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

ISSN 2704-7318 • n. 1/2026 • DOI 10.32091/RIID0278 • articolo sottoposto a peer review • pubblicato in anteprima il 11 giu. 2026

Matilde Bellingeri

Prove digitali e ruolo delle piattaforme alla luce del pacchetto Europeo *e-Evidence*

Le informazioni rilevanti per il processo penale sono frequentemente generate, conservate e rese accessibili da parte dei prestatori di servizi digitali secondo logiche infrastrutturali che rendono incerta la localizzazione fisica del dato. In questo contesto le categorie tradizionali della cooperazione giudiziaria, costruite intorno alla territorialità della prova e alla relazione tra autorità statali, meritano di essere ripensate secondo un modello di accesso alla prova elettronica uniforme e diretto. Il presente contributo, dopo aver analizzato il contenuto del pacchetto *e-Evidence*, composto dal Regolamento (UE) 2023/1543 e dalla Direttiva (UE) 2023/1544, delinea la struttura degli ordini europei di produzione e conservazione, concentrandosi sulla tassonomia dei dati, sulla graduazione delle garanzie, oltreché sui rapporti tra Stato di emissione, Stato di esecuzione e prestatori di servizi. Per finire, si propone di verificare se la cooperazione diretta tra lo Stato di emissione e i prestatori di servizi riesca a coniugare efficienza investigativa e tutela dei diritti fondamentali, senza tradursi in una riduzione del controllo giurisdizionale.

Prova elettronica – Piattaforme digitali – e-Evidence – Cooperazione giudiziaria europea – Prestatori di servizi

Digital evidence and the role of platforms under the European e-Evidence package

In the current digital environment, information relevant to criminal proceedings is frequently generated, stored, and made accessible by digital service providers that make the physical location of data uncertain. In this context, the traditional categories of judicial cooperation, built around the territoriality of evidence and the relationship between state authorities, deserve to be rethought according to a uniform and direct model of access to electronic evidence. This paper, after analyzing the content of the e-Evidence package, consisting of Regulation (EU) 2023/1543 and Directive (EU) 2023/1544, outlines the structure of the European production and preservation orders, focusing on data taxonomy, the levels of guarantees, as well as the relationships between issuing and executing states, and service providers. Finally, the aim is to examine whether direct cooperation between the issuing State and service providers currently succeeds in combining investigative efficiency and the protection of fundamental rights, without reducing judicial review.

Electronic evidence – Digital platforms – e-Evidence – European judicial cooperation – Internet service providers

L'Autrice è dottoranda nel corso di Dottorato in Scienze giuridiche europee e internazionali dell'Università di Verona

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

1. Introduzione

La progressiva digitalizzazione delle relazioni sociali, economiche e comunicative ha inciso profondamente sulla fisionomia della prova nel processo penale. Una quota crescente delle informazioni rilevanti ai fini investigativi non si manifesta più attraverso supporti materiali o fonti dichiarative tradizionali, ma mediante dati informatici generati, trasmessi, archiviati o elaborati all'interno di ecosistemi digitali complessi: comunicazioni elettroniche, metadati di accesso, cronologie di navigazione, contenuti conservati in cloud, dati di geolocalizzazione, transazioni su piattaforme online, account personali e professionali[1]. La prova penale contemporanea tende così a smaterializzarsi, assumendo carattere dinamico, diffuso e strutturalmente transnazionale[2]. A questa evoluzione si accompagna la necessità di governare in modo rigoroso tale patrimonio informativo, il quale, per la sua intrinseca modificabilità, per la velocità con cui circola e per il rischio di dispersione cui è esposto, richiede presidi adeguati nelle fasi di conservazione, acquisizione e analisi[3].

La rivoluzione digitale ha messo in crisi uno dei presupposti impliciti del processo penale: la possibilità di ricondurre l'elemento probatorio a una determinata collocazione spaziale, così da individuare l'autorità competente alla sua acquisizione. Oggi, infatti, i dati rilevanti per l'accertamento penale sono spesso generati, conservati o elaborati in ambienti digitali gestiti da prestatori di servizi privati, i quali detengono la disponibilità tecnica delle informazioni e ne governano, in concreto, le condizioni di accesso. Ne deriva una centralità crescente di tali soggetti nella filiera acquisitiva della prova elettronica: in molti casi la loro cooperazione è indispensabile; in altri, pur essendo astrattamente praticabili canali alternativi, questi risultano più invasivi, più onerosi o incompatibili con le esigenze di segretezza dell'attività investigativa[4].

In questo contesto si colloca il c.d. pacchetto europeo *e-Evidence*[5], composto dal Regolamento (UE) 2023/1543, relativo agli ordini europei di produzione e di conservazione delle prove elettroniche

1. Svantesson–Osula 2025, p. 52 ss.; Siracusano 2017, p. 181.
2. Daskal 2015, p. 365 ss.
3. Cutrignelli 2023.
4. Franssen–Tosza 2025, p. 2.
5. Il pacchetto europeo *e-Evidence* – composto dal Regolamento (UE) 2023/1543 relativo agli ordini europei di produzione e di conservazione di prove elettroniche nei procedimenti penali [da ora in avanti "Regolamento" o "Reg."] e dalla Direttiva (UE) 2023/1544 recante norme armonizzate sulla designazione degli stabilimenti e sulla nomina dei rappresentanti legali ai fini dell'acquisizione di prove elettroniche [da ora in avanti "Direttiva" o "Dir."] – è entrato in vigore il 18 agosto 2023. Ai sensi dell'art. 35 del Regolamento, esso troverà applicazione soltanto a decorrere dal 18 agosto 2026, mentre il termine per il recepimento della Direttiva è fissato al 18 febbraio 2026. Deve pertanto ritenersi che la piena operatività del sistema europeo *e-Evidence* decorrerà dal 18 agosto 2026.

e dalla Direttiva (UE) 2023/1544, concernente la designazione di stabilimenti designati e la nomina di rappresentanti legali dei prestatori di servizi ai fini dell'acquisizione di tali prove[6].

Il nuovo assetto normativo muove dall'intento di rendere più rapido ed effettivo l'accesso transfrontaliero ai dati digitali, riducendo i tempi e gli oneri della cooperazione tradizionale, senza rinunciare, almeno nelle intenzioni del legislatore unionale, a una cornice di garanzie coerente con i principi di necessità, proporzionalità e tutela dei diritti fondamentali. La portata del pacchetto eccede, tuttavia, il piano meramente tecnico-procedurale; non solo introduce nuovi strumenti di acquisizione probatoria, ma incide direttamente sulla geografia dei poteri nel processo penale, ridefinendo il rapporto tra autorità pubbliche e operatori privati. E proprio in questa transizione – dalla piattaforma come spazio tecnico alla piattaforma come snodo regolato della cooperazione giudiziaria – si coglie una delle linee evolutive più significative del diritto processuale penale europeo nell'era delle prove digitali[7].

2. Genesi, struttura e finalità del pacchetto europeo *e-Evidence*

Le coordinate elaborate dalla giurisprudenza della Corte di giustizia hanno costituito il presupposto sistematico dell'intervento normativo dell'Unione europea, volto a tradurre, sul piano del diritto positivo, le esigenze emerse nel contesto digitale, di effettività investigativa e di tutela dei diritti fondamentali[8].

In questa prospettiva, il pacchetto *e-Evidence* si presenta quale risposta a una duplice crisi: quella inerente alla territorialità e quella dell'adeguatezza degli strumenti tradizionali di cooperazione, strutturati secondo un criterio di circolazione della prova mediato dal rapporto tra autorità statali.

Sebbene la progressiva evoluzione verso modelli di riconoscimento reciproco e di interazione tra autorità giudiziarie non sia nuova al diritto unionale (come dimostrano il mandato di arresto europeo[9], l'ordine europeo di indagine[10] e il sistema di riconoscimento reciproco dei provvedimenti di sequestro e confisca[11]), l'acquisizione delle prove elettroniche, pur collocandosi entro tale processo di trasformazione, presenta caratteri assai peculiari, legati alla natura immateriale dei dati, alla loro frequente dispersione transnazionale e al ruolo centrale assunto da soggetti privati estranei al circuito giurisdizionale, quali sono i prestatori di servizi[12].

Sotto tale profilo, l'elemento qualificante del nuovo assetto risiede nel superamento di una logica esclusivamente interstatale di cooperazione probatoria e nell'affermazione di un modello di interlocuzione diretta con i prestatori di servizi, funzionale a fronteggiare la rapidità di circolazione del dato digitale e la frequente irrilevanza della sua localizzazione fisica[13]. Da qui, l'introduzione di due strumenti specifici – l'ordine europeo di produzione e l'ordine europeo di conservazione – i quali non

6. Gaudieri 2023, pp. 1234-1235; Forlani 2023, p. 174 ss.
7. Aguinaldo–De Hert 2025, p. 200 ss.
8. Caianiello 2022, p. 165; Allegrezza 2020, p. 1123 ss.
9. Decisione quadro 2002/584/GAI, attuata nell'ordinamento interno con la legge n. 69/2005.
10. Direttiva 2014/41/UE, attuata con il d.lgs. n. 108/2017. In argomento si veda: Calavita 2025; Ertola 2025; Raucci 2025, p. 1 ss.; Nascimbeni 2022, p. 410 ss.
11. Regolamento (UE), 2018/1805, attuato con il d.lgs. 7 agosto 2020, n. 137. Sul tema, si vedano: Grandi 2021; Maugeri 2019.
12. Commissione Europea, *Impact Assessment*, SWD (2018) 118, § 2.1 e § 2.2, che evidenziano come la maggior parte delle prove elettroniche sia detenuta da prestatori di servizi privati e come l'accesso ai dati nelle indagini penali richieda forme strutturate di cooperazione diretta tra autorità pubbliche e prestatori di servizi.
13. Il considerando n. 12 del regolamento chiarisce, non a caso, che il meccanismo degli ordini europei di produzione e conservazione consente alle autorità nazionali competenti di inviare tali ordini direttamente ai prestatori di servizi. È in questo passaggio che si coglie il mutamento di paradigma: l'efficienza acquisitiva non viene più affidata soltanto all'intermediazione di un'altra autorità statale, ma si fonda sulla possibilità di raggiungere immediatamente il soggetto privato che detiene o governa il dato.

eliminano il ricorso all'ordine europeo di indagine, ma ne ridimensionano la centralità nei casi in cui l'oggetto dell'acquisizione sia costituito da dati elettronici già esistenti, detenuti da prestatori di servizi rientranti nell'ambito applicativo del Regolamento.

L'obiettivo perseguito dal legislatore unionale è duplice: da un lato, predisporre strumenti capaci di assicurare un accesso tempestivo alle prove elettroniche in contesti transfrontalieri; dall'altro, sottoporre tale accesso a una cornice uniforme di garanzie, coerente con i principi di necessità e proporzionalità e con la tutela dei diritti fondamentali, in particolare del giusto processo, della protezione dei dati personali e della riservatezza delle comunicazioni. Il Regolamento (UE) 2023/1543, costituisce il nucleo sostanziale e procedurale della disciplina: introduce gli ordini europei di produzione e di conservazione delle prove elettroniche, ne definisce i presupposti, le categorie di dati, le garanzie applicabili e il meccanismo di trasmissione diretta ai prestatori di servizi[14], al fine di assicurare un elevato grado di armonizzazione ed evitare soluzioni nazionali eterogenee[15]. La Direttiva (UE) 2023/1544, assolve una funzione complementare di carattere organizzativo. Essa mira ad armonizzare la designazione di stabilimenti designati e la nomina di rappresentanti legali[16], così da assicurare, all'interno dell'Unione, un referente certo per la ricezione, l'ottemperanza e l'esecuzione degli ordini[17].

Non si tratta, dunque, di due atti contigui, ma di segmenti normativi reciprocamente integrati: il Regolamento appronta il titolo europeo di acquisizione o conservazione; la Direttiva ne garantisce l'effettività operativa mediante la costruzione di un punto di contatto giuridico con il soggetto privato che detiene, conserva o gestisce il dato.

Il sistema delineato dal Regolamento non ha carattere esclusivo; gli strumenti tradizionali di cooperazione giudiziaria continuano a trovare applicazione nei rapporti con Stati terzi e nelle ipotesi che non rientrano nell'ambito oggettivo o soggettivo del pacchetto[18].

Su questa architettura si innesta la disciplina nazionale chiamata a regolare gli aspetti organizzativi e procedurali rimessi agli Stati membri. Nell'ordinamento interno, i d.lgs. 30 dicembre 2025, n. 215 e n. 216 confermano la logica bipartita del pacchetto: il primo adegua il sistema interno al Regolamento, sul piano delle competenze e delle procedure; il secondo dà attuazione alla Direttiva, rendendo operativa la figura dello stabilimento designato e del rappresentante legale.

3. Le prove elettroniche oggetto di acquisizione: categorie di dati e diversi livelli di intrusività

La nozione di prova elettronica assunta dal Regolamento riguarda dati elettronici già esistenti, detenuti da prestatori di servizi rientranti nell'ambito applicativo della disciplina europea e suscettibili di essere prodotti o conservati a fini probatori. A tale riguardo, l'art. 3 del Regolamento individua i dati relativi agli abbonati, i dati di accesso, i dati di traffico e i dati relativi al contenuto delle comunicazioni[19]. Questa delimitazione oggettiva condiziona l'intera architettura del sistema, individuando il

14. Cfr. artt. 1, 3, 4-11 Reg.
15. Cfr. considerando 7, 8 e 9 Reg., dai quali emerge l'esigenza di superare la frammentazione degli strumenti nazionali, assicurare un quadro comune per l'acquisizione transfrontaliera di prove elettroniche e rafforzare certezza giuridica, efficacia e rapidità della cooperazione con i prestatori di servizi.
16. Cfr. artt. 1-3 Dir.
17. Cfr. art. 3 Dir., relativo alla designazione di stabilimenti designati e alla nomina di rappresentanti legali. Si veda anche art. 4, sulle notifiche e sulle lingue, e art. 6, sulle autorità centrali. La direttiva precisa che stabilimenti designati e rappresentanti legali fungono da destinatari delle decisioni e degli ordini finalizzati all'acquisizione di prove elettroniche nei procedimenti penali.
18. Il pacchetto opera entro il perimetro unionale e riguarda i prestatori che offrono servizi nell'Unione, anche se stabiliti in Paesi terzi, i quali sono tenuti a designare uno stabilimento o a nominare un rappresentante legale nell'Unione ai fini della ricezione e dell'esecuzione degli ordini europei.
19. Cfr. art. 3, nn. 8-13, Reg., il quale definisce la nozione di "prova elettronica" e distingue le categorie di dati rilevanti: dati relativi agli abbonati, dati richiesti al solo scopo di identificare l'utente, dati relativi al traffico e dati relativi al contenuto. Si veda altresì, art. 2, sull'ambito di applicazione, e art. 3, n. 3 e n. 7, sulla nozione di prestatore di servizi e di stabilimento.

perimetro applicativo degli ordini europei di produzione e conservazione, nonché il grado di interferenza che l'atto acquisitivo è idoneo a produrre sui diritti fondamentali. La classificazione dei dati non assolve una funzione meramente definitoria: essa costituisce il presupposto della graduazione delle garanzie, poiché consente di distinguere tra dati funzionali all'identificazione dell'utente, dati capaci di ricostruire le modalità esteriori delle comunicazioni e dati che investono direttamente il contenuto informativo delle stesse.

La prima categoria è costituita dai dati relativi agli abbonati. Si tratta delle informazioni concernenti l'identità dell'utente, la sottoscrizione o l'attivazione del servizio, gli elementi di contatto e, più in generale, i dati idonei a collegare una determinata utenza digitale a una persona fisica o giuridica[20]. La loro minore intrusività, rispetto ai dati di traffico e di contenuto, non deve tuttavia essere intesa in termini assoluti. Anche il dato apparentemente identificativo può assumere una rilevanza investigativa decisiva, nella misura in cui consente di trasformare un identificativo tecnico (ad esempio, un account, un indirizzo IP, un numero telefonico, un codice cliente) in un riferimento soggettivo utilizzabile nel procedimento penale. Proprio per questa ragione il Regolamento individua una categoria ulteriore di dati, ossia quelli richiesti al solo fine di identificare l'utente.

Tale scelta assume particolare interesse sistematico: essa comporta la sottrazione di una parte dei dati tecnici alla disciplina più rigorosa prevista per i dati di traffico valorizzando non soltanto la natura del dato ma la funzione della richiesta. Tale categoria di dati comprende, in particolare, gli indirizzi IP e, ove necessario, le porte di origine e la marcatura temporale, nonché equivalenti tecnici di tali identificativi, quando siano richiesti esclusivamente per individuare l'utente in una specifica indagine penale[21]. Il medesimo dato può quindi assumere un diverso grado di intrusività a seconda che sia utilizzato per una mera identificazione oppure per ricostruire sequenze comunicative, relazioni, accessi o condotte digitali.

Più problematico risulta essere il trattamento dei dati relativi al traffico; essi non rivelano il contenuto della comunicazione, ma ne descrivono gli elementi esteriori, quali origine, destinazione, tempo, durata, percorso, servizio utilizzato e altri parametri tecnici dell'interazione digitale. La distinzione tra contenuto e dati esterni della comunicazione, pur conservando rilievo dogmatico, non è sufficiente a fondare una rigida gerarchia di tutela. La giurisprudenza della Corte di giustizia ha progressivamente chiarito che i dati relativi al traffico e all'ubicazione, specie se considerati nel loro insieme, possono consentire inferenze estremamente precise sulla vita privata dell'interessato, sulle sue abitudini, sui suoi spostamenti e sulle sue relazioni personali[22]. Il metadato, in altri termini, non è un dato neutro: la sua capacità rivelatrice cresce in funzione della quantità, della durata temporale dell'acquisizione e delle possibilità di aggregazione.

La categoria più invasiva resta quella dei dati relativi al contenuto. Essa comprende il contenuto sostanziale delle comunicazioni o delle informazioni conservate mediante il servizio digitale: messaggi, testi, immagini, video, file, documenti, registrazioni o altri materiali caricati, trasmessi o archiviati. In questo caso, l'interferenza con la sfera privata è diretta, poiché l'autorità procedente accede non soltanto agli indici esteriori della comunicazione, ma al suo contenuto semantico. Per tale ragione, l'acquisizione dei dati di contenuto impone un controllo particolarmente rigoroso di legalità, necessità e proporzionalità, oltre a una più attenta verifica dei presupposti di emissione dell'ordine.

20. Cfr. art. 3, n. 9, Reg., relativo alla definizione di "subscriber data", sul rilievo pratico dei dati di abbonamento nell'identificazione dell'utente.

21. Cfr. art. 3, n. 10, Reg. Sul punto si veda anche Wahl 2023, p. 165 ss., che segnala l'introduzione, accanto alle categorie tradizionali dei dati di abbonamento, traffico e contenuto, di una quarta categoria relativa ai dati richiesti esclusivamente per identificare l'utente.

22. Cfr. Corte giust., Grande Sezione, 8 aprile 2014, cause riunite C-293/12 e C-594/12, *Digital Rights Ireland Ltd*; Corte giust., Grande Sezione, 21 dicembre 2016, cause riunite C-203/15 e C-698/15, *Tele2 Sverige AB e Watson*; Corte giust., Grande Sezione, 2 marzo 2021, causa C-746/18, *Prokuratuur*. In quest'ultima decisione la Corte ha escluso che il pubblico ministero, quando dirige le indagini e sostiene l'accusa, possa essere considerato autorità indipendente idonea ad autorizzare l'accesso ai dati relativi al traffico e all'ubicazione ai fini dell'indagine penale.

Al riguardo, il Regolamento conferma questa impostazione graduata, sicché l'ordine europeo di produzione avente ad oggetto dati relativi agli abbonati o dati richiesti al solo fine di identificare l'utente può essere emesso per tutti i reati; al contrario, l'ordine relativo a dati di traffico o di contenuto è ammesso, in linea generale, solo per reati punibili nello Stato di emissione con pena detentiva pari, nel massimo, ad almeno tre anni, salve alcune ipotesi specificamente individuate[23].

Tale graduazione incide anche sul profilo soggettivo dell'autorità competente. Il Regolamento consente infatti al pubblico ministero di emettere ordini europei di produzione per dati relativi agli abbonati e per dati richiesti al solo fine di identificare l'utente, nonché ordini europei di conservazione; viceversa, quando l'ordine di produzione abbia ad oggetto dati di traffico o dati di contenuto, l'intervento del pubblico ministero richiede la convalida da parte di un giudice, di un organo giurisdizionale o di un giudice istruttore[24].

Tale differenziazione non elimina, tuttavia, ogni margine problematico. Il rischio è che la classificazione normativa venga intesa come automatismo, secondo una logica per cui i dati diversi dal contenuto sarebbero, per ciò solo, scarsamente lesivi. L'esperienza della prova digitale mostra, al contrario, che la capacità conoscitiva del dato dipende, non soltanto dalla sua appartenenza formale a una categoria, ma anche dal modo in cui esso viene combinato con altri dati, dalla durata dell'osservazione, dalla posizione del soggetto interessato e dal contesto investigativo. La proporzionalità dell'acquisizione non può quindi essere esaurita nella qualificazione astratta del dato, ma richiede una valutazione concreta della sua incidenza.

In questa prospettiva, la classificazione prevista dal Regolamento deve essere letta come primo presidio di garanzia, non come criterio autosufficiente di legittimazione. Essa serve ad orientare l'autorità procedente nella scelta dello strumento, nella delimitazione dell'oggetto dell'ordine e nella motivazione della richiesta. Al tempo stesso, vincola il prestatore di servizi destinatario dell'ordine a svolgere una verifica circa la natura dei dati domandati e del regime applicabile.

Proprio questo sembra essere il punto di intersezione tra la dimensione probatoria e quella organizzativa del pacchetto *e-Evidence*: la prova elettronica, nel modello europeo, non è soltanto un'informazione da acquisire, ma un dato collocato presso un soggetto privato che diviene snodo necessario della cooperazione penale transfrontaliera. La delimitazione dell'oggetto dell'acquisizione rileva nel rapporto con gli altri strumenti di cooperazione giudiziaria. Il Regolamento 2023/1543 non disciplina ogni forma di evidenza elettronica e non esclude, in via generale, il ricorso ad altri strumenti dell'Unione o internazionali[25].

Ne discende che la corretta qualificazione della categoria di dati richiesta costituisce il primo momento di una più ampia verifica di legalità probatoria. Prima ancora di individuare lo strumento da attivare, l'autorità procedente è chiamata a precisare quale dato intenda acquisire, quale grado di intrusività lo caratterizzi e quale regime di garanzie debba accompagnarne la circolazione transfrontaliera.

4. Le piattaforme digitali nel nuovo ecosistema investigativo europeo

Né il Regolamento (UE) 2023/1543 né la Direttiva (UE) 2023/1544 assumono la "piattaforma" quale categoria normativa autonoma. Entrambi gli atti operano, piuttosto, attraverso la nozione più ampia e funzionale di prestatore di servizi. Tale scelta non è priva di rilievo sistematico, poiché consente di ricomprendere entro un'unica cornice regolatoria una pluralità di soggetti eterogenei – prestatori di servizi di comunicazione elettronica, fornitori di hosting, cloud providers, piattaforme di messaggistica, social network, marketplace e altri intermediari digitali – accomunati dalla posizione infrastrutturale che occupano rispetto alla

23. Cfr. art. 5, parr. 3 e 4, Reg.

24. Cfr. art. 4 Reg., sul diverso ruolo del pubblico ministero a seconda della categoria di dati richiesta.

25. Art. 32, par. 1, Reg. Sul carattere non esclusivo dello strumento, si veda Espina Ramos 2025, secondo il quale l'autorità di emissione conserva la possibilità di ricorrere, a seconda del caso concreto, agli ordini europei di produzione o conservazione oppure ad altri strumenti dell'Unione o internazionali.

generazione, conservazione e accessibilità dei dati rilevanti per l'accertamento penale[26].

Da questo punto di vista, la piattaforma rileva anzitutto come infrastruttura probatoria. Essa non costituisce solo uno spazio digitale nel quale gli utenti comunicano, acquistano beni, condividono contenuti o conservano informazioni, ma rappresenta l'ambiente tecnico-organizzativo in cui si formano elementi suscettibili di assumere valore investigativo: dati di registrazione, identificativi tecnici, log di accesso, metadati, cronologie di interazione, contenuti archiviati, informazioni relative a dispositivi, sessioni, indirizzi IP, localizzazioni e modalità di utilizzo del servizio.

La prova elettronica, dunque, non è semplicemente collocata presso il prestatore di servizi: la sua individuazione, estrazione e verificabilità dipendono dalle modalità con cui la piattaforma organizza le informazioni, ne disciplina la conservazione e la cancellazione e ne rende possibile l'estrazione secondo procedure tecniche interne[27]. L'accesso al dato presuppone, pertanto, non solo un titolo giuridico legittimante, ma anche la cooperazione tecnica e organizzativa del soggetto che governa l'infrastruttura digitale entro cui quel dato è generato, conservato o reso accessibile.

Il Regolamento prende atto di tale trasformazione e costruisce un modello nel quale il prestatore di servizi diviene destinatario diretto dell'ordine europeo. La novità non consiste soltanto nella riduzione dei tempi di acquisizione, ma investe la struttura stessa del rapporto cooperativo: rispetto agli strumenti tradizionali, fondati sull'intermediazione dello Stato di esecuzione, l'autorità competente dello Stato di emissione può rivolgersi direttamente al soggetto privato che detiene, conserva o controlla i dati richiesti.

Il confronto con l'ordine europeo di indagine (OEI) consente di precisare la portata di questo mutamento. L'OEI conserva la funzione di strumento generale per l'acquisizione transnazionale della prova e mantiene rilievo per gli atti che richiedano l'intervento dell'autorità dello Stato di esecuzione o che non rientrino nell'ambito applicativo del Regolamento. L'*e-Evidence* opera, invece, secondo una logica di specialità funzionale: quando l'acquisizione riguarda dati elettronici già esistenti e detenuti da un prestatore di servizi rientrante nell'ambito soggettivo della disciplina europea, l'ordine europeo di produzione o di conservazione diviene il canale tipico di accesso alla prova. In questo schema, la piattaforma non è più un terzo occasionalmente coinvolto nel circuito acquisitivo, ma il punto di raccordo tra l'autorità giudiziaria e l'ambiente tecnico nel quale il dato è generato, conservato, organizzato e reso disponibile[28].

In questo contesto la Direttiva completa il modello sotto il profilo organizzativo, mirando a garantire che tale titolo abbia un destinatario certo, stabile e giuridicamente responsabile all'interno dell'Unione. L'obbligo di designare uno stabilimento o nominare un rappresentante legale non costituisce un adempimento meramente formale, ma il presupposto operativo dell'intero sistema. Senza un punto di contatto giuridicamente individuabile, l'ordine europeo rischierebbe di restare ineffettivo, soprattutto nei confronti di prestatori

26. Sul ricorso a una nozione funzionale, e non tipologica, di prestatore di servizi, si veda l'art. 3, n. 3, Reg.; nonché gli artt. 1 e 2 Direttiva (UE) 2023/1544, quanto all'ambito soggettivo degli obblighi di designazione dello stabilimento o di nomina del rappresentante legale. Si veda inoltre il considerando n. 16 Reg., ove sono richiamati, a titolo esemplificativo, mercati online, servizi di hosting, cloud computing, piattaforme di gioco online e piattaforme di gioco d'azzardo online.

27. Per una lettura della prova digitale come evidenza la cui formazione, conservazione e intelligibilità dipendono dall'ambiente tecnico nel quale il dato è generato e gestito, si veda: Corte suprema di Cassazione, Ufficio del Massimario e del Ruolo, Servizio penale, *Relazione su novità normativa n. 25/2026*, 7 aprile 2026, Parte I, § 1, secondo cui il passaggio da fonti probatorie materialmente localizzate a informazioni digitali, la cui esistenza, conservazione e intelligibilità dipendono da infrastrutture tecnologiche, determina una trasformazione epistemologica della prova penale.

28. *Ibidem*; cfr. considerando n. 12 e artt. 5-7, 9-11 Reg., relativi alle condizioni di emissione degli ordini europei di produzione e conservazione, ai destinatari, ai certificati degli ordini e alla loro esecuzione.

non stabiliti nello Stato di emissione o strutturati secondo modelli societari transnazionali[29].

L'effetto complessivo sembra essere quello di una responsabilizzazione organizzativa delle piattaforme, chiamate a predisporre canali di ricezione, procedure di verifica, sistemi di identificazione delle richieste, meccanismi di conservazione selettiva e modalità di trasmissione dei dati compatibili con i termini e le garanzie previsti dal Regolamento. Il prestatore di servizi deve essere in grado di distinguere tra dati relativi agli abbonati, dati richiesti al solo fine di identificare l'utente, dati di traffico e dati di contenuto; deve conservare o produrre soltanto quanto richiesto; deve rispettare i termini ordinari o emergenziali; deve eventualmente far valere i motivi di impossibilità, opposizione o conflitto normativo previsti dalla disciplina europea. In questo contesto, la tassonomia dei dati esaminata nel paragrafo precedente non rileva soltanto per l'autorità che emette l'ordine, ma anche per il destinatario privato, il quale è chiamato a tradurre la richiesta giuridica in operazione tecnica selettiva[30].

Tale responsabilizzazione non equivale, tuttavia, all'attribuzione di una funzione pubblica in senso proprio, né determina una privatizzazione dell'attività investigativa; la decisione sull'acquisizione resta ancorata a un titolo emesso dall'autorità competente, soggetto ai controlli previsti dal Regolamento. Ciò che muta è la dipendenza funzionale dell'accertamento pubblico dall'infrastruttura privata: l'effettività dell'ordine europeo presuppone la cooperazione tecnica, organizzativa e documentale del prestatore[31]. In questa prospettiva, la formula della collaborazione para-giurisdizionale dei prestatori di servizi può essere accolta solo in senso descrittivo, per indicare una funzione procedimentale intermedia nella quale obblighi di cooperazione, capacità tecnica e organizzazione interna concorrono a rendere possibile – o, al contrario, a ostacolare – l'accesso alla prova elettronica. La posizione delle piattaforme sembra dunque collocarsi in una zona intermedia tra soggezione all'ordine pubblico e autonomia organizzativa privata. Da un lato, esse sono destinatarie di obblighi giuridici tipizzati e possono essere esposte a conseguenze sanzionatorie in caso di inottemperanza; dall'altro, l'esecuzione concreta dell'ordine dipende da sistemi tecnici e procedure interne che restano in larga misura nella disponibilità del prestatore. Il controllo di legalità, pertanto, non può arrestarsi al provvedimento emesso dall'autorità giudiziaria, ma deve estendersi alla verificabilità della filiera acquisitiva, comprensiva della fase esecutiva svolta presso il soggetto privato[32].

Il punto assume particolare rilievo con riferimento all'ordine europeo di conservazione, la cui funzione non è quella di acquisire immediatamente il dato, ma di impedirne la cancellazione, l'alterazione o la dispersione in vista di una successiva produzione.

La piattaforma diviene il soggetto presso il quale si realizza una forma di tutela anticipata della

29. Sulla funzione organizzativa della direttiva, cfr. artt. 1 e 3 Dir.: la disciplina mira a garantire che i prestatori di servizi che offrono servizi nell'Unione dispongano di uno stabilimento designato o di un rappresentante legale incaricato della ricezione, dell'ottemperanza e dell'esecuzione degli ordini e delle decisioni diretti all'acquisizione di prove elettroniche nei procedimenti penali. Cfr., altresì, artt. 4 e 5 Dir., in tema di notifiche e sanzioni. Per l'attuazione nell'ordinamento italiano, si veda d.lgs. 30 dicembre 2025, n. 216.

30. Sulla tassonomia dei dati quale presupposto non solo dell'emissione, ma anche dell'esecuzione selettiva dell'ordine si veda, supra, § 3, nonché art. 3, nn. 9-12, Reg. Gli obblighi del prestatore si ricavano, in particolare, dagli artt. 10 e 11 Reg., relativi all'esecuzione dell'ordine europeo di produzione e dell'ordine europeo di conservazione, e dall'art. 12, che disciplina l'impossibilità di esecuzione, i motivi di rifiuto e i meccanismi di riesame. Cfr. altresì artt. 7 e 9 Reg., sui destinatari degli ordini e sui certificati degli ordini, dai quali emerge la necessaria traduzione della richiesta giuridica in un'operazione tecnica di individuazione, selezione e trasmissione del dato.

31. De Maio 2026.

32. La posizione intermedia del prestatore emerge dal combinato disposto degli artt. 7, 9-12 e 15 Reg. Sul versante organizzativo, si vedano gli artt. 1, 3 e 5 Dir., dai quali risulta che lo stabilimento designato o il rappresentante legale deve disporre dei poteri e delle risorse necessari per ricevere, ottemperare ed eseguire gli ordini e le decisioni rivolti al prestatore. In tale quadro, la fase esecutiva svolta presso il soggetto privato diviene parte essenziale della filiera acquisitiva, con conseguente rilievo della verificabilità delle operazioni tecniche di individuazione, conservazione, selezione e trasmissione del dato.

fonte digitale: non vi è ancora accesso conoscitivo da parte dell'autorità, ma vi è già un vincolo giuridico sulla gestione privata del dato. Questo profilo mostra con chiarezza come, nell'ambiente digitale, la conservazione della prova sia distinta dalla sua acquisizione e possa costituire una fase autonoma e strategica dell'attività investigativa[33].

La centralità del prestatore produce, infine, inevitabili tensioni con la dimensione transnazionale dell'economia digitale. Molte piattaforme operano attraverso gruppi societari globali, infrastrutture distribuite e centri decisionali collocati anche al di fuori dell'Unione. Ne discende il rischio di conflitti tra l'obbligo di ottemperare all'ordine europeo e vincoli derivanti da ordinamenti di Paesi terzi, specie quando la produzione del dato possa violare divieti, procedure autorizzative o discipline straniere in materia di protezione dei dati, segreto, sicurezza nazionale o comunicazioni elettroniche. Il Regolamento prende in considerazione tale eventualità, prevedendo meccanismi di obiezione e riesame; nondimeno, il problema resta strutturale, poiché il prestatore globale è chiamato a muoversi entro una pluralità di regimi normativi potenzialmente incompatibili[34].

In definitiva, le piattaforme non diventano titolari del potere di decidere se e come procedere all'accertamento penale, ma governano le condizioni tecniche e organizzative di accesso a una parte crescente delle evidenze rilevanti per il processo. Per tale ragione, la loro funzione non può essere ridotta a quella di meri archivi privati, né sovrapposta a quella delle autorità giudiziarie; esse rappresentano, piuttosto, uno snodo regolato del nuovo ecosistema investigativo europeo, nel quale l'effettività della cooperazione penale transfrontaliera dipende dall'interazione tra titolo giudiziario, infrastruttura digitale, compliance privata e garanzie processuali. Questa interdipendenza costituisce uno dei tratti più innovativi e, al tempo stesso, più problematici del pacchetto *e-Evidence*.

5. Garanzie processuali e diritti fondamentali nella cooperazione diretta con le piattaforme

Il ruolo infrastrutturale delle piattaforme, descritto nel paragrafo precedente, assume rilievo soprattutto sul piano delle garanzie. La maggiore efficienza nell'acquisizione transfrontaliera delle prove elettroniche, perseguita attraverso gli ordini europei di produzione e di conservazione, impone di verificare la tenuta del modello di cooperazione diretta con i prestatori di servizi. La questione non si esaurisce nella tutela della riservatezza e della protezione dei dati personali, ma investe, in maniera più ampia, l'equilibrio tra rapidità dell'azione investigativa, controllo giurisdizionale, diritti della difesa ed effettività dei rimedi. Proprio perché l'ordine europeo può essere indirizzato direttamente al soggetto privato che detiene, conserva o controlla il dato, con un coinvolgimento solo eventuale o ridimensionato dell'autorità dello Stato di esecuzione, il profilo decisivo diviene la distribuzione dei controlli lungo l'intera filiera acquisitiva[35].

Il punto critico non risiede nell'assenza di garanzie, bensì nella loro diversa collocazione procedimentale. Il Regolamento delinea un sistema nel quale la verifica dei presupposti dell'ordine è affidata principalmente all'autorità dello Stato di emissione; l'autorità dello Stato di esecuzione

33. Sulla natura preservativa, e non immediatamente acquisitiva, del Certificato europeo di ordine di conservazione, si vedano gli artt. 6 e 11 Reg., relativi, rispettivamente, alle condizioni di emissione e all'esecuzione dell'ordine europeo di conservazione; cfr. altresì considerando n. 31 e n. 33 del medesimo regolamento, che valorizzano la funzione di impedire la cancellazione, alterazione o dispersione dei dati in vista di una successiva produzione. Nello stesso senso, Corte suprema di Cassazione, Ufficio del Massimario e del Ruolo, Servizio penale, *Relazione su novità normativa n. 25/2026*, 7 aprile 2026, § 5.4, sulla conservazione quale fase autonoma e anticipata di tutela della fonte digitale.

34. Il problema è espressamente considerato dall'art. 17 Reg., che disciplina il riesame dell'ordine europeo di produzione in caso di conflitto con obblighi derivanti dal diritto di un Paese terzo, consentendo al destinatario del Certificato europeo dell'ordine di produzione di formulare un'obiezione motivata ove l'esecuzione dell'ordine possa comportare la violazione di tali obblighi.

35. Cfr. artt. 5 e 6 Reg., sui requisiti di necessità, proporzionalità e ammissibilità della misura in un caso interno comparabile; artt. 8, 10-12 e 16 Reg., sul coinvolgimento dell'autorità di esecuzione, sull'esecuzione degli ordini e sui motivi di rifiuto; artt. 13 e 18 Reg., rispettivamente in tema di informazione dell'interessato e ricorsi effettivi.

interviene solo in ipotesi determinate, mentre la prima presa in carico dell'ordine si realizza presso il prestatore di servizi destinatario della richiesta. Ne deriva un assetto nel quale l'effettività della tutela dipende, non soltanto dalla qualità del titolo emesso dall'autorità procedente, ma anche dalla possibilità che l'interessato sia tempestivamente informato, che l'autorità di esecuzione possa intervenire nei casi necessari e che il prestatore sia in grado di riconoscere e segnalare eventuali profili ostativi all'esecuzione dell'ordine[36].

In questa architettura, i requisiti di necessità e proporzionalità costituiscono il primo argine all'ingiustificata espansione dello strumento. Tanto l'ordine europeo di conservazione quanto l'ordine europeo di produzione possono essere emessi solo se necessari e proporzionati rispetto alle finalità del procedimento penale e nel rispetto dei diritti della persona sottoposta alle indagini o imputata. Nel primo caso, il giudizio è calibrato sull'esigenza di impedire la cancellazione, la rimozione o la modifica dei dati; nel secondo, sull'acquisizione conoscitiva dell'informazione a fini probatori. In entrambi, il Regolamento introduce una clausola di equivalenza interna, richiedendo che una misura analoga sia ammissibile in un caso interno comparabile[37]. Tale clausola impedisce che lo strumento europeo sia impiegato come via più agevole per eludere le garanzie previste dall'ordinamento nazionale. La proporzionalità, pertanto, non può ridursi a una formula motivazionale di stile, ma deve tradursi in una verifica concreta della pertinenza, selettività e indispensabilità dei dati richiesti, specie quando l'ordine sia rivolto a piattaforme digitali capaci di concentrare una quantità elevatissima di informazioni relative non solo all'indagato, ma anche a terzi estranei al procedimento.

La graduazione delle garanzie si innesta sulla tassonomia dei dati elettronici prevista dal Regolamento. Gli ordini aventi a oggetto dati identificativi[38] o relativi agli abbonati[39] sono assoggettati a un regime più flessibile; quelli relativi a dati di traffico non richiesti al solo scopo di identificare l'utente o a dati di contenuto sono invece sottoposti a presupposti più rigorosi, in ragione della maggiore capacità intrusiva di tali informazioni. Per gli ordini europei di produzione relativi a dati di traffico o di contenuto, il Regolamento rafforza il controllo sull'emissione e collega l'accesso, salvo eccezioni specificamente individuate, alla gravità del reato, richiedendo che esso sia punito nello Stato di emissione con pena detentiva pari, nel massimo, ad almeno tre anni. La classificazione dei dati opera così come tecnica di regolazione dell'intrusività: quanto più l'informazione richiesta consente di ricostruire comunicazioni, relazioni, spostamenti, abitudini o contenuti della vita privata, tanto più il sistema pretende un controllo qualificato sull'accesso[40].

L'art. 1, par. 2, del Regolamento riconosce alla persona sottoposta alle indagini o imputata, nonché al suo difensore, la possibilità di richiedere

36. Cfr. art. 13 Reg., sull'informazione alla persona i cui dati sono richiesti; artt. 8 e 12 Reg., sul coinvolgimento dell'autorità di esecuzione e sui motivi di rifiuto; artt. 10, parr. 5-8, e 11, parr. 4-7, Reg., sulle interlocuzioni tra destinatario dell'ordine e autorità di emissione in caso di impossibilità o criticità esecutive; art. 17 Reg., sull'obiezione motivata per conflitto con obblighi derivanti dal diritto di un Paese terzo.
37. Le menzionate regole sull'adozione degli ordini sono contenute nell'art. 5 Reg. per l'OEP e nel successivo art. 6 per l'OEC.
38. I dati richiesti al solo scopo di identificare l'utente appaiono individuati secondo un criterio teleologico. Pensiamo agli indirizzi IP, dai quali si possono trarre informazioni anche con riguardo al sito visitato dall'utente, ma che rientrano nella categoria *de qua* se richiesti al solo scopo di identificazione. Per la definizione completa, si veda l'art. 3, n. 10, Reg.
39. I dati relativi agli abbonati sono, per esempio, quelli inerenti all'indirizzo e-mail fornito dall'utente o alla durata del servizio al quale si è abbonato; tra i "dati sul traffico", a titolo di esempio, rientrano quelli relativi alla fonte ed al destinatario di un messaggio e quelli sull'ubicazione, mentre sono "relativi al contenuto" i dati come il testo, la voce, i video, le immagini o il suono. Per le definizioni complete, si veda: art. 3, nn. 9, 11 e 12 Reg.
40. Cfr. art. 5, paragrafo 4, Reg. Al riguardo, la soglia edittale è ritenuta essere troppo bassa da Corhay 2021, pp. 448-449; stigmatizza invece l'assenza di un vaglio circa la sussistenza di un compendio indiziario minimo in ordine al fatto per cui si procede, Geraci 2019, p. 1360.

all'autorità competente l'emissione di un ordine europeo di produzione o di conservazione. Si tratta di una previsione significativa, perché sottrae gli strumenti *e-Evidence* a una lettura esclusivamente accusatoria e ne consente, almeno in astratto, l'impiego anche nella ricerca di elementi favorevoli all'indagato o all'imputato.

Questa apertura non elimina, tuttavia, le criticità connesse alla conoscibilità dell'acquisizione. Per l'ordine europeo di conservazione non è previsto un obbligo generale di informazione dell'utente, i cui dati siano oggetto di preservazione; l'interessato può dunque restare ignaro della misura anche dopo la sua esecuzione. Diversamente, per l'ordine europeo di produzione, il Regolamento impone all'autorità di emissione di informare senza indebito ritardo la persona i cui dati sono richiesti, pur consentendo che tale comunicazione sia ritardata o omessa quando ciò risulti necessario per non compromettere le indagini. La valutazione è rimessa alla stessa autorità procedente e si fonda su presupposti ampi, potenzialmente idonei a comprimere l'effettività del diritto all'informazione.

Ne deriva una tensione evidente tra segretezza investigativa e accesso ai rimedi. L'informazione all'interessato costituisce, infatti, il presupposto pratico per contestare la legittimità dell'acquisizione. Sebbene il Regolamento riconosca alla persona i cui dati siano stati prodotti mediante un ordine europeo di produzione, il diritto a un mezzo di impugnazione effettivo dinanzi a un organo giurisdizionale dello Stato di emissione, l'effettività di tale rimedio dipende dalla conoscenza dell'avvenuta acquisizione. Ancora più problematica appare la posizione dell'interessato rispetto all'ordine di conservazione, poiché non è previsto né un rimedio specifico avverso gli effetti della misura, né un obbligo generale di informazione che consenta di contestarne tempestivamente la legittimità[41].

Il profilo più delicato resta il ridimensionamento del ruolo dell'autorità di esecuzione.

Nel modello ordinario dell'*e-Evidence*, il rapporto primario intercorre tra autorità di emissione e prestatore di servizi. Per l'ordine europeo di conservazione e per l'ordine europeo di produzione avente a oggetto dati relativi agli abbonati o dati richiesti al solo scopo di identificare l'utente, il prestatore provvede senza il necessario coinvolgimento dell'autorità dello Stato in cui è stabilito il rappresentante o lo stabilimento designato: nel primo caso, preservando i dati; nel secondo, trasmettendoli all'autorità di emissione entro il termine previsto[42].

Qualora emergessero difficoltà di esecuzione dell'ordine, il primo interlocutore del destinatario rimane l'autorità di emissione. Il prestatore di servizi deve indicare le ragioni per le quali l'ordine non può essere eseguito, o non può esserlo nei termini, instaurando un dialogo diretto con l'autorità procedente, la quale può modificare o ritirare l'ordine. L'autorità di esecuzione viene coinvolta solo in ipotesi specifiche, ad esempio quando l'adempimento possa interferire con immunità o privilegi, con norme sulla libertà di stampa o di espressione oppure, con riferimento all'ordine europeo di produzione, quando possa determinare la violazione di obblighi derivanti dal diritto di un Paese terzo[43].

41. Cfr. artt. 13 Reg., il quale disciplina l'informazione alla persona i cui dati sono richiesti, consentendone tuttavia il ritardo o la limitazione nei casi previsti; 18 Reg., il quale riconosce alla persona i cui dati siano stati richiesti mediante ordine europeo di produzione il diritto a un ricorso effettivo dinanzi a un organo giurisdizionale dello Stato di emissione. Quanto all'ordine europeo di conservazione, si veda l'art. 11 Reg., il quale disciplina l'esecuzione senza prevedere un autonomo rimedio dell'interessato avverso la misura conservativa.
42. Cfr. artt. 11, par. 1, Reg., secondo il quale il destinatario dell'ordine europeo di conservazione deve conservare i dati richiesti senza indebito ritardo per il periodo previsto; 10, parr. 1 e 3, Reg., il quale disciplina l'esecuzione dell'ordine europeo di produzione, imponendo al destinatario di trasmettere i dati richiesti direttamente all'autorità di emissione o alle autorità di contrasto indicate nel certificato europeo dell'ordine di produzione, entro i termini stabiliti.
43. Cfr. art. 11, par. 4, Reg., per l'ordine europeo di conservazione, e art. 10, par. 5, Reg., per l'ordine europeo di produzione, i quali disciplinano le ipotesi in cui il destinatario dell'ordine non possa ottemperarvi, o non possa farlo entro il termine stabilito, prevedendo l'interlocuzione con l'autorità di emissione e, nei casi indicati, il coinvolgimento dell'autorità di esecuzione. Quanto al conflitto con obblighi derivanti dal diritto di un Paese terzo, si veda l'art. 17 Reg., il quale introduce una procedura di riesame dell'ordine europeo di produzione.

Lo Stato di esecuzione riacquista una posizione più incisiva solo in una fase successiva, qualora il prestatore non adempia e l'autorità di emissione richieda l'attivazione di meccanismi coercitivi. In tale ipotesi, l'autorità di esecuzione può ingiungere formalmente al destinatario di ottemperare, salva la possibilità di far valere motivi di rifiuto nei termini previsti dal Regolamento. L'inottemperanza successiva può esporre il prestatore a sanzioni particolarmente elevate, fino alla soglia massima individuata dal diritto unionale[44].

Un regime più garantito sembra essere previsto per gli ordini europei di produzione relativi a dati di traffico o di contenuto, quando non ricorrano determinate circostanze che riconducono il caso allo Stato di emissione. In tali ipotesi opera il c.d. regime con notifica: l'autorità di emissione deve notificare l'ordine anche all'autorità di esecuzione, la quale dispone di un termine per far valere eventuali motivi di rifiuto. Il coinvolgimento anticipato dello Stato di esecuzione consente, almeno in tali casi, un controllo ulteriore, soprattutto quando vengano in rilievo immunità, privilegi, libertà di stampa o libertà di espressione[45]. La portata di tale garanzia resta, tuttavia, circoscritta. Il regime con notifica non opera quando vi sia fondato motivo di ritenere che il reato sia stato commesso, sia in atto o possa essere commesso nello Stato di emissione, oppure quando la persona i cui dati sono richiesti risieda in tale Stato[46]. Considerato che, in molti procedimenti, l'unico elemento transfrontaliero consiste nella localizzazione del prestatore, del rappresentante legale o dello stabilimento designato in un altro Stato membro, è plausibile che la vicenda resti integralmente riconducibile allo Stato di emissione, con conseguente esclusione del regime notificatorio. Inoltre, la verifica delle condizioni che escludono la notifica è rimessa alla stessa autorità di emissione, con il rischio di una lettura restrittiva del coinvolgimento dello Stato di esecuzione.

Anche in questo caso il confronto con l'OEI permette di cogliere la portata del pacchetto. Nell'OEI l'autorità di esecuzione conserva un ruolo strutturale: interloquisce con quella di emissione, partecipa al riconoscimento e all'esecuzione dell'atto e può verificare, tra l'altro, la compatibilità della misura richiesta con i diritti fondamentali. Nel sistema *e-Evidence*, invece, una parte della funzione di filtro che nell'OEI appartiene all'autorità di esecuzione risulta essere anticipata sul prestatore di servizi. Nonostante il testo definitivo del Regolamento abbia corretto alcune criticità rispetto alla proposta originaria, introducendo il regime con notifica per taluni ordini relativi a dati di traffico o di contenuto[47], riconoscendo all'autorità di esecuzione la possibilità di far valere il motivo di rifiuto fondato sulla violazione dei diritti fondamentali[48], al di

44. Cfr. art. 16 Reg., il quale disciplina la procedura di esecuzione forzata degli ordini europei di produzione e conservazione in caso di mancata ottemperanza da parte del destinatario, attribuendo all'autorità di esecuzione il compito di ingiungere formalmente l'adempimento e di valutare gli eventuali motivi di rifiuto; si veda altresì l'art. 15 Reg., il quale impone agli Stati membri di prevedere sanzioni effettive, proporzionate e dissuasive, le quali possono arrivare sino al 2% del fatturato mondiale totale annuo del prestatore di servizi nell'esercizio precedente.
45. Cfr. art. 8 Reg., che disciplina la notifica all'autorità di esecuzione dell'ordine europeo di produzione relativo a dati di traffico, diversi da quelli richiesti al solo scopo di identificare l'utente, o a dati relativi al contenuto, salvo che il reato sia stato commesso, sia in corso o possa essere commesso nello Stato di emissione, oppure che la persona i cui dati sono richiesti risieda in tale Stato; art. 12 Reg., sui motivi di rifiuto opponibili dall'autorità di esecuzione, tra cui le ipotesi relative a immunità, privilegi, libertà di stampa e libertà di espressione in altri mezzi di comunicazione.
46. Cfr. art. 8, par. 2, Reg.
47. Cfr. art. 8 Reg.
48. Cfr. art. 12 Reg. Particolarmente significativa è, inoltre, la formulazione del motivo di rifiuto fondato sulla violazione dei diritti fondamentali. Gli artt. 12 e 16 del Regolamento lo ammettono soltanto in situazioni eccezionali, quando vi siano validi motivi per ritenere, sulla base di elementi concreti e oggettivi, che l'esecuzione o l'applicazione dell'ordine comporterebbe una violazione manifesta di un diritto fondamentale sancito dall'art. 6 TUE e dalla Carta. La Direttiva OEI, invece, consente il rifiuto quando vi siano seri motivi per ritenere che l'esecuzione dell'atto richiesto sia incompatibile con gli obblighi dello Stato di esecuzione ai sensi dell'art. 6 TUE e

fuori delle ipotesi di notifica, l'intervento dell'autorità pubblica dello Stato di esecuzione resta eventuale e successivo, mentre il primo filtro operativo è rimesso al destinatario privato[49]. E proprio sotto questo punto di vista, il ruolo centrale attribuito alle piattaforme, si mostra nella sua problematicità. Il prestatore può segnalare difficoltà di esecuzione, interferenze con immunità, privilegi o libertà fondamentali, nonché conflitti con obblighi derivanti da ordinamenti di Paesi terzi. Tuttavia, esso non è un'autorità indipendente di garanzia, non è collocato in posizione di neutralità istituzionale e non dispone necessariamente delle competenze giuridiche richieste per valutare compiutamente l'incidenza dell'ordine sui diritti fondamentali. A ciò si aggiunge che il prestatore opera sotto la pressione di un possibile apparato sanzionatorio, circostanza che può incentivare l'adempimento anche nei casi in cui un controllo pubblico più approfondito sarebbe opportuno[50].

Il ridimensionamento del ruolo dello Stato di esecuzione emerge, poi, anche sul piano temporale. Esso, quando viene coinvolto, dispone di termini assai brevi (10 giorni) per far valere eventuali motivi di rifiuto[51]. Inoltre, il Regolamento non contiene una disposizione analoga a quella dell'OEI che impone, ove in un caso interno comparabile sia necessaria l'autorizzazione di un organo giurisdizionale nello Stato di esecuzione, il ricorso alla medesima autorizzazione, con il risultato che il controllo dello Stato di esecuzione sia meno intenso e strutturato[52].

Anche il regime dei rimedi sembra confermare questa impostazione. La persona i cui dati siano stati prodotti mediante un ordine europeo di produzione ha diritto a un ricorso effettivo dinanzi a un organo giurisdizionale dello Stato di emissione. La scelta è coerente con la giurisprudenza della Corte di giustizia in materia di ordine europeo di indagine, che ha valorizzato la necessità di rimedi effettivi nello Stato emittente[53]; tuttavia, il Regolamento non contempla espressamente la possibilità di impugnare l'ordine anche nello Stato di esecuzione. La clausola secondo cui restano salve le garanzie dei diritti fondamentali nello Stato di esecuzione presenta, sotto questo profilo, un contenuto ambiguo: non è chiaro se essa possa fondare un controllo effettivo sulle garanzie previste dall'ordinamento dello Stato di esecuzione, né se il giudice dello Stato di emissione sia sempre il soggetto più idoneo a svolgere tale verifica. In molti casi, lo Stato di esecuzione non viene neppure informato circa l'esecuzione di un ordine rivolto a un prestatore stabilito o rappresentato nel proprio territorio. La ragione di una simile scelta risiede nella peculiarità del nuovo modello: lo Stato di esecuzione è spesso tale soltanto perché in esso si trova il rappresentante legale o lo stabilimento designato del prestatore di servizi, mentre il procedimento, il reato e la persona interessata possono non presentare alcun legame effettivo con quell'ordinamento[54].

Questa spiegazione, tuttavia, non esaurisce il problema. Il Regolamento non sembra considerare

della Carta. La differenza lessicale non è neutra: nel Regolamento *e-Evidence* la tutela dei diritti fondamentali appare costruita come eccezione qualificata alla regola dell'esecuzione, mentre nell'OEI essa opera come limite generale alla cooperazione.

49. Cfr. Commissione europea, doc. COM(2018) 225, 17 aprile 2018.
50. Tosza 2021, p. 8 ss.
51. Cfr. art. 12 Reg.
52. Segnatamente, come detto, dieci giorni dalla notifica, ove prevista (art. 12, paragrafo 1, Reg.); cinque giorni lavorativi dalla ricezione della documentazione proveniente dall'autorità di emissione a seguito dell'inadempimento del privato, in linea generale (art. 16, paragrafo 2, Reg.).
53. Cfr. Corte giust., 11 novembre 2021, C-852/19, *Gavanozov II*, sul diritto a un ricorso effettivo nello Stato di emissione dell'ordine europeo di indagine; con riferimento all'art. 18 Reg. e ai profili problematici del rimedio nello Stato di emissione, si veda Kiejnich-Kruk 2024, p. 135.
54. Cfr. art. 8 Reg., sulla notifica all'autorità di esecuzione e sulle ipotesi in cui essa non è richiesta; art. 7 Reg., sull'individuazione del destinatario dell'ordine nello stabilimento designato o nel rappresentante legale; art. 3, nn. 13-16, Reg., sulle nozioni di Stato di emissione e Stato di esecuzione, sul carattere in parte artificiale del collegamento con lo Stato di esecuzione, quando esso dipenda dalla sola localizzazione del rappresentante o dello stabilimento designato del prestatore.

adeguatamente l'ipotesi in cui la persona interessata risieda in uno Stato membro diverso sia da quello di emissione sia da quello in cui è stabilito il rappresentante del prestatore. In tale situazione, l'autorità più prossima alla tutela delle prerogative individuali potrebbe non coincidere né con quella di emissione né con quella di esecuzione, bensì con quella dello Stato di residenza dell'interessato. La mancata previsione di un coinvolgimento di tale Stato è stata letta come una occasione mancata per costruire un sistema di garanzie più aderente alla natura realmente transnazionale della prova elettronica[55].

Alla luce di questi elementi, il pacchetto *e-Evidence* si colloca in una posizione ambivalente. Da un lato, positivizza condizioni, categorie di dati, requisiti di proporzionalità, limiti oggettivi e rimedi, superando la frammentarietà delle prassi precedenti e offrendo una base uniforme all'acquisizione transfrontaliera delle prove elettroniche. Dall'altro, il modello di cooperazione diretta, il ridimensionamento dello Stato di esecuzione, la centralità del prestatore di servizi e la debolezza di alcuni obblighi informativi fanno emergere il rischio di una riduzione del livello di tutela rispetto agli standard maturati nell'ambito dell'OEI e della giurisprudenza della Corte di giustizia.

Il punto, naturalmente, non è negare l'esigenza di strumenti più rapidi ed efficaci. La volatilità dei dati, la loro frequente delocalizzazione e la centralità tecnica dei prestatori rendono spesso inadeguati i canali cooperativi tradizionali. Tuttavia, l'efficienza investigativa non può tradursi in una riduzione strutturale delle garanzie. Se la cooperazione diretta costituisce la via più funzionale per raggiungere i dati detenuti dalle piattaforme, essa deve essere accompagnata da controlli capaci di compensare la disintermediazione dello Stato di esecuzione e il coinvolgimento di soggetti privati nella fase esecutiva[56].

In conclusione, il sistema delineato dal Regolamento non appare privo di garanzie, ma presenta un equilibrio ancora instabile. La sua tenuta dipenderà dalla capacità delle autorità nazionali e della giurisprudenza europea di interpretare i requisiti di necessità e proporzionalità in modo sostanziale, di assicurare un controllo effettivo sugli ordini più invasivi, di valorizzare il diritto all'informazione e al ricorso e di evitare che il prestatore di servizi divenga il principale filtro di tutela dei diritti individuali.

La questione decisiva non sembra dunque consistere nella necessità di stabilire se la cooperazione diretta con i prestatori di servizi sia, in astratto, compatibile con la tutela dei diritti fondamentali, quanto piuttosto nell'individuare quali siano le condizioni in cui essa possa esserlo, senza che la rapidità nell'accesso alla prova elettronica si traduca in una riduzione strutturale del controllo giurisdizionale, dell'informazione dell'interessato e dell'effettività dei rimedi.

6. Considerazioni conclusive.

Complessivamente, il pacchetto *e-Evidence* sembra costituire una prima effettiva risposta alla trasformazione digitale dell'accertamento penale, attraverso l'introduzione di un modello di accesso più diretto, uniforme e calibrato sulle caratteristiche dell'ambiente digitale[57].

Le novità non si esauriscono nella creazione di nuovi strumenti acquisitivi ma investono l'intero processo penale. L'autorità giudiziaria non si rivolge più, solo, ad un'altra autorità statale, secondo il paradigma classico della cooperazione penale, bensì direttamente al prestatore di servizi digitali determinando, parallelamente, una parziale disintermediazione dello Stato di esecuzione ed una crescente responsabilizzazione dei soggetti privati che detengono, organizzano e/o rendono accessibili le informazioni digitali[58].

55. Cfr. Christakis 2025, p. 198.
56. Sachoulidou 2024, p. 267 ss.; Tosza 2024, p. 147 ss., pp. 152-153; Calavita 2021, p. 204; Rosanò 2020, pp. 16-17.
57. Cfr.: considerando nn. 7-9 e 12 Regolamento (UE) 2023/1543; Commissione europea, Impact Assessment, SWD (2018) 118 final, §§ 2.1-2.2; Corte suprema di cassazione, Ufficio del Massimario e del Ruolo, Servizio penale, Rel. n. 25/2026, 7 aprile 2026, Parte I, § 1.
58. Sulla cooperazione diretta con i prestatori di servizi quale elemento qualificante del nuovo modello e sul conseguente ridimensionamento dello schema interstatale tradizionale, si veda il considerando 12 Regolamento (UE) 2023/1543; gli artt. 7, 9-11 Regolamento (UE) 2023/1543.

In questo scenario i prestatori di servizi possono essere definiti come *gatekeepers* della cooperazione penale digitale[59]: non titolari della funzione giurisdizionale, né del potere di decidere sull' *an* dell'acquisizione probatoria, bensì detentori delle condizioni tecniche e organizzative di accesso alla prova. Del resto, in assenza di un loro diretto coinvolgimento, l'effettività dell'acquisizione probatoria rischierebbe di risultare compromessa.

Come analizzato, il pacchetto tenta di governare questa interdipendenza attraverso una duplice strategia: da un lato, tipizza gli ordini europei, le categorie di dati, i presupposti di emissione, i termini di risposta e i rimedi; dall'altro, attraverso la Direttiva (UE) 2023/1544, costruisce l'interfaccia organizzativa necessaria affinché l'ordine possa raggiungere operatori spesso transnazionali, imponendo la designazione di uno stabilimento o la nomina di un rappresentante legale. Il legislatore europeo ha dunque predisposto le condizioni affinché il potere di richiedere la cooperazione diretta all'infrastruttura privata che governa il dato possa essere effettivamente esercitato

L'equilibrio resta, tuttavia, instabile.

La maggiore efficienza dell'acquisizione transfrontaliera si ottiene attraverso un modello che concentra molte garanzie nello Stato di emissione, riduce il ruolo ordinario dello Stato di esecuzione e attribuisce al prestatore la funzione di primo filtro operativo. Se, da un certo punto di vista, ciò produce benefici evidenti in termini di tempestività, specialmente di fronte a dati esposti a cancellazione, sovrascrittura o dispersione; d'altro canto, solleva interrogativi circa l'effettività della tutela rivolta alla persona interessata[60].

Sebbene il pacchetto nasca con l'intento di rispondere all'esigenza di acquisire prove elettroniche nel corso di procedimenti penali nei quali l'elemento transfrontaliero generalmente dipende dalla localizzazione del prestatore di servizi, la logica che esso inaugura (accesso diretto al soggetto privato che detiene la prova, riduzione dell'intermediazione statale, centralità della compliance privata), potrebbe incidere in modo più ampio sul futuro della cooperazione penale europea.

La sfida sembra essere duplice. Sul piano dell'effettività occorrerà in primo luogo verificare se i prestatori di servizi riusciranno a rispondere agli ordini europei nei tempi e con il livello di precisione stabiliti; in secondo luogo, se gli uffici giudiziari sapranno dotarsi di competenze tecniche e organizzative adeguate. Sul piano delle garanzie sarà necessario evitare che la rapidità dell'accesso alla prova elettronica si traduca in una riduzione strutturale del controllo giurisdizionale, del diritto all'informazione e dell'effettività dei rimedi.

In un simile contesto il compito del diritto processuale penale europeo sembra essere quello di governare la (necessaria) relazione tra autorità statali e prestatori di servizi digitali, assicurando che l'efficienza della cooperazione diretta non comporti l'esternalizzazione delle garanzie e che i prestatori di servizi, quali snodo indispensabile per l'acquisizione probatoria, non si trasformino in quel luogo in cui il controllo pubblico sulla formazione della prova si attenui.

Riferimenti bibliografici

A. Aguinaldo, P. De Hert (2025), *Moving in the Right Direction for Transborder Access to Digital Evidence in Criminal Matters? The Council of Europe and the Second Additional Protocol Introducing Direct Cooperation Mechanisms*, in V. Franssen, S. Tosza (Eds.), "The Cambridge Handbook of Digital Evidence in Criminal Investigations", Cambridge University Press, 2025

59. In senso affine, sul rischio di una privatizzazione della fiducia reciproca e sul ruolo dei prestatori di servizi quali snodi centrali della cooperazione penale digitale, si veda Mitsilegas 2018, pp. 264-265; Tosza 2024, p. 143 ss., p. 159 ss., ove i prestatori di servizi sono descritti come gatekeepers dei dati e, nel nuovo modello di cooperazione diretta, come primo filtro delle richieste provenienti dalle autorità di law enforcement, con conseguente spostamento su soggetti privati di valutazioni potenzialmente incidenti anche sulla tutela dei diritti fondamentali.

60. In senso critico sul modello di cooperazione diretta, con particolare riferimento alla concentrazione delle garanzie nello Stato di emissione, al ridimensionamento dell'autorità di esecuzione e al ruolo del prestatore di servizi quale primo filtro operativo dell'ordine, si veda Sachoulidou 2024, p. 267 ss.

S. Allegrezza (2020), *L'acquisizione delle prove elettroniche nel processo penale*, in "Rivista italiana di diritto e procedura penale", 2020

M. Caianiello (2022), *Il procedimento penale europeo*, Giappichelli, 2022

O. Calavita (2025), *L'ordine europeo di indagine penale. Presente e futuro della cooperazione probatoria nell'Unione europea*, CEDAM, 2025

O. Calavita (2021), *La proposta di Regolamento sugli ordini di produzione e conservazione europei: Commissione, Consiglio e Parlamento a confronto*, in "La legislazione penale", 2021

T. Christakis (2025), *From Mutual Trust to the Gordian Knot of Notifications: The EU e-Evidence Regulation and Directive*, in V. Franssen, S. Tosza (Eds.), "The Cambridge Handbook of Digital Evidence in Criminal Investigations", Cambridge University Press, 2025

M. Corhay (2021), *Private Life, Personal Data Protection and the Role of Service Providers: The EU e-Evidence Proposal*, in "European Papers", 2021, n. 1

S. Cutrignelli (2023), *La prova informatica nella pratica investigativa*, in "disCrimen", 2023, n. 2

V. Daskal (2015), *The Un-Territoriality of Data*, in "Yale Law Journal", 2015, n. 2

A. De Maio (2026), *L'acquisizione delle prove elettroniche nello spazio di libertà, sicurezza e giustizia: prime applicazioni dell'e-Evidence package*, in "RLF Express", 2026, n. 9

F. Ertola (2025), *L'ordine europeo di indagine penale*, in G. Ubertis, G.P. Voena (a cura di), "Trattato di procedura penale", Giuffrè, 2025

J.A. Espina Ramos (2025), *European Preservation and Production Orders: A Non-Exclusive Approach to E-Evidence within the EU*, in "Eucrim", 2025

G. Forlani (2023), *The E-Evidence Package. The Happy Ending of a Long Negotiation Saga*, in "Eucrim", 2023, n. 2

V. Franssen, S. Tosza (2025), *Introduction: Gathering Electronic Evidence and Cooperation with Service Providers in the Digital Era – A Jigsaw Puzzle of Technological and Legal Challenges*, in V. Franssen, S. Tosza (Eds.), "The Cambridge Handbook of Digital Evidence in Criminal Investigations", Cambridge University Press, 2025

A. Gaudieri (2023), *Novità in tema di cooperazione giudiziaria: i nuovi ordini europei di conservazione e produzione delle prove elettroniche*, in "Diritto penale e processo", 2023

R.M. Geraci (2019), *La circolazione transfrontaliera delle prove digitali in UE: la proposta di Regolamento e-Evidence*, in "Cassazione penale", 2019, n. 3

C. Grandi (2021), *Il mutuo riconoscimento dei provvedimenti di confisca alla luce del Regolamento (UE) 2018/1805*, in "La legislazione penale", 31 maggio 2021

A. Kiejnich-Kruk (2024), *Quo vadis Europa? Balancing between efficiency and guarantees in criminal proceedings using the example of EU production and preservation orders*, in "New Journal of European Criminal Law", 2024, n. 2

A.M. Maugeri (2019), *Il regolamento (UE) 2018/1805 per il reciproco riconoscimento dei provvedimenti di congelamento e di confisca: una pietra angolare per la cooperazione e l'efficienza*, in "Diritto penale contemporaneo", 16 gennaio 2019

V. Mitsilegas (2018), *The privatisation of mutual trust in Europe's area of criminal justice: The case of e-Evidence*, in "Maastricht Journal", 2018, n. 3

A. Nascimbeni (2022), *Ordine europeo di indagine penale e diritti fondamentali*, in "Rivista italiana di diritto e procedura penale", 2022

P. Raucci (2025), *L'ordine europeo di indagine e prove digitali: tra presunzione di legittimità degli atti compiuti all'estero e diritti fondamentali*, in "Giurisprudenza penale", 2025

A. Rosanò (2020), *Il nuovo mondo della cooperazione giudiziaria in materia penale nell'Unione europea: le proposte della Commissione europea sugli ordini di produzione e conservazione di prove elettroniche (e-evidence)*, in "La legislazione penale", 16 ottobre 2020

A. Sachoulidou (2024), *Cross-border access to electronic evidence in criminal matters: The new EU legislation and the consolidation of a paradigm shift in the area of "judicial" cooperation*, in "New Journal of European Criminal Law", 2024, n. 3

F. Siracusano (2017), *La prova informatica transnazionale: un difficile "connubio" tra innovazione e tradizione*, in "Processo penale e giustizia", 2017

D. Svantesson, A.M. Osula (2025), *Unresolved Jurisdictional Issues in Law Enforcement Access to Data,* in V. Franssen, S. Tosza (Eds.), "The Cambridge Handbook of Digital Evidence in Criminal Investigations", Cambridge University Press, 2025

S. Tosza (2024), *Mutual Recognition by Private Actors in Criminal Justice? E-Evidence Regulation and Service Providers as the New Guardians of Fundamental Rights*, in "Common Market Law Review", 2024, n. 1

S. Tosza (2021), *Internet service providers as law enforcers and adjudicators. A public role of private actors*, in "Computer Law & Security Review", vol. 43, 2021

T. Wahl (2023), *E-Evidence Regulation and Directive Published*, in "Eucrim", 2023