *Perquisizioni on-line:un fenomeno sfuggente e in continua evoluzione* in A. Spena e V. Mitiello, *Mobilità, sicurezza e nuove frontiere tecnologiche*.
186 A.M. Magliulo, *Illegittimo il trattenimento prolungato della copia integrale dei dati informatici in caso di sequestro probatorio* in *Processo penale e giustizia*, 2021, 3 648.

di cassazione ha limitato tale pratica affermando che non è consentito il trattenimento a tempo indeterminato della copia integrale dei dati informatici sequestrati, il pubblico ministero può conservare i dati solo per il tempo strettamente necessario alla selezione del materiale rilevante, soprattutto quando il sequestro ha ad oggetto dati appartenenti a soggetti estranei al reato. Il principio di proporzionalità e la sua esplicitazione nella motivazione del provvedimento costituiscano presupposti imprescindibili per garantire la conformità ai principi del giusto processo dell'atto. L'indisponibilità prolungata della copia integrale e la tempestiva selezione degli elementi utili al procedimento hanno una rilevanza fondamentale in funzione di garanzia della riservatezza e del diritto di difesa dell'imputato.[187]

3.1.6 La proposta normativa in tema di sequestro di dati informatici

Delineati i tratti essenziali del sequestro di dati informatici nella disciplina vigente, è opportuno soffermarsi sulla proposta normativa volta a conformare la disciplina del sequestro di dati informatici con la giurisprudenza della CGUE. Nelle sentenze *Landeck* e *Prokkuratuur*, la CGUE ha affermato che non è ammissibile affidarsi esclusivamente a meccanismi di controllo a posteriori, come la registrazione in rapporti ufficiali o l'informazione successiva dell'imputato. La Corte sottolinea la necessità di un'adeguata valutazione prima dell'esecuzione dell'operazione, ad eccezione di casi di urgenza debitamente giustificati.[188]

Sulla scorta di quanto affermato da parte della CGUE e dell'importanza del controllo giudiziale, il Senato ha recentemente approvata una proposta di legge che modifica il codice attraverso l'introduzione dell'art. 254ter c.p.p. In conformità rispetto alla suddetta disposizione, è il giudice ad autorizzare il pubblico ministero al sequestro di dispositivi e sistemi informatici o telematici,

187 O. Murro, *Sequestro dei dati informatici: verso l'art. 254ter c.p.p.? Breve note a margine del disegno di legge a.s. n.806.* in *Diritto e procedura penale* https://www.penaledp.it/sequestro-dei-dispositivi-informatici/, accesso 15 Luglio 2025.
188 Corte di Giustizia, Causa C-548/21 C.G. c. *Bezirkshauptmannschaft Landeck,* ECLI:EU:C:2024:830 in curia.europa.eu..

salvo casi di estrema urgenza. A seguito della duplicazione del contenuto il pubblico ministero deve procedere alla selezione del materiale rilevante, nel caso di dati aventi contenuto non comunicativo, dispone il sequestro dei dati strettamente pertinenti al reato e, comunque, nel rispetto dei criteri di necessità e proporzione; nel caso di dati aventi contenuto comunicativo, chiede al giudice il sequestro con gli stessi presupposti delle intercettazioni. La novella è vista con favore dalla dottrina, in quanto consente un rafforzamento delle garanzie procedurali, senza sacrificare eccessivamente le esigenze investigative.[189] La novella ha anche il pregio di porre maggiore attenzione al rispetto del principio della effettiva tutela giudiziale per mezzo di un controllo ex ante da parte del giudice. Inoltre, attraverso il vaglio giurisdizionale, la norma favorisce il rispetto dei principi di proporzionalità ed adeguatezza delle misure investigative

Tuttavia, l'art. 247 c.p.p. ha potenziale elusivo rispetto alla riforma in quanto strumento alternativo rispetto al 254ter c.p.p. La disciplina delle perquisizioni informatiche di cui all'art. 247 c.p.p. rischia di eludere le garanzie introdotte dall'art. 254ter c.p.p., consentendo una duplicazione e un'analisi surrettizia dei dati digitali in assenza di autorizzazione giudiziaria e senza il rispetto del contraddittorio. Parte autorevole della dottrina ha inoltre auspicato l'introduzione di una fase partecipativa successiva alla duplicazione, nella quale la difesa dell'imputato sia posta nella condizione di interloquire sulla selezione dei dati da acquisire, ovvero, quantomeno, di formulare osservazioni motivate al pubblico ministero prima della formalizzazione del decreto di sequestro, al fine di garantire il pieno contraddittorio.[190]

La novella segue la giurisprudenza costituzionale ed europea, ispiratasi alla legislazione europea in forza della quale, l'intervento giurisdizionale è

189 M. Caianiello, *Ancora in tema di sequestro di dispositivi, sistemi informatici o telematici o memorie digitali (disegno di legge C. 806)* in *Sistema Penale*, https://www.sistemapenale.it/it/documenti/caianiello-ancora-in-tema-di-sequestro-di-dispositivi-sistemi-informatici-o-telematici-o-memorie-digitali-disegno-di-legge-c-806, accesso 4 Luglio 2025.
190 Ibid.

esclusivamente limitato ai dati di contenuto.[191] Si rileva come anche l'accesso ad altre categorie di dati non "comunicativi" possa costituire una intrusione eccessiva della sfera privata, si pensi ad esempio ai dati di delocalizzazione del soggetto. La dottrina nota anche come non venga dato un termine di conservazione entro cui il giudice e il pubblico ministero siano tenuti a fare una cernita del materiale sequestrato.[192] Ciò contrasta con il dettato della cassazione secondo la quale l'estrazione della copia forense non giustifica il trattenimento prolungato dei dati personali.[193] Non solo, la proposta non contiene una soglia minima probatoria al ricorrere del quale la misura può essere attuata. Ciò costituisce una sostanziale differenza sia rispetto ai gravi indizi di reato delle intercettazioni sia dei più lievi sufficienti indizi di reato della data rentenion. Conseguentemente c'è il rischio che il sequestro così come codificato dalla novella possa essere utilizzato a meri fini esploratori, portando a violazione del diritto alla riservatezza in assenza di esigenze di sicurezza pubblica.[194]

Sebbene la proposta rappresenti un indubbio avanzamento del sistema nel contesto di indagini *data driven*, resta aperta la questione sul se questa norma favorisca efficacemente il rispetto del diritto di difesa. Una lacuna rispetto alla selezione dei dati che viene ripresa anche nella sentenza è l'assenza da parte della difesa nella selezione dei dati e soprattutto nella individuazione dei criteri di scelta. È raccomandabile che il pubblico ministero dia almeno conto dei criteri utilizzati nel corso delle investigazioni e ne informi il giudice, il quale potrà verificare la modalità di istruzione probatoria.[195]

3.1.7 Il captatore informatico: tra intercettazioni e perquisizione

Il progresso tecnologico ha comportato non solo l'adattamento degli strumenti probatori tradizionali, ma anche l'emersione di nuove tecniche investigative,

191 Corte cost., 27 settembre 2023, n. 170/2023.
192 Della Torre J., *audizione dinnanzi alla Commissione Giustizia della Camera dei Deputati nell'ambito dell'esame della proposta di legge C. 1822, approvata dal Senato, recante "Modifiche al Codice di procedura penale in materia di sequestro di dispositivi, sistemi informativi o telematici o memorie digitali*, in *Sistema penale*, 2025, 23.
193 Cass., Sez. VI, 14 giugno 2022, n. 35652 in onelegale.wolterskluwer.it.
194 J. Della Torre, op. cit., p.27.
195 Caianiello, op. cit., p.5.

quali il captatore informatico e la *data retention*, entrambi gli strumenti accrescono l'invasività del potere pubblico nelle sfere di riservatezza individuale.

L'istituto del captatore informatico rappresenta una figura a metà tra le perquisizioni da remoto e le intercettazioni. Per captatore informatico si intende l'inoculazione di un virus informatico (il c.d. trojan di stato) da parte dell'autorità giudiziaria in un sistema informatico, volto ad ottenere informazioni rilevanti ai fini dell'accertamento della responsabilità penale. Le iniziali difficoltà classificatorie sono determinate dalla vasta gamma di opzioni operative che l'autorità pubblica può adottare. Attraverso il malware, infatti, la polizia giudiziaria può spiare i contenuti informatici del sistema informatico mediante copia dell'hard disk, intercettare le comunicazioni, attivate periferiche video o audio o accedere a qualsiasi contenuto conservato e trarne una copia.[196]

L'uso pratico del virus determina una diversa classificazione nel corso del processo penale. Ad esempio, per quanto concerne la captazione di telecomunicazioni in tempo reale e in modo occulto, la disciplina delle intercettazioni troverà applicazione.[197] Il criterio discretivo è fondato sulla attualità e modalità di raccolta di nascosto, la trasmissione del messaggio in chat viene equiparata a quella telefonica, suscettibile di essere intercettata attraverso le telecomunicazioni tradizionali. Al contrario, quando il dato viene acquisito attraverso sequestro che segue alla perquisizione dei file e delle cartelle nella memoria accessibile, la comunicazione è gia "avvenuta", e le regole procedurali saranno diverse.[198] La conseguenza immediata della applicazione della disciplina delle intercettazioni risiede nell'applicazioni dei requisiti dei gravi

196 Valli, op. cit., p.9.
197 S. Torre, *Il captatore informatico: nuove tecnologie investigative e rispetto delle regole processuali,* Giuffrè, Milano, 2017
198 A. Nocera, *L'acquisizione delle chat WhatsApp e Messenger: intercettazione, perquisizione o sequestro?* Ius Penale https://ius-palfl-it.eu1.proxy.openathens.net/accessedo 24 Giugno 2025.

indizi di reato e della applicabilità alle sole fattispecie penali dotate di una certa rilevanza.

La Corte di cassazione nel 2009, a fronte della impossibilità di definire l'istituto secondo le categorie codicistiche, ha ricondotto l'utilizzo del Trojan di Stato alla categoria della prova atipica ex art. 189 c.p.p.[199] rimette alla valutazione del giudice la possibilità che mezzi di prova diversi rispetto a quelli elencati nel codice possano essere legittimamente utilizzati, purché essi non costituiscano modalità alternativa di assunzione della prova rispetto a quelle previste dalla legge. La dottrina riteneva che l'utilizzo del captatore informatico rappresentasse una elusione della forma delle garanzie processuali previste per la perquisizione informatica, e pertanto ne deduceva l'impossibilità che il captatore informatico fosse classificato come prova innominata.[200]

Ne discende una distinzione pratica tra la perquisizione informatica tout court e la perquisizione online. Quest'ultima è assimilabile al captatore informatico, in quanto prevede l'accesso al sistema informatico non direttamente e manualmente, ma attraverso l'utilizzo di malware da remoto.[201] Le perquisizioni informatiche sono assimilabili alle perquisizioni ordinarie in quanto atti a sorpresa ma ontologicamente conoscibili, diversa è la natura delle perquisizioni online che per essere efficaci necessitano di restare ignote all'indagato per tutta la loro durata.[202]

La dottrina ha inoltre ipotizzato la possibilità che la perquisizione on-line potesse configurare un esempio di prova incostituzionale. Una tale intrusione dell'intimità del soggetto in misura finora sconosciuta, secondo questa impostazione costituirebbe una violazione degli articoli 14 e 15 della Costituzione, posti a protezione del domicilio. Come già accennato in precedenza con riguardo alla perquisizione, il dettato costituzionale impone una

199 Cass., Sez. V, 14 ottobre 2009, n. 16556 in onelegale.wolterskluwer.it.
200 M. Griffo, *Perquisizione informatica… e dintorni* in *Giurisprudenza Penale* <www.giurisprudenzapenale.com> accesso 24 Giugno 2025.
201 Corasaniti, op. cit., p.212.
202 Griffo, op. cit., p.3.

riserva di legge per limitazioni del domicilio, considerato come la proiezione spaziale della vita privata dell'individuo. Il domicilio digitale è ritenuto meritevole di tutela al pari del domicilio fisico, e quindi l'interpretazione estensiva dell'art. 189 c.p.p. non soddisferebbe il requisito della riserva di legge.[203]

La Corte di cassazione ha equiparato l'utilizzo del captatore informatico alle intercettazioni ambientali. Pertanto, a detta della corte, per i reati comuni (reati non legati alla criminalità organizzata) è necessaria l'indicazione del luogo nel quale vengono portate a termine le attività investigative, la legge consente maggiore flessibilità per quanto concerne i reati di mafia visto l'ingente allarme sociale. Conseguentemente, in assenza della indicazione del luogo la prova ottenuta attraverso il captatore informatico sarebbe inutilizzabile per il perseguimento di reati comuni. La ratio è la tutela della privacy e della libertà del domicilio (artt. 14 e 15 Cost.), permettendo al giudice di delimitare con precisione gli ambiti su cui pesano i poteri invasivi.[204]

La Suprema Corte è intervenuta in materia e ha chiarito l'ambito applicativo del captatore informatico, fornendo anche una guida per il successivo intervento legislativo del 2017. In correlazione dell'elevato allarme sociale derivante dalla commissione del reato di associazione mafiosa la suprema corte ha affermato la possibilità di utilizzare tale strumento limitatamente ai delitti di criminalità organizzata, per i quali è consentita la captazione anche nei luoghi di privata dimora.[205]

In questo quadro, la sentenza Cass., sez. VI pen., 8 aprile 2021, n. 17007 ha ulteriormente precisato che l'utilizzabilità delle intercettazioni effettuate con captatore informatico non viene meno nel caso in cui il reato originariamente ipotizzato non rientri tra quelli per i quali è ammesso l'uso del captatore in ambito domiciliare, purché nel corso delle indagini emerga la riconducibilità del

203 A. Capone, *Intercettazioni e Costituzione. Problemi vecchi e nuovi*, in *Cassazione penale* 2017, 3,1263.
204 Cass., Sez. VI., 26 maggio 2015, n. 27100 in onelegale.wolterskluwer.it
205 Cass., Sez Un., 28 aprile 2016, n. 26889 in onelegale.wolterskluwer.it.

fatto a un delitto di criminalità organizzata. È dunque ammessa una riqualificazione ex post del titolo di reato, ai fini della legittimazione retroattiva dell'intercettazione.[206]

La captazione immediata e contestuale di screenshot di un foglio *Excel* da parte di un malware deve essere qualificata come intercettazione informatica, ai sensi dell'art. 266-bis c.p.p. Poiché l'acquisizione avviene simultaneamente alla formazione del dato, essa rappresenterebbe, secondo la Corte, la rilevazione di un comportamento comunicativo. La Suprema Corte ha altresì escluso che tale attività possa essere qualificata come perquisizione informatica, in quanto non si tratta di un dato preesistente, bensì in corso di elaborazione.[207] Questa interpretazione segna una discontinuità rispetto ai precedenti orientamenti giurisprudenziali, che ritenevano necessaria, ai fini dell'intercettabilità, l'esistenza di una comunicazione o interazione tra due o più soggetti elementi assenti nel caso degli screenshot unilaterali.[208]

La dottrina ha evidenziato il rischio che un'interpretazione estensiva della nozione di "comportamento comunicativo" porti a una legittimazione generalizzata di tutte le attività di *online surveillance* quali *screenshot*, *keylogger*, attivazione di webcam o microfono, anche in assenza di effettivi flussi comunicativi. Ciò comporterebbe il pericolo di un progressivo svuotamento delle garanzie costituzionali e processuali, in particolare di quelle a tutela della riservatezza, del domicilio informatico e del diritto di difesa.[209]

Il legislatore è intervenuto in materia di captatore informatico per ottemperare all'obbligo di riserva di legge contenuta nel testo costituzionale. Il decreto legislativo n. 216 del 2017 ha esteso rispetto la lista dei reati per i quali è possibile procedere con captatore informatico, aggiungendo i reati contro la

206 Cass., Sez. VI, 28 febbraio 2017, n. 15573 in onelegale.wolterskluwer.it.
207 Cass., Sez. VI, 20 settembre 2016 n. 15071 in onelegale.wolterskluwer.it.
208 Cass., Sez. V, 30 maggio 2017, n. 48370 in onelegale.wolterskluwer.it.
209 V. Mongillo, *Screenshot, captatore informatico e sorveglianza occulta online: la Cassazione ridisegna i confini dell'intercettazione informatica* in Sistema Penale, https://www.sistemapenale.it/it/scheda/cassazione-2022-3591-screenshot-captatore-informatico-online-surveillance, acesso 4 Luglio 2025

pubblica amministrazione e altri reati particolarmente gravi. L'art 266 comma 2 C.P.P. prevede oggi espressamente la possibilità di procedere ad intercettazioni mediante captatore informatico. L'utilizzo del captatore informatico è stato successivamente ulteriormente esteso anche rispetto ai delitti comuni, nel caso in cui sia assolutamente indispensabile e vi siano gravi indizi di reato.

Come per le intercettazioni i requisiti sono attenuati per i delitti di criminalità organizzata e assimilati. Vista l'invasività il giudice deve indicare le specifiche ragioni per le quali le intercettazioni tradizionali non sono sufficienti, nonché i luoghi e i tempi nei quali viene attivato il microfono. Il codice prevede invalidità speciali per quanto riguarda le intercettazioni mediante captatore informatico che avvengono senza seguire le disposizioni del decreto attuativo. Il programma informatico utilizzato deve rispettare i requisiti fissati dal decreto del ministero della giustizia, gli operatori.[210]

3.1.8 La data retention

La legge di attuazione della Convenzione di Budapest è intervenuta modificando l'art. 132 del codice della privacy. Quest'ultimo impone un obbligo in capo ai service provider di conservare per ventiquattro mesi i dati relativi al traffico telefonico, per dodici mesi i dati relativi al traffico telematico e di 30 giorni per i dati relativi alle chiamate senza risposta. Il termine da cui decorre il periodo di conservazione è dal momento in cui la comunicazione è stata effettuata per entrambi i tipi di dati. Le finalità di conservazione dei dati sono simili a quelle previste dalla Direttiva E-privacy e sono la prevenzione, l'indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali. In generale, Il codice della privacy dà attuazione alla normativa europea, la quale intende fornire una protezione dei diritti fondamentali nel contesto di indagini digitali che possono limitare l'esercizio di diritti fondamentali.[211]

210 A.P. Casati, *Le intercettazioni*, Giuffre, Milano, 2023, 93.
211 A. Caputo, *La conservazione dei dati di traffico telefonico e telematico nella normativa antiterrorismo* in *Archivio penale*, 2016, 1, 28.

L’art. 132 del codice privacy ha subito un *iter* legislativo tormentato a riprova del difficile bilanciamento tra diritto alla privacy e perseguimento dei reati. Dopo il 2008, una importante modifica è stata introdotta nel 2015 a seguito della decisiva sentenza *Digital Rights Ireland.* la quale ha dichiarato la direttiva Frattini del 2006 sulla data retention per incompatibilità con gli articoli artt. 7, 8 e 52, co. 1, della Carta dei Diritti Fondamentali dell’Unione Europea.[212] La sopracitata sentenza della CGUE affermava la sostanziale incompatibilità del sistema di protezione dei dati personali, in quanto insufficientemente protettivo del diritto alla privacy. L’art 15 della direttiva sulla privacy elettronica impone infatti il requisito della proporzionalità rispetto al fine della repressione dei reati dell’accesso alle comunicazioni, in quanto deroga al principio generale contenuto all’art. 5 della stessa direttiva che impone il principio di segretezza delle comunicazioni.

la Corte osservava come la direttiva non imponesse alcuna relazione tra i dati di cui prevede la conservazione e una minaccia per la sicurezza pubblica e, in particolare, non circoscrive la conservazione dei dati sulla base di fattori oggettivi quali l’area geografica e le persone coinvolte. La sentenza ha affermato un divieto generale di conservazione generale ed indifferenziata, in assenza di un’esigenza obiettiva nella repressione di gravi reati. Conseguentemente la Corte affermava che la misura di *data retention* così come definita dalla direttiva del 2006 era sproporzionata rispetto all’obiettivo perseguito.[213]

Le ripercussioni dell'invalidità della direttiva sugli ordinamenti interni sono significative, in quanto diversi Stati membri, tra cui l'Italia, avevano dato attuazione all’obbligo di trasposizione. Di conseguenza, le disposizioni di diritto interno conformi alla direttiva devono ritenersi in contrasto con quanto affermato

212 Direttiva 2006/24/CE del Parlamento europeo e del Consiglio del 15 marzo 2006 relativa alla conservazione dei dati generati o trattati in relazione alla fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione e che modifica la direttiva 2002/58/CE

213 Corte di Giustizia, *Digital Rights Ireland Ltd contro Minister for Communications, Marine and Natural Resources e altri*, Cause riunite C-293/12 e C-594/12, EU:C:2014:238 in in curia.europa.eu.

dalla CGUE nella sentenza *Digital Rights Ireland*. Alla luce del principio del primato del diritto dell'Unione, i giudici nazionali sono tenuti a disapplicare le disposizioni interne incompatibili con il diritto dell'UE, anche in assenza di un intervento legislativo abrogativo. Inoltre, Tale pronuncia ha influenzato numerose decisioni successive della Corte, tra cui *La Quadrature du Net*, nonché provvedimenti adottati a livello nazionale, limitando in modo rilevante la possibilità per gli Stati di imporre obblighi di conservazione dei dati a fini di sicurezza.[214]

Il legislatore ha provato ad adeguarsi rispetto alla sentenza della CGUE nel 2015. La norma all'art. 132 del codice privacy infatti consente, nei limiti di conservazione previsti dalla legge, l'accesso ai dati mediante decreto motivato del giudice, su richiesta del pubblico ministero, qualora sussistano sufficienti indizi di reato per il quale la legge prevede la pena dell'ergastolo o della reclusione non inferiore, nel massimo, a tre anni. Quando ricorrono ragioni di urgenza e vi è fondato motivo di ritenere che dal ritardo possa derivare grave pregiudizio alle indagini, il pubblico ministero dispone l'acquisizione dei dati con decreto motivato, che è comunicato immediatamente, e comunque non oltre quarantotto ore, al giudice competente per il rilascio dell'autorizzazione in via ordinaria. In questo modo viene ottemperato l'obbligo imposto dal CGUE di autorizzazione da parte di un'autorità indipendente e imparziale.[215]

Secondo autorevole dottrina,[216] la normativa italiana risulta ancora oggi non perfettamente conforme con il diritto dell'UE in quanto continua a prevedere un regime generalizzato e indiscriminato di conservazione dei dati, senza limitarlo alle ipotesi di criminalità particolarmente grave. Infatti, nel 2017 è stato inserito il comma 5-bis all'art. 132 del Codice della privacy, il quale estende a 72 mesi

214 L. Filippi, *Riservatezza e data retention: una storia infinita* in *Penale diritto e procedura* https://www.penaledp.it/riservatezza-e-data-retention-una-storia-infinita/, accesso 26/08/2025.
215 Alessandra Cardone, *Il sistema del Data Retention come strumento investigativo* in *Giurisprudenza Penale*, 2021, 1.
216 N. Marcolini, *Dalla data retention alle indagini ad alto contenuto tecnologico,* Giappichelli, Torino, 2022.

il termine di conservazione dei dati ai fini della repressione dei reati di maggiore gravità, tra cui il terrorismo.[217]

Tuttavia, il legislatore si è limitato ad estendere il termine di conservazione, senza restringere l'ambito applicativo della misura alle sole fattispecie più gravi. I termini di conservazione dei dati risultano del tutto sproporzionati rispetto alle indicazioni fornite dalla CGUE nelle sentenze riguardanti la conservazione dei dati. Nell'insufficienza di una interpretazione conforme al diritto europeo da parte del giudice nazionale, è necessario un intervento da parte del legislatore che limiti il periodo di conservazione e circoscriva la conservazione dei dati alle sole fattispecie più gravi.

L'intervento da parte del legislatore si ritiene ancor più urgente dal momento che l'attività ermeneutica della CGUE ha efficacia diretta limitatamente ai casi in cui non residuino, negli istituti giuridici regolati, concrete questioni di applicazione pratica applicativi l'intervento della discrezionalità legislatore nazionale. L'interpretazione proposta dalla CGUE è particolarmente vaga in quanto fa riferimento a concetti vaghi quali la "repressione di crimini gravi". È compito del legislatore quindi declinare all'interno dell'ordinamento italiano i principi generali espressi dalla CGUE.[218]

3.2 L'ammissibilità della prova digitale nel diritto nazionale

3.2.1 L'ammissibilità della prova in generale

A partire dal 1988, il modello processuale penale italiano si caratterizza per la sua natura accusatoria. In tale sistema, sono le parti a farsi carico dell'onere di fornire la prova della colpevolezza o dell'innocenza dell'imputato. Il giudice, terzo e imparziale, non svolge un ruolo attivo nella formazione della prova. In conformità a questo impianto, l'art. 190 del codice di procedura penale prevede che "le prove sono ammesse su richiesta di parte" e che l'ammissione d'ufficio

217 B. Martino, *Data retention, conservazioni dati a norma di legge* in Legal for digital https://legalfordigital.it/gdpr/data-retention-e-gdpr/, accesso 30/08/2025.
218 Aterno S., *Data retention: gli effetti della sentenza del 2 marzo 2021 della Corte di Giustizia Europea* in *E-Lex*, https://www.e-lex.it, accesso 7 luglio 2025.

da parte del giudice è consentita solo nei casi eccezionali espressamente previsti dalla legge, come stabilito, ad esempio, dall'art. 507 c.p.p. Nel valutare l'ammissibilità delle prove richieste dalle parti, la legge stabilisce precisi criteri e contempla anche alcune ipotesi di esclusione, come nel caso in cui la prova risulti manifestamente superflua o si riferisca a fatti irrilevanti perché estranei all'oggetto del processo. In altri termini, deve sussistere un nesso tra la prova e la *res iudicanda*, come delineato all'art. 187 c.p.p.[219]

La prova si forma nel contraddittorio tra le parti nel corso del dibattimento, in attuazione del principio sancito dall'art. 111, comma 4, della Costituzione, secondo cui: "La colpevolezza dell'imputato non può essere provata sulla base di dichiarazioni rese da chi, per libera scelta, si è sempre volontariamente sottratto all'interrogatorio da parte dell'imputato o del suo difensore." Tale disposizione costituzionale sancisce il diritto dell'imputato a confrontarsi con l'accusatore e ad essere parte attiva nel procedimento probatorio, affermando così il principio del contraddittorio nella formazione della prova. La Costituzione, tuttavia, prevede tre eccezioni a tale principio: il consenso dell'imputato, l'impossibilità oggettiva di assicurare la partecipazione dell'autore della dichiarazione, e la condotta illecita dimostrata da parte dell'imputato, che abbia determinato l'irreperibilità o la non disponibilità del dichiarante.

In aggiunta, ai sensi del c.2 art. 27, della Costituzione, in forza del principio di presunzione di innocenza, è il pubblico ministero a dover fornire la prova della responsabilità penale dell'imputato. Spetta dunque all'accusa l'onere della prova, nel rispetto delle garanzie processuali e del contraddittorio.[220]

Il codice di procedura penale del 1988 sancisce il principio della separazione tra la fase delle indagini preliminari e il dibattimento. In conformità al modello accusatorio, la prova deve essere assunta nel corso del dibattimento, che

219 Ferrua P., *Ammissibilità della prova e regole di esclusione della prova* in *Revista Brasileira de Direito Processual Penal* 2021, 7, 215.
220 Ferrua P., *La prova nel processo penale, vol. I, Struttura e procedimento*, Giappichelli, Torino, 2015.

costituisce la sede ordinaria della sua formazione, prevalentemente in forma orale e alla presenza del giudice, nel rispetto del principio di immediatezza. Una rilevante eccezione a tale principio è rappresentata dall'incidente probatorio, che costituisce uno degli strumenti principali per coniugare le esigenze di efficienza processuale con le garanzie proprie del modello accusatorio. Al fine di evitare che il giudice del dibattimento sia indebitamente influenzato dagli atti compiuti nella fase delle indagini, il codice prevede una netta distinzione tra giudice per le indagini preliminari e giudice del dibattimento. L'incidente probatorio è un procedimento di natura incidentale mediante il quale è possibile acquisire anticipatamente una prova davanti al giudice, in contraddittorio tra le parti, laddove sussista un fondato pericolo che la prova non possa essere raccolta nel corso del dibattimento.[221]

Il modello processuale italiano si caratterizza, inoltre, per una certa flessibilità: accanto ai mezzi di prova tipici, l'art. 189 c.p.p. riconosce il principio della libertà dei mezzi di prova, ammettendo anche strumenti atipici, purché idonei all'accertamento dei fatti. Tuttavia, ai sensi dell'art. 191 c.p.p., le prove acquisite in violazione dei divieti stabiliti dalla legge sono colpite dalla sanzione dell'inutilizzabilità. Ciò nonostante, L'utilizzabilità di una prova non esime il giudice dal doverne valutare la portata, l'attendibilità e la rilevanza ai fini della decisione. Anche una prova pienamente utilizzabile deve essere oggetto di autonoma valutazione da parte del giudice, secondo i criteri del libero convincimento e l'utilizzabilità processuale della prova costituisce un presupposto necessario, ma non sufficiente.[222]

Concluse le considerazioni sulla disciplina generale della prova, l'attenzione verrà ora rivolta alle principali problematiche relative, da un lato, all'acquisizione probatoria sul territorio nazionale e, dall'altro, alla raccolta della

221 C. Tonini e C. Conti, Mnuale di procedura penale, p.644.
222 G. Di Paolo, *Admissibility of E-Evidence, Transnational E-Evidence and Fair-Trial Rights in Italy* in Bachmaier Winter L. e Salimi F., *Admissibility of Evidence in EU Cross-Border Criminal Proceedings: Electronic Evidence, Efficiency and Fair Trial Rights*, Bloomsbury Publishing, Londra, 2024,75.

prova nell'ambito di indagini transnazionali, la quale solleva questioni legate all'extraterritorialità e al necessario raccordo con l'ordinamento interno. Tali questioni emergono in maniera particolarmente evidente nel caso Sky-ECC, che ha messo in luce le complessità derivanti dall'acquisizione e dall'utilizzabilità processuale di prove digitali raccolte in un contesto transnazionale.

3.2.2 Ammissibilità della prova digitale interna

Come si dava conto nel primo capitolo, in assenza di una definizione univoca all'interno del diritto interno la prova digitale ha subito diverse catalogazioni. Tali catalogazioni dipendono strettamente dalla legislazione sovranazionale e dal tipo di dato di cui la prova digitale è oggetto, cioè il dato informatico. La principale divisione che deve essere fatta per incasellare la prova digitale è tra prova digitale statica e dinamica. La prova digitale statica è quella che viene raccolta nella forma documentale ex post attraverso la perquisizione e il successivo sequestro. Al contrario, la prova digitale dinamica ha un grado maggiore di intrusione rispetto ai diritti fondamentali in quanto deriva da un monitoraggio in tempo reale del soggetto e può essere assimilata alla prova raccolta a seguito di intercettazioni.[223]

La prova digitale dinamica può essere raccolta a seguito di misure investigative individualizzate quali ad esempio l'utilizzo del captatore informatico, oppure attraverso la sorveglianza di massa che è una forma di raccolta generalizzata, indiscriminata e preventiva di dati personali o comunicazioni su larga scala da parte di autorità pubbliche, in particolare servizi di intelligence o forze dell'ordine. A differenza della sorveglianza mirata, che si concentra su individui specifici sospettati di determinati reati, la sorveglianza di massa non presuppone sospetti individuali, ma coinvolge intere popolazioni o categorie di utenti.

223 Sanna A., *L'irriducibile atipicità delle intercettazioni tramite virus informatico* in Scalfati A. *Le indagini atipiche*, Giappichelli, Torino, 2019.

La prova digitale è stata in primariamente intesa come prova documentale.[224] Talvolta, forme peculiari di prova digitale quali ad esempio il monitoraggio GPS o il captatore informatico prima della riforma, sono state incasellate tra le prove atipiche i sensi del 189 c.p.p. La situazione è particolarmente intricata nel caso di messagistica Whatsapp o Messanger. Nel caso in cui vi sia acquisizione statica di messaggi già memorizzati, e non attuale e in tempo reale, la norma di riferimento è il 234 c.p.p. sulla prova documentale in quanto la chat rappresenterebbe "fatti persone o cose mediante qualsiasi mezzo ivi compresa la fotografia, la cinematografia". Di tale avviso è la giurisprudenza maggioritaria che ha affermato la piena utilizzabilità di tale fonte di prova nel processo penale.[225] Gli screenshot di messaggi WhatsApp, se non contestati dalla parte controinteressata, possono essere valutati liberamente dal giudice ai sensi dell'art. 192 c.p.p. Tuttavia, se vi è contestazione, è necessario che vengano supportati da altri elementi.[226]

I dati contenuti nel cloud costituiscono prove documentali in quanto di accesso esclusivo da parte dei singoli individui. Essi rappresentano documenti in pieno possesso di coloro tra i quali avviene la comunicazione. La classificazione come documento informatico ha ricadute pratiche importanti. Il documento può essere sequestrato secondo le norme del c.p.p. implementate a partire dalla Convenzione di Budapest, facendo quindi copia forense e proteggendo la catena di custodia. La cassazione conferma anche che la copia forense di documenti informatici ha stessa efficacia probatoria dell'originale, purché non sussistano manipolazioni e costituiscano documenti "statici", non intercettazioni.[227]

Dalla natura di documento, secondo la cassazione discende la applicabilità dell'art. 237 c.p.p. in forza del quale "è consentita l'acquisizione, anche di ufficio, di qualsiasi documento proveniente dall'imputato, anche se sequestrato

224 G Illuminati, *'Digital evidence and admissibility'* in *Revue internationale de droit penal,* 2022, 2, 273, 274.
225 Cass., Sez. VI, 25 ottobre 2017, n. 49016 in onelegale.wolterskluwer.it.
226 Cass., Sez. II, 14 gennaio 2021, n. 1822 in onelegale.wolterskluwer.it.
227 Cass., Sez. VI, 27 aprile 2020, n. 12975 in onelegale.wolterskluwer.it.

presso altri o da altri prodotto". Da ciò consegue che sia possibile non solo utilizzare i documenti consegnati spontaneamente da parte dell'imputato ma anche quelli provenienti e conservati da terzi.[228]

La disciplina delle intercettazioni non si applica alla acquisizione statica del documento informatico che quindi può avvenire per qualsiasi reato, senza un previo provvedimento da parte del giudice che accerti un quadro indiziario significativo. Inoltre, non vi sono limitazioni per quanto concerne la conservazione, è pacifica la possibilità di utilizzazione in altri procedimenti penali o di altra natura, né è applicabile alcuna protezione per il contrato efficace alla indebita ed eccessiva diffusione del materiale. L'interpretazione che classifica la prova digitale statica all'interno della documentazione informatica è problematica. Infatti, il contenuto della stessa è comparabile a ciò che avviene in tempo reale, cambiano solo le modalità di raccolta. In virtù di ciò, l'acquisizione delle chat non è assistita da garanzie sufficienti rispetto alla riservatezza, attraverso pochi click è possibile acquisire la conoscenza anni di relazioni sociali e di informazioni particolarmente sensibili sulla vita dell'accusato o dell'indagato.[229]

La situazione è particolarmente delicata anche sul piano del diritto alla riservatezza dei terzi. È certo che, quando si procede alla acquisizione di grandi quantità di dati, le conversazioni riguardino anche uno o più soggetti del tutto estranei rispetto alla attività criminosa. Da ciò discende l'esigenza di tutelare il diritto alla riservatezza non solo dell'imputato ma anche di altri soggetti che partecipano alle conversazioni oggetto di prova nel processo penale. È opportuno prendere in considerazione tre diverse fattispecie.[230]

Nel caso di intercettazioni i soggetti terzi beneficiano della tutela prevista all'art. 269 c.p.p., infatti, possono richiedere la distruzione del materiale superfluo e privo di rilievo probatorio. Nel caso di messagistica acquisita mediante sequestro

228 Cass., Sez. V, 16 gennaio 2018, n. 1822 in onelegale.wolterskluwer.it.
229 P. Di Stefano, *Il trojan horse nel processo penale* in *Diritto e processo penale* 2020,1364.
230 Ibid.

probatorio vi è la possibilità da parte del terzo di chiedere il riesame a patto che esso sia anche il titolare del bene. La legge infatti legittima al riesame l'imputato e "la persona alla quale le cose sono state sequestrate" o "quella che avrebbe diritto alla restituzione. Nel caso in cui il terzo non abbia un diritto sulla cosa, egli resterà sprovvisto di una tutela nei confronti al diritto alla riservatezza. Infine, quando la messagistica è acquisita quale documento non vi è alcuna tutela nei confronti del terzo.[231]

3.2.3 Ammissibilità e le best practice

Come già anticipato, la legge di ratifica ha introdotto un riferimento esplicito alle *best practice* in materia di prova digitale. Da ciò è scaturito un interessante dibattito in merito alla sanzione processuale da applicare in caso di mancato rispetto di tali prassi. Le *best practice* rivestono un ruolo centrale in un sistema caratterizzato da un'elevata sofisticazione tecnologica e risultano essenziali per garantire la corretta raccolta della prova, analogamente a quanto accade per la prova scientifica. Il rispetto delle *best practice* deve costituire oggetto di contraddittorio, affinché il metodo di acquisizione degli elementi probatori possa essere sottoposto a verifica e, se del caso, contestato.[232]

La prima teoria elaborata in relazione alle conseguenze del mancato rispetto delle *best practice* è quella della nullità per violazione di norme costituzionali. A tale impostazione, tuttavia, si ritiene preferibile la sanzione dell'inutilizzabilità: la conformità alle *best practice* rappresenta infatti una componente essenziale dell'istruzione probatoria, la cui assenza è assimilabile alla mancanza di un elemento cruciale del procedimento istruttorio. La giurisprudenza, al contrario, tende a ricondurre la violazione delle *best practice* a una mera incidenza sull'attendibilità della prova, senza effetti sulla sua validità. Questa tesi appare condivisibile solo nei casi di violazioni non gravi nella raccolta del materiale probatorio.

231 M. Pittirruti, op. cit., p.148.
232 O. Kerr., *Digital Evidence and the New Criminal Procedure* in *Columbia Law Review*, 2005, 105, 279, 28.

Negli altri casi, invece, la violazione delle *best practice* dovrebbe essere ricondotta all'art. 191 c.p.p., che disciplina l'invalidità generale come espressione di una profonda carenza nel potere di istruzione e, dunque, di una violazione delle regole di acquisizione.[233] La soluzione della giurisprudenza che esclude l'esistenza di una regola di esclusione probatoria lascia troppa discrezionalità all'organo giudicante nella valutazione normativa. La giurisprudenza ha seguito questa teoria sin dal caso Trib. Bologna, 22 dicembre 2005, n. 1823, riconoscendo l'importanza delle *best practices* nella *digital forensics* e dimostrando un approccio valutativo e non sanzionatorio in senso stretto. Pur non obbligando all'esclusione, questa pronuncia insegna che il mancato rispetto delle prassi operative perde rilevanza solo se la prova digitale risulti comunque affidabile. Ha quindi cercato un equilibrio tra l'esigenza di certezza probatoria e il principio di legalità formale, fallendo però nel riconoscere la non alterabilità del dato informatico quale requisito intrinseco e non superabile della prova informatica.[234]

Il ricorso alle *best practice*, laddove previsto dalle norme del codice di procedura penale, consiste nella etero-integrazione da parte di fonti secondarie, che devono però essere sufficientemente autorevoli. Tra queste, particolare rilevanza assumono le *best practice* elaborate dalla Guardia di Finanza. La Guardia di Finanza ha sviluppato nel tempo una serie di prassi consolidate nella gestione della prova digitale, soprattutto in ambito di reati economico-finanziari, frodi fiscali e criminalità informatica. La guardia di finanza addestra personale specializzato I Gruppi Anticrimine Tecnologico (GAT) che dispongono di unità con competenze tecniche avanzate, formate su protocolli di acquisizione, cifratura e analisi forense, e sono soggetti ad una formazione continua su queste tematiche.[235]

---

233 A. Colaiocco, *La rilevanza delle best practices nell'acquisizione della digital evidence alla luce delle novelle sulla cooperazione giudiziaria*, in *Archivio penale*, 2019, 1, 3.
234 Trib. Bologna, 22 dicembre 2005, n. 1823.
235 Comando generale della Guardia di Finanza, III Reparto Operazioni – Ufficio Tutela Entrate, Manuale operativo in materia di contrasto all'evasione e alle frodi fiscali (Circolare n. 1/2018), Vol. II, online at gdf.gov.it

Per quanto concerne la fase delle indagini preliminari, parte della dottrina più avvertita ha evidenziato come il bilanciamento tra le esigenze investigative e le garanzie difensive debba realizzarsi attraverso forme di contraddittorio tecnico graduato. In tale prospettiva, l'intervento del difensore anche nella fase predibattimentale, pur in presenza di atti a sorpresa, risponde all'esigenza di evitare sia l'assenza totale di contraddittorio, particolarmente rischiosa data la complessità tecnica della prova digitale, sia un suo utilizzo distorto attraverso il preavviso all'indagato, che potrebbe compromettere l'efficacia delle indagini. Non può infatti escludersi che la disponibilità materiale dei dati da parte dell'indagato consenta una loro alterazione o cancellazione, con conseguenti effetti pregiudizievoli per l'affidabilità del risultato probatorio.[236]

Gli accorgimenti tecnici, sulla scorta di quanto esplicitato dalla Guardia di Finanza, sono particolarmente rilevanti, e devono essere visti con favore, nel terreno delle *digital evidence* in cui il contraddittorio si forma per lo più *ex post* nella fase dibattimentale, sulle operazioni di indagine informatica precedentemente svolte dalla polizia giudiziaria. La contestazione da parte della difesa circa la correttezza della raccolta e utilizzo della prova avverrà sulla base di una duplice analisi. In primo luogo, la difesa può verificare se l'espletamento delle indagini digitali ha seguito la metodologia ideale per il caso concreto, valutata in termini di minore probabilità di alterazione del dato digitale. In secondo luogo, è necessario analizzare se la metodologia ideale è stata nella pratica seguita in modo conforme.[237]

Nella fase finale dell'analisi dibattimentale, che può svolgersi anche mediante il ricorso a periti tecnici nominati dal giudice o dalle parti, si procede all'elaborazione critica dei dati digitali, alla ricostruzione dei nessi logici tra essi e alla formulazione di una sintesi esplicativa. Tale sintesi ha la funzione di fornire al giudice, nella sua qualità di custode della realtà processuale e di intermediario

236 M. Daniele, *La prova digitale nel processo penale* in *Rivista di diritto processuale penale*, 2021, 2, 283, 297.
237 F. M. Molinari., *Le attività investigative inerenti alla prova di natura digitale* in Cassazione penale 2013, 3, 1259, 1265.

tra il sapere specialistico e il piano decisionale, gli strumenti conoscitivi necessari per valutare l'affidabilità e la rilevanza probatoria del materiale informatico acquisito.[238]

3.2.4 Ammissibilità della prova digitale transnazionale nel processo penale: la rogatoria internazionale e gli atti di un altro procedimento

L'acquisizione della prova digitale transnazionale può avvenire mediante OEI, qualora lo Stato interessato appartenga all'UE, oppure tramite rogatoria internazionale, nell'ipotesi in cui si tratti di un Paese terzo. Il codice di procedura penale contiene una disposizione, ritenuta dalla dottrina piuttosto laconica, in merito all'utilizzabilità nel procedimento penale interno delle prove acquisite mediante rogatoria internazionale, come prevista dagli strumenti tradizionali di assistenza giudiziaria, quali la Convenzione europea del 1959: si tratta dell'art. 729 c.p.p. Ci si concentra ora sull'ipotesi in cui sia l'Italia a formulare una richiesta di prova all'estero e tale elemento debba essere successivamente ammesso nel procedimento interno.[239]

L'art. 729 del codice di procedura penale sancisce l'obbligo, per l'autorità giudiziaria italiana, di rispettare le condizioni eventualmente poste dallo Stato estero per l'utilizzazione degli atti acquisiti mediante rogatoria, e richiama, al contempo, l'art. 191, c.2 c.p.p. in tema di inutilizzabilità rilevabile d'ufficio in ogni stato e grado del procedimento. La riforma del 2017, intervenuta nell'ambito di una revisione complessiva del Libro XI del codice, ha introdotto due ulteriori commi che prevedono la sanzione processuale dell'inutilizzabilità: da un lato, nel caso in cui lo Stato estero dia esecuzione alla rogatoria italiana secondo modalità difformi da quelle richieste, purché l'inutilizzabilità sia espressamente prevista dalla legge; dall'altro, al fine di impedire aggiramenti della disciplina, nel caso in cui dichiarazioni rese da chiunque riproducano il contenuto di atti già dichiarati inutilizzabili. Tale riforma ha, eliminato il

238 Colaiocco, op. cit., p.8.
239 M. Chiavario, *Cooperazione giudiziaria internazionale in materia penale*, Giappichelli, Torino, 2022.

riferimento specifico alla Convenzione del 1959 introdotto nell'art. 696, considerato superfluo.[240]

Tuttavia, un possibile aggiramento della normativa è sempre possibile sulla base degli scambi informali di informazioni o la cooperazione tra forze di polizia. Più rapidi ed efficienti rispetto alle lungaggini della procedura formale di mutua assistenza legale, gli scambi informali avvengono senza contraddittorio o particolari garanzie procedimentali. Nondimeno, il comma 2 l'art. 729bis c.p.p. secondo il quale le informazioni spontaneamente trasmesse sono utilizzabili solo nel rispetto delle condizioni poste dallo Stato trasmittente e l'art. 78 delle disp. att. del c.p.p., limita questa possibilità vietando che vengano ammesse prove in frode rispetto al principio del contraddittorio.[241]

Nel caso inverso, ossia quando si intenda utilizzare, in un procedimento penale, atti già formati in altro procedimento, anche estero, trova applicazione l'art. 238 c.p.p. per esplicita menzione da parte dell'art. 78 delle disp. att. al c.p.p. Tale disposizione non configura uno strumento di cooperazione internazionale, come le lettere rogatorie, bensì una norma interna di diritto processuale che disciplina le condizioni di utilizzabilità degli atti formati *extra iudicium*. L'acquisizione si caratterizza per la sua natura passiva: non si sollecita la formazione ex novo dell'atto da parte dell'autorità straniera, ma si introduce nel processo ciò che è già stato prodotto in altro contesto, prescindendo da un'attività cooperativa attiva, attraverso un "trasferimento probatorio".[242]

La disposizione all'art. 238 c.p.p. consente la acquisizione di prove documentali provenienti da un altro procedimento penale al ricorrere di alcune condizioni. Se la prova digitale si considera atto ripetibile è essenziale che vi sia stato contraddittorio tra le parti, altrimenti è comunque ammessa l'acquisizione della

240 G.Spangher, *Codice di procedura penale. Commentato con la giurisprudenza*, Giappichelli Torino, 2023.
241 Chiavario, op cit., p.103.
242 Canestrini N., *La cooperazione giudiziaria penale europea esige il rispetto della tutela dei diritti fondamentali, fondamento della fiducia reciproca fra gli stati membri*, in *Cassazione penale,* 2023, 6/63, 2113.

documentazione nel caso in cui la ripetizione dell'atto è divenuta impossibile per fatti o circostanze sopravvenuti, l'acquisizione è ammessa se si tratta di fatti o circostanze imprevedibili.[243.]

3.2.5 Ammissibilità della prova digitale transnazionale nel processo penale: l'attuazione della direttiva sull'ordine di indagine europeo

Il silenzio del legislatore europeo in materia di ammissibilità della prova determina incertezze dovute alla mancanza di raccordo tra gli ordinamenti penali dei diversi Stati membri. Tali incertezze si riflettono anche nel contesto italiano, in cui la prova digitale non è ancora oggetto di una compiuta disciplina normativa. Come evidenziato nei capitoli precedenti, il rispetto dei diritti fondamentali alla privacy e al giusto processo risulta fortemente compromesso nella raccolta transnazionale delle prove digitali.[244]

La principale criticità risiede nel rischio di una compromissione del principio del contraddittorio e dell'equilibrio tra accusa e difesa. La prova digitale, per via della sua complessità tecnica, è particolarmente vulnerabile a usi impropri o fraudolenti. Tale rischio è accentuato dalla dimensione transnazionale dell'acquisizione probatoria, che rende difficile per la difesa verificare la correttezza delle operazioni svolte all'estero. Ne deriva, di fatto, un'inversione dell'onere della prova a carico della difesa, chiamata a contestare l'attendibilità di elementi probatori formatisi in un altro ordinamento, specie quando questi risultino carenti sotto il profilo dell'autenticità o del rispetto delle *best practices* in materia di prova digitale. Difficilmente la difesa sarà in grado di verificare le modalità acquisitive della prova e di contestare quanto svolto nel corso delle investigazioni digitali.[245]

---

243 Gaito A., *La circolazione delle prove e delle sentenze* in *Archivio Penale*, 2011, 3, 17.
244 P. Raucci, *L'Ordine europeo di indagine e prove digitali: tra presunzione di legittimità degli atti compiuti all'estero e diritti fondamentali* in *Penale Diritto e Procedura* https://www.penaledp.it/lordine-europeo-di-indagine-e-prove-digitali-tra-presunzione-di-legittimita-degli-atti-compiuti-allestero-e-diritti-fondamentali/ accesso 12 Luglio 2025.
245 D. La Muscatella, *La ricerca delle fonti di prova sulle reti di* cloud computing*: le nuove frontiere delle investigazioni digitali tra profili giuridici e questioni operative*, in *Ciberspazio e diritto*, 2013, 477.

La Direttiva è stata oggetto di attuazione nell'ordinamento interno,[246] il codice di procedura penale contiene oggi le disposizioni da 696bis al 696decies c.p.p., dedicate alla cooperazione europea in materia di raccolta della prova. Il principio del mutuo riconoscimento e le sue limitazioni, già entrati nel nostro ordinamento grazie al principio di primazia del diritto europeo, sono esplicitati all'art. 696bis c.p.p. che afferma che "L'autorità giudiziaria provvede al riconoscimento e all'esecuzione se non sussistono fondate ragioni per ritenere che l'imputato o il condannato verrà sottoposto ad atti che configurano una grave violazione dei principi fondamentali dell'ordinamento giuridico dello Stato, dei diritti fondamentali della persona riconosciuti dall'art. 6 del Trattato sull'Unione europea o dei diritti, delle libertà e dei principi sanciti nella Carta dei diritti fondamentali dell'Unione europea.".

La più interessante innovazione della norma di attuazione della direttiva OEI il d.lgs. 1 giugno 2017, n. 108 è rappresentata dall'art. 31, il quale estende la legittimazione attiva per richiedere l'OEI anche al difensore o all'indagato. La richiesta è soggetta a una specifica condizione di ammissibilità: essa deve contenere l'indicazione dell'atto da assumere all'estero e le ragioni che ne giustificano la rilevanza. In caso di rigetto, il pubblico ministero provvede con decreto motivato, mentre il giudice decide con ordinanza, previa audizione delle parti. Qualora l'atto richiesto consista in un sequestro probatorio, in caso di rigetto da parte del pubblico ministero, trova applicazione il meccanismo di controllo sostitutivo del giudice previsto dall'art. 368 del codice di procedura penale.[247]

Per quanto concerne la utilizzabilità delle prove, ai sensi dell'art. 36 del d.lgs. 108/2017, confluiscono nel fascicolo per il dibattimento sia i documenti acquisiti all'estero mediante ordine europeo di indagine, sia i verbali degli atti non ripetibili raccolti con le medesime modalità. Inoltre, possono essere inseriti

246 Direttiva 2014/41/UE del Parlamento europeo e del Consiglio, del 3 aprile 2014, relativa all'ordine europeo di indagine penale [2014] GU L130/1
247 Circolare del Ministero della Giustizia 26 ottobre 2017, Manuale operativo sull'attuazione della direttiva 2014/41/UE relativa all'ordine europeo di indagine penale (Ottobre 2017).

anche i verbali di ulteriori atti istruttori eseguiti all'estero, purché i difensori siano stati posti in condizione di parteciparvi e di esercitare le facoltà previste dalla normativa processuale italiana. La ratio della disposizione risiede nella necessità di garantire il rispetto del contraddittorio e dei diritti della difesa nella fase di formazione della prova. In aggiunta, nei casi e con le modalità previste dall'art. 512bis c.p.p., il giudice può procedere alla lettura in aula dei verbali contenenti dichiarazioni rese all'estero e acquisite tramite ordine europeo di indagine nella fase delle indagini preliminari, qualora tali atti non rientrino tra quelli già inseriti nel fascicolo dibattimentale ai sensi dell'art. 431 c.p.p. Tale meccanismo consente di valorizzare le risultanze istruttorie transfrontaliere, senza pregiudicare i principi di immediatezza e oralità propri del dibattimento.[248]

3.2.6 Le sentenze gemelle Sky-Ecc e i successivi sviluppi

Il caso Sky-ECC rappresenta un esempio paradigmatico delle problematiche connesse all'acquisizione di prove digitali in un contesto transnazionale. Nel 2021, le autorità francesi e belghe hanno svolto un ruolo centrale nello smantellamento della piattaforma di comunicazione criptata Sky-ECC, utilizzata in larga misura da organizzazioni criminali per lo scambio di messaggi ritenuti sicuri e non intercettabili. Le evidenze così acquisite sono state poi trasmesse ad altri Stati membri, tra cui l'Italia, sollevando delicati interrogativi circa l'utilizzabilità processuale di tali prove nel rispetto dei principi nazionali e sovranazionali in materia di giusto processo. ,[249] la Corte di cassazione si è infatti interessata alla tematica sempre più rilevante della acquisizione di prove derivanti dai c.d. criptofonini in due sentenze dal contenuto sovrapponibile.[250]

In entrambe le sentenze possiamo sentire le ripercussioni della sentenza *Encrochat* nei confronti del diritto nazionale.[251]

248 Gaito, op. cit., p.23.
249 Corte di Giustizia, Causa C-670/22 Encrochat, ECLI:EU:C:2024:372 in curia.europa.eu.
250 Cass., pen., sez. VI, 29 Febbraio 2024, n.23755 e 23756. in onelegale.wolterskluwer.it.
251 Corte di Giustizia, Causa C-670/22 Encrochat, ECLI:EU:C:2024:372 in curia.europa.eu..

La Corte di cassazione ha rimarcato la non necessarietà di un intervento da parte del giudice nella emissione dell'OEI conformemente a quanto stabilito dalla Direttiva e dalla giurisprudenza della CGUE, la quale ha sottolineato la natura di misura che può essere richiesta da parte del pubblico ministero ai sensi dell'art. 2 della Direttiva OEI. Come già affermato dalla CGUE, infatti, l'OEI non è una decisione giurisdizionale in senso stretto, ma uno strumento di cooperazione che consente di disporre una misura investigativa in un altro Stato membro.[252]

Sebbene non ci sia un obbligo di controllo preventivò, ciò che rileva è infatti l'esistenza di un rimedio *ex post* che sia idoneo secondo il principio di equivalenza a garantire un rimedio giurisdizionale effettivo nello stato di emissione dell'OEI. Da ciò discende che l'accusato debba essere messo in condizione di impugnare la misura investigativa potendone contestare la regolarità e necessità della stessa. Questa affermazione è rafforzata dal fatto che i motivi di merito possono essere contestati ex art. 14 della direttiva OEI solo nello stato di emissione.[253]

La Corte di cassazione è stata chiamata a pronunciarsi sulle modalità di ammissione di tali prove alla luce sia della normativa sovranazionale che di quella nazionale, con particolare riguardo all'utilizzabilità della prova digitale transnazionale acquisita tramite un OEI. Le sentenze "gemelle" hanno innanzitutto affrontato la questione della qualificazione giuridica più adeguata, secondo l'ordinamento italiano, dell'atto di acquisizione probatoria. La Cassazione ha escluso l'applicabilità dell'art. 234-bis c.p.p., relativo all'acquisizione di documenti e dati informatici conservati all'estero, ritenendolo uno strumento alternativo e non compatibile con il ricorso all'OEI.

Le Sezioni Unite hanno dato rilievo al fatto che nel caso di specie venivano in gioco prove già autonomamente raccolte dalle autorità straniere prima

252 Corte di giustizia, Causa C-584/19, *HP*, ECLI:EU:C:2020:1027 in curia.europa.eu.
253 Corte di Giustizia, Causa C-852/19 *Gavanozov II*, ECLI:EU:C:2021:422 in curia.europa.eu.

dell'emissione dell'OEI, l'equivalenza con in casi interni simili deve essere parametrata in rapporto non alla disciplina nazionale della formazione, ma a quella della "circolazione" delle prove fra procedimenti diversi.[254] La disciplina ritenuta applicabile al caso di specie è invece quella prevista dall'art. 238 c.p.p., in forza del rinvio contenuto nell'art. 78 delle disp. Att. Del c.p.p. Qualora, tuttavia, le prove siano qualificate come intercettazioni, viene altresì in rilievo l'art. 270 c.p.p., che disciplina i limiti all'utilizzabilità delle intercettazioni acquisite in procedimenti diversi da quello in cui si intendono utilizzare.[255]

La Corte di cassazione ha verificato il rispetto della *lex fori* italiana, attribuendo rilievo ai requisiti previsti dall'art. 270 c.p.p., e valutando se la misura investigativa sarebbe stata ammissibile in un caso analogo nell'ordinamento interno, conformemente all'art. 6 della Direttiva OEI. La verifica ha incluso anche un giudizio di compatibilità della misura con i diritti fondamentali tutelati dall'ordinamento italiano conformemente all'art. 10 della medesima Direttiva. In questo accertamento, complesso e caratterizzato da un necessario bilanciamento tra le esigenze del procedimento penale e la salvaguardia delle garanzie fondamentali, la Corte ha individuato la necessità che la misura investigativa fosse assistita da un'autorizzazione preventiva da parte dell'autorità giudiziaria e che riguardasse reati per i quali è previsto l'arresto obbligatorio in flagranza. Concludendo positivamente tale analisi, la Corte ha ritenuto che tali condizioni fossero rispettate dall'autorità esecutiva straniera, riconoscendo così l'utilizzabilità della prova digitale acquisita mediante OEI nel procedimento italiano.[256]

---

254 S. Agnino, *Sky ecc, ordine europeo di indagine tra giurisprudenza nostrana e comunitaria* in *Giustizia Insieme* https://www.sistemapenale.it/it/scheda/daniele-ordine-europeo-di-indagine-penale-e-comunicazioni-criptate-il-caso-sky-ecc-encrochat-in-attesa-delle-sezioni-unite, accesso 06/05/2025.

255 M. Daniele, *Le sentenze "gemelle" delle Sezioni Unite sui criptofonini. La mappa del controllo giurisdizionale quando l'OEI ha ad oggetto prove già in possesso dell'autorità straniera* in *Sistema Penale* https://www.sistemapenale.it/it/scheda/daniele-le-sentenze-gemelle-delle-sezioni-unite-sui-criptofonini, accesso 08/04/2025.

256 N. Gallo *Questioni aperte sull'ordine europeo di indagine penale. L'acquisizione all'estero della messaggistica criptata sulla piattaforma SKY-ECC*, in *Archivio Penale*, 2023, 3.

Sulla scorta di quanto affermato nella sentenza *Encrochat*, appare necessario, ai fini dell'ammissibilità della prova, che le parti siano messe in condizione di commentarla efficacemente. La CGUE ha affermato che l'art. 14, paragrafo 7, impone alle autorità nazionali di garantire il principio del contraddittorio, quale sintesi della tutela dei diritti della difesa e del diritto a un equo processo secondo il diritto europeo. Le norme sull'ammissibilità della prova dovrebbero essere interpretate alla luce delle affermazioni della CGUE, al fine di garantire una lettura conforme al diritto dell'Unione. Sebbene la verifica di conformità alla *lex fori* possa ritenersi adeguata rispetto al diritto interno, la Corte non ha accertato il rispetto specifico della regola di esclusione prevista a livello europeo. In effetti, appare difficile sostenere che il principio del contraddittorio sia stato rispettato in un contesto investigativo in cui alla difesa è preclusa la possibilità di verificare puntualmente le modalità di acquisizione della prova.[257]

L'orientamento espresso dalle Sezioni Unite è stato confermato anche in una recente sentenza, in cui la Corte ha aderito all'interpretazione secondo la quale non esisterebbe una vera e propria regola di esclusione della prova europea, ridimensionando la portata delle sentenze *Encrochat*, *La Quadrature du Net I* e *Prokuratuur*, che riconoscono invece l'esistenza di una simile regola.[258]

In particolare, la Cassazione ha escluso che l'assenza di un'autorizzazione preventiva da parte del giudice possa integrare una violazione del principio del contraddittorio. Ha inoltre negato che la violazione della norma europea possa determinare, *ipso iure*, l'inutilizzabilità della prova. La Corte ha infatti ridotto l'ambito di applicazione della regola di esclusione al solo caso in cui risulti totalmente preclusa la possibilità di commentare le prove acquisite. La Corte ha fatto leva sul principio di autonomia procedurale degli Stati membri, evidenziando come, in assenza di una compiuta armonizzazione in materia probatoria, spetti ai singoli ordinamenti disciplinare le modalità di acquisizione

257 Veronica V., *'Criptofonini e indagini digitali transfrontaliere su larga scala: un difficile equilibrio tra privacy, fairness processuale ed esigenze di repressione dei reati'* in Giurisprudenza Penale 2025, 1.
258 M. Panzavolta, *Exclusion of Evidence in Times of Mass Surveillance,* p.202.

e di utilizzazione della prova, nel rispetto dei principi di equivalenza ed effettività.

Capitolo 4 Service provider e prova digitale

4.1 Il ruolo dei service provider: la sfida ai diritti fondamentali

Nel rapporto tra soggetto privato e autorità pubblica, tipico del procedimento penale, si inserisce sempre più di frequente un terzo soggetto, rappresentato dai service provider. Essi assumono un ruolo intermedio di rilievo, fungendo da detentori di informazioni digitali suscettibili di rilevanza probatoria e ponendosi, di conseguenza, al crocevia tra esigenze investigative dello Stato, interessi economici propri e tutela dei diritti fondamentali degli individui. [259].

La sua peculiarità principale risiede nella natura privata del soggetto, che tuttavia interviene nella gestione di interessi pubblici, soprattutto quando questi si intrecciano con il delicato bilanciamento dei diritti fondamentali. Questi soggetti rivestono anche un ruolo di rilievo sul piano economico, poiché costituiscono alcuni tra i principali operatori del mercato digitale. A causa della sempre maggior rilevanza di servizi online, sono aumentate in modo drastico le richieste di cooperazione giudiziaria che sono spesso rivolte agli operatori economici privati.[260]

Il Regolamento E-evidence introduce una definizione ampia e articolata di "prestatore di servizi", delineando le categorie di soggetti destinatari degli OEC e OEP. La nozione comprende tanto le persone fisiche quanto quelle giuridiche che forniscono servizi rientranti in tre macrocategorie: i servizi di comunicazione elettronica, i servizi relativi ai nomi di dominio e agli indirizzi IP, e infine altri servizi della società dell'informazione, purché consentano la comunicazione tra utenti o comportino la conservazione o il trattamento di dati per conto degli stessi. Questa definizione rivela chiaramente l'intento del legislatore europeo di ricomprendere nell'ambito di applicazione del regolamento tutti gli attori tecnologici centrali, a prescindere dalla loro forma

259 H. Abraha, *'Law enforcement access to electronic evidence across borders: mapping policy approaches and emerging reform initiatives'* in *International Journal of Law and Information Technology*, 2021, 29, 118.
260 Regolamento E-evidence, considerando 8.

giuridica o dalla specifica natura commerciale. Viene così riconosciuto il ruolo centrale svolto dai prestatori di servizi nel trattamento e nella conservazione di dati potenzialmente rilevanti ai fini investigativi.[261]

Tale approccio risulta coerente con l'evoluzione della criminalità e delle comunicazioni, sempre più mediate da piattaforme private, che fungono da infrastrutture fondamentali tanto per le interazioni personali quanto per le attività economiche. Di conseguenza, l'inclusione anche di servizi come i social media, i cloud storage o le app di messaggistica, garantisce che le autorità inquirenti possano disporre di strumenti effettivi per accedere a fonti probatorie ormai indispensabili. È evidente, dunque, che la figura del prestatore di servizi, così come delineata nel Regolamento, assume un rilievo centrale non solo per l'efficacia dell'azione penale, ma anche per il bilanciamento tra le esigenze investigative e la tutela dei diritti fondamentali degli utenti. In questo equilibrio si gioca, in ultima analisi, la legittimità dell'intervento pubblico nel dominio digitale.[262]

Il regolamento interagisce in modo significativo con la normativa preesistente in materia di trattamento dei dati personali, introducendo nuovi diritti e obblighi a carico dei service provider.

4.1.1 L'interazione del regolamento E-evidence con GDPR e Digital Service Act

Il Regolamento E-evidence presenta interessanti punti di contatto con la normativa di riferimento del settore. Da un lato, con il GDPR, che rimane la cornice generale di riferimento in materia di protezione dei dati personali e di diritti fondamentali; dall'altro, con il più recente e innovativo Digital Services

261 J. Hafetz, *Possibilities and limitations of Corporations as Protectors of Privacy in the digital age* in D. Cole e F. Fabbrini, *Surveilance, Privacy, and Trans-Atlantic Relations*, Hart Publishing, Oxford, 2017.
262 M. Corhay, *Private Life, Personal Data Protection and the Role of Service Providers: The EU e-Evidence Proposal* in *European Papers,* 2021, 6/1, 441.

Act, che ridefinisce la responsabilità delle piattaforme digitali, rafforzando trasparenza e cooperazione nei confronti delle autorità pubbliche.

Il GDPR si applica alla materia penale con limiti particolarmente stringenti, infatti, questo non si applica ai trattamenti di dati effettuati per attività tra cui la prevenzione, indagine, accertamento e perseguimento dei reati. Ciò significa che per il settore penale esiste una disciplina specifica e separata: la già citata Direttiva E-privacy. La Direttiva regola il trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati, nonché di esecuzione delle sanzioni penali. essa è stata recepita in Italia con il d.lgs. 51/2018.[263]

Il GDPR, quale principale atto normativo riguardante la tutela della riservatezza degli individui ha diversi punti di contatto con la materia penale. Gli stessi dati utilizzati in fase nel processo penale come prove digitali sono stati conservati e trattati dal fornitore di servizi per larga parte della loro vita ai sensi del GDPR. Nel corso del processo penale le autorità pubbliche sono sottoposte alla direttiva E-privacy, mentre le aziende private restano sottoposte al GDPR. Inoltre, larga parte della Direttiva riproduce le definizioni e i principi contenuti nel GDPR.[264]

Entrambi gli strumenti normativi prevedono una disciplina volta a tutelare l'individuo attraverso principi quali la liceità, correttezza; specificità della finalità; minimizzazione; esattezza; limitazione della conservazione; sicurezza. Entrambi richiedono una base giuridica chiara e proporzionata, nel caso del GDPR si parla di un consenso lecito e informato, mentre la direttiva E-privacy richiede la necessarietà per la giustizia penale e la sicurezza pubblica. L'interessato è dotato di Diritti simili, ma più limitati nel contesto penale per non compromettere le indagini. Infine, Entrambi sottolineano il ruolo essenziale del

263 J. Sajfert e T. Quintel, *Data Protection Directive (EU) 2016/680 for Police and Criminal Justice Authorities*, in M. Cole e F. Boehm, *GDPR Commentary*, Edward Elgar Publishing, Cheltenham, 2018.
264 P. De Hert e V. Papakonstantinou, *The New Police and Criminal Justice Data Protection Directive: A First Analysis*' in *New Journal of European Criminal Law*, 2016, 7/1, 18.

controllo giurisdizionale, e prevedono regole stringenti per i trasferimenti di dati verso Paesi terzi.[265]

Il DSA rappresenta il nuovo contesto regolamentare di base nel quale le piattaforme fornitrici di servizi digitali si trovano ad operare.[266] Esso prevede obblighi di trasparenza e collaborazione particolarmente gravosi, i provider devono spiegare in modo chiaro e comprensibile le proprie condizioni generali, incluse le politiche di moderazione dei contenuti, l'uso di algoritmi e i criteri di rimozione o limitazione di contenuti. Gli Stati membri possono inviare ordini vincolanti ai provider, che devono eseguirli tempestivamente e le autorità giudiziarie e amministrative possono richiedere informazioni sugli utenti. Il regolamento prevede inoltre, analogamente al regolamento E-evidence l'istituzione di punti di contatto legali: i provider devono designare un rappresentante legale nell'UE e un punto di contatto per garantire la comunicazione con le autorità.[267]

L'interazione tra i due strumenti si presenta come complementare: il DSA rafforza la trasparenza e la prevedibilità dei rapporti con i provider nel quadro generale del mercato digitale, mentre il Regolamento e-Evidence traduce questa cornice in un meccanismo giuridico specifico, pensato per la materia penale, che consente alle autorità di accedere ai dati digitali in tempi rapidi, superando la rigidità delle procedure tradizionali di mutua assistenza. La loro sinergia riflette l'emergere di un approccio europeo coerente e integrato, che da una normativa di applicazione generale si spinge a disciplinare anche gli aspetti più delicati e sensibili, come la raccolta e l'utilizzo delle prove penali.[268]

---

265 Studio per il parlamento europeo (n.288), 42

266 Regolamento (UE) 2022/2065 del Parlamento europeo e del Consiglio del 19 ottobre 2022 relativo a un mercato unico dei servizi digitali e che modifica la direttiva 2000/31/CE (Digital Services Act).

267 W. Henderman, *Transparency Under the EU Digital Services Act* in *Mason* in *Hayes , Curran Insgìights* https://www.mhc.ie/latest/insights/transparency-under-the-eu-digital-services-act?utm_source=chatgpt.com, accesso 24/08/2025.

268 D. Zapf e F. Malaga, *EU breaks down digital borders: New e-Evidence rules facilitate cross-border investigations* in White and Case Publications https://www.whitecase.com/insight-alert/eu-breaks-down-digital-borders-new-e-evidence-rules-facilitate-cross-border?utm_source=chatgpt.com, accesso 26/08/2025.

4.1.2 Gli obblighi dei service provider

La Direttiva impone agli Stati membri di assicurare che i fornitori di servizi che operano nell'UE designino almeno un rappresentante legale per ricevere, eseguire e far rispettare decisioni e ordini emessi dalle autorità competenti degli Stati membri a fini probatori in procedimenti penali. I fornitori interessati sono gli stessi previsti dal Regolamento e-evidence. I fornitori stabiliti nell'UE e attivi in più Stati membri devono designare uno o più stabilimenti incaricati di svolgere tali funzioni. I fornitori non stabiliti nell'UE, ma che offrono servizi nell'Unione come molte aziende statunitensi, devono nominare uno o più rappresentanti legali. In linea di principio, i fornitori sono liberi di scegliere quanti referenti designare e in quali Stati membri, e gli Stati non possono limitare questa scelta. Tuttavia, per garantire l'efficienza operativa, il rappresentante legale deve trovarsi in uno Stato membro in cui il fornitore è attivo e partecipa agli strumenti giuridici rilevanti. In caso di più referenti, è obbligatorio indicarne il campo di competenza territoriale.[269]

La Direttiva consente anche che più fornitori condividano lo stesso referente, a condizione che ciò non comprometta la protezione dei dati. Questa possibilità può risultare utile soprattutto per le piccole e medie imprese. Il ruolo dei referenti non si limita all'attuazione del Regolamento, ma si estende anche ad altri strumenti come l'Ordine Europeo di Indagine (OEI), la Convenzione UE sull'assistenza giudiziaria e le norme nazionali. I fornitori devono quindi garantire che i referenti dispongano dei poteri e delle risorse necessarie per adempiere agli ordini provenienti da qualsiasi Stato membro partecipante. Gli Stati hanno l'obbligo di verificare che questa condizione sia rispettata e rimanga tale. Infine, ogni fornitore deve notificare all'autorità centrale competente, entro sei mesi dal termine di recepimento della Direttiva o dall'inizio della propria attività nell'UE, lo Stato membro in cui è attivo e dove si trova il referente

269 A. Wulf, *E-Evidence Regulation: New obligations for service providers from 2026* in *Heuking News & Events https://www.heuking.de/en/news-events/newsletter-articles/detail/e-evidence-regulation-new-obligations-for-service-providers-from-2026.html?utm_source=chatgpt.com, accesso 23/08/2025.*

designato. Nella notifica devono essere indicati anche le lingue utilizzabili e l'ambito territoriale di ciascun referente.[270]

I fornitori di servizi devono produrre i dati entro i termini stabiliti. In caso di ricezione di un Ordine europeo di conservazione, i dati devono essere preservati senza indebito ritardo e mantenuti per il periodo previsto. Il fornitore di servizi ha inoltre obblighi informativi nei confronti dell'autorità emittente ed esecutiva qualora intenda sollevare obiezioni all'esecuzione degli ordini (art. 10 e 11 del Regolamento). Infine, è tenuto a garantire la riservatezza, la segretezza e l'integrità dei dati prodotti e conservati (Art. 4 del Regolamento). L'obbligo di istituire procedure adeguate non è estraneo all'ordinamento italiano il quale all'art. 132 *bis* del Codice Privacy prevede che "i fornitori istituiscono procedure interne per corrispondere alle richieste effettuate in conformità alle disposizioni che prevedono forme di accesso a dati personali degli utenti" al fine di rispondere in modo adeguato rispetto alle richieste di produzione dei dati da parte dell'autorità giudiziaria. Da ciò consegue una responsabilità da parte del service provider di istituire assetti organizzativi e procedure interne idonee allo scopo di fornire risposte adeguate e tempestive all'autorità giudiziaria.[271]

4.1.3 Sanzioni ed incentivi a collaborare per i service provider

Il Regolamento prevede una procedura di esecuzione e un regime sanzionatorio nel caso in cui il fornitore di servizi non rispetti l'obbligo di eseguire un Certificato di Ordine Europeo di Produzione o di Conservazione (EPOC ed EPOC-PR). Lo stesso vale se il fornitore non adotta misure tecniche e operative all'avanguardia per garantire la riservatezza, la segretezza e l'integrità nella trasmissione dei dati, come previsto dall'art. 13(4). In tal senso, il Regolamento impone agli Stati membri di stabilire norme e misure per l'imposizione di sanzioni pecuniarie e di comunicarle tempestivamente alla Commissione.[272]

---

270 R. Di Pietra, *Principali impatti sulle Società Telco per il Regolamento E-Evidence* in *Sicurezza e Giustizia* https://www.sicurezzaegiustizia.com/principali-impatti-sulle-societa-telco-per-il-regolamento-e-evidence/, accesso 10 Agosto 2025.
271 A.Wulf, op. cit., p.5.
272 T. Whal, *E-evidence Regulation and Directive Published* in *Eurcrim,* 2023, 2, 165, 166.

Il Regolamento richiede che tali sanzioni siano efficaci, proporzionate e dissuasive, lasciando però agli ordinamenti nazionali la facoltà di decidere come sanzionare, anche tramite il diritto penale. Precisa, inoltre, che la sanzione pecuniaria può arrivare fino al 2% del fatturato mondiale annuo del fornitore di servizi. Infine, se il fornitore agisce in buona fede nell'adempiere agli obblighi derivanti da un EPOC o EPOC-PR, non sarà ritenuto responsabile per eventuali danni arrecati agli utenti o a terzi, fatto salvo quanto previsto dalle norme in materia di protezione dei dati.

La previsione secondo cui le sanzioni devono essere efficaci, proporzionate e dissuasive costituisce un tratto distintivo del diritto dell'Unione europea. Tale formula rappresenta la cristallizzazione normativa di principi elaborati dalla Corte di giustizia a partire dalla fine degli anni Novanta.[273] Sia la Corte sia il legislatore europeo se ne avvalgono per garantire che gli Stati membri non si limitino a introdurre sanzioni meramente simboliche, ma adottino misure realmente idonee ad assicurare l'effettività del diritto dell'Unione, nel rispetto dei principi fondamentali del diritto penale.[274]

Il regolamento E-evidence disciplina altresì il tema del rimborso delle spese sostenute dai prestatori di servizi per l'esecuzione degli ordini europei. L'articolo 14 prevede che gli Stati membri garantiscano a tali soggetti il diritto a un rimborso "ragionevole" dei costi derivanti dall'adempimento agli ordini di produzione o conservazione, al fine di non trasferire integralmente sugli operatori privati l'onere economico della cooperazione giudiziaria. Questa previsione riflette un bilanciamento tra l'interesse pubblico all'efficace acquisizione di prove digitali e la necessità di non gravare eccessivamente sui fornitori, preservandone la disponibilità e la collaborazione.

Nonostante la previsione sia significativa e meriti una valutazione positiva, sussiste il rischio che il rimborso possa rivelarsi meramente simbolico. Inoltre,

273 Corte di giustizia, *Commissione delle Comunità europee c. Repubblica ellenica, C-68/88 EU:C:1989:339* in curia.europa.eu.
274 A. Kilp, op. cit, p.345.

la disposizione sembra orientarsi verso un'interpretazione restrittiva, che lo ammette solo laddove lo Stato membro ne abbia espressamente previsto la possibilità.[275]

4.1.4 I diritti dei service provider

Nel sistema delineato dal Regolamento E-evidence sull'OEP, i fornitori di servizi non sono meri destinatari passivi degli obblighi di consegna dei dati, ma godono di alcune prerogative che riflettono la necessità di garantire un equilibrio tra l'efficacia investigativa e la tutela di diritti e obblighi giuridici di rango superiore. L'art. 10, paragrafo 6, attribuisce infatti al *service provider* la facoltà di richiedere chiarimenti all'autorità di emissione qualora l'ordine presenti elementi di incompletezza, errori manifesti o informazioni insufficienti a consentirne l'esecuzione. Si tratta di un meccanismo di natura procedurale che, da un lato, tutela l'affidamento del provider e ne limita la responsabilità in caso di inadempimento dovuto a carenze formali dell'ordine, e dall'altro contribuisce a rafforzare la certezza giuridica e la correttezza procedimentale nell'attuazione dello strumento di cooperazione.[276]

Accanto a questa possibilità, il Regolamento prevede anche due ipotesi tassative di motivi giuridici di non esecuzione da parte del fornitore. In primo luogo, l'art. 10, paragrafo 5, contempla il rispetto di immunità e privilegi riconosciuti dall'ordinamento, i quali possono escludere la consegna dei dati richiesti; tale previsione appare coerente con la necessità di preservare ambiti protetti dal segreto professionale o da garanzie funzionali, che non possono essere compressi da un ordine investigativo transfrontaliero. In secondo luogo, l'art. 17, paragrafi 1 e 2, riconosce il diritto del provider di sollevare un conflitto con obblighi derivanti dal diritto applicabile di un Paese terzo: questa clausola riflette la complessità del contesto globale in cui operano i grandi fornitori di servizi,

275 R. Di Pietra, *Principali impatti sulle Società Telco per il Regolamento E-Evidence,* p.4.
276 R. Di Pietra, *Il Regolamento UE sulla E-Evidence* in *Sicurezza e Giustizia* https://www.sicurezzaegiustizia.com/il-regolamento-ue-sulla-e-evidence/, accesso 10 Agosto 2025

spesso soggetti a regimi giuridici plurimi e potenzialmente contrastanti, come dimostra il noto problema di interferenza con la normativa statunitense.[277]

L'introduzione di tali meccanismi evidenzia come il legislatore europeo abbia inteso contemperare la rapidità e l'efficacia delle indagini penali nello spazio europeo con la necessità di garantire certezza del diritto e rispetto degli obblighi internazionali. Si riconosce, dunque, che l'effettività dell'OEP non può essere perseguita a scapito della tutela di valori fondamentali o degli obblighi giuridici esterni all'ordinamento dell'Unione, ma deve piuttosto integrarsi in un quadro multilivello di salvaguardie. In questo senso, la disciplina conferma il ruolo dei *service provider* come interlocutori attivi nel sistema della cooperazione giudiziaria digitale, la cui collaborazione è funzionale ma non cieca, e deve sempre svolgersi nel rispetto dei limiti derivanti da immunità, privilegi e conflitti normativi transnazionali.[278]

4.1.5 Il difficile equilibrio tra la pretesa punitiva dello stato, la privacy dell'accusato e l'intermediazione del service provider

L'espansione delle tecnologie digitali e l'accresciuta capacità di raccolta e trattamento dei dati personali hanno reso sempre più urgente una riflessione sulle minacce alla riservatezza degli individui e sulla necessità di strumenti idonei a garantire un effettivo equilibrio tra interessi pubblici, logiche di mercato e tutela dei diritti fondamentali. Occorre interrogarsi sull'effettiva idoneità del ruolo attribuito ai *service provider* quali 'protettori della privacy', considerato che, oltre a essere destinatari di obblighi di tutela dei dati personali e portatori di interessi economici propri, possono essi stessi rendersi responsabili di condotte lesive della riservatezza degli individui.

Tra gli esempi più rilevanti di violazioni da parte dei prestatori di servizi, si possono menzionare il pericolo di una profilazione occulta senza un consenso

277 G. Forlani, The E-evidence Package: The Happy Ending of a Long Negotiation Saga in *Eurcrim*, 2023, 2, 174.
278 G. Robinson, *Effective Data Protection and Direct Cooperation on Digital Evidence* in Franssen V. e Tosza S., *The Cambridge Handbook of digital evidence in criminal investigations,* Cambridge University Press, Cambridge,2025.

realmente libero, intendendosi per profilazione qualsiasi forma di trattamento automatizzato di dati personali finalizzato a valutare determinati aspetti personali di una persona fisica, in particolare per analizzare o prevedere elementi riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, la posizione o gli spostamenti dell'interessato. A ciò si aggiunge la possibile cessione dei dati a soggetti privati terzi per finalità di pubblicità mirata, nonché l'eventualità di *data breach*, ossia violazioni di sicurezza che comportano l'accesso non autorizzato, la distruzione, la perdita o la divulgazione illecita di dati personali sensibili, talvolta realizzate anche con finalità criminose, quali il furto di identità o altre forme di frode.[279]

I *service provider* non vendono i dati ai soli soggetti privati, ma anche agli Stati, e a volte disegnano i propri prodotti al fine di soddisfare le agenzie pubbliche di *intelligence*. Ciò desta altrettante preoccupazioni per il diritto alla privacy poiché casi come *Big Brother Watch*, emersi a seguito delle rivelazioni di Edward Snowden,[280] hanno messo in evidenza come lo Stato stesso possa costituire una minaccia alla riservatezza degli individui allorché vengano adottate pratiche di sorveglianza di massa.[281] Lo stato è dotato di un minore accesso ai dati ma di una forza coercitiva particolare, essendo titolare del "monopolio della forza". In caso di indagini penali, il rischio di abusi di questo potere in assenza di una normativa chiara è ingente.[282]

L'individuo è quindi spesso disarmato dinanzi alla disparità di risorse nel processo penale rispetto alla forza pubblica. In questo rapporto bilaterale si

279 Studio per il Parlamento Europeo, Fighting Cyber Crime and Protecting Privacy in the Cloud (Ottobre 2012).
280 Nel 2013, Edward Snowden, ex consulente della National Security Agency (NSA), rese pubblici documenti riservati che rivelavano l'esistenza di programmi di sorveglianza di massa condotti dalle autorità statunitensi e dai loro partner internazionali. Le rivelazioni hanno sollevato interrogativi di portata globale circa la proporzionalità di tali strumenti di intelligence rispetto al diritto alla privacy e alle garanzie proprie di uno Stato di diritto.
281 D. Bilchitz, *The Right to Privacy surveillance and the Global Obligations of Corporations*, in D. Cole.e F. Fabbrini, *Surveilance, Privacy, and Trans-Atlantic Relations*, Hart Publishing, Oxford, 2017.
282 G. Robinson, op. cit., p.75.

inserisce il service provider che secondo alcuni dovrebbe ergersi a paladino della protezione dei dati dell'individuo, rifiutando l'accesso da parte dello stato a dati che possono essere utilizzati come prove penali qualora le condizioni imposte dalla legge non vengano rispettate. Questo ruolo non sembra essere adatto secondo altri ai *service provider*, soggetti privati orientati al profitto, non in grado di fornire un imparziale giudizio sul rispetto dei diritti fondamentali in quanto disinteressati rispetto a questo scopo. Al contrario, sono spesso gli stessi *service provider* ad essere considerati veri e propri nemici della privacy degli individui. I *service provider* hanno interesse nel controllo di più dati possibili; quindi, nella massimizzazione della raccolta delle informazioni e nelle limitazioni degli obblighi legali di *compliance* che comportano spese e riducono i profitti.[283]

Da queste considerazioni deriva la necessità di una regolamentazione pubblica equilibrata e sovranazionale che sia in grado di rispondere alle esigenze contemporanee di protezione dei diritti fondamentali, è inoltre auspicabile il controllo da parte di un soggetto di natura imparziale e slegato rispetto a interessi di natura economica, quale il potere giurisdizionale. Sebbene sembri difficile assegnare ai *service provider* un ruolo di veri e propri protettori della privacy degli individui, sembra auspicabile l'impegno di questi ultimi al rispetto della normativa privacy anche in considerazione dei riflessi sul procedimento penale.

4.1.6 Il ruolo assegnato ai service provider nella protezione dei diritti fondamentali

Il nuovo Regolamento E-evidence introduce un modello innovativo, invece di passare sempre dalle autorità giudiziarie dello Stato di esecuzione, gli ordini OEP e OEC indirizzati direttamente al rappresentante legale del provider stabilito nell'UE. Quindi, I fornitori di servizi diventano i destinatari diretti degli ordini e devono eseguirli senza l'intervento immediato dello Stato membro di esecuzione. Questo segna una rottura rispetto alla logica classica del mutuo

283 V. Mitsilegas, *The privatisation of mutual trust in Europe's area of criminal justice:The case of e-evidence* in *Maastricht Journal of European and Comparative Law* 2018, 25/3, 263.

riconoscimento (come nel MAE o OEI), dove la cooperazione è sempre tra autorità pubbliche. Il Regolamento affida ai provider compiti tipici delle autorità giudiziarie, che devono valutare se un ordine sia manifestamente abusivo o contrario alla CDFUE, sollevare obiezioni e rifiutare l'esecuzione in tali casi, gestire conflitti di legge.[284]

Si parla di una vera e propria riallocazione delle funzioni di garanzia e "privatizzazione" del mutuo riconoscimento. Delle responsabilità che in uno Stato di diritto spettano a giudici e autorità pubbliche vengono trasferite a soggetti privati con finalità commerciali. Ciò determina rischi di responsabilizzazione eccessiva dei provider, che non hanno legittimazione democratica né l'indipendenza necessaria per bilanciare esigenze investigative e diritti fondamentali. Inoltre, diversi attori hanno sottolineato che ciò può generare conflitti di interessi e disomogeneità nella tutela dei diritti. Il Parlamento, consapevole delle criticità, ha proposto di ridurre il ruolo dei provider come "guardiani dei diritti", riaffidando a giudici o autorità indipendenti la valutazione di proporzionalità e legalità, per evitare che i privati rivestano funzioni che ordinariamente spettano ad organi giurisdizionali.[285]

Alcuni commentatori hanno accolto positivamente il ruolo attribuito dal Regolamento ai *service provider*, ritenendolo un passo significativo verso la modernizzazione e la diversificazione degli strumenti di cooperazione giudiziaria nella raccolta della prova digitale. il coinvolgimento dei fornitori rappresenterebbe un adattamento necessario alle trasformazioni del cyberspazio e al ruolo centrale che tali attori svolgono nella gestione dei dati, superando i limiti della tradizionale cooperazione fondata sul principio di territorialità e di rendere più rapida ed efficace l'acquisizione di dati elettronici.[286]

---

284 S. Tosza, *The E-Evidence Package is Adopted: End of a Saga or Beginning of a New One?* In (2023) 2 *European Data Protection Law Review,* 2023, 2 163.
285 T. Christakis, *From Mutual Trust to the Gordian Knot of Notifications* in V. Franssen e S. Tosza, *The Cambridge Handbook of digital evidence in criminal investigations,* Cambridge University Press, Cambridge,2025.
286 J. Frank e L. Cossette, *The e-Evidence Proposal – A Positive Step* in *Microsoft EU Policy Blog* https://blogs.microsoft.com/eupolicy/2018/04/18/the-eevidence-proposal-a-positive-step-

Il rischio di conflitto col diritto alla privacy non è limitato alla circostanza che il Regolamento assegni un ruolo centrale ai *service provider*, ma si estende anche ad altre preoccupazioni. L'art. 1 paragrafo 3 del Regolamento afferma espressamente che esso "si applica senza pregiudizio per i principi fondamentali, in particolare la libertà di espressione e di informazione, compresa la libertà e il pluralismo dei media, il rispetto della vita privata e familiare, la protezione dei dati personali, nonché il diritto a una tutela giurisdizionale effettiva". Resta tuttavia da verificare se tale dichiarazione programmatica troverà effettiva attuazione. Una delle principali preoccupazioni emerse in dottrina riguarda infatti la compatibilità del nuovo strumento con i criteri elaborati dalla Corte di giustizia nelle sentenze *Digital Rights Ireland* e *Tele2 Sverige.*Sebbene il regolamento non determini una conservazione generalizzata dei dati c'è il rischio che richieste relative a dati di traffico e di contenuto possano essere emesse non solo per reati gravi, ma anche per fattispecie di media gravità, abbassando così la soglia di tutela e ampliando sensibilmente il potenziale ambito applicativo dell'istituto.[287]

Un ulteriore profilo problematico riguarda la disciplina dei rimedi effettivi prevista dall'EPOR. L'art. dedicato impone agli Stati membri di garantire la possibilità di contestare la necessità e proporzionalità degli ordini, ma lascia ampi margini di discrezionalità circa le modalità concrete di attuazione. La regolamentazione è dunque minima, poiché si limita a stabilire alcuni requisiti di principio, demandando al diritto nazionale la definizione degli strumenti procedurali attraverso cui i destinatari possano esercitare i propri diritti. L'effettività dei rimedi dipenderà in larga misura dal regime di informazione degli interessati. L'art. 13 EPOR stabilisce che la persona i cui dati sono stati acquisiti debba essere informata "senza indebito ritardo" circa l'adozione di un ordine di produzione. Tuttavia, la stessa disposizione consente all'autorità

---

forward/, acesso 21/08/2025; EDRi, *'Position Paper on the European Commission's Proposal for a Regulation on European Pro-duction and Preservations Orders for Electronic Evidence in Criminal Matters'*(25 Aprile 2019).

287 M. Böse, *An Assessment of the Commission's Proposals on Electronic Evidence* in *Studi del Parlamento Europeo*, 2018.

emittente di ritardare, limitare o addirittura omettere la notifica per ragioni che riguardano, tra l'altro, la tutela delle indagini, la prevenzione e repressione dei reati o la salvaguardia di interessi nazionali.[288]

288 S.Tosza, *The E-Evidence Package is Adopted: End of a Saga or Beginning of a New One?* In *European Data Protection Law Review,* 2023, 2 163.

Capitolo 5 Le sfide alla protezione dei diritti di privacy e difesa nell'epoca digitale

5.1 Diritti fondamentali nella dialettica tra sicurezza e libertà

L'era digitale ha acuito il conflitto tra l'esigenza di garantire la sicurezza, intesa come prevenzione e repressione della criminalità, e la tutela delle libertà fondamentali riconosciute dalla Costituzione e dalle principali convenzioni sui diritti umani cui l'Italia aderisce come la CEDU e la CDFUE. In linea generale, il bilanciamento tra principi di rango costituzionale viene operato attraverso il test di proporzionalità, le stesse convenzioni internazionali forniscono criteri di valutazione per risolvere tale conflitto. Tuttavia, l'elevato valore dei diritti e degli interessi coinvolti rende la composizione di questo contrasto particolarmente complessa e sempre esposta a tensioni interpretative e applicative.[289]

I principali rischi di compressione dei diritti fondamentali a causa della prova digitale si hanno nei confronti del diritto alla privacy e al diritto di difesa dell'imputato. I dati digitali possono essere raccolti o utilizzati in modo sproporzionato rispetto alla finalità di repressione dei reati, determinando un'erosione della protezione della sfera privata dell'individuo. Gli stessi dati possono inoltre essere acquisiti o impiegati nel corso di un procedimento penale in frode alle garanzie previste dalla legge, compromettendo i diritti difensivi dell'imputato. Privacy e diritto di difesa, pur diversi nel contenuto sostanziale, risultano profondamente interconnessi nelle modalità attraverso le quali la lesione viene perpetrata e nei rimedi che possono essere approntati nel contesto digitale.[290]

289 F. Ferri., *Il bilanciamento dei diritti fondamentali nel mercato unico digitale,* Giappichellli, Torino, 2022, 169.
290 M. Simonato, op. cit., p.264.

5.2 Prova digitale e diritto alla privacy

5.2.1 Il test di proporzionalità

Dalla tutela del domicilio inteso in senso fisico e della corrispondenza intesa in senso strettamente materiale protette da parte della Costituzione, i recenti anni, sulla spinta sovranazionale sono stati caratterizzati da una estensione di questi diritti alla tutela della vita privata e dei dati personali nell'era digitale.[291] Già la CEDU conteneva una disposizione particolarmente avanzata in tema di tutela della riservatezza, l'art. 8, che stabilisce che ogni persona ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e della propria corrispondenza. L'ingerenza di un'autorità pubblica in questo diritto è vietata, eccetto nei casi in cui sia prevista dalla legge, persegua interessi pubblici importanti e legittimi e sia necessaria in una società democratica.[292]

Gli articoli 7 e 8 della CDFUE rispondono alle medesime finalità. Tuttavia, l'art. 8 non si limita a sancire il diritto alla protezione dei dati personali, ma esplicita anche i valori essenziali connessi a tale diritto. Questo stabilisce che il trattamento dei dati personali deve avvenire secondo il principio di lealtà, per finalità determinate e in base al consenso della persona interessata o su un fondamento legittimo previsto dalla legge. Le persone devono avere il diritto di accedere ai propri dati personali e di ottenerne la rettifica, e il rispetto di tale diritto deve essere soggetto al controllo di un'autorità indipendente.[293]

Tutte queste previsioni costituzionali sono attuate dalla legislazione secondaria e implementate dalle leggi nazionali, Sia il GDPR sia la Direttiva e-privacy costituiscono il cuore della normativa europea avanzata in materia di protezione dei dati e riservatezza delle comunicazioni elettroniche. In ottica comparatistica, la normativa europea è considerata universalmente come lo standard

291 M. Trogu, *Introusioni segrete nel domicilio informatico* in A. Scalfati, *Le indagini atipiche,* Giappichelli, Torino, 2019, 571.
292 W. A. Shabas, *The European Convention on Human Rights: A Commentary,* Oxford University Press, Oxford, 2015.
293 S. Peers, T.K. Hervey, J. Kenner e A. Ward, *The EU Charter of Fundamental Rights: A Commentary*, Hart Publishing, Oxford, 2021.

internazionale in materia di protezione dei dati, tant'è che altri ordinamenti si sono ispirati fortemente alle norme comunitarie.[294]

L'utilizzo nel procedimento penale dei dati informatici rappresenta una sfida sia per la privacy dell'individuo sia per quella di terzi soggetti coinvolti nel procedimento. Le informazioni raccolte da parte della pubblica autorità non riguardano solo il fatto illecito e spesso non solo l'accusato. Le informazioni, da sole o combinate tra di loro, rivelano abitudini intime, relazioni personali, opinioni politiche o credenze religiose. Per questa ragione è sempre necessario valutare la corrispondenza delle attività intrusive della privacy rispetto agli articoli 8 e 52 CDUE, i quali esplicitano un test di proporzionalità per le misure restrittive dei diritti fondamentali.[295]

Applicato alla privacy l'art. 52 CDFUE fornisce il quadro per valutare la legittimità delle limitazioni al diritto alla vita privata e alla protezione dei dati personali, sanciti dagli articoli 7 e 8 CDFUE. Ogni restrizione deve essere "prevista dalla legge", ovvero basata su norme chiare e prevedibili o sul consenso informato; deve rispettare l'essenza del diritto, che non può essere svuotata attraverso forme di sorveglianza indiscriminata; deve perseguire un obiettivo legittimo, come la tutela della sicurezza nazionale o la prevenzione dei reati; infine, deve rispettare il principio di proporzionalità, imponendo soltanto misure strettamente necessarie e non eccedenti quanto indispensabile al fine perseguito. [296]

Tra le limitazioni più significative alla tutela della riservatezza, oggi, si annoverano le intercettazioni mirate e le pratiche di sorveglianza di massa, oggetto di un'ampia elaborazione da parte della giurisprudenza della Corte EDU e della CGUE

294 M. Schwartz, *Global Data Privacy: The EU Way* in *New York University Law Review,* 2019, 94/771.
295 Agenzia dell'Unione europea per i diritti fondamentali, *Manuale sul diritto europeo in materia di protezione dei dati*, Ufficio delle pubblicazioni dell'Unione europea, Lussemburgo,2018.
296 M. Pittirruti, op. cit., p.163.

5.2.2 Intercettazioni mirate e sorveglianza di massa nella giurisprudenza EDU

Per quanto concerne le indagini informatiche è opportuno distinguere tra due possibili modalità di captazione delle telecomunicazioni, entrambe suscettibili di limitare fortemente il diritto alla privacy: l'intercettazione informatica mirata e la sorveglianza di massa. Le intercettazioni mirate si contrappongono alla sorveglianza di massa perché non colpiscono indiscriminatamente un'intera popolazione o categoria di utenti, ma si concentrano su soggetti o comunicazioni specificatamente individuati.[297]

Nella sentenza *Zakharov*, la Corte EDU ha individuato alcuni criteri minimi al ricorrere dei quali un regime di sorveglianza segreta mirata sia compatibile con l'art. 8 CEDU. Le norme devono essere chiare, accessibili e prevedibili, in modo da dare modo ai cittadini di sapere le circostanze e le modalità di intercettazione dei dati. È essenziale che siano previsti limiti qualitativi e quantitativi. L'intercettazione può avvenire per soli crimini gravi e la durata dell'intercettazione e regole sul rinnovo devono essere esplicitate, così da evitare controlli illimitati. L'attivazione della misura deve dipendere da un'autorizzazione preventiva da parte di un giudice, e le modalità di esecuzione e raccolta dei dati devono essere regolate puntualmente. Inoltre, l'individuo deve essere informato, almeno ex post e quando non vi siano più rischi per le indagini, dell'avvenuta sorveglianza, così da poter esercitare i propri diritti di ricorso in giudizio. Infine, la Corte ha ribadito l'importanza di un controllo indipendente e di rimedi effettivi, strumenti indispensabili per prevenire abusi e garantire che la sorveglianza segreta resti entro i limiti accettabili in una società democratica.[298]

In *Big Brothers Watch* questi requisiti sono stati rielaborati e adattati all'orwelliana sorveglianza di massa e ai più avanzati strumenti tecnologici.[299]

297 Corte EDU e Agenzia per i diritti fondamentali dell'Unione Europea, *Joint Factsheet: Mass Surveillance – ECtHR and CJEU Case-Law* (28 Febbraio 2025)
298 Corte EDU, Roman Zakharov c. Russia, ricorso n. 47143/06 (4 dicembre 2015) in hudoc.echr.coe.int.
299 Corte EDU Big Brother Watch c United Kingdom, ricorso n. 58170/13 (25 Maggio 2021) in hudoc.echr.coe.int.

La Corte non ha escluso a priori l'utilizzo da parte dei governi di tecniche di sorveglianza di massa, ma ne ha adattato i requisiti fondamentali già elaborati in *Zakharov,* senza elaborane degli aggiuntivi. La Corte ha ammesso che la sorveglianza di massa costituisca un'intrusione decisiva nei confronti della vita privata e ha incoraggiato il legislatore a prevedere delle restrizioni significative alla stessa, palesando l'incompatibilità della normativa interna rispetto alla CEDU. La Corte ha definito l'intervento da parte di un'autorità indipendente ex ante rispetto all'intrusione dei diritti fondamentali come *best practice* in materia, ma non essenziale e sostituibile da parte di un rimedio efficace ex post. La Corte ha inoltre sottolineato l'inapplicabilità dei requisiti della preventiva autorizzazione e della notifica al termine delle indagini, la natura stessa di intercettazione senza un preciso destinatario ne precluderebbe l'attuazione di questi principi.[300]

L'importanza di adeguati metodi di filtraggio dei dati è stata constata da parte della Corte che ha riscontrato come la normativa inglese si prestasse ad abusi, infatti, oltre ai contenuti delle comunicazioni, il regime consentiva la raccolta e l'esame illimitato dei metadati, in assenza di alcun controllo indipendente. Il problema principale evidenziato è che, pur ammesso un certo controllo sui contenuti delle comunicazioni, i metadati erano esclusi da qualsiasi forma di salvaguardia. In conclusione, con un esplicito richiamo alla CGUE, la corte EDU ha rimarcato l'importanza della finalità di combattimento a gravi forme di crimine, quale requisito essenziale per attuare tecniche particolarmente invasive de diritti fondamentali.[301]

Nel contesto della sorveglianza di massa con finalità di antiterrorismo la Corte EDU ha specificato una limitazione della discrezionalità dell'esecutivo, affinché questa non si trasformi in arbitrio "In materia di diritti fondamentali, la

300 G. Formici, *La digital mass surveillance al vaglio della Corte Europea dei Diritti dell'Uomo: da Zakharov a Big Brother Watch* in *Federalismi.it*, 2020, 23
301 F. Ertola, *Mass surveillance e diritto alla privacy*, in *Rivista italiana diritto e procedura penale,* 2019, 653.

legislazione che attribuisce discrezionalità al potere esecutivo nel settore della sicurezza nazionale deve indicare l'ambito di tale discrezionalità e le modalità del suo esercizio con sufficiente chiarezza, così da offrire all'individuo una protezione adeguata contro ingerenze arbitrarie." Tale limitazione dell'intervento intrusivo da parte dello stato può avvenire ad esempio delimitando in maniera accurata il range di soggetti nei confronti dei quali la sorveglianza è diretta. Nel contesto della sorveglianza segreta, la necessità che l'ingerenza sia "necessaria in una società democratica" deve essere interpretata nel senso che qualsiasi misura adottata debba risultare strettamente necessaria sia, in termini generali, per salvaguardare le istituzioni democratiche, sia, in termini specifici, per ottenere informazioni essenziali in una singola operazione.[302]

5.2.3 I recenti sviluppi in tema di data retention nell'UE

Nell'ambito del diritto comunitario, l'annullamento della direttiva sulla *data retention* in *Digital Rights Ireland* non ha posto fine alle preoccupazioni circa l'utilizzo delle prove digitali nel procedimento penale, in quella pronuncia la CGUE aveva dichiarato contraria al diritto dell'Unione la conservazione indiscriminata dei dati. Successivamente, in *Tele2 Sverige*, la Corte ha ribadito tali principi, annullando le legislazioni di Regno Unito e Svezia che non prevedevano condizioni sufficientemente precise e rigorose per la conservazione dei dati.[303]

Nonostante il divieto generale di raccolta massiva e indiscriminata, la giurisprudenza successiva ha introdotto una scala di legittimità graduata: la conservazione generalizzata può essere ammessa solo in casi eccezionali di grave minaccia alla sicurezza nazionale; per la lotta alla criminalità grave, la *retention* deve essere invece mirata, cioè circoscritta a condizioni specifiche e

302 Corte EDU, *Szabó e Vissy c. Ungheria*, ricorso n. 37138/14, (12 gennaio 2016) in hudoc.echr.coe.int.
303 G. Caggiano, *Il bilanciamento tra diritti fondamentali e finalità di sicurezza in materia di conservazione dei dati personali da parte dei fornitori di servizi di comunicazione* in *Rivista di diritto dei media*, 2018, 2.

obiettive; per i reati minori, la conservazione è esclusa, salvo eccezioni limitate (es. indirizzi IP).[304]

Un approccio diverso è stato adottato in *Schrems*, dove la CGUE, senza applicare il test di proporzionalità, ha sancito l'invalidità dei trasferimenti di dati verso ordinamenti, come quello statunitense, che consentono una conservazione indiscriminata senza limitazione allo stretto necessario. In tal caso, la Corte ha affermato in modo assoluto l'inviolabilità del diritto alla riservatezza.[305]

Infine, nelle sentenze più recenti (*Privacy International*, *La Quadrature du Net* e *Prokuratuur*), la Corte ha confermato che la *retention* deve essere sempre mirata e proporzionata. Il giudizio di proporzionalità della misura investigativa consiste in un bilanciamento tra il grado intrusività della misura investigativa e la gravità del crimine perseguito. Tale controllo di proporzionalità deve essere performato da un soggetto terzo ed imparziale; quindi, in grado di bilanciare i diversi interessi in gioco.[306] In *Privacy International* a Corte ha chiarito che l'eccezione alla riservatezza delle comunicazioni non può trasformarsi nella regola. La raccolta massiva e indiscriminata può essere illegittima, sproporzionata ed incompatibile con la CDFUE anche nel caso in cui si persegua una finalità di Sicurezza pubblica e lotta alla criminalità anche grave.

La Corte ha sottolineato che la *retention* e l'accesso ai dati devono essere accompagnati da garanzie adeguate: autorizzazione preventiva di un giudice o di un'autorità indipendente, limiti temporali, criteri di selezione trasparenti, sistemi informatici sicuri e divieto di profilazione. Inoltre, ha chiarito che l'analisi automatizzata dei dati costituisce di per sé un'ingerenza rilevante nella vita privata e richiede un riesame umano in caso di risultati positivi. l'analisi

304 Corte di Giustizia, Cause riunite C-511/18, C-512/18 e C-520/18 *La Quadrature du Net e altri c. Premier Ministre e altri*, ECLI:EU:C:2020:791. in curia.europa.eu.
305 Corte di Giustizia, causa C-311/18, *Schrems II*, EU:C:2020:559 in curia.europa.eu
306 Corte di giustizia, causa C-623/17, *Privacy International*, EU:C:2020:790 in curia.europa.eu; Corte di Giustizia, Cause riunite C-511/18, C-512/18 e C-520/18 *La Quadrature du Net e altri c. Premier Ministre e altri*., ECLI:EU:C:2020:791 in curia.europa.eu; Corte di Giustizia, Causa C-746/18 *H.K. c. Prokuratuur,* ECLI:EU:C:2021:152 in curia.europa.eu.

deve avvenire per un periodo strettamente limitato e deve essere autorizzata da un organo indipendente con decisioni vincolanti, soggette a revisione efficace. Poiché esiste un margine di errore, i risultati positivi di un'analisi automatizzata devono essere riesaminati manualmente prima di adottare misure che incidano sulla persona.[307]

Tuttavia, in *La Quadrature du Net II* si registra un parziale arretramento: la conservazione generalizzata degli indirizzi IP, utilizzati per l'identificazione degli utenti, non è più considerata una "grave interferenza" con la vita privata e può essere giustificata anche dalla necessità di perseguire reati minori, purché accompagnata da misure tecniche e organizzative adeguate. In questo senso, il controllo di un'autorità indipendente è stato ridimensionato da requisito essenziale a mera garanzia tecnica, segnalando un orientamento più favorevole all'enforcement online a scapito della tutela dell'anonimato in rete.[308]

5.3 Prova digitale e diritto alla difesa

5.3.1 Il diritto di difesa e le indagini informatiche

L'art. 6 CEDU riassume, in modo non esaustivo, i principi, i diritti procedurali individuali e le garanzie aggiuntive che fissano uno standard di equità processuale e di procedura penale conforme allo Stato di diritto. L'art. 6, paragrafo 1, enuncia il principio generale di equità, mentre l'art. 6, paragrafo 2 la presunzione di innocenza, e l'art. 6, paragrafo 3 elenco dei diritti minimi dell'imputato, costituiscono "applicazioni specifiche" di tale principio. Il principio generale di equità consente alla Corte EDU di esaminare se il procedimento, considerato nel suo complesso, sia equo: ciò oltrepassa le differenze giurisdizionali e mira a sviluppare principi comuni sottesi al processo penale. Il carattere non esaustivo degli aspetti specifici del diritto a un equo

307 V. Mitsilegas, *Data retention and the future of large-scale surveillance: The evolution and contestation of judicial benchmarks*, *European Law Journal*, 2023, 29, 176.
308 M. Rojszczak, *Data Retention Laws and La Quadrature du Net II* in *Verfasublblog* https://verfassungsblog.de/data-retention-laws-and-la-quadrature-du-net-ii/, accesso 03/08/2025

processo permette alla Corte di ampliare e sviluppare nuove garanzie procedurali in contesti differenti e di conformarli rispetto all'avanzamento tecnologico.[309]

Il diritto a una tutela giurisdizionale efficace è suddiviso in molti sotto-principi. Le indagini digitali mettono in discussione principalmente, ma non esclusivamente, il principio della parità delle armi. Secondo il principio della parità delle armi, sia l'accusa che la difesa devono avere la possibilità di conoscere e commentare il campo di osservazioni e le prove addotte dalla controparte.[310] La giurisprudenza della Corte EDU richiede che le due parti siano uguali nel processo di formazione della prova. Purtroppo, la necessità di un'azione penale efficace può compromettere il pieno raggiungimento della parità delle armi. L'avvento del digitale all'interno del processo penale ha prodotto una modifica sostanziale dei rapporti tra difesa ed accusa, minando principalmente il principio del contraddittorio e l'equità delle armi. Tale squilibrio è stato accentuato e ha diminuito le garanzie difensive dell'imputato con riguardo ad alcuni aspetti fondamentali della parità delle armi quali, producendo asimmetrie non risolvibili attraverso le regole processuali nate in un contesto analogico.

5.3.2 La sfida al diritto di difesa

Se la sfida al diritto alla privacy è di immediata comprensione, poiché l'acquisizione di dati digitali comporta inevitabilmente l'ingerenza in sfere intime della vita personale e professionale dell'individuo, quella al diritto di difesa si presenta come più complessa e subdola, ma non per questo meno rilevante sul piano della tutela dei diritti fondamentali. Il diritto dell'imputato ad avere tempi e mezzi adeguati a preparare la difesa si complica quando l'accusa acquisisce masse enormi di dati, spesso irrilevanti o difficilmente gestibili. In primo luogo, in caso di prova elettronica è sempre decisiva la raccolta nella fase delle investigazioni, Il rischio è che il processo decisionale si fondi su dati digitali di difficile comprensione e scarsa attendibilità, ma comunque trattati

309 A.W. Shabas, op. cit., p.359.
310 M. Simonato, op cit., p.40.

come fonti autorevoli, con conseguenze quali accuse indeterminate, inversione dell'onere della prova e compromissione del giusto processo. Ne discende l'esigenza che l'attività investigativa si avvalga di procedure in grado di garantire l'accuratezza fattuale e la conformità alle regole processuali. In assenza di un formale procedimento di validazione, infatti, gli esiti delle analisi forensi non possono essere adeguatamente rappresentati né sottoposti a contraddittorio in sede dibattimentale. Considerato l'uso sempre più ampio e polivalente della prova digitale da parte delle autorità, un sistema di garanzia della qualità deve essere assicurato sin dalla fase delle indagini.[311]

In *Rowe and Davis contro Regno Unito*, la Corte EDU ha ribadito che la mancata comunicazione di elementi probatori essenziali alla difesa, soprattutto quando rilevanti per la valutazione dell'attendibilità di una prova ai fini dell'accertamento della responsabilità penale, costituisce una violazione del principio del contraddittorio e quindi dell'equità del processo.[312]

Nel contesto delle indagini digitali, questa asimmetria è particolarmente problematica, in quanto le prove digitali presentano una natura tecnica complessa e richiedono analisi approfondite, spesso all'interno di database vastissimi e non strutturati. La criticità si manifesta in modo evidente nei casi in cui la difesa non dispone delle competenze tecniche o delle risorse economiche e strumentali necessarie per effettuare una verifica autonoma dei dati digitali, o per contestare l'integrità, la provenienza o la rilevanza probatoria degli stessi.[313]

In caso di limiti temporali inadeguati rispetto alla mole dei dati l'accusa ha anche dalla sua il fattore tempo. In alcuni ordinamenti, tra cui quello italiano, la *disclosure* delle prove non avviene in modo tempestivo, ma solo in una fase avanzata del procedimento. Questo consente alla pubblica accusa di disporre del tempo necessario per elaborare una strategia processuale efficace, mentre la

311 R. Stoykova, *The right to a fair trial as a conceptual framework for digital evidence rules in criminal investigations* in *Computer Law and Security Rev*iew 2023, 49.
312 Corte EDU, *Rowe e Davis c. Regno Unito*, ricorso n. 28901/95 (16 febbraio 2000) in hudoc.echr.coe.int.
313 M. Simonato, op. cit., p.43.

difesa si trova spesso ad affrontare un considerevole svantaggio temporale e informativo. [314]

In generale, la preparazione della difesa e il processo di *discovery* risultano gravati dal fatto che la parte difensiva difficilmente può verificare, nell'immediato, la quantità e l'estensione dei dati originari, nonché i risultati che ne derivano, con un conseguente incremento di tempi e risorse nella gestione della prova digitale. Risulta dunque di importanza cruciale l'accesso alla catena di custodia, la conoscenza delle operazioni di trattamento in ciascuna fase e la disponibilità di informazioni sulla responsabilità delle attività svolte, al fine di valutare la legalità e la proporzionalità della misura investigativa, l'ampiezza dell'autorizzazione concessa e l'attendibilità della prova.[315]

Le scelte che restano in tali casi sono due ed equamente difficili da percorrere, la prima strada è quella della trasparenza massima, cioè la consegna di tutti i dati alla difesa, anche irrilevanti, in nome dell'eguaglianza delle armi. L'altra opzione è quella della selezione guidata attraverso limitazioni all'accesso, purché effettuate con criteri trasparenti e condivisi, evitando arbitrii. La corte EDU, nel caso *Sigurður Einarsson,* ha stabilito l'obbligo di includere la difesa nella selezione dei criteri di selezione dei dati pertinenti.[316]

Vieppiù, La difesa spesso non dispone di una vera e propria opportunità di contestare l'autenticità e l'affidabilità della prova digitale prodotta dall'accusa. Tale garanzia, infatti, non può realizzarsi se le operazioni di trattamento dei dati non vengono adeguatamente documentate al fine di ricostruirne l'origine, le modalità di acquisizione, di esame e di analisi.[317] Un ulteriore ordine di problematiche riguarda, poi, l'impiego da parte degli organi investigativi di

314 Galič M., op. cit., p.46.
315 R. Stoykova, *A New Right to Procedural Accuracy: A Governance Model for Digital Evidence in Criminal Proceedings* in *Computer Law & Security Review* 2024, 55.
316 L.Bartoli, *Parità delle armi e discovery digitale: qualche indicazione da Strasburgo* in *Legislazione Penale,* 2021, 1, 13.
317 G. Di Paola, voce *Prova informatica (diritto processuale penale)* in *Enciclopedia del diritto: Annali VI,* Giuffrè, Milano, 2013.

metodi e strumenti innovativi di *digital forensics*, le cui caratteristiche tecniche possono essere mantenute riservate.

In ultima analisi, ulteriori criticità sorgono a partire dal cieco affidamento, che spesso tutte le parti del processo penale ripongono nella ricerca scientifica e nella tecnologia come strumenti di amministrazione della giustizia. Gli strumenti di *digital forensics* vengono infatti impiegati con facilità, dando per presupposta la validità scientifica di metodologie sperimentali e tecnicamente complesse, la cui contestazione richiede un elevato livello di competenze specialistiche. Ciò rende difficile la contestazione della prova digitale quando assunta attraverso l'ausilio di esperti e periti, la cui autorevolezza tecnica tende a limitare la possibilità di un effettivo scrutinio critico da parte del giudice e della difesa. Inoltre, la nomina di un consulente tecnico di parte implica oneri economici significativi, che possono limitare concretamente la possibilità della difesa di avvalersi di un supporto specialistico.[318]

l'impiego di diverse tecnologie volte alla sorveglianza e alla raccolta di informazioni su soggetti sospettati, possono minare il principio di presunzione di innocenza e determinano, di fatto, un'inversione dell'onere della prova. Ciò avviene in ragione del rischio di una costruzione parallela dei fatti, della raccolta massiva di informazioni personali che compromette il diritto al silenzio, dell'elusione dei meccanismi di garanzia propri del processo penale e della "preconfezione" del materiale probatorio ben prima della formulazione di un'imputazione. Alcune forme di profilazione possono tradursi in una presunzione di colpevolezza di fatto. Inoltre, la mancata conoscenza da parte del sospettato delle informazioni ritenute rilevanti rischia di pregiudicare l'effettiva possibilità di difesa e di privare di tutela soggetti con comportamenti atipici o non convenzionali, ma non per questo criminali.[319]

318 J. Vuille, L. Lupària and F. Taroni, *Scientific Evidence and the Right to a Fair Trial under Article 6 ECHR* in *Law, Probability and Risk* 2017, 16, 55.
319 J. Milaj. and J. P. Bonnici, *Unwitting Subjects of Surveillance and the Presumption of Innocence* in *Computer Law & Security Review*, 2014, 30, 419.

5.3.3 L'effettiva tutela giurisdizionale come rimedio

Viste le ingenti sfide poste dalla prova digitale, dottrina e giurisprudenza si sono interrogate circa la possibilità di prevedere rimedi efficaci rispetto alle sfide giuridiche che sono state poste. Una salvaguardia costante che si trova nella giurisprudenza interna e sovranazionale con riguardo alla prova digitale è il diritto ad un'efficacia tutela giudiziaria. Il ricorso ad un'autorità giurisdizionale od amministrativa indipendente viene visto come principale protezione contro gli abusi che possono scaturire dall'utilizzo della prova digitale. Il diritto ad una efficace tutela giurisdizionale è infatti strumentale rispetto alla tutela di altri diritti, in questo caso il diritto alla privacy e il diritto di difesa dell'imputato.[320]

La Corte EDU ha riconosciuto che possono verificarsi situazioni di estrema urgenza in cui l'obbligo di un controllo giudiziario preventivo rischierebbe di far perdere tempo prezioso. Ha sottolineato, tuttavia, che in tali casi qualsiasi misura di sorveglianza autorizzata ex ante da un'autorità non giudiziaria deve essere necessariamente sottoposta a un controllo giudiziario ex post. La Corte ha riconosciuto che possono verificarsi situazioni di estrema urgenza, nelle quali l'obbligo di un controllo giudiziario preventivo rischierebbe di compromettere l'efficacia delle indagini. Tuttavia, l'interpretazione della nozione di urgenza deve essere restrittiva, al fine di evitare che l'eccezione si trasformi in prassi ordinaria e che misure intrusive sfuggano a un controllo giurisdizionale adeguato.[321]

Mentre il controllo *ex ante* è preferibile e svolge un ruolo cruciale nel garantire i diritti fondamentali, i rimedi *ex post* possono ritenersi necessari ma non sufficienti. A causa della struttura del sistema probatorio, a volte il *controllo ex post* è insufficiente, e non può compensare l'assenza di un controllo giudiziario preventivo, in quanto può avvenire solo dopo che la violazione dei diritti

320 M. Bonelli, M. Eliantonio e G. Gentile, *Article 47 of the EU Charter and Effective Judicial Protection, Volume 1*, Bloomsbury Publishing, Londra, 2023, 203.
321 M. Palmisano, *The Surveillance Cold War: Recent Decisions of the European Court of Human Rights and their Application to Mass Surveillance in the United States and Russia*, in *Gonzaga Journal of International Law*, 2017, 2/22, 14.

fondamentali ha già avuto luogo. La Corte ha chiarito che, in alcuni casi, quali ad esempio le intercettazioni massicce o l'accesso a dati di traffico e contenuto, sia essenziale una preventiva autorizzazione giudiziaria.[322]

La CGUE in *Prokuratuur* ha definito anche le caratteristiche del soggetto deputato al controllo giurisdizionale. L'autorità che effettua il controllo deve essere un soggetto terzo rispetto a chi conduce le indagini, libero da condizionamenti esterni, non inserito nella gerarchia dei servizi investigativi o di sicurezza. L'organo deve essere neutrale nei confronti delle parti del procedimento e non avere interessi propri nell'esito del caso. Il vaglio non può essere meramente formale, ma deve comprendere un esame sostanziale della sussistenza di una minaccia grave, attuale o prevedibile alla sicurezza nazionale, verificando la proporzionalità e necessità dell'interferenza con i diritti fondamentali. L'organo deve poter chiedere prove ai servizi di sicurezza e avere la capacità di imporre decisioni vincolanti, inclusa la possibilità di negare o interrompere la misura.[323]

322 Corte di Giustizia, Causa C-746/18 *H.K. c. Prokuratuur*, ECLI:EU:C:2021:152 in curia.europa.eu.
323 Corte di Giustizia, Causa C-746/18 H.K. c. *Prokuratuur*, ECLI:EU:C:2021:152 in curia.europa.eu.

Conclusioni

Da questa analisi è emerso come la prova digitale rivesta un valore imprescindibile nel diritto processuale penale: le sue caratteristiche di intangibilità, alterabilità e ubiquità impongono una ridefinizione del quadro normativo, in ragione delle sfide che essa pone al principio di territorialità e alla tutela dei diritti fondamentali.

Le principali organizzazioni internazionali di cui l'Italia è parte, ossia l'Unione europea e il Consiglio d'Europa, hanno contribuito in maniera determinante a delineare l'attuale assetto normativo, sia attraverso l'adozione di strumenti giuridici vincolanti, sia mediante la giurisprudenza delle rispettive Corti. In tale prospettiva, la Convenzione di Budapest, la Direttiva sull'Ordine Europeo di Indagine e il Regolamento E-evidence costituiscono tappe fondamentali verso una maggiore efficienza investigativa e una progressiva armonizzazione della disciplina in materia di prove digitali.

Il diritto interno, dal suo canto, regola la raccolta e l'ammissibilità della prova secondo principi generali elaborati per le prove tradizionali, i quali, pur applicabili anche al dato digitale, risultano talvolta inadeguati a fronte delle specificità tecniche e delle problematiche di natura transnazionale che quest'ultimo comporta.

In questo scenario è opportuno constatare il sempre crescente ruolo dei *service provider*, ciò conferma la tendenza alla "privatizzazione" della ricerca della prova digitale, affidata a soggetti economici che incidono profondamente sui diritti fondamentali dell'individuo. Tale evoluzione richiede una riflessione critica sul rischio di delegare a entità private responsabilità che attengono al nucleo della giurisdizione statale e sul come garantire una collaborazione proficua tra il pubblico e il privato.

La sfida principale sarà dunque quella di impedire che l'esigenza investigativa si traduca in una compressione irreversibile delle libertà fondamentali. Occorre un quadro normativo che, pur garantendo l'efficacia delle indagini digitali,

riconosca un valore primario al diritto alla riservatezza e al contraddittorio nell'era informatica. La prova digitale è ormai diventata il banco di prova per la tenuta dello Stato di diritto. La giustizia penale digitale deve seguire un cammino orientato all'effettiva tutela dei diritti fondamentali, affinché l'innovazione tecnologica si traduca in uno strumento di garanzia e non in una minaccia per l'ordine democratico.

Per il futuro, si potrebbe prospettare un riadattamento del tradizionale principio del giusto processo alla prova digitale. In tale prospettiva, il modello partecipativo del processo penale dovrebbe essere garantito sin dalla fase preprocessuale, attraverso un controllo giudiziario anticipato e l'attribuzione di diritti difensivi attivi, in particolare il diritto di accesso al materiale probatorio, calibrati sulle peculiarità dei processi digitali.

Bibliografia

Legislazione

Consiglio d'Europa

- CEDU
- Convenzione sulla criminalità informatica, aperta alla firma il 23 novembre 2001, ETS n. 185.
- Convenzione europea di assistenza giudiziaria in materia penale, firmata a Strasburgo il 20 aprile 1959, ETS n. 030.
- Secondo Protocollo addizionale alla Convenzione sulla criminalità informatica sulla cooperazione rafforzata e la divulgazione delle prove elettroniche, aperto alla firma il 12 maggio 2022, CETS n. 224.

UE

- TUE
- TFUE
- Carta dei diritti fondamentali dell'Unione europea
- Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali e alla libera circolazione di tali dati
- Regolamento (UE) 2017/1939 del Consiglio, del 12 ottobre 2017, che attua una cooperazione rafforzata sull'istituzione della Procura europea («EPPO») [2017] GU L283/1
- Regolamento (UE) 2023/1543 del Parlamento europeo e del Consiglio, del 12 luglio 2023, relativo agli ordini europei di produzione e di conservazione delle prove elettroniche in procedimenti penali e all'esecuzione delle pene detentive pronunciate al termine di procedimenti penali [2023] GU L191/118
- Regolamento (UE) 2022/2065 del Parlamento europeo e del Consiglio del 19 ottobre 2022 relativo a un mercato unico dei servizi digitali e che modifica la direttiva 2000/31/CE (Digital Services Act)

- Direttiva 2002/58/CE del Parlamento europeo e del Consiglio, del 12 luglio 2002, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (direttiva relativa alla vita privata e alle comunicazioni elettroniche) [2002] GU L201/37
- Direttiva 2014/41/UE del Parlamento europeo e del Consiglio, del 3 aprile 2014, relativa all'ordine europeo di indagine penale [2014] GU L130/1
- Direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati [2016] GU L119/89

Italia

- Codice di procedura penale (DPR 22 settembre 1988, n. 447), GU Serie Generale n.250 del 24 ottobre 1988
- Decreto del Presidente della Repubblica 22 settembre 1988, n. 447, Codice di procedura penale; Decreto legislativo 30 giugno 2003, n. 196, Codice in materia di protezione dei dati personali.
- Legge 18 marzo 2008, n. 48, Ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica, firmata a Budapest il 23 novembre 2001, e norme di adeguamento dell'ordinamento interno, GU Serie Generale n. 80 del 4 aprile 2008.

Giurisprudenza

CGUE

- Corte di Giustizia, Causa 33/*76*, *Rewe-Zentralfinanz e Rewe-Zentral AG c. Landwirtschaftskammer für das Saarland*, ECLI:EU:C:1976:188 in curia.europa.eu.
- Corte di giustizia, *Commissione delle Comunità europee c. Repubblica ellenica*, C-68/88, EU:C:1989:339 in curia.europa.eu.

- Corte di Giustizia, Causa C-419/14 *WebMindLicenses Kft c. Nemzeti Adó- és Vámhivatal Kiemelt Adó- és Vámigazgatósága*, ECLI:EU:C:2015:832 in curia.europa.eu.
- Corte di Giustizia, Cause riunite C-511/18, C-512/18 e C-520/18 La *Quadrature du Net e altri c. Premier Ministre e altri I*, ECLI:EU:C:2020:791 in curia.europa.eu.
- Corte di Giustizia, Causa C-746/18 *H.K. c. Prokuratuur*, ECLI:EU:C:2021:152 in curia.europa.eu.
- Corte di Giustizia, Causa C-619/18 *Commissione c. Polonia*, ECLI:EU:C:2021:153 in curia.europa.eu.
- Corte di Giustizia, Causa C-584/19, *A. e a. HP,* ECLI:EU:C:2020:1027 in curia.europa.eu.
- Corte di Giustizia, Causa C-852/19 *Gavanozov* II, ECLI:EU:C:2021:422 in curia.europa.eu.
- Corte di Giustizia, Causa C-310/16 *Dzivev* e altri ECLI:EU:C:2019:21 in curia.europa.eu.
- Corte di Giustizia, Causa C-140/20 *Garda Commissioner c. Garda Síochána Ombudsman Commission*, ECLI:EU:C:2022:258 in curia.europa.eu.
- Corte di Giustizia, Causa C-670/22 *Encrochat*, ECLI:EU:C:2024:372 in curia.europa.eu.
- Corte di Giustizia, Cause riunite C-293/12 e C-594/12, *Digital Rights Ireland Ltd contro Minister for Communications, Marine and Natural Resources e altri*, EU:C:2014:238 in curia.europa.eu.
- Corte di Giustizia, Causa C-623/17, *Privacy International*, EU:C:2020:790 in curia.europa.eu.
- Corte di Giustizia, Causa C-497/20 *Procura della Repubblica presso il Tribunale di Bolzano*, ECLI:EU:C:2024:371 in curia.europa.eu.
- Corte di Giustizia, Causa C-548/21 C.G. c. *Bezirkshauptmannschaft Landeck*, ECLI:EU:C:2024:830 in curia.europa.eu.

- Corte di Giustizia, Causa C-511/18, C-512/18 e C-520/18 *La Quadrature du Net and Others v Premier ministre and Others* II, ECLI:EU:C:2020:791 in curia.europa.eu.
- Corte di Giustizia, *Parere 2/13 Adesione dell'UE alla CEDU*, ECLI:EU:C:2014:2454, [2014] ECR I-0000 in curia.europa.eu.

CEDU

- Corte EDU, *Schenk c. Svizzera*, ricorso n. 10862/84 (12 luglio 1988) in hudoc.echr.coe.int.
- Corte EDU, *Mantovanelli c. Francia*, ricorso n. 21497/93 (18 marzo 1997) in hudoc.echr.coe.int.
- Corte EDU, *Khan c. Regno Unito*, ricorso n. 35394/97 (12 maggio 2000)
- Corte EDU, *Rowe e Davis c. Regno Unito*, ricorso n. 28901/95 16 febbraio 2000) in hudoc.echr.coe.int.
- Corte EDU, *Hulki Güneş c. Turchia*, ricorso n. 28490/95 (19 giugno 2003) in hudoc.echr.coe.int.
- Corte EDU, *Jalloh c. Germania*, ricorso n. 54810/00 (11 luglio 2006) in hudoc.echr.coe.int.
- Corte EDU*, Bykov c. Russia*, ricorso n. 4378/02 (10 marzo 2009) in hudoc.echr.coe.int.
- Corte EDU, *Budak c. Turchia*, ricorso n. 69762/12 (24 settembre 2012) in hudoc.echr.coe.int.
- Corte EDU, *Roman Zakharov c. Russia*, ricorso n. 47143/06 (4 dicembre 2015) in hudoc.echr.coe.int.
- Corte EDU, *Szabó e Vissy c. Ungheria*, ricorso n. 37138/14, (12 gennaio 2016) in hudoc.echr.coe.int.
- Corte EDU, *Sigurður Einarsson e altri c. Islanda*, ricorso n. 39757/15 (4 giugno 2019) in hudoc.echr.coe.int.
- Corte EDU, *Rook c. Germania*, ricorso n. 1586/15 (25 luglio 2019) in hudoc.echr.coe.int.
- Corte EDU, *Brazzi c. Italia*, ricorso n. 57278/11, (27 settembre 2018) in hudoc.echr.coe.int.

- Corte EDU, Murtazaliyeva c. Russia, ric. n. 36658/05, Grande Camera (18 dicembre 2018) in hudoc.echr.coe.int.
- Corte EDU, *Centrum för rättvisa c. Svezia*, ricorso n. 35252/08 (25 maggio 2021) in hudoc.echr.coe.int.

Corte costituzionale

- Corte cost., 27 settembre 2023, n. 170/2023 in onelegale.wolterskluwer.it

Corte di cassazione

- Cass., Pen., sez. III, 14 dicembre 2007, n. 6465 in onelegale.wolterskluwer.it
- Cass., Pen., Sez. V, 14 ottobre 2009, n. 16556 in onelegale.wolterskluwer.it
- Cass. Pen., Sez. II, 16 giugno 2015, n. 24998 in onelegale.wolterskluwer.it.
- Cass., Pen., Sez. Un., 28 aprile 2016, n. 26889 in onelegale.wolterskluwer.it.
- Cass. Pen., Sez. VI, 28 febbraio 2017, n. 15573 in onelegale.wolterskluwer.it.
- Cass., Pen., Sez. V, 30 maggio 2017, n. 48370 in onelegale.wolterskluwer.it.
- Cass., Pen., Sez. VI, 25 ottobre 2017, n. 49016 in onelegale.wolterskluwer.it.
- Cass., Pen., Sez. V, 16 gennaio 2018, n. 1822 in onelegale.wolterskluwer.it.
- Cass., Pen., Sez. VI, 27 aprile 2020, n. 12975 in onelegale.wolterskluwer.it.
- Cass., Pen., Sez. II, 14 gennaio 2021, n. 1822 in onelegale.wolterskluwer.it.
- Cass., Pen., Sez. VI, 14 giugno 2022, n. 35652 in onelegale.wolterskluwer.it

- Cass., pen., sez. VI, 29 Febbraio 2024, n.23755 e 23756 in onelegale.wolterskluwer.it.
- Cass. pen., sez.VI, 8 aprile 2025, n. 413 in onelegale.wolterskluwer.it

Giurisprudenza di merito

- Trib. Bologna, 22 dicembre 2005, n. 1823. in onelegale.wolterskluwer.it.

Dottrina

- Abraha H., *Law enforcement access to electronic evidence across borders: mapping policy approaches and emerging reform initiatives* in *International Journal of Law and Information Technology* 2021, 29/118.
- Agenzia dell'Unione europea per i diritti fondamentali, *Manuale sul diritto europeo in materia di protezione dei dati*, Ufficio delle pubblicazioni dell'Unione europea, Lussemburgo,2018.
- Agnino S., Sky ecc, *ordine europeo di indagine tra giurisprudenza nostrana e comunitaria* in *Giustizia Insieme* https://www.sistemapenale.it/it/scheda/daniele-ordine-europeo-di-indagine-penale-e-comunicazioni-criptate-il-caso-sky-ecc-encrochat-in-attesa-delle-sezioni-unite, accesso 06/05/2025.
- Aterno S., *La Convenzione di Budapest del 2001 e la L. n. 148/2008* in Cadoppi A., *Cybercrime*, Utet Giuridica, Torino, 2023, 1578.
- Aterno, *Data retention: gli effetti della sentenza del 2 marzo 2021 della Corte di Giustizia Europea* in E-Lex https://www.e-lex.it, accesso 7 luglio 2025.
- Balducci P., voce *Perquisizione* in *Enciclopedia del diritto* vol XXXIII, Giappichelli, Torino, 2000.
- Bargis M., voce *Perquisizione* in *Digesto delle discipline penalistiche vol IX*, Utet Giuridica, Torino, 1995.
- Bartoli L., *The Handling of Digital Evidence in Italy'* in Caianiello M. e Camon A., *Digital Forensic Evidence. Towards Common European*

Standards in Anttifraud Administrative and Criminal Investigations Wolters Kluwer, Torino, 2023

- Bartoli L., *Parità delle armi e discovery digitale: qualche indicazione da Strasburgo* in *Legislazione Penale*, 2021, 1.
- Bachmaier L., *Mutual Admissibility of Evidence and Electronic Evidence in the EU: A New Try for European Minimum Rules in Criminal Proceedings?* in *eucrim* 2022,3, 117.
- Belfiore R, *The European Investigation Order in Criminal Matters: Developments in Evidence-Gathering across the EU'* in *European Criminal Law Review*, 2015, 5 317.
- Bilchitz D., *The Right to Privacy surveillance and the Global Obligations of Corporations*, in Cole D e Fabbrini F., *Surveilance, Privacy, and Trans-Atlantic Relations*, Hart Publishing, Oxford, 2017.
- Bonelli M, Eliantonio M. e Gentile G. *Article 47 of the EU Charter and Effective Judicial Protection, Volume 1*, Bloomsbury Publishing, Londra, 2023.
- Böse M., *An Assessment of the Commission's Proposals on Electronic Evidence* in *Studi del Parlamento Europeo*, 2018.
- Braghò G., *L'ispezione e la perquisizione di dati, informazioni e programmi informatici* in Luparia G., *Criminalità informatica*, Giappichelli, Torino, 2022.
- Buccarella M., *Il secondo Protocollo addizionale alla Convenzione di Budapest sulla criminalità informatica: cooperazione rafforzata e disclosure delle prove elettroniche* in Quaderni AISDUE, 2023, 8.
- Busillo E, *Conservazione e produzione della prova digitale nella nuova disciplina europea: il potenziale disallineamento con i principi espressi dalla giurisprudenza di settore* in *Freedom, Security & Justice: European Legal Studies*, 2023, 3, 27.
- Cadoppi A., *Cybercrime*, Utet Giuridica, Torino, 2023.

- Caianiello M. e Camon A., *Digital Forensic Evidence Towards Common European Standards in Antifraud Administrative and Criminal Investigations,* Wolters Kluwer, Torino, 2021.
- Caianiello M, *Ancora in tema di sequestro di dispositivi, sistemi informatici o telematici o memorie digitali (disegno di legge C. 806)* in *Sistema Penale,* https://www.sistemapenale.it/it/documenti/caianiello-ancora-in-tema-di-sequestro-di-dispositivi-sistemi-informatici-o-telematici-o-memorie-digitali-disegno-di-legge-c-806, accesso 4 Luglio 2025.
- Calavita O., *La proposta di regolamento sugli ordini di produzione e conservazione europei: Commissione, Consiglio e Parlamento a confronto* in *Legislazione Penale* https://www.lalegislazionepenale.eu/la-proposta-di-regolamento-sugli-ordini-di-produzionee-conservazione-europei-commissione-consiglio-e-parlamento-a-confronto-oscar-calavita/, accesso 17 Marzo 2025.
- Calavita O., *L'Ordine europeo di indagine penale. Presente e futuro della cooperazione probatoria nell'Unione europea*, Wolters Kluwer, Torino 2023.
- Calderini B., *Cloud Act: la norma USA che fa a pugni con la privacy europea, i nodi, 23 marzo 2023*, in Agenda digitale https://www.agendadigitale.eu/sicurezza/privacy/cloud-act-la-norma-usa-che-fa-a-pugni-con-la-privacy-europea-i-nodi/ accesso i9 luglio 2025.
- Canestrini N., *La cooperazione giudiziaria penaleeuropea esige il rispetto della tuteladei diritti fondamentali, fondamentodella fiducia reciproca fra gli stati membri*, 2023 6/63 Casssazione penale, 2023, 6/63 2113.
- Caggiano G., *Il bilanciamento tra diritti fondamentali e finalità di sicurezza in materia di conservazione dei dati personali da parte dei fornitori di servizi di comunicazione* in *Rivista di diritto dei media*, 2018, 2.

- Capone A., *Intercettazioni e Costituzione. Problemi vecchi e nuovi* in *Cassazione penale*, 2017, 3, 1263.
- Caputo A., *La conservazione dei dati di traffico telefonico e telematico nella normativa antiterrorismo* in *Archivio penale*, 2016, 1, 28.
- Cardamone D, *La sentenza della CEDU, Brazzi c. Italia: sono arbitrarie le perquisizioni disposte dall'autorità giudiziaria* in *Questioni di Giustizia* https://www.questionegiustizia.it/art./la-sentenza-della-cedu-brazzi-c-italia-sono-arbitrarie-le-perquisizioni-disposte-dall-autorita-giudiziaria-_15-01-2019.php, accesso 23 giugno 2025.
- Cardone A., *Il sistema del Data Retention come strumento investigativo* in *Giurisprudenza Penale*, 2021, 1.
- Casati A.P., *Le intercettazioni*, Giuffre, Milano, 2023.
- Chiavario M., *Cooperazione giudiziaria internazionale in materia penale*, Giappichelli, Torino, 2022.
- Christakis T., *From Mutual Trust to the Gordian Knot of Notifications* in Franssen V. e Tosza S., *The Cambridge Handbook of digital evidence in criminal investigations*, Cambridge University Press, Cambridge,2025.
- Clough J., *A World of Difference: The Budapest Convention of Cybercrime and the Challenges of Harmonisation* in *Monash University Law Review* 2014, 40, 698.
- Colaiocco A., *La rilevanza delle best practices nell'acquisizione della digital evidence alla luce delle novelle sulla cooperazione giudiziaria*, in *Archivio penale*, 2019.
- Cordero F., *Procedura penale*, Giuffrè, Milano 2012.
- Capone A., *Intercettazioni e Costituzione. Problemi vecchi e nuovi* in *Cassazione penale* 2017, 3, 1263.
- Corasaniti G., *Cybercrime. Le nuove frontiere della responsabilità penale e della prova digitale*, Giuffrè, Milano, 2022.
- Corhay M., Private Life, *Personal Data Protection and the Role of Service Providers: The EU e-Evidence Proposal in European Papers*, 2021, 6/1, 441.

- Council of Europe, *Handbook on European Court of Human Rights Case Law Concerning the Use of Electronic Evidence*, Council of Europe, Strasburgo, 2024.
- Daniele M, *La prova digitale nel processo penale* in *Rivista di diritto processuale penale*, 2011, 2 283.
- Daniele M., *Ricerca e formazione della prova* in Kostoris R., *Manuale di procedura penale europea*,Giappichelli, Torino, 2019, 518.
- Daniele M., *Scope of Judicial Review in the Executing State in EIO Proceedings*, *European Criminal Law Review*, 2024, 14/2, 177.
- Daniele, *Le sentenze "gemelle" delle Sezioni Unite sui criptofonini. La mappa del controllo giurisdizionale quando l'OEI ha ad oggetto prove già in possesso dell'autorità straniera* in *Sistema Penale* https://www.sistemapenale.it/it/scheda/daniele-le-sentenze-gemelle-delle-sezioni-unite-sui-criptofonini, accesso 8 Aprile 2025.
- De Flammineis S., *Le sfide della prova digitale: sequestri, chat, processo penale telematico e intelligenza artificiale* in *Sistema penale*, 2024.
- De Hert, P, *The Microsoft Ireland case and the cyberspace sovereignty trilemma: Post-territorial technologies and companies question territorial state sovereignty and regulatory state monopolies*, *in Brussels Privacy Hub Working Paper* 2018, 4/11.
- De Hert P. e Papakonstantinou V,, *The New Police and Criminal Justice Data Protection Directive: A First Analysis*' in *New Journal of European Criminal Law*, 2016, 7/1, 18.
- De Vries A, *Evidence and Transnational Punitive Enforcement Proceedings in the European Union*, Intersentia, Anversa, 2024.
- Della Torre J., *Audizione dinnanzi alla Commissione Giustizia della Camera dei Deputati nell'ambito dell'esame della proposta di legge C. 1822, approvata dal Senato, recante "Modifiche al Codice di procedura penale in materia di sequestro di dispositivi, sistemi informativi o telematici o memorie digitali*, in *Sistema penale*, 2024

- Depauw S, 'Electronic Evidence in Criminal Matters: How About E-Evidence Instruments 2.0?' *New Journal of European Criminal Law,* 2011, 1, 76.
- Di Paola G., *Prova informatica (diritto processuale penale)* in *Enciclopedia del diritto*: *Annale 6*, Giuffrè, Milano, 2013.
- Di Paolo, *Admissibility of E-Evidence, Transnational E-Evidence and Fair-Trial Rights in Italy* in Bachmaier Winter L. and Salimi F., *Admissibility of Evidence in EU Cross-Border Criminal Proceedings: Electronic Evidence, Efficiency and Fair Trial Rights*, Bloomsbury Publishing, Oxford, 2024, 75.
- Di Pietra R., *Il Regolamento UE sulla E-Evidence* in *Sicurezza e Giustizia* https://www.sicurezzaegiustizia.com/il-regolamento-ue-sulla-e-evidence/, accesso 10 Agosto 2025.
- Di Pietra R., *Principali impatti sulle Società Telco per il Regolamento E-Evidence* in *Sicurezza e Giustizia* https://www.sicurezzaegiustizia.com/principali-impatti-sulle-societa-telco-per-il-regolamento-e-evidence/, accesso 10 Agosto 2025.
- Ertola F., *Mass surveillance e diritto alla privacy* in *Rivista italiana diritto e procedura penale*, 2019, 653.
- Faiola N., *Data retention ed accesso ai dati per scopi securitari: condizioni e limiti alla luce della giurisprudenza della Corte di giustizia dell'Unione europea* in *Il diritto dell'Unione europea* 2023, 1, 77.
- Felicioni P., *Le ispezioni e le perquisizioni*, Giuffrè, Milano, 2004.
- Felicioni P., *le ispezioni e perquisizioni di dati e sistemi* in Cadoppi A., *Cybercrime*, Utet Giuridica, Torino, 2023, 1599.
- Ferri F., *Il bilanciamento dei diritti fondamentali nel mercato unico digitale,* Giappichellli, Torino, 2022.
- Ferrua P., *'Ammissibilità della prova e regole di esclusione della prova'* Rev Brasileira de Direito Processual Penal, 2021, 7, 215.
- Ferrua P*., La prova nel processo penale: vol. I Struttura e procedimento*, Giappichelli, Torino, 2015.

- Feiler D., *New EU Regulation on Digital Evidence Opens Up Risk of Data Misuse* in *Connect on Tech by Backer Mckenzie* https://connectontech.bakermckenzie.com/new-eu-regulation-on-digital-evidence-opens-up-risk-of-data-misuse, accesso 1 luglio 2025.
- Filippi L., *Riservatezza e data retention: una storia infinita* in *Penale diritto e procedura* https://www.penaledp.it/riservatezza-e-data-retention-una-storia-infinita/, accesso 26/08/2025.
- Forlani G., *The E-evidence Package: The Happy Ending of a Long Negotiation Saga* in *Eurcrim*, 2023, 2, 174.
- Formici G., *La digital mass surveillance al vaglio della Corte Europea dei Diritti dell'Uomo: da Zakharov a Big Brother Watch* in *Federalismi.it*, 2020, 23
- Franssen V., *The European Commission's E-evidence Proposal: Toward an EU-wide Obligation for Service Providers to Cooperate with Law Enforcement?* in *European Law Blog* https://europeanlawblog.eu/2018/10/12/the-european-commissions-e-evidence-proposal-toward-an-eu-wide-obligation-for-service-providers-to-cooperate-with-law-enforcement/, accesso 29 Giugno 2025.
- Frunza-Nicolescu A, *Electronic Evidence Collection in Cases of the European Public Prosecutor's Office. Legal Framework, Procedures, and Specifics* in *Eucrim*, 2023, 2, 210.
- Gaito A., '*La circolazione delle prove e delle sentenze'* in *Archivio Penale*, 2011, 3, 17.
- Galič M., *Defence Rights in the Context of Huge Data Sets and Big Data Forensic Tools in Criminal Proceedings* in *Journal Boom Strafblad*, 2021, 2/2 41.
- Gallo N., *Questioni aperte sull'ordine europeo di indagine penale. L'acquisizione all'estero della messaggistica criptata sulla piattaforma SKY-ECC*, *Archivio Penale*, 2023, 3.
- Giunchedi F., *Gli accertamenti tecnici irripetibili: tra prassi devianti e recupero della legalità*, UTET Giuridica, Torino, 2009.

- Gless S. and Richter T., *Do Exclusionary Rules Ensure a Fair Trial? A Comparative analysis*, Springer, Cham, 2019.
- Gordon R. and Moffatt R., *EU Law in Judicial Review*, Oxford university press, Oxford, 2014.
- Griffo M., *Perquisizione informatica… e dintorni'* in *Giurisprudenza penale,* 2019, 5.
- Halberstam D., *Understanding National Remedies and the Principle of National Procedural Autonomy: A Constitutional Approach* in *Cambridge Yearbook of European Legal Studies*, 2021, 23, 128.
- Hafetz J., *Possibilities and limitations of Corporations as Protectors of Privacy in the digital age* in Cole D e Fabbrini F., *Surveilance, Privacy, and Trans-Atlantic Relations*, Hart Publishing, Oxford, 2017.
- Henderman W., *Transparency Under the EU Digital Services Act* in *Mason,Hayes,CurranInsights* https://www.mhc.ie/latest/insights/transparency-under-the-eu-digital-services-act?utm_source=chatgpt.com, accesso 24/08/2025.
- Illuminati G., *Prova penale e Unione europea*, Bononia University Press, Bologna, 2009.
- Illuminati G., *Digital evidence and admissibility* in *Revue internationale de droit penal*, 2020, 2, 273.
- Juszczak A., *The Use of Electronic Evidence in the European Area of Freedom, Security, and Justice: An Introduction to the New EU Package on E-evidence* in *Eurcrim 2023,2, 183, 187.*
- Kanakakis A., *The EncroChat Judgment (Case C-670/22, MN): CJEU Steering a Bold Course through the Symplegades of Evidence Admissibility* in *Blog UKAEL* https://ukael.org/2024/07/01/the-encrochat-judgment-case-c-670-22-mn-cjeu-steering-a-bold-course-through-the-symplegades-of-evidence-admissibility accesso 2 Giugno 2025.
- O. Kerr., *Digital Evidence and the New Criminal Procedure* in *Columbia Law Review*, 2005, 105, 279.

- Klip A, *European Criminal Law: An Integrative Approach*, Intersentia, Anversa, 2021.
- Lasagni G., *Admissibility of Evidence in Criminal Proceedings: Lessons and Problems from the Data Retention Saga* in Bachmaier Winter L. and Salimi F., *Admissibility of Evidence in EU Cross-Border Criminal Proceedings: Electronic Evidence, Efficiency and Fair Trial Rights*, Springer, Berlino, 2019.
- Ligeti K., *Admissibility of Evidence in Criminal Proceedings in the EU* in *Eucrim* 2020, 3, 201.
- Ligeti K., *The European Public Prosecutor's Office at Launch: Adapting National Systems, Transforming EU Criminal Law*, Hart Publishing, Oxford, 2022.
- Luchtman M., *Pertinent Issues of Punitive Enforcement in a Composite Legal Order* in Luchtman M., Ligeti K. and Vervaele J., *EU Enforcement Authorities: Daniele Punitive Law Enforcement in a Composite Legal Order*, Hart Publishing, Oxford, 2023.
- Luparia L. e Ziccardi G., *Investigazione penale e tecnologia informatica* Giuffrè, Milano, 2007.
- Marcolini, *Dalla data retention alle indagini ad alto contenuto tecnologico* Giappichelli, Torino, 2022.
- Martinez Santos A., *Admisibilidad mutua de prueba penal transfronteriza en la Unión Europea: La Propuesta de Directiva del European Law Institute*' in Revista General de Derecho Procesal, 2023, 61.
- B. Martino*, Data retention, conservazioni dati a norma di legge* in *Legal for digital* https://legalfordigital.it/gdpr/data-retention-e-gdpr/, accesso 30/08/2025.
- Magliulo M.R., *Illegittimo il trattenimento prolungato della copia integrale dei dati informatici in caso di sequestro probatorio'* in *Processo penale e giustistizia*, 2021, 3, 648.

- Milaj J. and Bonnici J. P., *Unwitting Subjects of Surveillance and the Presumption of Innocence* in *Computer Law & Security Review*, 2014, 30, 419.
- Mitsilegas V. *The privatisation of mutual trust in Europe's area of criminal justice: the case of e-evidence* in *Maastricht Journal of European and Comparative Law* 2018, 25/3, 263.
- Mitsilegas V, *European prosecution between cooperation and integration: The European Public Prosecutor's Office and the rule of law* in *Maastricht Journal of European and Comparative Law*, 2021, 28/2.
- Mitsilegas V., *Data retention and the future of large-scale surveillance: The evolution and contestation of judicial benchmarks* in *European Law Journal*, 2023, 29/176.
- Molinari F.M., *Le attività investigative inerenti alla prova di natura digitale*, in *Cassazione penale* 2013, 3, 1259.
- Mongillo V, *Screenshot, captatore informatico e sorveglianza occulta online: la Cassazione ridisegna i confini dell'intercettazione informatica* in *Sistema Penale* https://www.sistemapenale.it/it/scheda/cassazione-2022-3591-screenshot-captatore-informatico-online-surveillance, acesso 31 Aprile 2025.
- Mosna A., *Judicial Protection in EU Cross-Border Evidence-Gathering: The EIO as a Case Study* in *European Criminal Law Review*, 2024, 14/2, 148.
- Murro O., *Lo smartphone come fonte di prova. Dal sequestro del dispositivo all'analisi dei dati*, Cedam, Padova, 2024.
- Murro O., *Sequestro dei dati informatici: verso l'art. 254ter c.p.p.? Breve note a margine del disegno di legge a.s. n.806.* in *Diritto e procedura penale* https://www.penaledp.it/sequestro-dei-dispositivi-informatici/, accesso 15 Luglio 2025.
- Nocera N., *L'acquisizione delle chat WhatsApp e Messenger: intercettazione, perquisizione o sequestro*, *Ius Penale* https://ius-giuffrefl-it.eu1.proxy.openathens.net/, accesso 24 June 2025.

- Oddis M., *L'acquisizione della messaggistica digitale nel processo penale: tra cortocircuiti processuali e prospettive de iure condendo* in *Sistema Penale* https://www.sistemapenale.it/it/art./oddis-lacquisizione-della-messaggistica-digitale-nel-processo-penale-tra-cortocircuiti-processuali-e-prospettive-de-iure-condendo, accesseo 4 Luglio 2025.
- Oerlemans J-J e van Toor D., *Legal Aspects of the EncroChat Operation: A Human Rights Perspective* in *European Journal of Crime, Criminal Law and Criminal Justice*, 2022, 30, 309.
- Osula A.M.,'*Transborder access and territorial sovereignty'* in *Computer Law & Security Review*, 2015, 31/6, 719.
- Osula A.M., *Mutual Legal Assistance and Other Mechanisms for Accessing Extraterritorially* in *Masaryk University Journal of Law and Technology*, 2018, 9/1.
- Orlando C., *'Mutua ammissibilità della prova tra gli Stati membri dell'Unione europea ed e-evidence: riflessioni a margine della Proposta di Direttiva dello European Law Institute'* in *Sistema Penale*, 2023, 11, 117.
- Palla S., Art. 352 in Spangher G., *il codice di procedura penale: annotato con la giurisprudenza*, Giuffe, Milano, 2024.
- Palmisano M., *The Surveillance Cold War: Recent Decisions of the European Court of Human Rights and their Application to Mass Surveillance in the United States and Russia* in *Gonzaga Journal of International Law*, 2017, 2/22, 14.
- Panzavolta M., *Streamlining the Exclusion of Illegally Obtained Evidence in Criminal Justice, progetto Defence Rights in Evidentiary Procedures*, Progetto Giustizia Commissione europea, Bruxelles, 2021, 62.
- Panzavolta M., *Exclusion of Evidence in Times of Mass Surveillance: In Search of a Principled Approach to Exclusion of Illegally Obtained Evidence in Criminal Cases in the European Union* in *Internationanal Journal of Proof and evidence*, 2022, 26/3, 199, 202.

- Papucharova G, *The Request for Mutual Assistance and the European Investigation Order – Is the Modern Legal Assistance Instrument Better than its Predecessor* in *International Conference Knowledge-Based Organization,* 2015, 31/6, 211.
- Parlato L., *Perquisizioni on-line: un fenomeno sfuggente e in continua evoluzione* in A. Spena e V. Mitiello, *Mobilità, sicurezza e nuove frontiere tecnologiche.*
- Parodi C., *Indagini informatiche e acquisizione dei file: accertamento o rilievo?* in *Ius Penale* giuffreflit.eu1.proxy.openathens.net/dettaglio/8354475/Documento?ticket=AQIC5wM2LY4Sfcx0bFbxB3jWNurXNhsO1952GD7RvoARGEc.%2aAAJTSQACMDMAAlNLABMyNjc3MzE4ODE4MTYxNDkyMjkxAAJTMQACMDI.%2a accesso 10 Luglio 2025.
- Paolucci C.M., *Cooperazione giudiziaria e di polizia in materia penale* UTET Giuridica, Milano, 2007.
- Peers S., Tamara K Hervey, Jeff Kenner and Angela Ward, *The EU Charter of Fundamental Rights: A Commentary*, Hart Publishing, Oxford, 2021.
- Pezzuto R., *Accesso Transnazionale alla Prova Elettronica mel Procedimento Penale: la Nuova Iniziativa Legislativa della Commissione Europea al Vaglio del Consiglio dell'Unione* in *Diritto Penale Contemporaneo* 2019, 1, 57, 82.
- Sajfert J. e Quintel T., *Data Protection Directive (EU) 2016/680 for Police and Criminal Justice Authorities*, in Cole M. e Boehm F., *GDPR Commentary,*, Edward Elgar Publishing, Cheltenham, 2018.
- Savignano N., *La tutela dei diritti fondamentali nella raccolta transnazionale della prova penale tra gli Stati membri dell'Unione europea*, Tesi PhD, Università degli Studi di Napoli Federico II, 2019.
- Prechal S., *Effective Judicial Protection: Some Recent Developments – Moving to the Essence*, in *Review of Europrean Administrative Law*, 2020, 13, 175.

- Pittirruti M., *Digtital evidence e procedimento penale*, Giappichelli, Torino 2017
- Pushkar P., *The Right to a Fair Trial and Use of Unlawfully Obtained Evidence and Guilty Pleas in the Case-Law of the European Court of Human Rights'* in *Constitutional Law Review* 2010, 2, 38.
- Raucci P., *L'Ordine europeo di indagine e prove digitali: tra presunzione di legittimità degli atti compiuti all'estero e diritti fondamentali*, *Penale Diritto e Procedura*, https://www.penaledp.it/lordine-europeo-di-indagine-e-prove-digitali-tra-presunzione-di-legittimita-degli-atti-compiuti-allestero-e-diritti-fondamentali/, accesso 12 Luglio 2025.
- Ricci A.E., *Digital evidence e irripetibilità delle operazioni acquisitive*, in Diritto penale e procedura., 2010, 33.
- Roberts P., *Criminal Evidence*, Oxford University Press, Oxford, 2022.
- Robinson G. *Effective Data Protection and Direct Cooperation on Digital Evidence* in Franssen V. e Tosza S., *The Cambridge Handbook of digital evidence in criminal investigations,* Cambridge University Press, Cambridge, 2025.
- Rojszczak M., *Data Retention Laws and La Quadrature du Net II* In *Verfasublblog* https://verfassungsblog.de/data-retention-laws-and-la-quadrature-du-net-ii/, accesso 03/08/2025.
- Rosanò A, *La "privatizzazione" nello spazio di libertà, sicurezza e giustizia: tre esempi* in *Rivista di diritto europeo*, 2020, 1.
- Ruotolo G., *La disciplina dell'e-evidence e la cooperazione rafforzata nel secondo Protocollo addizionale alla Convenzione di Budapest*, in *Diritto penale e processo*, 2022, 8, 1026.
- Sachoulidou A., *'The Court of Justice in Staatsanwaltschaft Berlin v M.N. (EncroChat): From Cross-Border, Data-Driven Police Investigations to Evidence Admissibility' in Maastricht Journal of European and Comparative Law* 2024, 31/4, 510.

- Samartzis A., *Weighing Overall Fairness: A Critique of Balancing under the Criminal Limb of Article 6 of the European Convention on Human Rights* in *Human Rights Law Review*, 2020, 21, 409.
- Sanna A., *L'irriducibile atipicità delle intercettazioni tramite virus informatico* in Scalfati A. *Le indagini atipiche*, Giappichelli, Torino, 2019.
- Satzger H., *International and European Criminal Law*, C.H. Beck, Monaco, 2021
- Savignano N., *La tutela dei diritti fondamentali nella raccolta transnazionale della prova penale tra gli Stati membri dell'Unione europea* (Tesi PhD, Università degli Studi di Napoli Federico II 2019).
- Scalas A., 'I confini mobili della digital evidence: una necessaria tassonomia per la tutela delle garanzie' (2023) 2 Archivio Penale.
- Schwartz M., *Global Data Privacy: The EU Way* in *New York University Law Review*, 2019, 94/771.
- Simonato M., *'Defence Rights and the Use of IT in Criminal Procedure'* in *International Journal of Penal Law,* 2019, 1/85.
- Spangher G., *Codice di procedura penale. Commentato con la giurisprudenza* (Torino Giuffrè 2023)
- Steinborn S. and Świeczkowski D., *Verification in the Issuing State of Evidence Obtained on the Basis of the European Investigation Order* in *Review of European and Comparative Law*, 2023, 54/3,169.
- Stoykova R., *The right to a fair trial as a conceptual framework for digital evidence rules in criminal investigations* Computer Law & Security Review, 2023, 49, 1.
- Radina Stoykova, *A New Right to Procedural Accuracy: A Governance Model for Digital Evidence in Criminal Proceedings* in *Computer Law & Security Review* 2024, 55.
- Smuha N., *Towards the EU Harmonization of Access to Cross-Border E-Evidence: Challenges for Fundamental Rights and Consistency'* in *European Criminal Law Review*, 2018, 8/1, 83.

- Tonini P. e Conti C., *Manuale di Procedura penale*, Giuffre, Milano 2024.
- Tonini P. e Conti C., *Il diritto delle prove penali*, Giuffrè, Milano, 2014.
- Torre S., *Il captatore informatico: nuove tecnologie investigative e rispetto delle regole processuali,* Giuffrè, Milano, 2017.
- Torre M., *La ricerca della prova digitale: le perquisizioni online nel contesto del processo penale telematico*, Tesi PhD, Università di Firenze, 2025.
- Tósza M., *All Evidence is Equal, but Electronic Evidence is More Equal than Any Other: The Relationship between the European Investigation Order and the Admissibility of Evidence in Criminal Proceedings'* in *New Journal of European Criminal Law*, 2020, 11/2 161.
- Tosza S., *The E-Evidence Package is Adopted: End of a Saga or Beginning of a New One?* In *European Data Protection Law Review,* 2023, 2 163.
- Trogu M., *Intrusioni segrete nel domicilio informatico* in Scalfati A. *Le indagini atipiche*, Giappichelli, Torino, 2019.
- Valli R., *La perquisizione informatica e la perquisizione da remoto* in *IUS Diritto Processuale Penale* https://ius.giuffrefl.it/dettaglio/6618776/la-perquisizione-informatica-e-la-perquisizione-da-remoto, accesso 23 June 2025.
- Van Wijk M., *Cross-border Evidence Gathering: Equality of Arms within the EU*, Eleven International Publishing, L'Aia, 2017.
- Veronica V., *Criptofonini e indagini digitali transfrontaliere su larga scala: un difficile equilibrio tra privacy, fairness processuale ed esigenze di repressione dei reati* in *Giurisprudenza Penale* 2025, 1.
- Vervaele J., *Lawful and Fair Use of Criminal Evidence in the EU: The Unwritten Script for European Enforcement Agencies* in Luchtman M., Ligeti K. and Vervaele J., *EU Enforcement Authorities: Punitive Law Enforcement in a Composite Legal Order*, Hart Publishing, Oxford, 2023.

- Vuille J., Lupària L. and Taroni F., *Scientific Evidence and the Right to a Fair Trial under Article 6 ECHR* in *Law, Probability and Risk* 2017, 16, 55.
- Whal T., *ECJ Ruled in EncroChat Case* (eucrim, 7 March 2024) https://eucrim.eu/news/ecjruled-in-encrochat-case/ accessed 17 March 2025.
- Whal T., *E-evidence Regulation and Directive Published* in *Eurcrim,* 2023, 2, 165, 166.
- Zajac K., 'The Admissibility of Tainted Evidence in Criminal Proceedings as a Rule of Law Issue Under the ECHR' (2025) 36 Criminal Law Forum 33.
- Wulf A., *E-Evidence Regulation: New obligations for service providers from 2026* in *Heuking News & Events* https://www.heuking.de/en/news-events/newsletter-articles/detail/e-evidence-regulation-new-obligations-for-service-providers-from-2026.html?utm_source=chatgpt.com, accesso 23/08/2025.
- Zapf D. e Malaga F., *EU breaks down digital borders: New e-Evidence rules facilitate cross-border investigations* in *White and Case Publications* https://www.whitecase.com/insight-alert/eu-breaks-down-digital-borders-new-e-evidence-rules-facilitate-cross-border?utm_source=chatgpt.com, accesso 26/08/2025.
- Zerbes I. *Legal Issues of Transnational Exchange of Electronic Evidence in Criminal Proceedings* in *European Criminal Law Review* 2015, 5, 304.

Report

- Consiglio d'Europa, Relazione esplicativa alla Convenzione europea di assistenza giudiziaria in materia penale (aprile 1959)
- Consiglio d'Europa, Rapporto esplicativo della Convenzione sulla criminalità informatica (novembre 2001)
- Consiglio d'Europa, Rapporto esplicativo al Secondo Protocollo addizionale alla Convenzione sulla criminalità informatica sulla

cooperazione rafforzata e la divulgazione delle prove elettroniche, CETS n. 224 (maggio 2022.)

- Commissione europea, Libro verde sull'ottenimento di prove in materia penale tra Stati membri e sulla loro ammissibilità (novembre 2009)
- Commissione europea, Documento di lavoro dei servizi della Commissione: valutazione d'impatto che accompagna la proposta di regolamento relativo agli ordini europei di produzione e conservazione delle prove elettroniche in materia penale (aprile 2018)
- Eurojust e Rete Giudiziaria Europea, Nota congiunta sull'applicazione pratica dell'ordine europeo di indagine (giugno 2019)
- Eurojust, Sfide e buone prassi nei casi di criminalità informatica trattati da Eurojust (novembre 2020)
- Istituto Europeo del Diritto (ELI), Proposta di direttiva del Parlamento europeo e del Consiglio sulla reciproca ammissibilità delle prove e sulle prove elettroniche nei procedimenti penali (marzo 2023)
- SIRIUS Project (Eurojust and Europol), *EU Electronic Evidence Situation Report 2024* (November 2024) https://www.europol.europa.eu/sirius-project
- Progetto SIRIUS (Eurojust ed Europol), La Convenzione di Budapest sulla criminalità informatica e l'accesso transfrontaliero alle prove elettroniche (gennaio 2024)
- Circolare del Ministero della Giustizia 26 ottobre 2017, Manuale operativo sull'attuazione della direttiva 2014/41/UE relativa all'ordine europeo di indagine penale (Ottobre 2017).
- U.S. Department of Justice, *CLOUD Act Resources*, (Marzo 2018).
- Comando generale della Guardia di Finanza, III Reparto Operazioni – Ufficio Tutela Entrate, Manuale operativo in materia di contrasto all'evasione e alle frodi fiscali (Circolare n. 1/2018), Vol. II, online at gdf.gov.it.
- Studio per il Parlamento Europeo, Fighting Cyber Crime and Protecting Privacy in the Cloud (Ottobre 2012).

- Corte EDU e Agenzia per i diritti fondamentali dell'Unione Europea, Joint Factsheet: Mass Surveillance – ECtHR and CJEU Case-Law (28 Febbraio 2025)
- EDRi, Position Paper on the European Commission's Proposal for a Regulation on European Pro-duction and Preservations Orders for Electronic Evidence in Criminal Matters (25 Aprile 2019).