



*Classificazione Decimale Dewey*

— 345.406 (23.) DIRITTO PENALE. PROVE. EUROPA

*Thema*

— Soggetto: LNFx. Procedura penale

— Qualificatori: 3MR. XXI secolo, 2000-2100

GUIDO ROSSI

**LA CIRCOLAZIONE  
DELLA *DIGITAL EVIDENCE*  
NEL CONTESTO GIUDIZIARIO  
TRANSAZIONALE**





ISBN  
979-12-218-2808-5

PRIMA EDIZIONE  
**ROMA** 20 LUGLIO 2026

*A mio padre.  
In uno degli infiniti mondi paralleli,  
prima o poi ci ritroveremo*



## INDICE

### 9     *Introduzione*

### 17    Capitolo I

#### Il percorso evolutivo verso lo “Spazio di libertà sicurezza e giustizia”

1. L'esigenza di cooperazione e assistenza giudiziaria e di polizia in materia penale. Il cammino verso lo “Spazio di libertà sicurezza e giustizia”, 17 – 1.1. Il cammino verso lo “Spazio di libertà sicurezza e giustizia”. L'accordo Schengen e l'alba dello spazio senza frontiere, 21 – 1.1.1. I Trattati degli anni Novanta e l'istituzionalizzazione della cooperazione, 31 – 1.1.2. Il cammino verso il primo germe di diritto penale europeo. Il fallimento del Trattato per una nuova Costituzione e la firma del Trattato di Lisbona, 43 – 1.1.2.1. Il superamento della divisione in pilastri, 48 – 1.1.2.2. Il valore giuridicamente vincolante della Carta dei diritti fondamentali dell'Unione Europea, 50 – 1.1.3. La regolamentazione dello “Spazio di libertà sicurezza e giustizia” nel nuovo Titolo V TFUE, 52 – 1.1.4. Il ravvicinamento delle disposizioni di diritto penale. Rapporti tra diritto dell'Unione Europea, diritto penale e diritto processuale, 57 – 1.1.5. Cenni introduttivi sull'istituzione e ruolo del Pubblico ministero europeo, 61 – 1.1.5.1. Il magistrato di collegamento, 67 – 1.1.5.2. La collaborazione a rete, 70 – 1.1.5.3. Europol, 74 – 1.1.5.4. OLAF, 84 – 1.1.5.6. Eurojust, 88 – 1.1.5.7. Riflessioni sull'istituzione della Procura Europea, 98.

### 107   Capitolo II

#### La digital evidence

1. La prova digitale nella sua nozione comunitaria, 107 – 1.1. L'elemento costitutivo della prova digitale, 118 – 1.2. Il requisito della genuinità, 122 – 2. La prova digitale: distinzione tra supporto e contenuto della prova, 132 – 3. Prova digitale e circolazione: il cyberterrorismo, 137. SEZIONE I. Il contenuto della prova digitale nell'ambito della cooperazione nello spazio giudiziario europeo, 137 – 4. Le garanzie nella circolazione della prova elettronica, 152 – 4.1. Il delicato rapporto tra pubblico e privato per la crescita delle infrastrutture: il binomio tra esigenze di pubblica sicurezza e di sviluppo economico, 154 – 4.2. L'idea di regole conformi per la catalogazione e indicizzazione delle prove: l'individuazione di termini e tecniche di scelta condivisa, 163 – 4.3. La trasmissione di prove digitali e forme di controllo: un intervento preventivo contro gli eccessi e gli abusi, 173 – 5.4. La specializzazione necessaria per il personale coinvolto nelle procedure di cooperazione circolazione della digital evidence, 181. SEZIONE II.

La catalogazione dei dati e degli archivi, 184 – 5. Il sistema degli Archivi e delle banche dati: dubbi operativi, 184 – 6. Le banche dati dell'Unione europea appartenenti ad Europol, Eurojust e Olaf, 189 – 6.1. Le altre principali banche dati UE, 199 – 7. Le banche dati nazionali: perplessità e benefici, 198. SEZIONE III. La prova digitale, i diritti della persona e le esigenze di giustizia e di sicurezza interna ed esterna, 208 – 8. Prova digitale ed equo processo: il rapporto tra acquisizione, contraddittorio e valutazione, 208 – 9. Il Regolamento UE 2023/1543 e il rapporto con la prova elettronica, 218 – 10. Prova digitale e diritto di difesa, 224 – 11. Pericoli e strategie di contenimento: a) il vulnus ai diritti individuali, 229 – 12. Segue: b) l'inattendibilità della conoscenza e gli ostacoli al diritto di difesa, 235 – 13. Il diritto alla privacy del terzo e dell'imputato, 244. SEZIONE IV. Criptofonini e ordine europeo di indagine penale; gli strumenti utilizzati dalla criminalità transazionale Sky ECC/Encrochat. Perplessità a seguito della pronuncia delle Sezioni Unite, 247 – 14. Premessa, 247 – 15. L'annosa questione dell'acquisizione delle comunicazioni criptate custodite nei server esteri, 248 – 16. L'acquisizione libera, 250 – 17. Perplessità sulla libertà nell'acquisizione dei dati, 250 – 18. L'OEI quale garanzia nell'acquisizione libera; controllo giurisdizionale, proporzionalità ed equivalenza, 252 – 19. Strumenti posti a garanzia, 254 – 20. L'inutilizzabilità quale sanzione per l'omesso controllo giurisdizionale nazionale sull'acquisizione delle comunicazioni, 256 – 21. L'inutilizzabilità quale sanzione per violazione del diritto di difesa, 258.

## 263 Capitolo III

La circolazione della prova digitale nell'ambito della Cooperazione nello spazio giudiziario europeo

1. La necessità di un linguaggio condiviso nelle procedure di cooperazione e circolazione della prova, 263 – 1.1. Le scelte linguistiche di alcuni organi e nelle principali procedure di cooperazione, 271 – 2. Le modalità per una genuina acquisizione della prova digitale: il rapporto tra la disciplina comunitaria e quella nazionale, 280 – 3. La circolazione dell'*electronic evidence*, 289 – 4. La trasmigrazione di dati. Dal sistema centralizzato al principio di domanda diretta nel iure condito comunitario: una svolta nella cooperazione informativa, 298.

## 313 Capitolo IV

La cooperazione giudiziaria e di polizia in prospettiva *de iure condendo*.

Riforma del sistema e della circolazione della prova digitale ai fini di giustizia

1. Il ruolo centrale di Europol, Eurojust e Olaf: l'incremento dei poteri degli organi comunitari per una cooperazione effettiva, 313 – 2. La genuinità della digital evidence nell'Unione Europea: prospettive di armonizzazione e di incremento della cooperazione nello spazio giudiziario europeo, 319 – 3. Gli standard minimi di garanzia dei diritti fondamentali nella circolazione della prova elettronica, 324 – 4. Il sistema e-Edes e il progetto di digital justice; la digitalizzazione della cooperazione giudiziaria transfrontaliera, 326 – 5. La nuova piattaforma digitale per le squadre investigative comuni, 331 – 6. Perplessità nazionali, 336 – 7. Il "sogno americano": la legislazione americana sul Cloud Act. e sistemi informatizzati, 341 – 8. Diritti fondamentali e conservazione degli elementi digitali (c.d. data retention), 343 – 9. La proporzionalità nel contesto digitale europeo, 345 – 10. Perplessità ed anticipazioni conclusive, 354.

## 359 Conclusioni

## 365 Bibliografia

## INTRODUZIONE

Il carattere di immaterialità della prova informatica, unito al crescente sviluppo dell'interconnessione digitale, comporta inevitabilmente che l'evidenza digitale da acquisire possa trovarsi all'interno di *server* ubicati presso paesi differenti da quello ove si svolge l'attività investigativa.

Anche per quanto concerne le indagini portate avanti dall'autorità italiana accade non di rado che, sebbene si proceda per crimini commessi nel nostro territorio, le prove informatiche siano stoccate in sistemi di memorizzazione collocati all'estero<sup>(1)</sup>.

Proprio questo tratto transfrontaliero della *digital evidence*<sup>(2)</sup> impone

---

(1) Sul punto occorre precisare che non sono solo i crimini informatici gli unici idonei a lasciare tracce digitali. Infatti, l'ingerenza che le nuove tecnologie stanno avendo nella quotidianità di chiunque, comporta l'evenienza, cosa che ormai costituisce la normalità, che anche tutti gli altri reati possano avere una loro componente informatica. Basti pensare a reati organizzati su *chat online*, o a documenti salvati sul dispositivo, etc. Cfr. R. MURENEC, *Digital forensics*, Ed. Egaf 2024 ISBN-10:8835214769 p. 115, dove per l'autore «oggi potrebbe risultare arduo immaginare un crimine che non abbia una dimensione per così dire "digitale"»; M. CAIANIELLO – A. CAMON, *Digital forensic evidence*, Cedam, 2021; G. Verde, *Il percorso della prova digitale nelle attività di Digital Forensics, una review*», *i-lex*. Bologna, Italy, 18(1), pagg. 49–69. doi: 10.6092/issn.1825-1927/21507; R. DE VITA, *La prova digitale nel processo penale*, Devitalw EAN: 9791221089509, ISBN: 1221089501, 2025. F. D'USO, *Informazioni e dati nella digital forensics: tra tutela dei diritti ed esigenze probatorie*, in *Il processo penale alla prova delle nuove tecnologie e dell'intelligenza artificiale*, (a cura di A. DE CARO, V. MAFFEO, G. ROSSI, G. TESSITORE), ISBN 9791221113891, Giappichelli Ed. 2026.

(2) F. LAZZINI, *Acquisizione della prova informatica all'estero*, l'autore ritiene che la natura transnazionale della prova digitale viene ricondotta a tre aspetti specifici, ovvero: «*localizzazione e conservazione della prova digitale*» atteso che la prova digitale può essere memorizzata e

un approccio per così dire internazionale, in ottica di cooperazione giudiziaria fra gli Stati.

Una corretta comunicazione tra le autorità giudiziarie e le forze dell'ordine dei vari paesi che possono essere coinvolti nelle operazioni di *digital forensics*, infatti, costituisce spesso la chiave di volta per una rapida e buona riuscita dell'indagine, soprattutto per quanto riguarda la fase di acquisizione degli elementi di prova.

Ad ogni modo, allo stato attuale (*salvo alcuni tentativi*) non vi è ancora stata una reale armonizzazione tra gli ordinamenti giuridici in tema di *digital forensics*, sicché potrebbero verificarsi situazioni di incertezza con riferimento all'attendibilità di evidenze ottenute presso stati esteri ove non vengono rispettati i principi da noi considerati cardine a garanzia della genuinità della prova nonché, più in generale, le regole costituzionali in materia di giusto processo e tutela dei diritti fondamentali della persona.

In assenza di regole condivise, lo strumento principale per l'acquisizione all'estero rimane, dunque, anche in tema di indagini digitali, la tradizionale rogatoria internazionale, già vigente per l'assunzione degli altri tipi di prova<sup>(3)</sup>.

---

conservata in qualsiasi parte del mondo; «*sede dell'Internet Service Provider (ISP privato)*», giacché la maggior parte delle prove digitali si trovano nei *server* di *provider* privati che spesso possono avere la sede legale presso altri paesi; «*natura transnazionale del presunto crimine*», poiché può capitare, specie per i crimini informatici, che il reato coinvolga molteplici giurisdizioni con conseguente aggravamento delle attività di raccolta, acquisizione e utilizzo processuale della prova digitale, p. 116 e ss.; P. FELICIONI, *L'acquisizione da remoto di dati digitale nel procedimento penale*, in *Processo Penale e Giustizia*, 2016; F. RUGGIERO, *Individuazione nel cyberspazio del soggetto penalmente responsabile e ruolo dell'internet provider*, in *Giur. Merito*, Milano, 2001; R. BELFIORE, *L'acquisizione transfrontaliera di prove digitali*, in *Indagini e prove nella società digitale. Questioni attuali e prospettive future*, a cura di G. DI PAOLO – L. PRESSACCO, Quaderni della facoltà di Giurisprudenza Università di Trento, 95/2025 p. 81. Il volume citato raccoglie le relazioni e gli interventi svolti nel corso dell'incontro di studio «Indagini e prove nella società digitale. Questioni attuali e prospettive future», tenutosi a Trento il 26 e 27 settembre 2024, nell'ambito delle iniziative legate al Dipartimento d'eccellenza 2023-2027; G. TABASCO, *L'acquisizione transfrontaliera delle prove elettroniche*, in *proc. pen. e giust.*, fasc. 4/2025; G. DI PAOLO, *Admissibility of E-Evidence, Transnational E-Evidence and Fair-Trial rights in Italy*, in L. BACHMAIER WINTER – F. SALIMI (a cura di) *Admissibility of Evidence in EU Cross-Border Criminal Proceedings Electronic Evidence, Efficiency and Fair Trial Rights*, in corso di pubblicazione per la Oxford University Press (OUP).

(3) S. ALLEGREZZA – A. MOSNA – F. NICOLICCHIA, *L'acquisizione della prova all'estero e i profili transazionali*, in G. CANZIO – L.D. CERQUA – L. LUPARIA (a cura di), *Diritto Penale delle Società*, seconda edizione, Cedam, 2016, 157 ss; V. MAFFEO – G. TESSITORE, *L'intelligenza*

Quanto appena detto, però, vale nei rapporti tra Stati non appartenenti alla Comunità Europea.

Per gli Stati membri dell'Unione, però, un'eccezione è rappresentata dalla direttiva del Parlamento europeo e del Consiglio n. 41/2014/UE del 2014 – recepita nel nostro ordinamento con decreto legislativo n. 108 del 2017 – che ha istituito la procedura del c.d. ordine europeo di indagine (OEI).

Successivamente, un altro timido tentativo, la cui effettiva portata applicativa in termini di efficacia inizierà a conoscersi soltanto nel 2026, è rappresentata dal Regolamento 2023/1543 previsto contro la criminalità informatica relativo agli ordini europei di produzione e conservazione di prove elettroniche nei procedimenti penali e per l'esecuzione di pene detentive a seguito di procedimenti penali.

Oltre al Regolamento di cui sopra, vi è la Direttiva (UE) 2023/1544 recante norme armonizzate sulla designazione di stabilimenti designati e sulla nomina di rappresentanti legali ai fini dell'acquisizione di prove elettroniche nei procedimenti penali<sup>(4)</sup>.

---

*artificiale nel giusto processo: impatto sulle indagini e nel contesto transnazionale*, in Accertamento Penale, AI e Cybersicurezza Inventari e prime sperimentazioni nella prospettiva dell'IA ACT e della legge n. 132 del 2025: opportunità, problemi e nuovi diritti, Atti del Convegno di Campobasso (6 e 7 novembre 2025) (a cura di) A. DE CARO, B.C. ALONGI, F. BARBIERI, A. DE MARCO, P. RAUCCI, G. ROSSI, G. TESSITORE, A. VELE, G. VERDE, Editoriale scientifica, Napoli, ISBN 979-12-235-0577-9, 2026.

(4) La Direttiva (UE) 2023/1544 del Parlamento europeo e del Consiglio, del 12 luglio 2023, disciplina norme armonizzate sulla designazione di stabilimenti designati e sulla nomina di rappresentanti legali ai fini dell'acquisizione di prove elettroniche nei procedimenti penali (GU L 191 del 28.7.2023, pag. 181). La direttiva è stata recepita nel nostro ordinamento. Pubblicati in Gazzetta Ufficiale n.11 del 15 gennaio 2026 i decreti legislativi del 30 dicembre 2025 n. 215 e 216, che danno attuazione alla direttiva (UE) 2023/1544 del 12 luglio 2023 e completano il recepimento italiano del pacchetto europeo "e-evidence". I provvedimenti rendono operativo nel nostro ordinamento il sistema europeo di acquisizione diretta delle prove elettroniche nei procedimenti penali, integrando il quadro delineato a livello UE sugli ordini di produzione e conservazione dei dati digitali. La finalità del provvedimento è superare i limiti della cooperazione giudiziaria tradizionale, spesso poco efficace rispetto alla natura transnazionale dei servizi digitali, e garantire alle autorità giudiziarie strumenti rapidi e standardizzati per l'accesso alle prove elettroniche. Il decreto si applica ai prestatori di servizi digitali che offrono servizi nell'Unione europea, come fornitori di comunicazioni elettroniche, piattaforme online, servizi di archiviazione e trattamento dei dati, nonché soggetti che gestiscono nomi di dominio e numerazioni IP. Restano esclusi i servizi finanziari e i prestatori che operano esclusivamente all'interno di un singolo Stato membro. Non rileva la mera accessibilità tecnica dei servizi dall'Europa: ciò che conta è l'esistenza di un collegamento sostanziale con l'Unione, desumibile dallo stabilimento in uno Stato membro oppure, in mancanza, dal numero significativo di utenti o dall'orientamento delle attività verso il

La Direttiva (UE) 2023/1544, è stata tecnicamente recepita nel nostro ordinamento con il d.lgs. 216 del 30 dicembre 2025<sup>(5)</sup> entrato in

mercato europeo. Il perno della disciplina è l'obbligo, per i prestatori che operano nell'Unione, di individuare uno stabilimento designato nell'UE oppure di nominare un rappresentante legale incaricato di ricevere ed eseguire gli ordini delle autorità giudiziarie. L'obiettivo è assicurare l'individuazione di un referente certo e responsabile sul territorio europeo, evitando che l'acquisizione delle prove digitali sia ostacolata dall'assenza di interlocutori giuridicamente identificabili. La designazione deve essere effettiva: allo stabilimento o al rappresentante devono essere attribuiti poteri e risorse adeguati per dare concreta esecuzione agli ordini. Il sistema si fonda su obblighi di comunicazione verso le autorità nazionali competenti, relativi ai dati di contatto degli stabilimenti designati o dei rappresentanti legali, all'ambito territoriale di competenza e alle lingue utilizzabili per le comunicazioni ufficiali. Queste informazioni consentono alle autorità giudiziarie di indirizzare correttamente gli ordini di produzione o conservazione dei dati e permettono un controllo effettivo sul rispetto degli obblighi da parte dei prestatori. Il decreto introduce un apparato sanzionatorio significativo in caso di inadempimento, con sanzioni amministrative pecuniarie elevate per la mancata designazione dei soggetti responsabili, per l'inosservanza degli obblighi di cooperazione o per irregolarità nelle notifiche. Un profilo centrale è la responsabilità solidale tra prestatore, stabilimento designato e rappresentante legale: eventuali carenze organizzative interne non possono essere addotte per sottrarsi all'esecuzione degli ordini delle autorità, salvo che la condotta integri un reato. La vigilanza e l'applicazione delle sanzioni sono affidate a un'autorità centrale nazionale, chiamata anche a cooperare con le omologhe autorità degli altri Stati membri. Il rafforzamento degli strumenti investigativi è accompagnato da limiti precisi. Il sistema *e-evidence* non legittima forme di conservazione generalizzata e indiscriminata dei dati né introduce nuove modalità di intercettazione. L'accesso è circoscritto alle informazioni già detenute dai prestatori, nel rispetto dei diritti fondamentali e delle regole sulla protezione dei dati personali. È inoltre prevista la possibilità di sollevare conflitti con obblighi derivanti da ordinamenti di Paesi terzi. La disciplina europea considera prove elettroniche non solo i dati presenti su dispositivi o server, ma anche: dati di sottoscrittore e identificativi; *traffic data*; dati di contenuto, inclusi messaggi, email e file archiviati dai provider. L'ampliamento della nozione di prova digitale è particolarmente rilevante per la difesa, perché incide direttamente sulle categorie di dati che possono essere oggetto di un ordine europeo *e-evidence* e rafforza l'esigenza di un controllo puntuale su pertinenza, proporzionalità e tutela dei diritti fondamentali. Per l'autorità giudiziaria, il nuovo assetto consente canali diretti e standardizzati verso i prestatori di servizi, con una riduzione sensibile dei tempi di acquisizione delle prove digitali rispetto ai tradizionali strumenti di cooperazione internazionale. Per la difesa, il decreto apre un terreno particolarmente delicato. Diventano centrali il controllo sulla legittimità e sulla proporzionalità degli ordini, la verifica delle categorie di dati richiesti – che possono includere dati identificativi, di traffico e contenuti – e il rispetto delle garanzie in materia di protezione dei dati personali. La rapidità dei nuovi meccanismi impone agli avvocati un approccio più reattivo: eventuali profili di illegittimità o di compressione dei diritti fondamentali devono essere intercettati tempestivamente, anche alla luce dei possibili conflitti con ordinamenti di Paesi terzi. Sul punto cfr. C. DE LAZZARO, *L'acquisizione delle prove elettroniche nello spazio di libertà, sicurezza e giustizia: una prima implementazione dell'e-evidence package*, in Sist. Pen. (web), 2026; M. ODDIS, *L'acquisizione della messaggistica digitale nel processo penale: tra cortocircuiti processuali e prospettive de iure condendo*, in Sist. Pen. (web) 6/2025.

(5) Il provvedimento rende operativo nel nostro ordinamento il sistema europeo di acquisizione diretta delle prove elettroniche nei procedimenti penali, integrando il quadro delineato a livello UE sugli ordini europei di produzione e conservazione dei dati digitali. La finalità del

vigore il 30.01.2026, che ha così reso operativo anche gli strumenti del Regolamento (UE) 2023/1543.

Ad ogni modo l'Ordine Europeo di Indagine, discostandosi dal meccanismo della richiesta proprio della rogatoria internazionale e poggiando le basi sul mutuo riconoscimento delle decisioni e dei provvedimenti delle autorità giudiziarie straniere, segue le logiche dell'ordine ad eseguire<sup>(6)</sup>.

Più propriamente l'OEI, come noto, consiste in un provvedimento mediante il quale l'autorità giudiziaria o amministrativa procedente richiede ad altra autorità di un paese membro di svolgere attività di indagine o di assunzione probatoria – che in materia di *digital forensics* può coincidere, appunto con l'acquisizione in copia forense di evidenze digitali – al fine di acquisire informazioni o prove già disponibili presso il paese a cui è rivolto (art. 1, lett. a d.lgs. n. 108 del 2017)<sup>(7)</sup>.

Una volta rivolto allo stato estero, l'OEI viene sottoposto da quest'ultimo a un giudizio di ammissibilità; in talune circostanze espressamente previste può essere rifiutato<sup>(8)</sup>, mentre in ogni altro caso deve essere eseguito con rapidità.

Per quanto riguarda le regole esecutive dell'OEI la disciplina lascia ampio margine discrezionale allo Stato di emissione, che può prescrivere all'autorità di esecuzione di utilizzare le proprie modalità attuative.

Di conseguenza, parte della dottrina, ritiene che le evidenze digitali ottenute senza il rispetto delle prescrizioni indicate dallo Stato di emissione, non potrebbero che condurre alla loro inutilizzabilità in sede giudiziale<sup>(9)</sup>.

---

provvedimento è superare i limiti della cooperazione giudiziaria tradizionale, spesso poco efficace rispetto alla natura transnazionale dei servizi digitali, e garantire alle autorità giudiziarie strumenti rapidi e standardizzati per l'accesso alle prove elettroniche.

(6) F. CAJANI, “La cooperazione internazionale nelle indagini digitali”, in “*Cyber forensics e indagini digitali Manuale tecnico-giuridico e casi pratici*”, cit., p. 237; M. GRIFFO, *L'intelligenza artificiale: strumento “per” o “contro” la giustizia?*, in *Intelligenza artificiale e processo un possibile ruolo nelle fasi iniziali e conclusive dell'accertamento* a cura di V. MAFFEO – R. AUGUSTO – P. TRONCONE, Ed. Giappichelli 2024.

(7) *Ivi*, p. 238 dove si specifica che l'ambito di applicazione dell'OEI, in ogni caso, si limita esclusivamente agli atti di indagine e agli atti di ricerca della prova espressamente previsti dalla direttiva n. 49/2014/UE.

(8) Si pensi ad esempio al caso in cui l'OEI avanzi richiesta di svolgimento di attività d'indagine che si pongano in contrasto con i principi e le libertà dei diritti umani sostenute dall'UE, che siano oggettivamente impossibili da portare ad esecuzione, o ancora che si pongano in contrasto con i principi fondamentali dello stato cui si rivolge la richiesta o ne mettano a rischio l'ordine pubblico.

(9) S. ALLEGREZZA, *Cooperazione giudiziaria, mutuo riconoscimento e circolazione della prova penale nello spazio giudiziario europeo*, in T. RAFARACI (a cura di), *L'area di libertà, sicurezza*

Secondo tale filone dottrinale, pertanto, anche la violazione delle *best practices* accolte dal nostro ordinamento con la legge n. 48/2008 comporterebbe un'ipotesi di inutilizzabilità<sup>(10)</sup>, se fossero poste alla base delle modalità di esecuzione.

Infine, non tutte le attività volte all'assunzione della prova digitale all'estero sono sottoposte al regime della rogatoria internazionale o dell'ordine di esecuzione europeo.

All'art. 234 *bis* del c.p.p., infatti è specificato che «è sempre consentita l'acquisizione di documenti e dati informatici conservati all'estero, anche diversi da quelli disponibili al pubblico, previo consenso, in quest'ultimo caso, del legittimo titolare».

Il consenso prestato dal titolare del dato informatico, dunque, fa venire meno l'obbligo di adozione delle formalità contemplate dalle procedure sopra analizzate<sup>(11)</sup>.

Sulla base di tale presupposto, l'autorità competente potrà procedere alla raccolta a distanza, senza che si pongano problematiche attinenti all'utilizzabilità, di tutte le evidenze liberamente accessibili al pubblico in rete.

Secondo un'interpretazione nemmeno troppo estensiva della norma, la libera accessibilità deve infatti essere letta come un consenso preventivo del titolare del dato all'acquisizione dello stesso.

Ciò che rileva maggiormente, però, è che la circolazione della *digital evidence*, nel contesto transnazionale, necessita di linee guida certe onde evitare dubbi di sorta in relazione alla sua utilizzabilità concreta nello Stato di destinazione.

---

*e giustizia: alla ricerca di un equilibrio tra priorità repressive ed esigenze di garanzia*, Giuffrè, Milano, 2007, p. 708 ss.; A. COLAIOTTO, *La rilevanza delle best practices nell'acquisizione della digital evidence alla luce delle novelle sulla cooperazione giudiziaria*, in *Arch. pen.* 1/2019, p. 8 e ss.; L. BARTOLI, *Digital evidence for the criminal trial: limitless cloud and state boundaries*, in *Eurojus*, 2019, 96 ss.; R.E. KOSTORIS, *Gli organismi centralizzati della cooperazione giudiziaria*, in R.E. KOSTORIS (a cura di), *Procedura penale europea*, 5° ed., Milano, 2022, pp. 287-305; L. BACHMAIER WINTER (ed.), *The European Public Prosecutor's Office*, Cham, 2018.

(10) *Ibidem*, in senso difforme si veda R. MURENEC, *op. cit.*, p. 139 dove, invece, si legge «non determinerebbe nessuna invalidità delle prove raccolte, per converso, la mancata adozione delle Best Practices dell'informatica richieste a livello nazionale, il cui impiego è suscettibile, al più, di riverberarsi sull'affidabilità cognitiva delle prove ottenute».

(11) Sul punto si veda Cass. Pen., Sez. VI, n. 18907 del 20 aprile 2021, mediante la quale è stata dichiarata la piena validità processuale dell'acquisizione di conversazioni via *chat* scambiate tra telefoni del tipo *Blackberry* e protette da sistema *pin to pin*, decryptate grazie alla collaborazione volontaria del produttore del sistema operativo, avente sede all'estero, senza che siano state attivate le formalità procedurali della rogatoria internazionale.

Infine, appare preminente ritenere, come sia necessario che tutti gli Stati recepiscano la Direttiva (UE) 2023/1544 al fine di garantire regole comuni da seguire in materia di acquisizione delle prove digitali onde evitare problemi di sorta rendendo inoltre anche operativo il Regolamento (UE) 2023/1543.



## CAPITOLO I

### IL PERCORSO EVOLUTIVO VERSO LO “SPAZIO DI LIBERTÀ SICUREZZA E GIUSTIZIA”

#### 1. L'esigenza di cooperazione e assistenza giudiziaria e di polizia in materia penale. Il cammino verso lo “Spazio di libertà sicurezza e giustizia”

Nel settore penale all'interno dell'Unione Europea, la necessità di una collaborazione tra Stati, sia di tipo giudiziario che di polizia, si è manifestata fin dal conseguimento dei primi successi nell'ambito della costruzione comunitariae, più che mai, continua, indiscriminatamente, a manifestarsi oggi, atteso l'espandersi del crimine transnazionale.

Agli albori della Comunità Europea, era radicata la convinzione che il diritto penale non potesse in alcun modo rientrare tra le sue competenze essendo, la materia, di esclusivo compito di ciascuno Stato Membro<sup>(1)</sup>.

---

(1) Si veda *Commissione europea, Ottava relazione generale sull'attività delle Comunità europee nel 1974*, 11 febbraio 1975, par. 145, 90, nella quale la Commissione afferma che il diritto penale non rientra nelle competenze della Comunità, bensì “in quelle di ciascun Stato Membro” e rileva che, poiché le risorse proprie e le spese del bilancio comunitario non erano sottoposte alla legislazione nazionale, sarebbe stato opportuno redigere “*un progetto di convenzione relativo ai principi di applicazione del diritto nazionale, allo scopo di colmare tale lacuna*”. Ancora, il Parlamento europeo aveva evidenziato: “*The Community legislation, just like any other, should undoubtedly be enforced; this can only be achieved by a system of sanctions, whatever this system may be. It can be purely administrative, it can be based on civil law, but the best system would be one based on criminal law such as we have in all our national legal systems [...] For this we must also make use (although not exclusively) of provisions pertaining to criminal law*” (cfr. Parlamento europeo, *Report (doc. 531/76) on behalf of the Legal Affairs Committee on the relationship between Community law and criminal law*,

Nonostante l'assenza nei Trattati istitutivi di un qualunque riferimento al diritto penale, nell'erronea convinzione che lo *ius puniendi*, quale massima espressione della sovranità nazionale, potesse rimanere immune al processo di integrazione originariamente orientato ad obiettivi di carattere essenzialmente economico-commerciale, la materia penale ha, però, ben presto svelato la sua fisiologica permeabilità al processo di unificazione<sup>(2)</sup>.

Infatti, accanto agli effetti cosiddetti “riflessi” prodotti dal diritto comunitario sui sistemi penali degli Stati Membri<sup>(3)</sup>, l'istituzione della Comunità Europea, ed in particolare della Comunità economica<sup>(4)</sup>, aveva fatto emergere una serie di beni “istituzionali”, correlati all'esercizio delle competenze e dei poteri alle stesse demandate dai Trattati, nonché di beni “comunitari” derivanti dall'attività normativa delle Comunità,

---

in *Official Journal of the European Communities*, n. 212, febbraio 1977, 212. Il ricorso al diritto penale, infatti, era visto come strumento “to have the Community functioning effectively and [...] to command respect for the institutions and the way they operate, and at the same time guarantee the protection of the Communities' interests, and indirectly those of the states and in particular, those of the citizens, not only in order to uphold the important principle of the need to enforce the law, but also from the point of view of the principle of distributive justice”.

(2) Tale considerazione trova fondamento all'interno degli artt. 82 e 83 del TFUE, che regolano, rispettivamente, la cooperazione giudiziaria in materia penale nell'Unione, fondata sul principio di riconoscimento reciproco delle sentenze e delle decisioni giudiziarie, e la possibilità, per il Parlamento europeo e il Consiglio, di emanare direttive secondo la procedura legislativa ordinaria, al fine di stabilire norme minime relative alla definizione dei reati e delle sanzioni in sfere di criminalità particolarmente gravi e che presentino una dimensione transnazionale, derivante dal carattere o dalle implicazioni di tali reati, o da una particolare necessità di combatterli su basi comuni. Cfr. sul tema R. SICURELLA, “Eppur si muove”: alla ricerca di un nuovo equilibrio nella dialettica tra legislatore comunitario e legislatore nazionale per la tutela degli interessi dell'Unione europea, in G. GRASSO – R. SICURELLA (a cura di), *Per un rilancio del progetto europeo. Esigenze di tutela degli interessi comunitari e nuove strategie di integrazione penale*, Milano, Giuffrè, 2008, 192.

(3) Il fenomeno può essere ricollegato a diversi fattori. Un esempio lampante che induca a una perfetta comprensione di una (delle tante) ragioni sottostanti è, a mero titolo esemplificativo, la circostanza che, in numerosi settori della vita economica, la norma penale interviene in funzione sanzionatoria di discipline extra-penali, con la conseguenza che la diretta caducazione della regolamentazione nazionale da parte della normativa comunitaria renderà inapplicabili le connesse disposizioni incriminatrici. Sul tema si veda G. GRASSO, *Diritto penale dell'economia, normativa comunitaria e coordinamento delle disposizioni sanzionatorie nazionali*, in *Riv. Dir. Int. Priv. Proc.*, 1987, 227 ss.

(4) Il Trattato che istituisce la Comunità economica europea, firmato il 25 marzo del 1957, ha posto le basi per una cooperazione sovranazionale (inizialmente esclusivamente dedicata al settore economico) la quale ha dimostrato di essere ancor più radicata nelle menti degli Stati Membri all'affiancarsi dei successivi Trattati CEEA ed Euratom.

entrambinecessitanti della predisposizione di un’adeguata tutela contro le varie forme di aggressione cui venivano sottoposti<sup>(5)</sup>.

Infatti, non può non emergere con evidenza, come la realizzazione delle quattro libertà fondamentali – libera circolazione delle merci, dei capitali, dei servizi e delle persone – abbia comportato una crescita esponenziale della cosiddetta criminalità transnazionale.

Il venir meno delle frontiere interne e dei controlli ad esse inerenti, unitamente alla piena libertà di circolazione garantita dal Trattato se, da un lato, ha garantito un’indiscussa opportunità di incremento economico e di progresso sociale, dall’altro lato ha costituito un’occasione per le organizzazioni criminali di sfruttare a proprio profitto la liberalizzazione dei mercati e dei movimenti di persone, capitali, merci e servizi.

Proprio in tale contesto è maturata l’indubbia necessità di adottare rimedi e presidi tali da arginare le nuove opportunità criminali.

Esigenza, questa, che è stata affrontata attraverso la proliferata e caotica emanazione di provvedimenti adottati in una prospettiva unicamente repressiva. Ed è proprio all’emergere di tali problematiche, che il diritto penale e il diritto processuale sono stati ‘europeizzati’.

In questo scenario di progressivo aumento degli strumenti volti ad assicurare le esigenze di collaborazione transfrontaliera e di una conseguente, progressiva, europeizzazione delle indagini, degli atti e dei dati, spesso le garanzie e i diritti dell’individuo sono rimaste, tuttavia, circoscritte entro i confini del territorio nazionale<sup>(6)</sup>.

L’obiettivo che l’Unione Europea si è prefissata e che merita, indubbiamente, di essere perseguito e raggiunto, è quello di conservare e sviluppare in tutto il suo ambito territoriale uno spazio di libertà, sicurezza e giustizia.

---

(5) Si pensi, ad esempio, alla disciplina della concorrenza, alla tutela dell’ambiente, alla lotta all’immigrazione clandestina o alla tutela del mercato europeo dei capitali. Sul tema, *ex multis*, G. GRASSO, *Comunità europee e diritto penale. I rapporti tra l’ordinamento comunitario e i sistemi penali degli Stati Membri*, Milano, Giuffrè, 1989, 9 ss.; L. PICOTTI, *Diritto penale comunitario e Costituzione europea*, in S. CANESTRARI – L. FOFFANI (a cura di), *Il diritto penale nella prospettiva europea. Quali politiche criminali per quale Europa*, Milano, Giuffrè, 2005, 332 ss.; R. SICURELLA, *Diritto penale e competenze dell’Unione europea; linee guida per un sistema integrato di tutela dei beni giuridici sopranazionali e dei beni giuridici di interesse comune*, Milano, Giuffrè, 2005, 324 ss.

(6) Laddove non siano stati, addirittura, compromessi quale effetto, ad esempio, dell’introduzione anche nel settore penale del principio del mutuo riconoscimento.

Le perplessità e i dubbi nascono, però, allorquando si analizzano gli attuali modi e mezzi di attuazione dello spazio citato.

O meglio, nascono ancor prima dal momento in cui ci si scontra con la constatazione della difficoltà del raggiungimento di una disciplina che possa essere definita realmente “comune” a tutti gli Stati parte del territorio dell’Unione.

Il processo di “penalizzazione” del diritto dell’Unione Europea sembra percorrere, infatti, una strada ancora in salita, irta di ostacoli, incertezze ed opposizioni, *in primis* da parte delle stesse autorità nazionali.

È vero, infatti, che se l’evoluzione della cooperazione giudiziaria in materia penale<sup>(7)</sup> ha certamente dato prova, in più occasioni, del fatto che esiste una concreta e reale volontà degli Stati di raggiungere uno spazio comune in cui possano vigere regole e strumenti comuni allo scopo di una maggiore sicurezza all’interno del territorio europeo è, però, altrettanto vero che è mancato un ruolo attivo, forte in questo senso da parte degli Stati.

Ciò ha fatto sì che, nonostante gli evidenti passi avanti riscontrabili alla luce delle novità legislative (e in un certo senso politiche) emerse nel corso dell’evoluzione di questo settore, ancora non si possa affermare, con assoluta certezza, di essere arrivati ad un livello di collaborazione “sufficiente” a contrastare i fenomeni – sempre più frequenti – di criminalità transnazionale.

Ciò premesso, pare imprescindibile procedere ad uno sguardo di insieme che ne ripercorra, seppur brevemente, le singole tappe di evoluzione, anche al fine di comprendere e contestualizzare le concrete risposte che nel corso degli anni sono state poste in essere per fronteggiare il dilagare dei fenomeni di criminalità transazionale.

---

(7) Come si è già avuto modo di precisare nella parte introduttiva del lavoro, nonostante all’interno delle discipline europee spesso si ritrovi l’utilizzo improprio del termine “cooperazione giudiziaria”, si ribadisce che, da un punto di vista prettamente tecnico, è possibile riferirsi al lemma “cooperazione” solo con riferimento all’utilizzo di strumenti di mutuo riconoscimento. Le altre attività, pertanto, devono essere più correttamente ricondotte al concetto di “assistenza” giudiziaria. Effettuata tale doverosa precisazione, si premette che all’interno del presente lavoro il termine “cooperazione” verrà utilizzato anche nel suo significato a-tecnico.