RIVISTA ITALIANA
DI INFORMATICA E DIRITTO
Periodico internazionale di diritto, giustizia e tecnologie

ISSN 2704-7318 • n. 1/2026 • DOI 10.32091/RIID0281 • articolo sottoposto a peer review • pubblicato in anteprima il 6 lug. 2026

Denise Boriero

Il sequestro di dispositivi e informazioni digitali

Il contributo analizza il sequestro di dispositivi e informazioni digitali nel processo penale, evidenziando le tensioni tra esigenze investigative e tutela dei diritti fondamentali. La crescente centralità degli strumenti informatici ha reso smartphone, computer e account digitali depositi di una vasta quantità di dati personali e comunicativi, mettendo in crisi le tradizionali categorie del sequestro, poiché l'oggetto dell'acquisizione è sempre più il contenuto informativo anziché il supporto materiale. L'elaborato approfondisce le caratteristiche del dato digitale e le modalità di acquisizione della prova informatica, con particolare attenzione alle garanzie di autenticità, integrità e tracciabilità del dato. Vengono inoltre esaminati il quadro normativo nazionale, europeo e sovranazionale nonché il ruolo della giurisprudenza nell'affermazione dei principi di proporzionalità, pertinenza e minimizzazione delle acquisizioni digitali, in una prospettiva di equilibrio tra efficacia investigativa, diritto di difesa e tutela della riservatezza.

Prova digitale – Sequestro informatico – Investigazioni digitali – Digital forensics – Digital due process

The seizure of digital devices and electronic information

This paper examines the seizure of digital devices and digital information in criminal proceedings, highlighting the tensions between investigative needs and the protection of fundamental rights. The growing centrality of digital technologies has transformed smartphones, computers, and online accounts into repositories of vast amounts of personal and communicative data, challenging traditional concepts of seizure, as the true object of acquisition is increasingly the informational content rather than the physical device itself. The study explores the distinctive features of digital data and the methods used to acquire digital evidence, with particular attention to the requirements of authenticity, integrity, and traceability. It also analyzes the national, European, and supranational legal frameworks governing digital investigations, as well as the role of case law in shaping the principles of proportionality, relevance, and data minimization in digital seizures. The analysis ultimately focuses on achieving a balance between investigative effectiveness, the right to defense, and the protection of privacy.

Digital evidence – Digital seizure – Digital investigations – Digital forensics – Digital due process

L'Autrice è Membro del Centro di Scienze della Criminalità e della Sicurezza dell'Università di Trento e di Verona; Dottoranda del Corso di Studi sulla Criminalità Organizzata dell'Università degli Studi di Milano

Questo contributo fa parte della sezione monografica *Transizione digitale e criminalità: prospettive evolutive tra categorie sostanziali e law enforcement – Parte 2,* a cura di Gaetana Morgante e Gaia Fiorinelli

Sommario: 1. Introduzione. Il sequestro della prova digitale: evoluzione tecnologica e crisi delle categorie tradizionali. – 2. Il dispositivo digitale tra supporto materiale e contenuto informativo. – 3. La nozione di informazione digitale e la complessità del dato informatico. – 4. Il sequestro digitale nel quadro delle investigazioni informatiche. – 4.1. Il sequestro probatorio di dispositivi e informazioni digitali. – 4.2. Sequestro preventivo di dispositivi e informazioni digitali. – 4.3. Sequestro conservativo di dispositivi digitali. – 5. Fasi operative del sequestro informatico e acquisizione dei dati digitali. – 6. Garanzie difensive e diritti fondamentali. – 7. Conclusioni.

1. Introduzione. Il sequestro della prova digitale: evoluzione tecnologica e crisi delle categorie tradizionali

Il sequestro di dispositivi e informazioni digitali costituisce oggi una delle principali aree di frizione tra esigenze investigative e tutela dei diritti fondamentali nel processo penale. La centralità assunta dagli strumenti informatici nella vita personale e professionale dell'individuo ha infatti trasformato smartphone, computer e account digitali in contenitori di una quantità estremamente ampia ed eterogenea di dati, spesso idonei a ricostruire in modo particolarmente penetrante abitudini, relazioni, spostamenti, comunicazioni e attività economiche del soggetto sottoposto a indagine.

In tale contesto, l'applicazione delle tradizionali categorie del sequestro evidenzia significative criticità. Con riferimento al sequestro probatorio, ad esempio, l'apprensione del supporto materiale non coincide più necessariamente con l'acquisizione della prova, mentre la distinzione tra "cosa" e "dato" tende progressivamente a sfumare. Il dispositivo digitale non costituisce, infatti, soltanto un bene materiale suscettibile di vincolo, ma soprattutto un punto di accesso a una pluralità di contenuti informativi autonomamente rilevanti sul piano probatorio.

Tale peculiarità incide direttamente sui presupposti di legittimità e sulle modalità esecutive del vincolo ablatorio. Diversamente dal sequestro tradizionale, l'acquisizione di dispositivi informatici pone problemi di selezione del materiale rilevante, di delimitazione dell'oggetto del vincolo e, soprattutto, di proporzionalità dell'ingerenza investigativa. La possibilità tecnica di estrarre integralmente il contenuto di un dispositivo comporta il rischio di acquisizioni generalizzate di dati non pertinenti rispetto al fatto oggetto di indagine, con conseguente incidenza sulla riservatezza e sulla segretezza delle comunicazioni.

La giurisprudenza nazionale ed europea più recente ha progressivamente evidenziato la necessità di distinguere tra il sequestro del "contenitore" materiale, del supporto, e l'acquisizione del contenuto informativo, valorizzando i criteri di pertinenza e proporzionalità nella selezione dei dati rilevanti. In particolare, il dibattito si è concentrato sul tema delle acquisizioni massive, delle copie forensi integrali e delle garanzie procedurali necessarie a evitare forme di ricerca meramente esplorativa incompatibili con i principi del giusto processo.

Ulteriori criticità emergono con riferimento ai dati conservati in ambiente remoto e ai servizi cloud, rispetto ai quali la tradizionale dimensione territoriale del sequestro mostra evidenti limiti applicativi. La dissociazione tra disponibilità materiale del dispositivo e localizzazione effettiva del dato impone infatti di confrontarsi con problematiche di giurisdizione, cooperazione internazionale e rapporti con i fornitori di servizi digitali, evidenziando altresì una crescente interazione tra soggetti pubblici e operatori privati nella gestione, conservazione e acquisizione delle informazioni. Ne deriva una progressiva ibridazione delle tradizionali categorie pubblicistiche

dell'attività investigativa, in un quadro normativo ancora frammentario e non pienamente coordinato.

L'analisi del sequestro di dispositivi e informazioni digitali impone dunque di verificare se gli strumenti processuali vigenti siano effettivamente idonei a governare le peculiarità della prova informatica o se, al contrario, l'evoluzione tecnologica richieda una più profonda revisione delle categorie tradizionali dei mezzi di ricerca della prova.

2. Il dispositivo digitale tra supporto materiale e contenuto informativo

Prima di affrontare le problematiche concernenti il sequestro della prova digitale, occorre svolgere una precisazione preliminare rispetto alla nozione di "dispositivo digitale". Sotto il profilo strettamente tecnico, infatti, il concetto non presenta particolari difficoltà definitorie, riferendosi comunemente a qualsiasi apparato elettronico idoneo alla memorizzazione, elaborazione o trasmissione di dati informatici, quali computer, smartphone, tablet, hard disk, server o ulteriori supporti di memoria digitale.

La vera complessità emerge tuttavia sul piano giuridico-processuale e concerne la necessità di distinguere – come anticipato – il dispositivo quale bene materiale dal contenuto informativo in esso conservato o accessibile per il suo tramite. In tale prospettiva, il sequestro del bene assume carattere meramente strumentale rispetto alla reale finalità investigativa, consistente nell'acquisizione del dato digitale. Ne deriva la necessità di delimitare con particolare rigore l'attività investigativa ai soli dati pertinenti all'accertamento del fatto, in applicazione dei principi di pertinenza e proporzionalità, considerata la potenziale estensione illimitata dell'accesso alle informazioni contenute nel dispositivo.

Il rischio è, infatti, quello di determinare una compressione eccessiva dei diritti fondamentali dell'interessato, unitamente a una indebita estensione del potere investigativo.

Proprio in ragione di tali criticità, la giurisprudenza ha progressivamente evidenziato la necessità di evitare forme di sequestro esplorativo prive di adeguata delimitazione dell'oggetto della ricerca, andando a redigere vere e proprie linee guida sulle perquisizioni e sui sequestri digitali[1]. In particolare, si richiede che, a seguito dell'apprensione del dispositivo, venga immediatamente effettuata una copia integrale del contenuto, con successiva restituzione del bene all'avente diritto e analisi dei dati secondo criteri di pertinenza e proporzionalità rispetto al capo d'imputazione.

In tale contesto, la Corte di Cassazione ha talvolta utilizzato la nozione di "copia mezzo", quale strumento funzionale alla separazione tra acquisizione e analisi del dato.

Il provvedimento di sequestro deve inoltre essere sorretto da una motivazione rafforzata, idonea a dar conto sia del nesso di pertinenza tra l'ipotesi di reato e il bene oggetto di vincolo, sia delle specifiche operazioni tecniche da eseguire e della loro durata.

La necessità della duplicazione integrale risponde altresì all'esigenza di preservare l'integrità della prova informatica. Il dato digitale, infatti, presenta caratteristiche ontologicamente differenti rispetto alla prova documentale tradizionale, essendo connotato da volatilità, immaterialità e suscettibilità di alterazione anche in assenza di modificazioni del supporto fisico. Ne deriva l'importanza centrale delle tecniche di copia forense e delle procedure idonee a garantire autenticità, immodificabilità e tracciabilità dell'acquisizione.

Ulteriori complessità derivano dalla frequente dissociazione tra disponibilità del dispositivo e localizzazione effettiva del dato, che talvolta rende difficoltosa – se non impossibile – l'individuazione del luogo di conservazione dell'informazione e del soggetto che ne detiene il controllo. Tale fenomeno impone, inoltre, forme sempre più strette di cooperazione tra autorità pubbliche e operatori privati, atteso che le infrastrutture di archiviazione e gestione dei dati sono spesso affidate a provider e servizi cloud.

In definitiva, non soltanto la categoria della prova digitale risulta in tensione con gli schemi tradizionali, in quanto solo parzialmente riconducibile alle categorie probatorie classiche, ma più in generale è l'intero impianto concettuale del diritto penale sostanziale e processuale ad essere sottoposto a una progressiva rielaborazione[2]. Ne risultano investite categorie fondamentali quali la competenza, la territorialità, la nozione stessa

1. Cass., Sez. VI, 22 settembre 2020 (dep. 2 dicembre 2020), n. 34265. Per un commento, si veda Pittiruti 2021.
2. Si veda, tra molti, Daniele 2011.

di fatto penalmente rilevante e le coordinate tradizionali di imputazione e accertamento, le quali mostrano crescenti difficoltà di adattamento rispetto a fenomeni caratterizzati da immaterialità, distribuzione transnazionale dei dati e immediata replicabilità delle informazioni digitali[3].

3. La nozione di informazione digitale e la complessità del dato informatico

Un ulteriore profilo preliminare concerne la definizione di "informazione digitale", categoria che costituisce il reale oggetto delle moderne investigazioni informatiche e che, proprio per la sua ampiezza e mutevolezza, presenta rilevanti difficoltà di sistematizzazione sul piano giuridico.

Per informazione digitale deve intendersi, in senso ampio, qualsiasi contenuto informativo rappresentato in forma binaria e generato, elaborato, trasmesso o conservato mediante sistemi informatici o telematici, indipendentemente dalla sua immediata percepibilità da parte dell'utente e dalla modalità con cui esso viene reso accessibile attraverso dispositivi o interfacce digitali.

In tale prospettiva si colloca la definizione elaborata dalla Convenzione di Budapest del Consiglio d'Europa del 2001 sulla criminalità informatica (c.d. Convenzione sul cybercrime), che, all'art. 1 lett. b) qualifica il dato informatico come "qualunque presentazione di fatti, informazioni o concetti in forma suscettibile di essere utilizzata in un sistema computerizzato, incluso un programma in grado di consentire ad un sistema computerizzato di svolgere una funzione".

Ne emerge sin da subito come tale categoria sia connotata da una significativa stratificazione interna, che eccede la sola dimensione del contenuto immediatamente fruibile. Accanto alle informazioni immediatamente percepibili – quali testi, immagini, file audio e video o comunicazioni elettroniche – assumono infatti crescente rilievo ulteriori livelli informativi, spesso non visibili all'utente ma dotati di significativa attitudine probatoria.

In primo luogo, si evidenziano i metadati, ossia dati relativi ad altri dati, i quali accompagnano ogni operazione digitale e consentono la ricostruzione di elementi essenziali quali la data di creazione o modifica di un file, il dispositivo utilizzato, le coordinate di geolocalizzazione o le modalità di accesso. In secondo luogo, assumono rilievo i log di accesso, vale a dire le tracce informatiche che registrano le interazioni tra utente e sistema, permettendo di individuare accessi, autenticazioni e attività svolte all'interno di piattaforme digitali.

Ulteriori profili informativi sono rappresentati dalle informazioni di sistema, comprendenti dati relativi al funzionamento del dispositivo, alle reti alle quali esso si è connesso, agli indirizzi IP utilizzati e alle configurazioni hardware e software. Infine, un ruolo sempre più significativo è svolto dai dati di traffico telematico, i quali consentono di ricostruire flussi comunicativi, tempi, destinatari e modalità delle interazioni digitali.

Tali informazioni sono suscettibili di sequestro nell'ambito delle indagini penali.

Sotto il profilo classificatorio, i dati informatici possono essere ricondotti a una duplice direttrice sistematica[4].

In prima battuta, sul piano tecnico-operativo, è possibile distinguere tra:

- *stored data*, ossia i dati memorizzati stabilmente all'interno di un sistema informatico o di un supporto digitale;
- *data in transit*, vale a dire i dati in fase di trasmissione tra sistemi informatici attraverso reti di comunicazione.

In seconda battuta, sul piano del contenuto e della funzione informativa, si distinguono:

- *traffic data* (dati di traffico), da intendersi come i dati informatici definiti dalla convenzione sopra citata;
- *personal data* (dati personali), intesi, ai sensi dell'art. 3, n. 1, della direttiva (UE) 2016/680, come "qualsiasi informazione riguardante

3. Per un quadro generale sulle tensioni tra le categorie classiche del diritto penale sostanziale e processuale con riferimento ai reati informatici si veda Ruggieri–Picotti 2011. Per approfondire il tema del *locus commissi delicti* con riferimento ai reati informatici, si veda ad esempio Corona 2021 e Aterno 2023. In tema di legge penale nello spazio, si veda ad esempio Flor 2019; per la letteratura straniera Kobrin 2001. Sulle esigenze relative alle garanzie, si rimanda invece, *ex multis*, a Centorame 2025, Dinacci 2025, Flor 2023, Flor–Panattoni 2023, Flor–Marcolini 2022.

4. Per un approfondimento Flor 2025.

una persona fisica identificata o identificabile" direttamente o indirettamente, "in particolare con riferimento ad un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici dell'identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale di tale persona fisica";

– *content data* (dati di contenuto), i quali attengono al contenuto sostanziale delle comunicazioni e delle interazioni digitali, comprendendo tutte le informazioni trasmesse mediante sistemi informatici e telematici. In tale categoria rientrano, tra gli altri, messaggi di testo, comunicazioni vocali, immagini, contenuti audio e video, nonché ulteriori forme di corrispondenza elettronica, secondo una nozione ormai consolidata anche nelle più recenti fonti internazionali in materia di criminalità informatica.

Come già evidenziato, tali informazioni presentano una intrinseca volatilità, essendo la loro esistenza strettamente connessa ai sistemi che le generano e le conservano. Esse possono essere alterate, sovrascritte o cancellate anche in assenza di modificazioni percepibili del supporto fisico e risultano spesso accessibili esclusivamente mediante infrastrutture tecnologiche esterne e dinamiche. Ne deriva che l'informazione digitale si configura come un fenomeno non soltanto complesso e stratificato, ma altresì strutturalmente instabile, la cui acquisizione e conservazione richiedono specifiche cautele tecniche e giuridiche.

A corollario delle investigazioni digitali emerge quindi la disciplina della *digital forensics*, la quale, mediante l'impiego di protocolli tecnici standardizzati e procedure di acquisizione controllata, consente la corretta cristallizzazione e conservazione delle tracce informatiche, garantendo che il dato acquisito mantenga piena integrità, autenticità e non alterazione rispetto al contenuto originario.

Accanto ai profili di complessità tecnica e volatilità del dato, spicca infine il carattere fortemente intrusivo del sequestro di informazioni digitali. La peculiare capacità ricostruttiva dei dati informatici consente infatti l'accesso ad una quantità estremamente ampia e dettagliata di informazioni, tale da distinguere il sequestro digitale dalle tradizionali forme di apprensione. Ne deriva un significativo ampliamento della capacità di penetrazione dell'attività investigativa nella sfera privata del soggetto interessato, con la conseguente necessità di un rigoroso bilanciamento tra esigenze di accertamento penale e tutela dei diritti fondamentali della persona.

4. Il sequestro digitale nel quadro delle investigazioni informatiche

Le considerazioni sin qui svolte consentono di comprendere come il sequestro digitale si collochi all'interno di un contesto investigativo profondamente diverso rispetto a quello cui erano originariamente rivolte le tradizionali categorie processual-penalistiche. Le investigazioni digitali, infatti, come evidenziato, si sviluppano in un ambiente caratterizzato da velocità, mutevolezza, volatilità e ubiquità del dato informatico, nel quale le informazioni risultano potenzialmente illimitate, immediatamente replicabili e spesso dislocate in infrastrutture tecnologiche transnazionali.

Parallelamente, l'evoluzione delle forme di criminalità contemporanea, sempre più caratterizzate dall'utilizzo di tecnologie di comunicazione avanzate, sistemi crittografici, piattaforme decentralizzate e strumenti di anonimizzazione, ha ulteriormente accentuato la centralità della prova digitale e delle tecniche di acquisizione informatica[5]. In tale contesto, il rischio è che l'attività di ricerca della prova finisca per trasformarsi, ove non adeguatamente delimitata, in una più ampia e indistinta attività di ricerca di notizie di reato, mediante forme di acquisizione massiva e indiscriminata di dati personali e comunicativi. La particolare capacità espansiva delle investigazioni digitali impone pertanto di interrogarsi sui limiti del potere investigativo e sulle garanzie necessarie a evitare indebite compressioni dei diritti fondamentali dell'individuo.

La difficoltà del diritto positivo di adattarsi con rapidità all'evoluzione tecnologica ha determinato, in questo settore, una significativa distanza tra innovazione tecnica e regolamentazione normativa. Le investigazioni digitali risultano infatti regolate da un sistema multilivello, composto da fonti interne, sovranazionali e convenzionali, la cui effettività

5. In rete e grazie alla rete non si sono sviluppate soltanto nuove forme di criminalità, ma si sono trasformate anche quelle tradizionali, comprese le organizzazioni mafiose; sul punto v. Picarella 2025.

è stata progressivamente integrata dall'elaborazione giurisprudenziale nazionale ed europea.

La limitata tipizzazione normativa degli strumenti di indagine informatica ha comportato l'attribuzione alla giurisprudenza di un ruolo centrale nella definizione dei limiti e delle modalità di esercizio dei poteri investigativi[6]. È stata infatti la prassi applicativa, insieme agli orientamenti delle corti nazionali e sovranazionali, a confrontarsi con l'impatto delle investigazioni digitali sui principi costituzionali, contribuendo all'adattamento degli strumenti tradizionali di ricerca della prova alle esigenze di contrasto alla criminalità tecnologica.

In tale prospettiva, il quadro normativo e giurisprudenziale si è sviluppato attorno a profili essenziali: le modalità di acquisizione e utilizzabilità della prova digitale, i limiti di ammissibilità delle tecniche investigative alla luce dei diritti fondamentali, le regole di conservazione e autenticazione del dato informatico, le problematiche della cooperazione internazionale e dell'acquisizione transfrontaliera delle prove, nonché le garanzie difensive e i poteri concretamente esercitabili dalla polizia giudiziaria nelle indagini informatiche.

L'assenza di una disciplina organica ha inoltre determinato l'adattamento dei tradizionali mezzi di ricerca della prova all'ambiente digitale. Perquisizioni, ispezioni, sequestri e attività di osservazione sono stati progressivamente reinterpretati alla luce delle peculiarità del contesto informatico, subendo significative trasformazioni funzionali e operative. Ne è derivato un ampliamento rilevante della capacità conoscitiva dell'autorità investigativa, che incide non solo sulle modalità di esecuzione degli atti, ma talvolta sulla loro stessa natura sostanziale.

Sul piano normativo interno, il principale riferimento resta la disciplina del sequestro probatorio di cui all'art. 253 c.p.p., ai sensi del quale (comma 1) "l'autorità giudiziaria dispone con decreto motivato il sequestro del corpo del reato e delle cose pertinenti al reato necessarie per l'accertamento dei fatti". Tale disposizione, concepita in relazione a beni materiali, è stata progressivamente estesa in via interpretativa anche a dispositivi digitali e dati informatici, evidenziando una tensione tra categorie tradizionali e realtà tecnologica[7].

In tale evoluzione si manifesta una delle principali criticità sistematiche della materia: nel sequestro digitale l'oggetto effettivo dell'attività investigativa non coincide più necessariamente con il supporto materiale, bensì con i dati in esso contenuti o accessibili tramite esso, con conseguente degradazione del bene fisico a mero strumento di accesso all'informazione.

A ciò si affiancano le innovazioni introdotte dalla legge 18 marzo 2008, n. 48, di ratifica della Convenzione di Budapest sul cybercrime[8], che ha inserito specifiche disposizioni relative ai sistemi informatici e telematici. Emerge, in particolare, l'art. 247, comma 1-*bis*, c.p.p., che disciplina la perquisizione di sistemi informatici mediante misure tecniche idonee a garantire la conservazione dei dati e la loro immodificabilità, nonché l'art. 254-*bis* c.p.p., relativo al sequestro di dati presso fornitori di servizi informatici, telematici e di telecomunicazioni, volto a regolare l'acquisizione di informazioni detenute da provider e operatori delle comunicazioni.

Il quadro è stato ulteriormente rafforzato dalla legge 28 giugno 2024, n. 90 in materia di cybersicurezza nazionale e reati informatici, che ha inciso su diversi profili processuali, ampliando il catalogo dei reati rilevanti e intervenendo su competenze, durata delle indagini e poteri di coordinamento

6. Si segnala la recentissima pronuncia della quinta sezione penale della Suprema Corte di fine aprile 2026 che, intervenendo sul tema del sequestro probatorio di dispositivi informatici e asset digitali, ha dichiarato illegittimo il sequestro che si traduce in un'acquisizione indiscriminata del patrimonio digitale del soggetto sottoposto ad indagini, in mancanza di criteri selettivi previamente determinati e di termini per la restituzione del materiale non pertinente.
7. Si ricorda che la prima giurisprudenza in materia di reti informatici riconosceva nel software un bene materiale, una res incorporata nel supporto materiale, al fine di poter applicare anche ad esso la disciplina codicistica. Solo successivamente, con l'emersione della dimensione reticolare e dematerializzata dell'informazione digitale, si è progressivamente affermata una concezione autonoma del dato informatico quale entità immateriale ma giuridicamente rilevante, suscettibile di tutela e apprensione indipendentemente dal supporto che lo contiene.
8. Consiglio d'Europa, Convenzione di Budapest sulla criminalità informatica, 23 novembre 2001. Sul punto, si veda Lupària 2009.

investigativo, oltre a introdurre discipline derogatorie in materia di intercettazioni per reati contro sistemi informatici di rilievo strategico[9].

In questa traiettoria si colloca anche il recente disegno di legge[10] volto all'introduzione dell'art. 254-*ter* c.p.p., finalizzato a rafforzare le garanzie di tutela della riservatezza mediante un obbligo di selezione rigorosa dei soli dati pertinenti, secondo criteri di necessità e proporzionalità.

Un ulteriore profilo rilevante attiene al rapporto con la disciplina europea in materia di protezione dei dati personali. In aggiunta, la Direttiva LED[11], attuata con il d.lgs. n. 51/2018, ha contribuito a definire un sistema fondato sui principi di proporzionalità, necessità e minimizzazione del trattamento, costituendo un parametro imprescindibile per la conformazione delle investigazioni digitali.

Le investigazioni informatiche si collocano, inoltre, in un contesto multilivello nel quale il diritto dell'Unione europea incide in modo significativo sull'equilibrio tra efficacia investigativa e tutela dei diritti fondamentali. Oltre alla Direttiva 2016/680 già citata, si sottolineano la Direttiva PNR[12] e l'AI Act[13], destinato a incidere anche sull'impiego di sistemi di intelligenza artificiale nelle attività investigative, unitamente alla disciplina sulla cooperazione giudiziaria e alla regolazione dei rapporti con i fornitori di servizi digitali.

Sul piano sovranazionale, assumono rilievo gli strumenti elaborati dalle Nazioni Unite, in particolare le Convenzioni di Palermo[14] e di Mérida[15], che disciplinano tecniche investigative speciali nel contrasto alla criminalità organizzata e alla corruzione. La recente Convenzione ONU sulla criminalità informatica[16] ha inoltre introdotto specifiche disposizioni in materia di perquisizione e sequestro di dati elettronici, intercettazione e raccolta in tempo reale dei dati di traffico, richiamando il rispetto dei diritti umani e del principio di proporzionalità.

Un ruolo centrale continua a essere svolto dal Consiglio d'Europa attraverso la Convenzione di Budapest[17], primo strumento internazionale organico in materia di criminalità informatica, successivamente integrato dal Secondo Protocollo addizionale, volto a rafforzare la cooperazione internazionale e l'acquisizione transfrontaliera delle prove digitali.

4.1. Il sequestro probatorio di dispositivi e informazioni digitali

Con riferimento a quanto già illustrato nei paragrafi precedenti, le principali forme di sequestro

9. Nel complesso, la materia delle investigazioni digitali è stata interessata da molteplici e successivi interventi normativi che hanno inciso su diversi istituti del codice di procedura penale, determinando una profonda riorganizzazione del sistema delle garanzie e degli strumenti investigativi in ambito informatico. Tra questi, si segnala in particolare la disciplina del captatore informatico, oggetto di ripetute riforme (d.lgs. n. 216/2017, l. n. 3/2019, l. n. 7/2020 e l. n. 137/2023). Tali profili, per la loro complessità e ampiezza, non possono essere qui approfonditi, ma vengono richiamati solo in via generale in considerazione della loro rilevanza sistematica all'interno dell'evoluzione della disciplina delle investigazioni digitali.
10. Disegno di Legge (ddl) n. 806, noto come ddl Zanettin–Bongiorno. Per un approfondimento sulle novità proposte in materia di sequestro di dispositivi e di dati si vedano Della Torre 2025 e Caianiello 2025.
11. Direttiva (UE) 2016/680 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 o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati (c.d. Law Enforcement Directive).
12. Direttiva (UE) 2016/681 sull'uso dei dati del codice di prenotazione (Passenger Name Record – PNR) a fini di prevenzione, accertamento, indagine e azione penale nei confronti dei reati di terrorismo e dei reati gravi.
13. Regolamento (UE) 2024/1689 del 13 giugno 2024 che stabilisce regole armonizzate sull'intelligenza artificiale (Artificial Intelligence Act).
14. Convenzione delle Nazioni Unite contro la criminalità organizzata transnazionale, 15 novembre 2000.
15. Convenzione delle Nazioni Unite contro la corruzione, 31 ottobre 2003.
16. Assemblea generale delle Nazioni Unite, Convenzione ONU sulla criminalità informatica, adottata il 24 dicembre 2024.
17. Cfr. nota 8.

rilevanti nell'ambito delle investigazioni digitali riconducono al sequestro probatorio, disciplinato dal codice di procedura penale e tradizionalmente configurato come uno dei mezzi di ricerca della prova maggiormente significativi nelle indagini informatiche palesi[18]. È proprio la citata dissociazione tra supporto fisico e dato digitale a rappresentare uno degli elementi di maggiore discontinuità rispetto alle tradizionali categorie del sequestro probatorio.

In ambito informatico, inoltre, il sequestro può avere ad oggetto una pluralità eterogenea di elementi – proprio alla luce della complessa natura del dato – quali siti web, infrastrutture di rete, dispositivi digitali o singole porzioni di dati[19]. Rientrano in tale prospettiva anche misure incidenti sull'accessibilità delle risorse online, quali l'oscuramento di siti Internet, il sequestro di server contenenti materiale illecito o il blocco di account utilizzati per la commissione di attività fraudolente.

Particolare attenzione è riservata dall'ordinamento alla tutela dell'integrità della prova digitale. In tale direzione si colloca l'art. 260, comma 2, c.p.p., il quale prevede che, quando il sequestro abbia ad oggetto dati, informazioni o programmi informatici, la loro duplicazione debba avvenire mediante copie su adeguati supporti, secondo procedure idonee a garantirne la conformità all'originale e l'immodificabilità. La disposizione recepisce le esigenze proprie della *digital forensics*, imponendo l'impiego di tecniche di copia forense e di sistemi di conservazione volti a preservare la genuinità e l'affidabilità del dato acquisito.

Il sequestro può essere disposto dal pubblico ministero o dal giudice e viene generalmente eseguito dalla polizia giudiziaria specializzata, anche mediante strumenti tecnici quali la duplicazione forense dei supporti, la cifratura dei dati o misure di inibizione dell'accesso a risorse online, tra cui il DNS blocking o il blocco degli indirizzi IP.

Completa il quadro il rilievo assunto dai principi elaborati dalla giurisprudenza, che – anche in materia di sequestro probatorio – impongono costantemente il rispetto dei criteri di proporzionalità, pertinenza e adeguata motivazione del provvedimento ablatorio, a garanzia dell'equilibrio tra esigenze investigative e tutela dei diritti fondamentali.

4.2. Sequestro preventivo di dispositivi e informazioni digitali

Accanto al sequestro probatorio, l'ordinamento prevede il sequestro preventivo, disciplinato dall'art. 321 c.p.p., configurabile come misura cautelare reale finalizzata a impedire la protrazione o l'aggravamento delle conseguenze del reato, ovvero la commissione di ulteriori illeciti. Nell'ambito delle investigazioni digitali, tale istituto assume particolare rilievo quando dispositivi informatici quali computer, smartphone, tablet o server risultano funzionalmente connessi alla realizzazione dell'attività criminosa o idonei a consentirne la continuazione.

A differenza del sequestro probatorio, che è strumentale all'acquisizione della prova, il sequestro preventivo è caratterizzato da una finalità eminentemente cautelare: esso non è diretto all'accertamento del fatto, bensì alla neutralizzazione del pericolo derivante dalla libera disponibilità del bene. In ambito digitale, ciò si traduce nell'esigenza di impedire l'accesso a dati sensibili, la prosecuzione di attività fraudolente, la diffusione di contenuti illeciti o l'utilizzo del dispositivo come strumento operativo per la commissione di nuovi reati.

Il sequestro preventivo di dispositivi informatici può riguardare l'intero bene oppure specifiche funzionalità o contenuti, sebbene nella prassi l'apprensione materiale del dispositivo rappresenti la modalità più frequente. Tale soluzione è spesso giustificata dall'esigenza di impedire immediatamente qualsiasi utilizzo del sistema informatico, soprattutto nei casi in cui esso risulti strettamente funzionale all'attività illecita, come nelle ipotesi di

18. Accanto a queste, si apre il mondo delle investigazioni digitali occulte, quale, ad esempio, l'utilizzo del captatore informatico. Tra i numerosi contributi su questo strumento, si vedano, ad esempio, Torre 2017 e Maggio 2021. Per uno studio sulle investigazioni digitali, si rimanda a Nicolini 2026, Signorato 2024, Torre 2024, Nocerino 2021, Marcolini 2015, Rivello 2014, Lupária–Ziccardi 2007 e Marinelli 2007. Un approfondimento, invece, sulle perquisizioni online si può rinvenire in Marcolini 2010.
19. Per un approfondimento sul sequestro di dispositivi digitali si rimanda, *ex multis*, a Lorenzetto 2025, Signorato 2025, Gramuglia 2021, Campanaro 2012, Vitkov 2012, Bettoni 2012 e Aterno 2008.

truffe online, cyberstalking, accessi abusivi a sistemi informatici o diffusione di materiale illecito.

Il provvedimento richiede la sussistenza dei presupposti tipici delle misure cautelari reali, ossia il *fumus commissi delicti* e il p*ericulum in mora*[20]. Quest'ultimo assume nel contesto digitale una particolare rilevanza, potendo consistere nel rischio di alterazione, cancellazione o dispersione dei dati, nella prosecuzione dell'attività illecita tramite il dispositivo ovvero nella compromissione dell'efficacia delle indagini in corso. Ne consegue che il sequestro deve essere sorretto da un'adeguata motivazione, che dia conto non solo della configurabilità del reato, ma anche della concreta necessità della misura in relazione al pericolo da neutralizzare. La giurisprudenza, inoltre, richiede il rigoroso rispetto dei principi di proporzionalità e adeguatezza.

4.3. Sequestro conservativo di dispositivi digitali

Un cenno merita, infine, il sequestro conservativo, disciplinato dagli artt. 316 e ss. c.p.p., volto a garantire le obbligazioni civili derivanti dal reato, quali il pagamento della pena pecuniaria o il risarcimento del danno in favore della parte civile. In tale prospettiva, anche dispositivi informatici possono essere assoggettati alla misura esclusivamente nella loro dimensione patrimoniale, in quanto beni suscettibili di valutazione economica e, dunque, potenzialmente aggredibili ai fini della garanzia creditoria. Diversamente, invece, i dati informatici non assumono autonoma rilevanza quale oggetto del vincolo, se non nei limiti in cui risultino incorporati o funzionalmente riconducibili a un bene patrimoniale[21].

5. Fasi operative del sequestro informatico e acquisizione dei dati digitali

La procedura di sequestro di un dispositivo informatico si articola, in via generale, attraverso una sequenza di fasi logicamente progressive. In primo luogo, si procede all'identificazione del dispositivo da sottoporre a vincolo, che può avvenire presso l'abitazione, il luogo di lavoro o altri contesti nella disponibilità dell'indagato. A tale fase segue l'adozione del decreto di sequestro da parte dell'autorità giudiziaria, secondo la disciplina normativa di riferimento.

Successivamente si realizza l'intervento operativo sul dispositivo, che comprende le attività di messa in sicurezza del sistema, spesso mediante l'attivazione della modalità aereo o l'utilizzo di strumenti di protezione forense, al fine di impedirne l'alterazione o l'uso da remoto. In questa fase può essere eseguita, ove necessario, la duplicazione forense dei dati, mediante la creazione di una copia integrale della memoria del dispositivo, idonea a garantire la conservazione dell'originale e l'analisi separata dei contenuti.

La fase successiva riguarda l'analisi dei dati acquisiti, effettuata mediante software forensi specializzati, che consentono l'estrazione e l'esame di informazioni quali fotografie, video, comunicazioni elettroniche, e-mail, dati di geolocalizzazione, cronologia di navigazione e ulteriori evidenze digitali rilevanti.

Al termine delle operazioni, viene redatto un verbale analitico contenente la descrizione delle attività svolte e l'elenco dei dati estratti, mentre la copia forense viene conservata integra e messa a disposizione delle parti, secondo le garanzie previste dall'ordinamento.

Elemento centrale dell'intero procedimento è rappresentato dalla catena di custodia, ossia il complesso delle regole e delle procedure volte a garantire la conservazione, la tracciabilità e l'integrità del reperto informatico dal momento dell'acquisizione fino al suo eventuale utilizzo in sede processuale[22]. Ogni fase di trattamento del dispositivo o dei dati deve essere accuratamente documentata mediante verbali, registrazioni e sistemi di controllo, idonei a escludere alterazioni, manipolazioni o contaminazioni della prova. La compromissione della catena di custodia può infatti incidere in modo significativo sull'affidabilità del dato e, conseguentemente, sulla sua utilizzabilità processuale.

La crescente dimensione transnazionale dei dati digitali impone, inoltre, il ricorso a strumenti di cooperazione giudiziaria internazionale. In ambito europeo assumono particolare rilievo gli ordini europei di produzione e conservazione delle prove elettroniche, finalizzati a consentire l'acquisizione

20. Per un approfondimento in materia di misure cautelari reali si rinvia, *ex multis*, a Cordero 1991 e Spangher 2017.
21. Per una riflessione sul valore del dato si rimanda a d'Agostino Panebianco 2023.
22. Sulla catena di custodia del dato informatico si rimanda a Bartoli–Maioli 2015.

rapida di dati detenuti da fornitori di servizi stabiliti in altri Stati membri, superando in parte le tradizionali lentezze delle rogatorie internazionali. L'utilizzo di tali strumenti richiede tuttavia il rispetto dei differenti ordinamenti giuridici e delle garanzie poste a tutela dei diritti fondamentali.

Infine, una delle principali criticità operative nelle indagini digitali riguarda l'accesso a sistemi protetti da password, autenticazione multifattoriale o crittografia avanzata. La diffusione di tecniche di cifratura end-to-end e di sistemi di protezione biometrica rende spesso complesso, se non impossibile, l'accesso immediato ai dati, imponendo il ricorso a strumenti tecnici altamente specialistici e a metodologie investigative sempre più sofisticate.

6. Garanzie difensive e diritti fondamentali

L'evoluzione delle tecnologie digitali e l'intensificazione delle attività investigative fondate sull'utilizzo di dati informatici impongono la progressiva elaborazione di un modello di *digital due process*, inteso quale adattamento delle garanzie del giusto processo alle peculiarità dell'ambiente digitale[23]. Tale impostazione muove dal presupposto che le garanzie processuali tradizionali non possano essere semplicemente trasposte nel contesto tecnologico, ma debbano essere reinterpretate alla luce delle caratteristiche strutturali della prova digitale, quali la volatilità, la replicabilità e la sua intrinseca immaterialità.

In tale prospettiva, il *digital due process* si articola attorno ad alcuni principi fondamentali, tra i quali assumono rilievo la tracciabilità delle operazioni tecniche, la trasparenza delle modalità di acquisizione, la piena effettività del contraddittorio e la verificabilità indipendente del dato informatico. Particolare importanza riveste, inoltre – come visto –, la catena di custodia, intesa come continuità documentata delle operazioni di conservazione e manipolazione del reperto digitale, la quale costituisce presupposto essenziale per garantirne l'affidabilità e l'utilizzabilità probatoria.

Tale sistema di garanzie si innesta necessariamente sul piano dei diritti fondamentali, imponendo un costante bilanciamento tra esigenze investigative e tutela della sfera privata dell'individuo. In questo senso, i dispositivi digitali sono sempre più frequentemente qualificati come estensione della dimensione personale dell'individuo, in quanto contenitori di informazioni idonee a riflettere la sua identità relazionale, comunicativa e comportamentale, con la conseguenza che su di essi si concentra una particolarmente elevata "aspettativa ragionevole di riservatezza"[24].

La giurisprudenza sovranazionale ha contribuito in modo significativo a delineare i confini di tale tutela. La Corte europea dei diritti dell'uomo ha infatti ricondotto le manifestazioni della vita privata anche alla dimensione digitale e alle forme di espressione della personalità online, riconoscendo la protezione dell'art. 8 CEDU anche rispetto al trattamento di dati e comunicazioni elettroniche (tra le altre, *Smirnova c. Russia*, 2003; *Copland c. Regno Unito*, 2007; *Bărbulescu c. Romania*, 2017). In tale prospettiva, la Corte ha inoltre elaborato criteri di valutazione della legittimità delle attività investigative tecnologiche, richiedendo che l'ingerenza sia prevista dalla legge, persegua uno scopo legittimo e risulti necessaria in una società democratica, secondo un rigoroso giudizio di proporzionalità (*Yüksel Yalçınkaya c. Turchia*, 2023).

Anche la giurisprudenza costituzionale nazionale si è progressivamente adeguata a tale evoluzione, estendendo la tutela della vita privata e della segretezza delle comunicazioni alla dimensione tecnologica. In particolare, è stato ribadito che la libertà e la segretezza della corrispondenza, di cui all'art. 15 Cost., si estendono alle comunicazioni elettroniche (Corte cost. n. 170/2023), che i limiti alle stesse devono essere predeterminati e giustificati (Corte cost. n. 2/2021), e che il domicilio

23. Per un approfondimento sul tema della due diligence e delle garanzie procedurali nel contesto europeo successivo al Digital Service Act si rimanda a Gentile 2024.

24. L'espressione "aspettativa ragionevole di riservatezza" è stata introdotta per la prima volta nel 1967 dalla giurisprudenza statunitense, all'interno della storica sentenza della Corte Suprema *Katz v. United States*. Tale principio ha sancito il superamento del criterio della violazione fisica della proprietà privata, stabilendo che la tutela costituzionale della riservatezza "protegge le persone, non i luoghi". Questo concetto ha ridefinito il diritto alla privacy a livello globale, influenzando profondamente la giurisprudenza europea e italiana in materia di intercettazioni, sorveglianza digitale e protezione dei dati personali.

rappresenta una proiezione spaziale della persona (Corte cost. n. 135/2002). In tale quadro, anche i dati biometrici — quali impronte digitali, riconoscimento facciale e dati vocali — assumono una particolare rilevanza quale categoria di dati personali altamente sensibili, la cui utilizzazione investigativa richiede un rigoroso rispetto dei principi di proporzionalità e minimizzazione del trattamento.

Ne consegue che il bilanciamento tra esigenze investigative e diritti fondamentali si configura come elemento strutturale del sistema, tanto più evidente nell'ambito della prova digitale.

Sul versante delle garanzie difensive, l'art. 24 Cost. estende la tutela del diritto di difesa anche alle attività di acquisizione e analisi della prova informatica. Nei casi più complessi è quindi prevista la partecipazione della difesa alle operazioni tecniche, anche mediante la nomina di consulenti tecnici di parte, nonché la possibilità di intervenire nelle attività caratterizzate da irripetibilità, secondo le regole del contraddittorio anticipato.

La prova digitale è inoltre soggetta alla disciplina generale in tema di utilizzabilità prevista dal codice di procedura penale. Violazioni delle modalità di acquisizione, del contraddittorio o delle garanzie difensive possono comportare l'inutilizzabilità del dato, con conseguente esclusione dal compendio probatorio. In caso di violazioni procedurali, possono altresì configurarsi nullità, relative o assolute, a seconda della gravità del vizio, le quali possono essere fatte valere mediante i rimedi impugnatori previsti dall'ordinamento, quali riesame, appello o ricorso per cassazione.

Il profilo delle garanzie assume particolare rilievo per quanto riguarda i mezzi di ricerca della prova atipici, i quali ricorrono frequentemente nell'ambito dei reati informatici, caratterizzati dall'assenza di una disciplina legislativa specifica e da un limitato controllo giurisdizionale preventivo. In tali ipotesi, infatti, viene meno sia il vaglio tipico del legislatore, sia il controllo del giudice del dibattimento, previsto, invece, in relazione ai mezzi di prova atipici ai sensi dell'art. 189 c.p.p., con conseguente ampliamento degli spazi di discrezionalità nell'acquisizione del dato probatorio.

In definitiva, la giurisprudenza europea evidenzia come la prova digitale si collochi in una posizione di intersezione tra tutela della riservatezza e garanzie del giusto processo, imponendo agli ordinamenti nazionali un costante adeguamento delle categorie processuali tradizionali. Ne emerge un modello europeo di equità digitale del processo, nel quale la legittimità della *digital evidence* non dipende esclusivamente dalla sua utilità investigativa, ma dalla qualità e dall'effettività delle garanzie che ne accompagnano l'acquisizione e l'utilizzazione.

7. Conclusioni

Alla luce delle criticità emerse nel corso dell'analisi, appare necessario valorizzare un'interpretazione sistematica della disciplina del sequestro e orientata ai principi costituzionali e convenzionali, con particolare riferimento al diritto di difesa, al giusto processo e alla tutela della riservatezza. In tale prospettiva, il sequestro di dispositivi e dati digitali impone una lettura evolutiva delle norme codicistiche, idonea a tenere conto delle peculiarità strutturali dell'ambiente informatico e della natura immateriale delle informazioni ivi contenute.

In questa cornice si colloca il concetto di *digital due process*, inteso come criterio ermeneutico funzionale ad adeguare le garanzie processuali tradizionali alle modalità operative del sequestro informatico. Esso consente di enfatizzare l'esigenza di un contraddittorio effettivo anche sul piano tecnico, nonché la necessità di assicurare la tracciabilità delle operazioni di acquisizione e la verificabilità delle modalità di estrazione e conservazione dei dati.

In prospettiva *de iure condendo*, una prima direttrice di intervento potrebbe consistere nell'introduzione di una disciplina organica del sequestro digitale, o di uno specifico statuto delle attività di apprensione informatica, che disciplini in modo puntuale le modalità esecutive, la duplicazione forense, la conservazione dei dati e le forme di accesso ai medesimi. Tale intervento dovrebbe altresì prevedere criteri chiari di validità e utilizzabilità, con particolare attenzione alla tutela della catena di custodia e alla completa documentazione delle operazioni compiute.

Più in generale, si evidenzia l'esigenza di un intervento legislativo di sistema, volto a ridurre la frammentazione normativa attualmente esistente e a garantire standard tecnici uniformi, idonei ad assicurare la controllabilità delle attività di sequestro informatico e l'effettiva partecipazione della difesa sin dalle fasi iniziali dell'acquisizione del dato.

In conclusione, il sequestro di dispositivi e informazioni digitali non rappresenta soltanto un'evoluzione tecnica dei tradizionali mezzi di ricerca della prova, ma costituisce un ambito nel quale si misura la capacità dell'ordinamento di mantenere un equilibrio effettivo tra esigenze investigative e tutela dei diritti fondamentali, nell'attuale contesto di progressiva digitalizzazione delle indagini penali.

Riferimenti bibliografici

S. Aterno (2023), *Profili penali della vita nel Metaverso*, in G. Cassano, G. Scorza (a cura di), "Metaverso. Diritti degli utenti, piattaforme digitali, privacy, diritto d'autore, profili penali, blockchain e NFT", Pacini Giuridica, 2023

S. Aterno (2008), *Acquisizione e analisi della prova informatica*, in "Diritto e Procedura Penale", Dossier, La prova scientifica nel processo penale, 2008

L. Bartoli, C. Maioli (2015), *La catena di custodia del dato digitale: tra anelli solidi e anelli mancanti*, in "Informatica e diritto", 2015

M. Bettoni (2012), *Il sequestro preventivo di siti web tramite ordine agli ISP: osservazioni sui casi Moncler e Vajont.info*, in "Ciberspazio e diritto" 2012, n. 1

M. Caianiello (2025), *Ancora in tema di sequestro di dispositivi, sistemi informatici o telematici o memorie digitali (disegno di legge C. 806)*, in "Sistema Penale", 2025

C. Campanaro (2012), *Legittimo il sequestro preventivo del sito internet se i contenuti sono diffamatori*, in "Diritto Penale Contemporaneo", 2012

F. Centorame (2025), *Le indagini Tecnologiche ad alto potenziale intrusivo fra esigenze di accertamento e sacrale inviolabilità dei diritti della persona*, in "Cassazione Penale", 2025, n. 2

F. Cordero (1991), *Procedura penale*, I ed., Giuffrè, 1991

F. Corona (2021), *Il cybercrime: soggetto, oggetto e condotta*, in Id. (a cura di), "Reati informatici e investigazioni digitali", Pacini Giuridica, 2021

M. d'Agostino Panebianco (2023), *Il "dato": bene immateriale con un proprio valore intrinseco*, in "Ambientediritto", 2023, n. 2

M. Daniele (2011), *La prova digitale nel processo penale*, in "Rivista di Diritto Processuale", 2011

J. Della Torre (2025), *Spunti di riflessione sulla proposta di legge in materia di sequestro di dispositivi e di dati*, in "Sistema Penale", 2025

F. Dinacci (2025), *Sequestro di dispositivi informatici: imposizioni tecnologiche e scelte interpretative. Alla ricerca di un recupero della legalità probatoria*, in "Archivio Penale", 2025

R. Flor (Ed.) (2025), *Investigations in the digital environment: procedural principles, rules and multi-actor cooperation*, Technical Report, 2025

R. Flor (2023), *Lawful hacking, vulnerabilità tecnologica e diritto penale, fra esigenze di accertamento dei reati e tutela di beni giuridici di nuova generazione*, in L. Picotti (a cura di), "Automazione, diritto e responsabilità", Edizioni Scientifiche Italiane, 2023

R. Flor (2019), *La legge penale nello spazio, fra evoluzione tecnologica e difficoltà applicative*, in A. Cadoppi, S. Canestrari, A. Manna, M. Papa (a cura di), "Cybercrime. Diritto e procedura penale dell'informatica", Utet Giuridica, 2019

R. Flor, S. Marcolini (2022), *Dalla Data Retention alle indagini ad alto contenuto tecnologico. La tutela dei diritti fondamentali quale limite al potere coercitivo dello Stato. Aspetti di diritto penale processuale e sostanziale*, Giappichelli, 2022

R. Flor, B. Panattoni (2023), *Digital criminal investigations in Italy. The intersection between data protection and cybersecurity*, in "New Journal of European Criminal Law", vol. 14, 2023, n. 4

G. Gentile (2024), *Between Online and Offline Due Process: The Digital Services Act*, in A. Engel, X. Groussot, G.T. Petursson (Eds.), "New Directions in Digitalisation", Springer, 2024

V. Gramuglia (2021), *Sequestro probatorio del reperto digitale e manifestazioni distorsive dell'attività di indagine*, in "Diritto di Internet", 2021

S.J. Kobrin (2001), *Territoriality and the Governance of Cyberspace*, in "Journal of International Business Studies", 2001

E. Lorenzetto (2025), *I sequestri di smartphone, dispositivi informatici e memorie digitali*, in G. Di Paolo, L. Pressacco (a cura di), "Indagini e prove nella società digitale. Questioni attuali e prospettive future", Università degli Studi di Trento, 2025

L. Lupária (a cura di) (2009), *Sistema penale e criminalità informatica: profili sostanziali e processuali nella Legge attuativa della Convenzione di Budapest sul cybercrime (L. 18 marzo 2008, n. 48)*, Giuffrè, 2009

L. Lupária, G. Ziccardi (a cura di) (2007), *Investigazione penale e tecnologia informatica*, Giuffrè, 2007

P. Maggio (2021), *Intercettazioni no limits: il captatore informatico "per istradamento"*, in "Processo penale e giustizia", 2021

S. Marcolini (2015), *Le indagini atipiche a contenuto tecnologico nel processo penale: una proposta*, in "Cassazione Penale", 2015, n. 2

S. Marcolini (2010), *Le cosiddette perquisizioni on line (o perquisizioni elettroniche)*, in "Cassazione Penale", 2010, n. 7-8

C. Marinelli (2007), *Intercettazioni processuali e nuovi mezzi di ricerca della prova*, Giappichelli, 2007

M. Nicolini (2026), *La Cassazione torna sul tema del sequestro finalizzato all'acquisizione di prove digitali consolidando l'evoluzione dello statuto del PM come organo di giustizia*, in "Sistema Penale", 2026

W. Nocerino (2021), *Nuove tecnologie e processo penale – Il tramonto dei mezzi di ricerca della prova nell'era 2.0*, in "Diritto Penale e Processo", 2021

L. Picarella (2025), *Criminalità in rete: Dalle piattaforme illegali alle cybermafie,* Donzelli editore, 2025

M. Pittiruti (2021), *Dalla Corte di cassazione un vademecum sulle acquisizioni probatorie informatiche e un monito contro i sequestri digitali omnibus*, in "Sistema penale", 2021

P.P. Rivello (2014), *La prova scientifica*, Giuffrè, 2014

F. Ruggieri, L. Picotti (a cura di) (2011) *Nuove tendenze della giustizia penale di fronte alla criminalità informatica. Aspetti sostanziali e processuali*, Giappichelli, 2011

S. Signorato (2025), *Il sequestro di dispositivi e informazioni digitali*, in "Sistema Penale", 2025

S. Signorato (2024), *Indagini e prove digitali*, in "Rivista di Diritto Processuale", 2024

G. Spangher (2017), *Le misure cautelari reali: "figlie di un dio minore"*, in "Libro dell'anno del diritto 2017", Treccani, 2017

M. Torre (2024), *Considerazioni su perquisizione, sequestro e intercettazioni digitali*, in "Diritto penale e processo", 2024, n. 6

M. Torre (2017), *Il captatore informatico. Nuove tecnologie investigative e rispetto delle regole processuali*, Giuffrè, 2017

V. Vitkov (2012), *Il sequestro preventivo di siti web: nota a Corte di Cassazione, Sez. V penale, sentenza del 19 settembre 2011, n. 46504*, in "Ciberspazio e diritto", 2012, n. 1