CORTE SUPREMA DI CASSAZIONE

UFFICIO DEL MASSIMARIO E DEL RUOLO

Servizio Penale

Relazione su novità normativa

Individuazione delle autorità competenti di cui all'articolo 31 del Regolamento (UE) 2023/1543 del Parlamento europeo e del Consiglio, del 12 luglio 2023, relativo agli ordini europei di produzione e agli ordini europei di conservazione di prove elettroniche nei procedimenti penali e per l'esecuzione di pene detentive a seguito di procedimenti penali, nonché' delle procedure per l'emissione, ricezione, esecuzione e riesame degli ordini europei di produzione e di conservazione
(d.lgs. 30 dicembre 2025, n. 215,* pubblicato sulla Gazzetta Ufficiale, Serie generale n. 11 del 15/01/2026 ed entrato in vigore il 30/01/2026*)

Rel. n. 25/2026 **Roma, 07 aprile 2026**

***

SOMMARIO:

PARTE I. Il quadro europeo della prova digitale.
1. Premessa sistematica: la prova digitale nel processo penale contemporaneo.
2. La costruzione giurisprudenziale europea in tema di acquisizione delle prove digitali.
3. Il quadro normativo europeo dell'*e-evidence*: struttura del sistema e opzioni di fondo.
4. Il rapporto tra *e-evidence* e ordine europeo di indagine nel sistema della cooperazione probatoria europea.

PARTE II. L'attuazione nazionale dell'*e-evidence package* e il modello processuale degli ordini europei.
5. Architettura eurounitaria degli ordini: tipologie, categorie di dati e condizioni di emissione.
6. Innesto nel processo penale italiano: competenze, iniziativa, formazione dell'atto e regime di conoscibilità dei dati (artt. 2 e 3 d.lgs. n. 215 del 2025).
7. Procedure di urgenza, emergenza e accelerazione nell'emissione ed esecuzione degli ordini europei (artt. 2, 3 e 4 d.lgs. n. 215 del 2025; artt. 10, par. 4, e 12 Reg.).
8. La cooperazione in entrata: ricezione, esecuzione e assetto delle competenze (artt. 5 e 6 d.lgs. n. 215 del 2025).
9. La cooperazione in uscita: notifica e controllo (artt. 8, 10 e 12 Reg.; art. 6 d.lgs. n. 215 del 2025).
10. Le obiezioni del prestatore di servizi e il riesame giurisdizionale nello Stato di emissione (art. 17 Reg.; art. 7 d.lgs. n. 215 del 2025).

11. La clausola di inutilizzabilità e il regime processuale della prova acquisita mediante ordine europeo (art. 2, comma 7, d.lgs. n. 215 del 2025).
12. Il coordinamento tra sistema *e-evidence* e disciplina nazionale della conservazione dei dati: adeguamento della *data retention* e introduzione dell'ordine di conservazione processuale (art. 9, comma 1, d.lgs. n. 215 del 2025; art. 132 d.lgs. n. 196 del 2003).
13. L'introduzione dell'ordine di conservazione nel processo penale (art. 9, comma 2, d.lgs. n. 215 del 2025; art. 263-*bis* c.p.p.).
14. Monitoraggio dell'attuazione e obblighi informativi nel sistema *e-evidence* (art. 8 d.lgs. n. 215 del 2025).

PARTE III. Le ricadute organizzative e le prospettive di sistema.
15. Prime ricadute sull'organizzazione degli uffici giudiziari.
16. Osservazioni conclusive.

****

Parte I

Il quadro europeo della prova digitale.

1. Premessa sistematica: la prova digitale nel processo penale contemporaneo.

Nel processo penale contemporaneo, la prova digitale ha assunto un ruolo strutturale, non più confinato a specifiche categorie di reati, ma rilevante anche per l'accertamento di fattispecie tradizionalmente estranee alla dimensione tecnologica. Comunicazioni elettroniche, dati di accesso, contenuti digitali e informazioni di traffico pervadono e accompagnano le nostre esistenze, sicché, di riflesso, costituiscono oggi una componente ordinaria dell'accertamento penale.

A tale evoluzione si collega l'esigenza di una gestione consapevole di tale patrimonio informativo, che – in ragione della sua modificabilità, della rapidità di circolazione e del rischio di dispersione – richiede cautele e regole adeguate di conservazione, raccolta e analisi[1].

Le caratteristiche appena descritte hanno inciso sia sulle modalità di formazione della prova digitale sia sui tradizionali criteri territoriali di acquisizione, evidenziando i limiti di un modello investigativo ancorato alla collocazione fisica del dato. L'immaterialità e la delocalizzazione delle informazioni elettroniche rendono, infatti, sempre più frequente la dissociazione tra il luogo dell'indagine, quello di conservazione dei dati e quello di stabilimento del prestatore di servizi. Ne risulta la crisi degli strumenti di cooperazione fondati su logiche territoriali e su forme di collaborazione mediata tra Stati, spesso incompatibili con l'esigenza di tempestivo conseguimento delle informazioni.

Assume rilievo centrale la tracciabilità delle operazioni di acquisizione, conservazione e analisi – comunemente ricondotta alla nozione di *chain of custody* – quale presupposto necessario per assicurare autenticità, integrità e affidabilità del materiale informativo utilizzato a fini investigativi[2]. Il controllo di legalità tende così a concentrarsi sulla verificabilità

[1] S. CUTRIGNELLI, *La prova informatica nella pratica investigativa*, in *Discrimen*, 3 luglio 2023.
[2] Cfr. S. CUTRIGNELLI, *op. cit.*, in tema di corretta acquisizione e conservazione del dato digitale quale presupposto della sua affidabilità probatoria.

documentale e tecnica delle operazioni compiute, in un contesto nel quale la fase esecutiva si svolge sempre più spesso presso soggetti privati detentori dei dati.

Le trasformazioni descritte non riguardano soltanto il piano tecnico-operativo, ma arrivano ad incidere sul modello stesso di accertamento penale. Il passaggio da fonti probatorie materialmente localizzate a informazioni digitali – la cui esistenza, conservazione e intelligibilità dipendono da infrastrutture tecnologiche – comporta una trasformazione epistemologica della prova penale, destinata a riflettersi tanto sulla dimensione spaziale dell'indagine quanto sugli equilibri interni del processo.

Si assiste, da un lato, a una progressiva attenuazione della centralità del dibattimento quale luogo esclusivo di formazione della prova; parallelamente, si rafforza il ruolo del giudice, chiamato a confrontarsi con metodologie tecniche e conoscenze specialistiche e ad esercitare un controllo critico sugli strumenti utilizzati, al fine di evitare indebite deleghe cognitive all'esperto[3].

Per lungo tempo, tali trasformazioni si sono sviluppate in assenza di una disciplina specificamente calibrata sulle caratteristiche dell'ambiente digitale, riflettendo il fisiologico ritardo di adattamento del processo alle innovazioni tecnologiche e scientifiche.

Le tensioni generate dalla delocalizzazione dei dati e dall'incidenza delle attività investigative sui diritti fondamentali hanno trovato una prima sistematica elaborazione nella giurisprudenza della Corte di giustizia dell'Unione europea (di seguito: CGUE), progressivamente chiamata a definire le condizioni di accesso ai dati elettronici a fini investigativi e il necessario bilanciamento tra effettività dell'azione penale e tutela della persona.

Tale evoluzione ha reso evidente la necessità di un intervento normativo unitario a livello sovranazionale, volto a superare i limiti dei tradizionali strumenti di cooperazione giudiziaria, con l'obiettivo di introdurre modalità più rapide ed efficaci di acquisizione transfrontaliera dei dati elettronici e di ricondurre l'accesso alle informazioni entro un quadro di garanzie uniforme e coerente con gli *standard* di tutela dei diritti fondamentali delineati dalla CGUE.

Si colloca in tale evoluzione l'adozione, da parte del legislatore dell'Unione europea, del sistema di acquisizione comunemente definito *e-evidence package*, composto dal regolamento (UE) 2023/1543 (di seguito: Regolamento), relativo agli ordini europei di produzione e di conservazione nei procedimenti penali, e dalla direttiva (UE) 2023/1544 (di seguito: Direttiva), concernente la designazione dei rappresentanti legali dei prestatori di servizi ai fini della raccolta di prove nei procedimenti penali.

A tale quadro normativo si collega l'intervento del legislatore nazionale, che ha dato attuazione al nuovo sistema mediante i d.lgs. 30 dicembre 2025, nn. 215 e 216. Oggetto del

[3] Dinamiche analoghe erano già emerse, invero, con riferimento alle intercettazioni e alla prova scientifica, ambiti nei quali l'ingresso di saperi tecnici specialistici ha imposto un rafforzamento del ruolo di controllo del decidente sull'affidabilità metodologica degli strumenti utilizzati. Sul rapporto tra giudice e prova scientifica, in dottrina si vedano: G. CANZIO-L. DONATI LUPARIA (a cura di), *Prova scientifica e processo penale*, Milano, 2022; A. FAMIGLIETTI, *Questioni aperte: un giudizio penale che prescinde dalle leggi scientifiche?*, in *Archivio Penale*, 2025, n. !; L. FERRAJOLI, *Diritto e ragione. Teoria del garantismo penale*, Roma-Bari, 2009; G. GENNARI, *Il giudice e la prova scientifica*, Torino, 2012; F. GIANGRECO, *Limiti, paradossi e potenzialità della prova algoritmica*, in *La Legislazione Penale*, 15 febbraio 2025; M. TARUFFO, *La prova dei fatti giuridici. Nozioni generali*, Milano, 1992; G. UBERTIS, *Perizia, prova scientifica e intelligenza artificiale nel processo penale*, in *Sist. pen.*, 3 giugno 2024.

presente studio è il primo dei decreti indicati, che introduce nel diritto nazionale la disciplina degli ordini europei di produzione e di conservazione di prove elettroniche.

1.1. L'indagine si articola in **tre parti**.

La Parte I ricostruisce il percorso evolutivo e le ragioni che hanno condotto, nel diritto dell'Unione europea, all'adozione del sistema di acquisizione transfrontaliera delle prove elettroniche, offrendo una chiave di lettura necessaria per cogliere la *ratio* dell'intervento normativo e orientarne l'interpretazione.

La Parte II è dedicata all'esame del d.lgs. n. 215 del 2025, con particolare riguardo alla struttura degli strumenti previsti, alle procedure applicabili e alle garanzie stabilite, con attenzione ai principali profili interpretativi e applicativi.

La Parte III considera le implicazioni sistematiche del nuovo assetto nel contesto del processo penale interno e del sistema di cooperazione giudiziaria penale.

1.2. La complessità del quadro delineato e la pluralità dei livelli normativi e operativi coinvolti rendono necessario precisare preliminarmente il significato delle **principali categorie terminologiche utilizzate**.

Le locuzioni "prova informatica", "prova elettronica" e "prova digitale" sono utilizzate nella prassi per indicare dati e informazioni in formato elettronico suscettibili di assumere rilievo probatorio nel processo penale, indipendentemente dal mezzo o dal supporto mediante il quale sono generati, trasmessi o conservati[4].

Nel prosieguo, l'espressione "prova digitale" – che, nel lessico del diritto dell'Unione europea, trova un riferimento nella nozione di *electronic evidence* (*e-evidence*) – sarà impiegata, in senso ampio e atecnico, quale categoria comprensiva dei dati informatici e telematici[5] e, in senso funzionale, quale formula di sintesi riferita all'insieme delle attività di acquisizione e utilizzo investigativo delle informazioni elettroniche, anche al di fuori della fase di formazione della prova processuale in senso stretto.

È altresì rilevante la distinzione tra informazioni elettroniche già esistenti e conservate – quali dati relativi agli abbonati, dati di accesso, dati di traffico o contenuti archiviati – e flussi comunicativi in corso, la cui acquisizione implica attività di captazione o monitoraggio in tempo reale.

---

[4] Cfr. S. CONTI, *La legislazione in materia di prove digitali nell'ambito del processo penale. Uno sguardo all'Italia*, in *Informatica e dir.*, 2015, n. 1-2, p. 153 e ss.

[5] Si registra un uso non sempre uniforme delle espressioni "prova informatica" e "prova digitale", frequentemente impiegate in senso sostanzialmente sovrapponibile. Tuttavia, la prima locuzione risulta storicamente connessa al dato trattato mediante sistemi informatici e al contesto originario della disciplina dei reati informatici nell'ordinamento interno, mentre la seconda tende a valorizzare la natura immateriale, replicabile e tecnologicamente neutra dell'informazione elettronica, affermandosi progressivamente anche nel lessico sovranazionale quale categoria più ampia, atta a ricomprendere l'insieme delle evidenze elettroniche rilevanti nel processo penale. La nozione di "prova telematica", invece, viene utilizzata per riferirsi più specificamente ai dati generati o trasmessi attraverso reti di comunicazione elettronica, con particolare riguardo alle comunicazioni e ai dati di traffico. Spunti ricostruttivi sul tema in: A. SANNA, *La prova informatica al vaglio del giudice, tra cattiva scienza e cattivi scienziati*, in *Discrimen*, 4 maggio 2022; L. CUOMO, *La prova digitale*, in G. CANZIO-L. LUPARIA DONATI (a cura di), *op. cit.*, p. 623 e ss. Nel presente lavoro, le espressioni saranno utilizzate tendenzialmente secondo un criterio funzionale: la locuzione "prova digitale" verrà impiegata quale categoria generale descrittiva del fenomeno probatorio connesso ai dati elettronici; il sintagma "prova elettronica" sarà utilizzato prevalentemente in riferimento al lessico proprio del diritto dell'Unione europea e, in particolare, alla disciplina dell'*electronic evidence*; la nozione di "prova informatica" verrà invece richiamata nei passaggi riferiti alla tradizione dogmatica e normativa dell'ordinamento interno.

Tale discrimine consente di cogliere l'ambito applicativo degli strumenti europei di acquisizione delle prove elettroniche, circoscritto ai dati già formati e non esteso alle attività di intercettazione. Recepita nel nostro diritto positivo[6] e valorizzata dalla giurisprudenza[7], la distinzione incide sul regime delle garanzie applicabili, sui presupposti di legittimità degli atti di accesso ai dati e sull'individuazione dell'autorità competente all'emissione e al controllo dei relativi provvedimenti.

Chiarito il significato delle categorie terminologiche di riferimento e delimitato l'ambito applicativo degli strumenti europei relativi alle prove elettroniche, è ora opportuno ricostruire il percorso evolutivo che, nel diritto dell'Unione europea, ha condotto all'elaborazione del nuovo sistema normativo.

2. La costruzione giurisprudenziale europea in tema di acquisizione delle prove digitali.

Il quadro normativo europeo in materia di acquisizione delle prove elettroniche affonda le proprie radici nella giurisprudenza della Corte di giustizia[8], che ha definito i limiti di compatibilità con il diritto dell'Unione dei regimi di conservazione generalizzata e indifferenziata dei dati di traffico, ammettendoli solo entro confini rigorosi e individuando, quale modello ordinario, forme di conservazione mirata, temporalmente circoscritta e giustificata da esigenze specifiche.

Il nuovo sistema *e-evidence* rispecchia tale impostazione: la disponibilità del dato digitale non è più affidata a obblighi generalizzati di conservazione, ma a meccanismi selettivi e funzionalizzati all'attività investigativa.

Volendo ripercorrere i momenti cruciali del percorso tracciato dalla Corte di giustizia, la prima tappa fondamentale è rappresentata da **CGUE, 8 aprile 2014, cause riunite C-293/12 e C-594/12, *Digital Rights Ireland***, con cui è stata dichiarata l'invalidità della direttiva 2006/24/CE sulla conservazione dei dati di traffico[9]. Nell'occasione, la Corte ha statuito che la conservazione generalizzata e indifferenziata dei dati elettronici relativi alle comunicazioni costituisce un'ingerenza di particolare gravità nei diritti fondamentali al rispetto della vita privata e alla protezione dei dati personali, garantiti dagli artt. 7 e 8 della Carta dei diritti fondamentali dell'Unione europea (di seguito: CDFUE).

---

[6] Nel diritto positivo interno, la distinzione tra flussi comunicativi in corso e dati comunicativi già formati e conservati trova un preciso riscontro normativo nella separazione tra la disciplina delle intercettazioni di comunicazioni, riservata alla captazione in tempo reale e assoggettata a presupposti rigorosi e a controllo giurisdizionale rafforzato (artt. 266 e ss. cod. proc. pen.), e il regime dell'accesso ai dati di traffico e ai tabulati telefonici e telematici, disciplinato dall'art. 132 d.lgs. 30 giugno 2003, n. 196.

[7] Cfr. emblematicamente: Sez. U, n. 23756 del 29/02/2024, Giorgi, Rv. 286589; Sez. U, n. 23755 del 29/02/2024, Gjuzi, Rv. 286573.

[8] Sul tema, G. FORMICI, *La CGUE torna a parlare agli Stati membri in materia di conservazione dei metadati e tutela dei diritti fondamentali: in un dialogo tra sordi,* repetita iuvant*?*, in *Diritti comparati*, 8 maggio 2023; ID*., La* data retention saga *al capolinea? Le ultime pronunce della CGUE in materia di conservazione dei metadati per scopi securitari, tra conferme e nuove aperture*, in *DPCE on line*, n. 1/2021, p. 1361 e ss.

[9] La pronuncia è intervenuta a seguito dei rinvii pregiudiziali promossi dalla *High Court* irlandese, nell'ambito di una controversia tra l'organizzazione *Digital Rights Ireland* e le autorità statali relativa alla legittimità delle misure nazionali di attuazione della direttiva 2006/24/CE, nonché dal *Verfassungsgerichtshof* austriaco, investito di plurimi ricorsi di legittimità costituzionale diretti all'annullamento della disciplina interna di recepimento della medesima direttiva.

Ha, inoltre, evidenziato la necessità di sottoporre l'intervento legislativo unionale a un controllo di proporzionalità particolarmente rigoroso, avuto riguardo all'ampiezza della misura e all'intensità dell'incidenza sui diritti protetti[10].

Tali principi sono stati precisati da **CGUE, 21 dicembre 2016, cause riunite C-203/15 e C-698/15, *Tele2 Sverige* e *Watson***, con cui la Corte ha escluso la compatibilità con il diritto unionale di regimi nazionali fondati su obblighi generalizzati e indiscriminati di conservazione dei dati[11].

È stato, inoltre, chiarito che l'accesso ai dati di traffico e di localizzazione, anche quando finalizzato al contrasto della criminalità, deve essere limitato allo stretto necessario, circoscritto nel tempo e riferito a categorie determinate di soggetti o situazioni, in considerazione della capacità delle informazioni ricavabili da essi di consentire una ricostruzione dettagliata della vita privata degli individui[12].

Queste pronunce segnano la prima fase della giurisprudenza eurounitaria, incentrata sulla messa in discussione dei modelli di conservazione generalizzata.

Successivamente, l'attenzione della giurisprudenza si è concentrata sulle condizioni di accesso ai dati e sulle garanzie richieste in funzione del diverso grado di intrusività della misura[13].

Assume rilievo **CGUE, 2 ottobre 2018, C-207/16, *Ministerio Fiscal***, nella quale la Corte ha precisato che l'incidenza sui diritti fondamentali varia in relazione alla natura dei dati richiesti, individuando un criterio di graduazione fondato sulla loro capacità informativa e ammettendo presìdi meno rigorosi solo quando le informazioni non consentono una ricostruzione dettagliata della vita privata[14].

A partire da queste indicazioni, la Corte ha definito i modelli di conservazione compatibili con il diritto dell'Unione. Sono state ritenute ordinariamente ammissibili soltanto forme di conservazione mirate, delimitate nel tempo, nello spazio o rispetto a categorie determinate di soggetti e idonee a contenere l'ingerenza entro limiti di stretta necessità. Solo con riguardo alla salvaguardia della sicurezza nazionale – in presenza di minacce gravi, reali e attuali o prevedibili – è stata ammessa, in via eccezionale, la possibilità di obblighi temporanei di conservazione generalizzata, purché accompagnati da garanzie particolarmente stringenti, tra cui il controllo di un'autorità indipendente e la limitazione temporale della misura.

---

[10] Cfr. V. FIORILLO, *Il principio di proporzionalità da parametro di validità a fondamento del diritto alla protezione dei dati personali nella recente giurisprudenza della Corte di giustizia dell'Unione europea*, in *Federalismi*, 26 luglio 2017.

[11] La decisione origina dai rinvii pregiudiziali promossi, rispettivamente, da giudici amministrativi svedesi nell'ambito di una controversia insorta a seguito della decisione di un operatore di telecomunicazioni di cessare la conservazione dei dati dopo la sentenza *Digital Rights Ireland*, ritenendo incompatibile con il diritto dell'Unione la normativa nazionale, e da giudici del Regno Unito, investiti di ricorsi proposti da privati avverso la disciplina interna che prevedeva obblighi generalizzati di *data retention* e accesso ai dati da parte delle autorità pubbliche.

[12] Sul tema: O. POLLICINO-M. BASSINI, *La Corte di Giustizia e una trama ormai nota: la sentenza Tele2 Sverige sulla conservazione dei dati di traffico per finalità di sicurezza e ordine pubblico*, in *Dir. pen. contemp.*, 9 gennaio 2017.

[13] Per ulteriori considerazioni sul tema, G. CAGGIANO, *Il bilanciamento tra diritti fondamentali e finalità di sicurezza in materia di conservazione dei dati personali da parte dei fornitori di servizi di comunicazione*, in *Media Laws*, 2018.

[14] La decisione origina dal rinvio pregiudiziale promosso da un giudice spagnolo nell'ambito di un procedimento penale relativo al furto di un telefono cellulare, volto a stabilire se l'accesso ai dati identificativi associati a una scheda SIM dovesse essere subordinato alla soglia della criminalità grave individuata dalla giurisprudenza *Tele2 Sverige e Watson*. La Corte ha affermato che il livello di tutela richiesto varia in funzione della natura dei dati richiesti e dell'intensità dell'ingerenza nei diritti fondamentali.

CGUE, Grande Sezione, 6 ottobre 2020, cause riunite C-511/18, C-512/18 e C-520/18, *La Quadrature du Net* e a., ha, poi, sistematizzato i diversi modelli di conservazione in funzione del grado di intrusività, distinguendo tra misure incompatibili con il diritto dell'Unione – quali la conservazione generalizzata per finalità di contrasto alla criminalità ordinaria – e ipotesi eccezionali giustificabili solo in presenza di gravi minacce alla sicurezza nazionale e assistite da rigorosi controlli indipendenti[15].

Definiti i limiti della conservazione, l'attenzione si è spostata sul momento dell'accesso ai dati, individuando le garanzie procedurali necessarie a impedirne un utilizzo eccedente lo stretto necessario.

Tale approdo ha trovato compiuta espressione in **CGUE, G.S., 2 marzo 2021, C-746/18, H.K. (Prokuratuur)**, che ha posto al centro dell'analisi i presìdi autorizzativi e il controllo preventivo dell'accesso ai dati conservati[16].

La Corte ha ribadito che l'accesso a dati di traffico e di ubicazione, in quanto idonei a consentire inferenze "precise, o addirittura molto precise" sulla vita privata, costituisce, in via generale, una forma di intrusione di particolare intensità. Pertanto, esso può essere giustificato soltanto dalla lotta alla criminalità grave o dalla prevenzione di gravi minacce alla sicurezza pubblica, mentre la mera limitazione temporale o quantitativa dell'accesso non è sufficiente ad attenuarne l'impatto.

Sul piano delle garanzie, è richiesto un controllo preventivo affidato a un'autorità terza e neutrale, con conseguente incompatibilità dei modelli che attribuiscano tale funzione al pubblico ministero titolare dell'indagine.

L'orientamento così delineato è stato confermato da **CGUE, Grande Sezione, 20 settembre 2022, cause riunite C-793/19 e C-794/19, *SpaceNet AG* e *Telekom Deutschland GmbH***, che ha ribadito l'inconciliabilità con il diritto dell'Unione di obblighi generalizzati di *data retention*, escludendo definitivamente la possibilità di ricorso a modelli intermedi o attenuati[17].

L'insieme delle pronunce richiamate – descritto, in dottrina, come *data retention saga* – delinea un modello europeo fondato su conservazione selettiva e accesso rigorosamente limitato,

---

[15] La sentenza è stata pronunciata a seguito dei rinvii pregiudiziali promossi da giudici francesi e belgi nonché dall'*Investigatory Powers Tribunal* del Regno Unito nell'ambito di controversie relative alla legittimità di regimi nazionali di conservazione generalizzata dei dati comunicativi adottati per finalità di sicurezza nazionale e contrasto alla criminalità. Per un interessante contributo dottrinale, si rinvia a F. RESTA, *La Corte di giustizia europea torna ancora sulla* data retention, in *Giust. Insieme*, 23 settembre 2022.

[16] Il pronunciamento della CGUE scaturisce dal rinvio pregiudiziale del *Riigikohus* (Corte suprema estone) relativo alla compatibilità con l'art. 15, par. 1, dir. 2002/58/CE di una normativa nazionale che consentiva l'accesso ai dati di traffico e di ubicazione nell'ambito di indagini penali sulla base di autorizzazione del pubblico ministero. La Corte ha chiarito che l'accesso a tali dati, integrando un'ingerenza grave nei diritti garantiti dagli artt. 7 e 8 CDFUE, deve essere subordinato a un controllo preventivo esercitato da un'autorità giurisdizionale o da un organismo indipendente e terzo rispetto all'autorità investigativa, requisito che, nel sistema estone, la Corte ha ritenuto non soddisfatto dal pubblico ministero, in quanto parte del procedimento penale e non dotato della necessaria indipendenza rispetto all'autorità investigativa. In dottrina, G. FORMICI, *L'incerto futuro della* data retention *europea: osservazioni a partire dalla sentenza H.K. v Prokuratuur*, in *SIDIBlog*, 27 aprile 2021.

[17] I rinvii pregiudiziali erano stati promossi da giudici tedeschi in relazione alla compatibilità con l'art. 15, par. 1, dir. 2002/58/CE di una normativa nazionale che imponeva obblighi generalizzati di conservazione dei dati di traffico e di ubicazione.

nel quale l'ingerenza nei diritti fondamentali è ammessa solo in presenza di finalità di rilievo e adeguate garanzie idonee a prevenire il rischio di abusi[18].

Si conferma una tensione strutturale tra esigenze investigative e tutela dei diritti fondamentali, resa evidente dalla centralità dei metadati nelle moderne strategie investigative e dall'opzione eurounitaria per forme di acquisizione mirata e giustificata caso per caso.

Il percorso può essere articolato in tre passaggi: dapprima, la messa in discussione dei modelli di conservazione generalizzata dei dati; quindi, la definizione delle condizioni sostanziali di accesso; infine, la precisazione delle garanzie procedurali e dei presìdi autorizzativi necessari a legittimarne l'utilizzo a fini penali.

Nasce da questo assetto quell'esigenza di positivizzazione e uniformazione delle discipline nazionali, che ha portato all'adozione del cd. *e-evidence package*. L'intervento normativo eurounitario segna il passaggio da logiche di accumulo preventivo delle informazioni a meccanismi di acquisizione mirata dei dati presso i soggetti che li detengono e inaugura un nuovo paradigma di cooperazione giudiziaria penale nello spazio europeo.

3. Il quadro normativo europeo dell'*e-evidence*: struttura del sistema e opzioni di fondo.

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 di effettività investigativa e di tutela dei diritti fondamentali emerse nel contesto digitale[19].

L'intervento si inserisce nel più ampio processo di trasformazione della cooperazione giudiziaria penale nello spazio europeo, nel quale, accanto alle forme mediate tra autorità statali, si affermano meccanismi di interazione diretta tra autorità giudiziarie finalizzati all'acquisizione probatoria e al riconoscimento di provvedimenti riguardanti persone, beni e dati. Ne costituiscono espressione il mandato di arresto europeo (decisione quadro 2002/584/GAI, attuata nell'ordinamento interno con la legge 22 aprile 2005, n. 69)[20], l'ordine europeo di indagine (direttiva 2014/41/UE, attuata con il d.lgs. 21 giugno 2017, n. 108)[21] e il sistema di

[18] In tal senso, S. DE FRANCESCO, *Corte di giustizia e accesso ai dati degli* smartphone*: nuovi problemi di (in)compatibilità tra diritto interno e diritto dell'Unione europea*, in *Dir. di dif.*, 6 novembre 2024.

[19] Per una diffusa trattazione del tema, anche in chiave problematica, si rinvia a: S. ALLEGREZZA, *L'acquisizione delle prove elettroniche nel processo penale*, in *Riv. it. dir. proc. pen.*, 2020, p. 1123 e ss.; M. CAIANIELLO, *Il procedimento penale europeo*, Torino, 2022, p. 165 e ss.; V. MITSILEGAS, *EU Criminal Law*, Oxford, 2022, spec. p. 400 e ss.

[20] Per approfondimenti recenti, cfr.: M. CAIANIELLO, *op. cit.*; G. ILLUMINATI, *Mutuo riconoscimento e garanzie individuali nel mandato d'arresto europeo*, in *Dir. pen. e proc.*, n. 4, 2022, p. 485 e ss.; V. MITSILEGAS, *EU Criminal Law*, Oxford, 2022, spec. cap. III; A. STIRONE, *Il mandato d'arresto europeo. Grammatica della consegna nello spazio giuridico europeo*, Torino, 2025; A. TAMIETTI, *Il mandato d'arresto europeo davanti alla Corte EDU*, in *Cass. pen.*, 2023, p. 2110 e ss.

[21] In argomento: M. CAIANIELLO, *op. cit.*; O. CALAVITA, *L'ordine europeo di indagine penale. Presente e futuro della cooperazione probatoria nell'Unione europea*, Padova, 2025; F. ERTOLA, *L'ordine europeo di indagine penale*, in G. UBERTIS-G.P. VOENA (a cura di), *Trattato di procedura penale*, Milano, 2025; V. MITSILEGAS, *op. cit.*, spec. p. 185 e ss.; A. NASCIMBENI, *Ordine europeo di indagine penale e diritti fondamentali*, in *Riv. it. dir. e proc. pen.*, 2022, p. 410 e ss.; P. RAUCCI, *L'ordine europeo di indagine e prove digitali: tra presunzione di legittimità degli atti compiuti all'estero e diritti fondamentali*, in *Giur. pen.*, 2025, p. 1 e ss.

riconoscimento reciproco dei provvedimenti di sequestro e confisca (regolamento (UE) 2018/1805, attuato con il d.lgs. 7 agosto 2020, n. 137)[22].

Pur rientrando in questo processo di trasformazione degli strumenti di cooperazione giudiziaria europea, l'acquisizione delle prove elettroniche presenta caratteri distintivi propri, derivanti dalla natura immateriale dei dati e dal ruolo centrale assunto da soggetti privati estranei al circuito giurisdizionale, quali i prestatori di servizi[23].

L'introduzione dei nuovi strumenti di acquisizione delle prove elettroniche è stata espressamente subordinata dal legislatore unionale al rispetto dei principi di necessità e proporzionalità e delle garanzie derivanti dalla CDFUE.

L'adozione del **regolamento (UE) 2023/1543** (di seguito: Regolamento) e della **direttiva (UE) 2023/1544** (di seguito: Direttiva) – che compongono il cd. *e-evidence package* – costituisce l'esito normativo dell'evoluzione richiamata, definendo un sistema unitario di accesso transfrontaliero ai dati elettronici.

I lavori preparatori del Regolamento evidenziano come il sistema si fondi sulla razionalizzazione, entro un quadro uniforme di garanzie, di prassi investigative già sviluppatesi, in modo non omogeneo, nei diversi ordinamenti nazionali[24].

3.1. Sotto il profilo strutturale, l'*e-evidence package* si articola in due strumenti normativi: il Regolamento e la Direttiva.

La scelta di affiancare un regolamento a una direttiva risponde a una precisa opzione di politica legislativa unionale. Il Regolamento disciplina in modo direttamente applicabile le condizioni di emissione ed esecuzione degli ordini europei di produzione e di conservazione, mentre la Direttiva impone agli Stati membri gli adeguamenti organizzativi necessari a garantirne l'effettiva attuazione.

Il **Regolamento** costituisce il **perno operativo**, disciplinando in modo compiuto le condizioni e le modalità di emissione, trasmissione ed esecuzione degli ordini europei di produzione (*European Production Orders* – EPOC) e degli ordini europei di conservazione (*European Preservation Orders* – EPOC-PR), al fine di garantire un elevato grado di armonizzazione ed evitare soluzioni nazionali eterogenee.

Ai fini dell'applicazione degli ordini, il Regolamento utilizza una nozione funzionale di "prove elettroniche", riferita a dati elettronici già esistenti, detenuti da prestatori di servizi rilevanti ai sensi delle sue stesse disposizioni e suscettibili di essere prodotti o conservati a fini probatori. Si

[22] Sul tema, si vedano: D. GRANDI, *Il mutuo riconoscimento dei provvedimenti di confisca*, in *Leg. pen.*, 31 maggio 2021; A.M. MAUGERI, *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 *Dir. pen. contemp*., 16 gennaio 2019; V. MILITELLO-A. SPENA (a cura di), *Mutuo riconoscimento in materia penale e diritti fondamentali*, Torino, 2023.

[23] COMMISSIONE EUROPEA, *Impact Assessment*, SWD(2018) 118 *final*, § 2.1 e § 2.2, evidenzia 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 *service providers*.

[24] Cfr. COMMISSIONE EUROPEA, *Proposal for a Regulation on European Production and Preservation Orders for electronic evidence in criminal matters*, COM(2018) 225 *final*, e *Impact Assessment*, *cit.*, nei quali si evidenziano i limiti degli strumenti tradizionali di cooperazione giudiziaria rispetto alla delocalizzazione dei dati e alle esigenze di tempestivo accesso alle prove elettroniche, anche in funzione di prevenzione della loro dispersione. In dottrina, G. DI PAOLO, La circolazione transfrontaliera delle prove elettroniche, in *Riv. pen. dir. e proc.*, 13 maggio 2024, spec. § 3.

tratta di un ambito distinto dalle attività di intercettazione o captazione in tempo reale, soggette a una disciplina autonoma e più rigorosa.

La **Direttiva** non incide sulle condizioni di emissione ed esecuzione degli ordini europei, ma mira ad **assicurare l'effettiva applicazione del sistema delineato dal Regolamento**. Essa impone ai prestatori che offrono servizi nell'Unione europea l'obbligo di designare uno stabilimento oppure di nominare un rappresentante legale all'interno dell'Unione, individuando così un destinatario stabile e giuridicamente responsabile degli ordini di produzione e di conservazione.

La distinzione di funzione tra Regolamento e Direttiva riflette una logica di complementarità: al primo spetta la disciplina delle condizioni e delle modalità di accesso ai dati elettronici; alla seconda la creazione delle condizioni organizzative e soggettive affinché tale accesso possa avvenire in modo effettivo.

Su tale architettura si innesta la disciplina nazionale, chiamata a regolare gli aspetti organizzativi e procedurali rimessi agli Stati membri e a garantire il coordinamento con il sistema processuale interno.

3.2. Il **rapporto tra i nuovi strumenti europei e i meccanismi tradizionali di cooperazione giudiziaria** non è di sostituzione, ma di coesistenza.

Il sistema delineato dal Regolamento non è concepito come esclusivo. Gli strumenti tradizionali di cooperazione giudiziaria continuano a trovare applicazione nei rapporti con Stati terzi, mentre l'*e-evidence package* opera entro il perimetro unionale e riguarda i prestatori – anche stabiliti in Paesi terzi – di servizi nell'Unione europea, tenuti a designare uno stabilimento o un rappresentante legale nell'Unione ai fini della ricezione ed esecuzione degli ordini europei, secondo quanto previsto dalla Direttiva.

3.3. Occorre, infine, considerare la **scansione temporale dell'intervento normativo europeo.**

Il quadro dell'*e-evidence* presenta un'articolazione temporale differenziata, derivante dalla compresenza di uno strumento direttamente applicabile e di uno soggetto a recepimento nazionale.

La Direttiva prevede, in particolare, che entro il 18 febbraio 2026:

- i prestatori di servizi che offrono servizi nell'Unione europea designino uno stabilimento oppure nominino un rappresentante legale (art. 3, par. 6);
- gli Stati membri notifichino alla Commissione le disposizioni nazionali in materia di sanzioni (art. 5);
- sia completato il recepimento nel diritto interno (art. 7, par. 1).

Le informazioni relative alle autorità competenti, alle lingue accettate e alle disposizioni nazionali così notificate sono rese accessibili dalla Commissione mediante pubblicazione su un apposito sito *web* o sul portale della Rete giudiziaria europea in materia penale, al fine di assicurare trasparenza e conoscibilità delle modalità operative del sistema.

Il Regolamento prevede, a sua volta, una distinta scansione temporale: entro il 18 agosto 2025 gli Stati membri erano tenuti a comunicare alla Commissione le autorità competenti e le lingue accettate ai sensi dell'art. 31, par. 1, mentre l'applicazione della disciplina degli ordini europei di produzione e di conservazione è fissata al 18 agosto 2026 (art. 34, par. 2).

In attuazione della descritta scansione temporale, il legislatore italiano ha disciplinato in via organica il sistema mediante l'adozione di due decreti legislativi. In particolare, il d.lgs. n. 215 del 2025 ha dato stabilità normativa alla designazione delle autorità competenti e all'assetto procedurale interno richiesto dal Regolamento, mentre il d.lgs. n. 216 del 2025 è stato diretto al recepimento della Direttiva e alla piena operatività del sistema.

Si realizza così un *iter* di implementazione del sistema europeo di acquisizione delle prove elettroniche, scandito dalle cadenze temporali stabilite dal diritto dell'Unione[25].

4. Il rapporto tra *e-evidence* e ordine europeo di indagine nel sistema della cooperazione probatoria europea.

Nel sistema della cooperazione giudiziaria penale dell'Unione, l'ordine europeo di indagine (di seguito: OEI) rappresenta lo strumento generale di acquisizione transnazionale della prova, idoneo a ricomprendere una pluralità eterogenea di atti investigativi e inserito in un modello di cooperazione fondato sul reciproco riconoscimento tra autorità giudiziarie, mentre il sistema e-*evidence* introduce un modello distinto, nel quale l'ordine europeo di produzione o di conservazione è rivolto direttamente al prestatore di servizi, con un coinvolgimento dello Stato di esecuzione significativamente ridimensionato.

In questo quadro si inseriscono gli approdi della giurisprudenza di legittimità in materia di OEI, che chiariscono la funzione del canale cooperativo europeo e i limiti al ricorso a strumenti unilaterali interni.

Le Sezioni unite della Corte di cassazione, con le sentenze 29 febbraio 2024, nn. 23755 e 23756[26], hanno statuito che, quando ricorrono i presupposti della cooperazione giudiziaria tra Stati membri, l'OEI costituisce lo strumento attraverso il quale deve essere realizzata l'acquisizione della prova in ambito transfrontaliero, con conseguente impossibilità di ricorrere a strumenti interni al fine di eludere il canale cooperativo europeo. L'art. 234-*bis* cod. proc. pen. opera, dunque, esclusivamente al di fuori delle ipotesi di cooperazione giudiziaria.

Le Sezioni unite hanno, inoltre, chiarito che, una volta attivato il canale cooperativo europeo, il controllo del giudice dello Stato di emissione si colloca prevalentemente sul piano dell'utilizzabilità della prova nel processo nazionale, senza trasformarsi in una verifica

[25] Sul carattere progressivo dell'implementazione nazionale dell'*e-evidence package*, modellata sulle scansioni temporali previste dagli strumenti unionali, C. DE LAZZARO, *L'acquisizione delle prove elettroniche nello spazio di libertà, sicurezza e giustizia: una prima implementazione dell'e-evidence package*, in *Sist. pen.*, 2 febbraio 2026.

[26] Per note di commento, si rinvia, tra gli altri, a: M. DANIELE, *Le sentenze "gemelle" delle Sezioni Unite sui criptofonini*, in *Sist. pen.*, 17 luglio 2024; M. GRIFFO, *Criptofonini ecc., dalle Sezioni unite una chiave di lettura per decifrare le prassi*, in *Cass. pen.*, 2025, p. 506 e ss.; L. FILIPPI, *Le SS.UU. sui criptofonini: ma l'"equo processo" ammette la prova a genesi ignota?*, in *Altalex*, 8 marzo 2024; A. NAPPI, *Le Sezioni unite sui criptofonini: plus dixerunt quam voluerunt?*, in *Cass. pen.*, 2024, p. 2575 e ss.; V. SCARLATO, *Commento alle sentenze delle Sezioni unite relative al caso dei cd. "criptofonini"*, in *Camm. Diritto*, 25 giugno 2024.

generalizzata delle modalità investigative adottate dall'autorità straniera, in coerenza con il principio di fiducia reciproca che governa gli strumenti di cooperazione giudiziaria dell'Unione.

Da questi principi si desume che il canale cooperativo europeo costituisce la modalità ordinaria di acquisizione della prova oltre confine – anche con riferimento ai dati digitali – e che il sindacato del giudice nazionale resta circoscritto al piano delle garanzie e dell'utilizzabilità.

Il rapporto tra *e-evidence* e OEI va ricostruito in termini di specialità funzionale: quando ricorrono i presupposti applicativi del Regolamento, l'ordine europeo di produzione o di conservazione costituisce la via propria per l'acquisizione della prova digitale presso i prestatori di servizi, mentre l'OEI continua a operare quale strumento generale per gli atti investigativi che richiedano l'intervento dell'autorità dello Stato di esecuzione o che restino estranei all'ambito oggettivo del Regolamento.

La distinzione riflette la coesistenza di due modelli cooperativi differenti: l'uno fondato sull'intervento dell'autorità giudiziaria dello Stato di esecuzione, l'altro caratterizzato dall'ordine diretto al prestatore di servizi.

Le modalità di integrazione del nuovo strumento europeo nel sistema processuale interno saranno esaminate nella Parte seguente.

PARTE II.
L'attuazione nazionale dell'*e-evidence package* e il modello processuale degli ordini europei.

5. Architettura eurounitaria degli ordini: tipologie, categorie di dati e condizioni di emissione.

L'implementazione nazionale dell'*e-evidence package* e il coordinamento con il sistema processuale interno sono stati realizzati mediante i d.lgs. nn. 215 e 216 del 2025[27], adottati in attuazione della legge 13 giugno 2025, n. 91 (legge di delegazione europea 2024), con l'obiettivo – evidenziato nei lavori parlamentari – di assicurare l'effettiva operatività degli strumenti previsti dal Regolamento[28].

Il Regolamento definisce direttamente le tipologie di ordini, le categorie di dati e le condizioni di emissione, mentre l'intervento nazionale si concentra sulla distribuzione delle competenze e sull'inserimento procedurale degli strumenti nel sistema processuale interno.

[27] Per i primi commenti di dottrina alla normativa di attuazione dell'*e-evidence package*, si rinvia a: C. DE LAZZARO, *op. cit.*; F. CRIMI, *In G.U. il D.lgs. 215/2025 sulla lotta alla volatilità della prova digitale*, in *Il quotidiano giur.*, 20 gennaio 2026; A. CISTERNA, *Le novità del dlgs 215 – Data retention fino a sei mesi per il congelamento dei dati*, in *NT+Diritto*, 28 gennaio 2026.

[28] Cfr. CAMERA DEI DEPUTATI – SERVIZIO STUDI, *Dossier n. 303, Schema di decreto legislativo recante disposizioni per l'adeguamento della normativa nazionale al regolamento (UE) 2023/1543 e alla direttiva (UE) 2023/1544*, p. 4 e s.

5.1. Il Regolamento distingue due strumenti complementari, ma funzionalmente distinti: l'ordine europeo di produzione e l'ordine europeo di conservazione delle prove elettroniche (artt. 5 e 6 Reg.).

L'**ordine europeo di produzione** consente l'acquisizione diretta di dati elettronici già esistenti e detenuti da un prestatore di servizi, imponendone la trasmissione all'autorità di emissione ai fini del loro utilizzo nel procedimento penale. Esso realizza un accesso conoscitivo pieno al contenuto informativo richiesto e costituisce lo strumento cardine del sistema *e-evidence*, fondato sull'interazione diretta tra autorità giudiziaria e prestatore di servizi.

L'**ordine europeo di conservazione** svolge, invece, una funzione esclusivamente preservativa. Esso è diretto a impedire la cancellazione, l'alterazione o la perdita dei dati elettronici per un periodo determinato, in vista della loro eventuale acquisizione mediante un successivo ordine di produzione, senza comportare accesso al contenuto né trasferimento delle informazioni all'autorità procedente.

La differenza tra i due strumenti si riflette sull'intensità dell'ingerenza nei diritti fondamentali: l'ordine di produzione incide direttamente sulla sfera della riservatezza e della protezione dei dati personali, mentre l'ordine di conservazione opera su un piano anticipato e meramente conservativo, limitandosi a garantire la permanenza della fonte di prova senza consentirne l'utilizzazione immediata.

5.2. Elemento portante dell'architettura del Regolamento è la **distinzione tra diverse categorie di dati elettronici**.

L'art. 3 Reg. individua i dati relativi agli abbonati, i dati di accesso, i dati di traffico e i dati relativi al contenuto delle comunicazioni. Tale classificazione non ha carattere meramente descrittivo, ma assolve a una funzione normativa, in quanto costituisce il criterio di graduazione dell'ingerenza nei diritti fondamentali e, correlativamente, delle condizioni di emissione degli ordini europei.

In ragione di ciò, l'art. 5 Reg. prevede una disciplina differenziata per l'ordine europeo di produzione:

- i dati relativi agli abbonati e quelli richiesti al solo scopo di identificare l'utente possono essere acquisiti per qualsiasi reato;
- l'accesso ai dati di traffico e ai dati relativi al contenuto è subordinato alla sussistenza di reati caratterizzati da una particolare gravità, individuati mediante soglie di pena ovvero mediante il riferimento a specifiche categorie di criminalità armonizzate a livello unionale.

Tale impostazione traduce in diritto positivo i criteri elaborati dalla giurisprudenza della Corte di giustizia in materia di accesso ai dati comunicativi.

Anche i requisiti di necessità e proporzionalità sono disciplinati direttamente dalla fonte eurounitaria. L'ordine deve essere emesso nell'ambito di un procedimento penale, per finalità investigative determinate e sulla base di un bilanciamento concreto tra utilità probatoria dei dati richiesti e sacrificio dei diritti fondamentali coinvolti.

Per l'ordine europeo di conservazione, invece, il Regolamento non prevede soglie di gravità analoghe a quelle stabilite per l'ordine di produzione, in ragione della diversa funzione della misura, che non comporta accesso conoscitivo ai dati.

5.3. La struttura così delineata spiega la tecnica normativa adottata dal legislatore italiano.

Il d.lgs. n. 215 del 2025 non riproduce nel proprio testo le definizioni, le categorie di dati e le condizioni sostanziali di emissione degli ordini europei, ma vi rinvia mediante richiami puntuali alle disposizioni del Regolamento. L'art. 2, comma 1, d.lgs. n. 215 del 2025 subordina, infatti, l'emissione dell'ordine europeo di produzione alla sussistenza delle condizioni previste dall'art. 5 Reg.; analogamente, l'art. 3 richiama, per l'ordine di conservazione, i presupposti stabiliti dall'art. 6 Reg.

Questa tecnica di rinvio, coerente con la natura direttamente applicabile del Regolamento, evita duplicazioni normative e possibili divergenze interpretative, configurando l'intervento nazionale come disciplina prevalentemente organizzativa e procedurale[29].

I presupposti sostanziali dell'ingerenza nei diritti fondamentali restano, dunque, ancorati alla fonte eurounitaria, mentre al legislatore interno compete la definizione delle autorità competenti, delle modalità di emissione e dei meccanismi di controllo inseriti nel sistema processuale nazionale.

5.4. Nell'architettura delineata dal Regolamento, la **conservazione** dei dati elettronici assume una **funzione autonoma rispetto all'acquisizione probatoria**.

Se l'ordine europeo di produzione realizza l'accesso conoscitivo ai dati e consente la loro immediata utilizzazione nel procedimento penale, l'ordine europeo di conservazione opera in una fase logicamente e funzionalmente anteriore, mirando esclusivamente a preservare l'esistenza della fonte di prova rispetto al rischio di cancellazione o alterazione.

La distinzione tra conservazione e acquisizione è il portato di una trasformazione delle tecniche investigative nell'ambiente digitale. A differenza dei mezzi di ricerca della prova tradizionali, nei quali l'acquisizione coincide normalmente con l'apprensione materiale dell'oggetto probatorio, il dato elettronico presenta una intrinseca instabilità, derivante sia dai meccanismi automatici di gestione e cancellazione dei sistemi informatici sia dalla distribuzione transnazionale delle informazioni presso prestatori di servizi privati. In tale contesto, la tutela anticipata della disponibilità del dato diviene condizione stessa della futura attività investigativa.

L'ordine europeo di conservazione impone al prestatore di servizi l'obbligo di preservare dati già esistenti al momento della ricezione dell'ordine per un **periodo temporalmente determinato**, non superiore a sessanta giorni, prorogabile nei casi previsti dal Regolamento ovvero sino alla successiva acquisizione mediante ordine europeo di produzione o altra richiesta giuridicamente idonea a ottenere i dati (art. 11 Reg.).

[29] Cfr. CAMERA DEI DEPUTATI – SERVIZIO STUDI, Dossier n. 303, *cit.*, scheda di lettura relativa all'art. 1, p. 13, ove si precisa che il decreto si limita a fissare le norme necessarie ad adeguare l'ordinamento nazionale alle disposizioni del Regolamento.

La disciplina della durata è integralmente regolata dalla fonte eurounitaria e non viene riprodotta dal decreto legislativo nazionale, confermando la funzione prevalentemente organizzativa e procedurale dell'intervento attuativo interno.

La limitazione temporale costituisce elemento essenziale dell'istituto: la conservazione non attribuisce nuovi poteri di raccolta delle informazioni, ma sospende temporaneamente i normali processi di cancellazione o modifica dei dati, assicurandone la disponibilità per eventuali successive determinazioni investigative.

Il Regolamento chiarisce che l'ordine europeo di conservazione non introduce alcun obbligo generale di conservazione dei dati né legittima forme di *retention* preventiva o indiscriminata delle informazioni elettroniche (considerando 31 e 33). La misura riguarda esclusivamente dati già esistenti e specificamente individuati, preservati in funzione di un procedimento penale determinato.

La conservazione europea non può, pertanto, essere assimilata ai regimi di *data retention* generalizzata né agli strumenti acquisitivi del processo penale interno. Essa non consente accesso conoscitivo al contenuto delle informazioni e non comporta trasferimento dei dati all'autorità procedente, limitandosi a garantire la permanenza della fonte informativa in vista di una successiva eventuale acquisizione.

Il Regolamento costruisce un modello investigativo nel quale il controllo di legalità e le garanzie giurisdizionali possono distribuirsi lungo una sequenza procedimentale più ampia, anticipando la tutela del dato senza anticiparne necessariamente l'utilizzazione probatoria, secondo una logica estranea al modello tradizionale delle misure probatorie del processo penale interno.

La novità dell'*e-evidence package* non risiede nell'introduzione della conservazione dei dati in quanto tale – già conosciuta agli strumenti di cooperazione internazionale –, ma nella trasformazione della sua funzione: da misura accessoria dell'acquisizione probatoria a strumento autonomo volto a garantire la disponibilità della prova digitale nell'ambito dell'accesso transfrontaliero ai dati.

6. Innesto nel processo penale italiano: competenze, iniziativa, formazione dell'atto e regime di conoscibilità dei dati (artt. 2 e 3 d.lgs. n. 215 del 2025).

L'assetto delineato dal Regolamento trova attuazione nell'ordinamento interno attraverso l'individuazione delle autorità competenti all'emissione e alla convalida degli ordini europei e la definizione delle modalità procedurali di formazione e trasmissione dell'atto, senza dar luogo alla creazione di un circuito processuale autonomo rispetto al sistema codicistico.

Il criterio ordinatore dell'intervento nazionale è rappresentato dalla modulazione delle competenze tra pubblico ministero e giudice in funzione della natura dei dati oggetto dell'ordine.

6.1. In tema di ordine europeo di produzione, l'art. 2 d.lgs. n. 215 del 2025 disciplina un modello di **competenza** graduato[30].

Quando l'ordine ha ad oggetto dati relativi agli abbonati o dati richiesti al solo scopo di identificare l'utente, il potere di emissione è attribuito al pubblico ministero. La scelta risulta coerente con il minore grado di intrusività riconosciuto a tali categorie di dati e con l'assetto ordinario delle competenze investigative nel sistema processuale interno.

Diversamente, qualora l'ordine riguardi dati di traffico o dati relativi al contenuto delle comunicazioni, è richiesto l'intervento del giudice competente a pronunciarsi nel merito del procedimento, individuato secondo le regole processuali interne in relazione alla fase in cui l'ordine è emesso. La soluzione adottata non radica la competenza in capo al giudice per le indagini preliminari, valorizzando la trasversalità dello strumento europeo, suscettibile di operare in ogni stato e grado del procedimento penale.

Il modello comporta un'intensificazione del controllo giurisdizionale in funzione della maggiore incidenza dell'atto sulla sfera privata dell'individuo, secondo una logica di continuità con le garanzie richieste per altri mezzi di ricerca della prova caratterizzati da significativa interferenza nei diritti fondamentali.

Analoga impostazione informa la disciplina dell'ordine europeo di conservazione prevista dall'art. 3 del decreto. La competenza è attribuita al pubblico ministero, trattandosi di misura che non comporta accesso conoscitivo ai dati né trasferimento immediato delle informazioni all'autorità procedente, ma si limita a imporre un obbligo temporaneo di preservazione. La diversa natura dell'atto giustifica l'assenza di un intervento giurisdizionale preventivo.

6.2. Per quel che concerne l'**iniziativa**, l'art. 2, comma 2, d.lgs. n. 215 del 2025 prevede che l'ordine europeo di produzione possa essere richiesto dal pubblico ministero, anche su istanza della persona offesa o del suo difensore, nonché direttamente dalla persona sottoposta alle indagini, dall'imputato, dalle parti private e dai rispettivi difensori.

La persona offesa, non ancora titolare di un autonomo potere di attivazione probatoria, può sollecitare l'adozione dell'ordine mediante istanza rivolta al pubblico ministero, al quale è rimessa la valutazione circa il suo eventuale recepimento[31]. Diversamente, l'indagato, l'imputato e le altre parti private sono legittimati, al pari del pubblico ministero, a rivolgere direttamente la richiesta al giudice competente, in coerenza con il principio di parità delle armi e con la struttura accusatoria del processo.

La disciplina conferma che l'ordine europeo di produzione è configurato come strumento utilizzabile non soltanto dall'accusa, ma anche dalla difesa e dalle altre parti, quale mezzo di acquisizione probatoria inserito nella dinamica del contraddittorio.

---

[30] Cfr. CAMERA DEI DEPUTATI – SERVIZIO STUDI, Dossier n. 303, *cit.*, scheda relativa all'art. 2, p. 14 e ss.

[31] Si tratta di uno schema ben noto e compatibile con l'impostazione generale codicistica, che attribuisce alla persona offesa essenzialmente facoltà di natura sollecitatoria nei confronti del pubblico ministero. Sul tema generale dei poteri e delle facoltà riconosciuti alla persona offesa, cfr.: T. BENE, *La persona offesa fra diritto di difesa e diritto alla giurisdizione: le nuove tendenze legislative*, in *Arch. pen.*, 2013, p. 487 e ss.; A. MARI-E. CONFORTI, *Persona offesa e processo penale. Facoltà, diritti e protezione nell'evoluzione normativa e giurisprudenziale*, Milano, 2022.

Con riguardo all'ordine europeo di conservazione, l'art. 3 del decreto prevede un'articolazione in parte analoga, ma introduce una significativa specificazione: prima dell'esercizio dell'azione penale provvede il pubblico ministero. La disposizione evidenzia la vocazione tipicamente investigativa della misura conservativa nella fase delle indagini preliminari, nella quale la direzione dell'attività probatoria spetta all'autorità requirente.

La differenziazione tra i due strumenti riflette la diversa funzione sistematica della conservazione rispetto alla produzione, in quanto solo quest'ultima si presta a un utilizzo pienamente dialettico nel processo.

6.3. L'**emissione e la trasmissione** degli ordini europei avvengono **mediante i certificati standardizzati allegati al Regolamento**, che costituiscono il veicolo formale necessario dell'atto.

La modulistica unionale non svolge una funzione meramente documentale. L'utilizzo del certificato standardizzato garantisce la verificabilità dell'atto, quanto alla sua provenienza, al contenuto e alla sussistenza dei presupposti richiesti, tanto nell'esecuzione transfrontaliera quanto, successivamente, nel procedimento penale interno, ove l'ordine e la relativa documentazione confluiscono nel fascicolo secondo le regole ordinarie di documentazione dell'attività investigativa.

6.4. L'art. 2, comma 6, d.lgs. n. 215 del 2025 stabilisce che l'autorità giudiziaria provvede, nei casi e nei modi previsti dalla legge processuale, a dare **conoscenza alle parti e ai difensori dei dati e della documentazione acquisiti mediante ordine europeo di produzione**.

A una prima lettura, anche in ragione della sua collocazione sistematica, la disposizione potrebbe essere intesa nel senso di imporre all'autorità giudiziaria un obbligo di immediata ostensione alle parti e ai difensori dei dati acquisiti. Una simile interpretazione, tuttavia, si porrebbe in contrasto con il regime del segreto investigativo e con le regole generali che governano la *discovery* nel procedimento penale.

Al fine di evitare tale esito, il richiamo espresso ai "casi e modi previsti dalla legge processuale" consente di ricondurre la disposizione nell'alveo della disciplina ordinaria, escludendo che essa introduca un autonomo obbligo di comunicazione anticipata.

La norma ha una funzione meramente ricognitiva, limitandosi a ribadire che anche i dati acquisiti mediante gli strumenti previsti dal sistema *e-evidence* sono soggetti alle ordinarie regole di conoscibilità processuale.

La disposizione va letta anche alla luce dell'art. 13 Reg., che riconosce **alla persona i cui dati sono stati acquisiti specifici diritti di informazione e accesso**, suscettibili di limitazioni o differimenti in presenza di esigenze investigative.

Le due discipline attengono a profili distinti ma complementari: mentre l'art. 2, comma 6, d.lgs. n. 215 del 2025 attiene alla conoscibilità processuale dei dati in favore delle parti e dei difensori, l'art. 13 Reg. riguarda i diritti dell'interessato in quanto tale, anche al di fuori della sua eventuale qualità di parte nel procedimento penale. Deve ritenersi che il sistema escluda forme di conoscenza immediata e automatica dei dati acquisiti, subordinandone l'accesso al rispetto

delle esigenze di segretezza e di efficacia delle indagini, con la conseguenza che l'informazione circa l'acquisizione dei dati può essere legittimamente differita, anche nei confronti dei soggetti estranei al procedimento, sino a quando ciò sia compatibile con le esigenze investigative.

Il Regolamento non individua in modo puntuale né il momento né le modalità della comunicazione, rimettendo agli ordinamenti nazionali la concreta definizione delle relative forme attuative.

La mancata informazione dell'interessato non sembra incidere sulla validità dell'acquisizione dei dati né determinare conseguenze processuali, non essendo configurabili ipotesi di inutilizzabilità o nullità. L'obbligo informativo, infatti, non attiene alla formazione o alla legittimità dell'atto di acquisizione, ma a un profilo successivo e distinto, e difetta, in ogni caso, una previsione espressa che ricolleghi alla sua violazione effetti invalidanti, in termini di nullità, secondo il principio di tassatività delle invalidità processuali, ovvero in termini di inutilizzabilità.

Sul piano civilistico, potrebbe ipotizzarsi una responsabilità risarcitoria ove la mancata informazione risulti non giustificata da esigenze investigative e si traduca in una lesione dei diritti riconosciuti all'interessato. Tale responsabilità sarebbe, in linea di principio, imputabile allo Stato, quale soggetto cui è riferibile l'attività dell'autorità giudiziaria.

La configurazione concreta della responsabilità resta, tuttavia, incerta[32] e la disposizione si inserisce in un'area nella quale il riconoscimento del diritto non è accompagnato da un apparato rimediale chiaramente definito, con il rischio di una tutela solo parziale, sostanzialmente rimessa alla prassi e all'elaborazione giurisprudenziale.

7. Procedure di urgenza, emergenza e accelerazione nell'emissione ed esecuzione degli ordini europei (artt. 2, 3 e 4 d.lgs. n. 215 del 2025; artt. 10, par. 4, e 12 Reg.).

La centralità del fattore temporale nell'accesso alla prova digitale, già evidenziata con riferimento alla funzione dell'ordine europeo di conservazione, trova ulteriore sviluppo nelle ipotesi di urgenza, nelle quali il rischio di dispersione del dato impone la riduzione dei tempi di emissione degli ordini europei. Il d.lgs. n. 215 del 2025 disciplina la tempistica in modo articolato e duttile.

Il legislatore ha previsto:

- **forme di intervento emergenziale interno**, disciplinate dagli artt. 2 e 3, che consentono un'anticipazione dell'iniziativa investigativa in situazioni di pericolo imminente;
- una **procedura accelerata di emissione**, introdotta dall'art. 4, volta a rimodulare i tempi decisionali senza incidere sui presupposti sostanziali dell'accesso ai dati;

[32] In particolare, si tratta di stabilire se la mancata informazione integri un illecito riconducibile all'attività giurisdizionale del magistrato — con conseguente applicazione della disciplina della responsabilità civile dello Stato per fatto del magistrato (l. 13 aprile 1988, n. 117) — ovvero se attenga a profili di carattere amministrativo o organizzativo dell'attività giudiziaria, suscettibili di dar luogo a responsabilità dello Stato ex art. 2043 cod. civ., anche in relazione alla violazione di obblighi informativi di matrice eurounitaria.

- un **meccanismo di emergenza previsto direttamente dal Regolamento**, che opera, invece, sul piano dell'esecuzione transfrontaliera degli ordini.[33].

Il fattore temporale diviene così oggetto di una regolazione differenziata, nella quale l'anticipazione dell'intervento investigativo non coincide mai con un abbassamento del livello delle garanzie, ma si traduce in una diversa distribuzione dei controlli lungo la sequenza procedimentale.

7.1. L'**ordinamento interno** prevede, agli artt. 2 e 3 d.lgs. n. 215 del 2025, un **modulo emergenziale destinato a operare nelle ipotesi di pericolo imminente per la vita, l'integrità fisica o la sicurezza di una persona ovvero per la sicurezza di infrastrutture critiche**.

In tali situazioni, gli ufficiali di polizia giudiziaria sono legittimati ad adottare l'ordine europeo con intervento immediato, ma con efficacia subordinata alla tempestiva convalida del pubblico ministero entro termini particolarmente ristretti.

Con riferimento all'ordine europeo di produzione, l'art. 2, comma 3, circoscrive, tuttavia, in modo rigoroso l'ambito applicativo dell'intervento emergenziale, consentendo alla polizia giudiziaria di emettere di urgenza esclusivamente ordini aventi ad oggetto dati relativi agli abbonati o dati richiesti al solo scopo di identificare l'utente.

L'urgenza determina un'anticipazione soggettiva dell'iniziativa investigativa – dalla titolarità del pubblico ministero a quella, temporanea, della polizia giudiziaria –, senza incidere sul livello delle garanzie richieste in funzione della tipologia dei dati. Rimane esclusa l'adozione secondo il modulo emergenziale di ordini aventi ad oggetto dati di traffico o dati relativi al contenuto, per i quali la disciplina ordinaria richiede l'intervento del giudice che procede.

Anche con riferimento all'ordine europeo di conservazione disciplinato dall'art. 3 del decreto, la procedura emergenziale attribuisce agli ufficiali di polizia giudiziaria un potere di iniziativa immediata, sottoposto a convalida del pubblico ministero, senza prevedere l'immediato intervento del giudice. La scelta si giustifica in ragione della natura conservativa della misura, che non comporta accesso ai dati né trasferimento delle informazioni all'autorità procedente, ma si limita a impedirne la cancellazione o l'alterazione presso il prestatore di servizi.

L'emergenza incide, dunque, esclusivamente sul fattore temporale dell'intervento investigativo, consentendo la subitanea adozione dell'atto senza modificare la struttura delle garanzie sostanziali: l'eventuale acquisizione conoscitiva dei dati resta, infatti, subordinata all'emissione di un successivo ordine europeo di produzione, soggetto al regime ordinario di competenze e ai relativi controlli giurisdizionali.

7.2. Se la disciplina emergenziale anticipa l'iniziativa investigativa in presenza di un pericolo imminente, la **procedura accelerata** interviene sul diverso piano della **gestione ordinaria dell'urgenza investigativa**, rimodulando i tempi decisionali.

[33] La distinzione tra modulo emergenziale interno, procedura accelerata nazionale ed emergenza eurounitaria emerge dal coordinamento tra gli artt. 2, 3 e 4 d.lgs. n. 215 del 2025 e l'art. 10 Regolamento, che operano su piani funzionalmente distinti della sequenza procedimentale.

Il meccanismo introdotto dall'art. 4 d.lgs. n. 215 del 2025 configura una procedura rapida di emissione degli ordini europei. Essa è destinata a operare in presenza di particolari esigenze di urgenza investigativa non riconducibili alle situazioni di pericolo imminente tipizzate dalla disciplina emergenziale.

La procedura accelerata non costituisce una deroga ai presupposti sostanziali di emissione degli ordini europei né introduce una nuova categoria eccezionale di intervento, ma incide esclusivamente sulle scansioni temporali del procedimento interno di formazione dell'atto.

L'art. 4 costruisce un sistema di velocizzazione procedurale, differenziato in relazione alla natura dei dati oggetto dell'ordine e al diverso livello di garanzie richiesto dal regime ordinario.

Quando l'ordine europeo di produzione riguarda dati di traffico o dati relativi al contenuto, il pubblico ministero può emettere l'atto con efficacia subordinata alla convalida del giudice per le indagini preliminari (art. 4, comma 1, lett. a). L'ordine deve essere trasmesso al giudice entro ventiquattro ore ed è soggetto a convalida, con decreto motivato, entro le successive quarantotto ore; solo a seguito della convalida l'atto può essere trasmesso al prestatore di servizi. L'accelerazione procedimentale si realizza, dunque, mediante l'anticipazione dell'adozione dell'ordine rispetto al controllo giurisdizionale, senza eliminare quest'ultimo, che resta condizione necessaria di efficacia.

Un diverso modulo è previsto per gli ordini di produzione aventi ad oggetto dati relativi agli abbonati o dati richiesti al solo scopo di identificare l'utente. L'art. 4, comma 1, lett. b), consente agli ufficiali di polizia giudiziaria di adottare l'ordine in via anticipata, con trasmissione al pubblico ministero entro ventiquattro ore e convalida entro le quarantotto ore successive. Anche in questo caso, la trasmissione del certificato europeo al prestatore di servizi resta subordinata all'esito positivo del controllo di legalità, coerentemente con il fatto che, nel regime ordinario, tali dati sono acquisibili su iniziativa del pubblico ministero senza intervento giurisdizionale preventivo.

Un autonomo meccanismo accelerato riguarda, infine, l'ordine europeo di conservazione ed è disciplinato dal comma 2 dell'art. 4, che attribuisce agli ufficiali di polizia giudiziaria un potere di iniziativa anticipata, sottoposto a convalida del pubblico ministero. Ancora una volta, la soluzione appare coerente con la natura conservativa della misura.

La procedura accelerata realizza una compressione controllata del fattore temporale all'interno del circuito decisionale nazionale, senza incidere sul livello delle garanzie sostanziali. Diversamente dal modulo emergenziale, essa non si fonda sulla necessità di prevenire un danno imminente a beni primari, ma sull'esigenza di evitare la dispersione della prova digitale in un contesto caratterizzato dall'intrinseca volatilità dei dati elettronici.

La scelta del legislatore nazionale si colloca entro lo spazio di autonomia organizzativa riconosciuto agli Stati membri dal Regolamento, il quale non impone un modello procedurale uniforme per l'emissione degli ordini europei, ma richiede il rispetto delle condizioni sostanziali e delle garanzie correlate alla natura dei dati richiesti.

7.3. Diversa dalle forme di urgenza disciplinate dal diritto interno è la **procedura di emergenza prevista direttamente dal Regolamento**, che opera non sul piano della formazione dell'ordine, ma su quello della sua esecuzione transfrontaliera.

Il Regolamento configura, infatti, un regime eccezionale di esecuzione accelerata attivabile esclusivamente in presenza di una minaccia imminente per beni di primaria rilevanza, quali la vita o l'integrità fisica di una persona ovvero la sicurezza di infrastrutture critiche. In tali situazioni, l'esigenza di intervento immediato giustifica una drastica compressione dei tempi di esecuzione dell'ordine europeo di produzione, imponendo al prestatore di servizi la trasmissione dei dati senza indebito ritardo e comunque entro termini significativamente ridotti rispetto al regime ordinario (art. 10, par. 4, Reg.).

L'accelerazione prevista dal diritto unionale incide, dunque, sul rapporto tra autorità di emissione e prestatore di servizi, proiettandosi verso l'esterno del procedimento nazionale. Essa non modifica i presupposti sostanziali di emissione dell'ordine né la ripartizione delle competenze stabilita dagli ordinamenti interni, che restano disciplinati dal diritto nazionale nel rispetto delle condizioni fissate dal Regolamento.

A tale compressione temporale sul piano esecutivo corrisponde un rigoroso sistema di contrappesi. Il Regolamento prevede, infatti, specifici meccanismi di controllo successivo, tra cui la possibilità per lo Stato di esecuzione di opporsi entro termini definiti e l'obbligo, per l'autorità di emissione, di limitare l'uso dei dati o di procedere alla loro cancellazione qualora l'opposizione risulti fondata. L'emergenza eurounitaria si configura, pertanto, come un modello eccezionale, caratterizzato da una accelerazione massima dell'esecuzione, bilanciata da garanzie altrettanto incisive sul piano del controllo successivo (artt. 10, par. 4, e 12 Reg.).

Il confronto con la disciplina interna consente di cogliere con maggiore chiarezza la diversa funzione dei moduli procedurali esaminati. Mentre le procedure emergenziali e accelerate previste dal d.lgs. n. 215 del 2025 incidono sul circuito decisionale nazionale, anticipando o rimodulando i momenti di emissione e convalida dell'ordine, la procedura di emergenza del Regolamento interviene esclusivamente nella fase esecutiva, una volta che l'ordine sia già validamente formato secondo il diritto interno.

Riassumendo e schematizzando, i tre modelli operano su piani complementari e non sovrapponibili:

- l'emergenza interna anticipa l'iniziativa investigativa;
- la procedura accelerata rimodula i tempi della decisione;
- l'emergenza eurounitaria comprime i tempi dell'esecuzione transfrontaliera[34].

[34] A titolo meramente esemplificativo, può trovare applicazione la procedura emergenziale interna nelle ipotesi in cui l'autorità procedente debba attivarsi con immediatezza per prevenire un pericolo attuale e concreto per la vita o l'integrità fisica di una persona – ad esempio nel contesto di un sequestro di persona o di una minaccia imminente di violenza –, situazioni nelle quali il ritardo nell'attivazione dello strumento investigativo renderebbe vano l'intervento. Può invece venire in rilievo la procedura accelerata nazionale quando, nell'ambito di un'indagine ordinaria, emerga un rischio concreto di cancellazione o perdita di dati digitali – quali *account*, messaggi o *log* di accesso detenuti da un prestatore di servizi – in assenza dei presupposti di pericolo imminente richiesti per l'attivazione del modulo emergenziale. Diversamente, la procedura di emergenza prevista dal Regolamento opera sul piano dell'esecuzione transfrontaliera dell'ordine già validamente emesso. Essa può venire impiegata, ad esempio, quando sia necessario ottenere con estrema rapidità dati detenuti da un prestatore stabilito in altro Stato membro per fronteggiare una minaccia imminente per la

8. La cooperazione in entrata: ricezione, esecuzione e assetto delle competenze (artt. 5 e 6 d.lgs. n. 215 del 2025).

L'art. 6 d.lgs. n. 215 del 2025 individua le **autorità competenti** per la ricezione delle notifiche e l'esecuzione degli ordini europei di produzione e di conservazione emessi da un altro Stato membro, attuando gli artt. 8, 9, 10 e 16 Reg. e riproducendo, anche nella fase passiva, il criterio di graduazione delle competenze e delle garanzie proprio della disciplina dell'emissione.

Più precisamente, la competenza alla ricezione delle notifiche è attribuita al procuratore della Repubblica presso il tribunale del capoluogo del distretto nel quale lo stabilimento designato o il rappresentante legale del prestatore di servizi è stabilito o risiede (art. 6, comma 1). Il criterio territoriale prescelto individua un punto di ingresso unitario del flusso cooperativo, riducendo il rischio di frammentazioni applicative e assicurando un riferimento stabile per l'autorità di emissione.

Quanto alla fase esecutiva, l'art. 6 distingue in funzione della tipologia di dati oggetto dell'ordine. L'esecuzione è attribuita al pubblico ministero distrettuale quando l'ordine concerne dati relativi agli abbonati o richiesti al solo scopo di identificare l'utente nonché in caso di ordine europeo di conservazione; quando, invece, riguarda dati di traffico o dati relativi al contenuto, la competenza spetta al giudice per le indagini preliminari presso il medesimo tribunale (art. 6, comma 2).

Il decreto legislativo disciplina, inoltre, la fase del riconoscimento dell'ordine europeo, prevista dall'art. 6, comma 4, quale momento funzionale all'individuazione dell'autorità nazionale chiamata all'esecuzione. Tale attività non integra un controllo sul merito dell'atto straniero né un procedimento di *exequatur*, ma consiste in una verifica preliminare di competenza volta a consentire l'inserimento dell'atto nel circuito processuale interno.

Qualora l'ufficio destinatario ritenga che al riconoscimento debba provvedere altra autorità giudiziaria, esso è tenuto a trasmettere immediatamente gli atti all'ufficio competente, dandone comunicazione all'autorità di emissione. L'eventuale insorgenza di contrasti è risolta mediante l'applicazione degli artt. 54, 54-*bis* e 54-*ter* cod. proc. pen., secondo i meccanismi ordinari di regolazione dei conflitti di competenza[35].

Il comma 7 dell'art. 6 stabilisce che il compimento degli atti necessari all'esecuzione resta regolato dalla legge italiana. Il Regolamento disciplina i presupposti e gli effetti dell'ordine; le modalità concrete dell'esecuzione sono, invece, governate dal diritto processuale nazionale, secondo un modello di integrazione tra titolo investigativo eurounitario ed esercizio domestico dei poteri processuali.

---

vita o l'integrità fisica di una persona, imponendo al prestatore tempi di risposta significativamente compressi rispetto al regime ordinario.

[35] Per approfondimenti recenti sul tema, si rinvia a: L. D'AMBROSIO, *I contrasti tra uffici del pubblico ministero e le nuove regole sulla competenza territoriale*, in *Cassa. Pen.*, n. 4, 2023, p. 1245 e ss.; F. SIRACUSANO, *Il coordinamento investigativo e la risoluzione dei conflitti tra procure alla luce della recente novella*, in *Arch. Pen.*, n. 1, 2024; G. VARRASO, *La nuova disciplina dei termini per la risoluzione dei contrasti di competenza tra uffici del pubblico ministero*, in *Dir. pen. e proc*, n. 2, 2023.

L'autorità giudiziaria competente non si limita a svolgere una funzione di controllo interno, ma provvede direttamente alla trasmissione dell'ordine europeo al prestatore di servizi e alla gestione del relativo rapporto esecutivo, assumendo la posizione di interlocutore del prestatore di servizi, senza svolgere attività investigativa autonoma. Tale configurazione discende dalla nozione di "autorità di esecuzione" di cui all'art. 3, punto 17, Reg., cui rinvia espressamente l'art. 6 d.lgs. n. 215 del 2025.

Il riparto delle competenze riflette un criterio sostanziale, in forza del quale alle forme di accesso più invasive, idonee a incidere in modo significativo nella vita privata, corrisponde un livello più elevato di controllo giurisdizionale. La fase esecutiva non è, dunque, concentrata in capo all'autorità requirente, ma distribuita secondo la diversa natura dei dati richiesti.

8.1. All'interno della fase passiva si colloca, con funzione sussidiaria, il **ruolo attribuito al Ministero della giustizia** dall'art. 5 d.lgs. n. 215/2025.

L'intervento ministeriale non incide sul merito dell'esecuzione, ma opera quale strumento di supporto e coordinamento nei rapporti con le autorità degli altri Stati membri, assicurando il corretto funzionamento del sistema nei casi in cui si renda necessario un raccordo istituzionale.

8.2. La disciplina della fase passiva conferma l'opzione di fondo del legislatore italiano per un'integrazione del nuovo strumento europeo nel tessuto delle competenze processuali interne, evitando la creazione di un circuito esecutivo parallelo e mantenendo una corrispondenza tra natura dell'atto, intensità dell'ingerenza e autorità chiamata a intervenire. La cooperazione in entrata riproduce così, in chiave speculare, il modello di graduazione delle garanzie già delineato per la fase di emissione, inserendosi in un assetto unitario nel quale effettività investigativa e tutela dei diritti fondamentali risultano bilanciate lungo entrambe le direttrici della cooperazione giudiziaria.

9. La cooperazione in uscita: notifica e controllo (artt. 8, 10 e 12 Reg.; art. 6 d.lgs. n. 215 del 2025).

Il sistema prevede specifici meccanismi di garanzia destinati a gestire i conflitti normativi derivanti dall'applicazione concorrente di normative di Paesi terzi.

Nel contesto della cooperazione in uscita, e dunque dal punto di vista dello Stato di emissione, le disposizioni del decreto legislativo non disciplinano – né potrebbero farlo – i poteri dell'autorità competente dello Stato destinatario della notifica, i quali trovano, invece la loro fonte nel Regolamento. Una sintetica ricostruzione di tali poteri è necessaria per comprendere il funzionamento del meccanismo di cooperazione in uscita.

Nei casi previsti dall'art. 8 Reg., l'emissione dell'ordine europeo di produzione da parte dell'autorità nazionale può essere accompagnata dalla notifica all'autorità competente dello Stato in cui è stabilito il prestatore di servizi o il suo rappresentante legale, con effetto sospensivo dell'esecuzione, salvi i casi di urgenza.

La notifica non è, tuttavia, sempre necessaria: essa è esclusa quando l'ordine ha ad oggetto dati richiesti al solo scopo di identificare l'utente, nonché quando l'autorità di emissione abbia

ragionevoli motivi per ritenere che il reato è stato commesso, è in corso o è probabile che venga commesso nello Stato di emissione e che la persona cui si riferiscono i dati vi risieda.

L'autorità notificata non è chiamata a dare esecuzione all'ordine, ma svolge un controllo, valutando la sussistenza di motivi di rifiuto, interloquendo con l'autorità di emissione e, ove ne ricorrano i presupposti, opponendosi, integralmente o parzialmente, alla trasmissione dei dati ovvero subordinandola a condizioni, nei termini e secondo le modalità previste dagli artt. 10 e 12 Reg.

10. Le obiezioni del prestatore di servizi e il riesame giurisdizionale nello Stato di emissione (art. 17 Reg.; art. 7 d.lgs. n. 215 del 2025).

Nel sistema delineato dal Regolamento, accanto ai meccanismi di controllo operanti nello Stato destinatario della notifica, è contemplato un distinto strumento di garanzia, destinato a operare nello Stato di emissione, attivato su iniziativa del prestatore di servizi. Il riferimento è alla disciplina delle obiezioni motivate prevista dall'art. 17 Reg., che rappresenta uno degli snodi più innovativi dell'intero sistema *e-evidence*, introducendo un meccanismo di gestione dei conflitti normativi derivanti dall'applicazione concorrente di ordinamenti di Paesi terzi.

Il prestatore destinatario di un ordine europeo di produzione può sollevare un'obiezione motivata qualora ritenga che l'esecuzione dell'ordine lo esporrebbe a violazione di obblighi giuridici derivanti dal diritto applicabile di un Paese terzo, in particolare in materia di protezione dei dati personali, segreto delle comunicazioni, divieti di divulgazione o normative extraterritoriali che subordinano la trasmissione dei dati a specifiche autorizzazioni interne. Situazioni di questo tipo possono verificarsi, ad esempio, in presenza di discipline assimilabili ai cd. *blocking statutes* ovvero nell'ambito dell'applicazione dello *U.S. CLOUD Act*, che regola le richieste di accesso ai dati detenuti da fornitori di servizi soggetti alla giurisdizione statunitense[36].

L'obiezione non attribuisce al prestatore un potere di veto sull'ordine europeo, ma attiva un procedimento di verifica strutturato, demandato alle autorità dello Stato di emissione. Il prestatore non è, infatti, un mero esecutore passivo dell'ordine, ma svolge una funzione di segnalazione del possibile conflitto normativo e di attivazione del controllo giurisdizionale. La soluzione del conflitto è così sottratta al soggetto privato e ricondotta alla sede giurisdizionale competente, in coerenza con l'impianto del Regolamento, che concentra nello Stato di emissione il momento decisivo del bilanciamento tra esigenze investigative e rispetto degli obblighi derivanti da ordinamenti terzi.

10.1. Il legislatore nazionale, nel dare attuazione alla disciplina unionale mediante l'art. 7 d.lgs. n. 215 del 2025, ha individuato l'autorità competente al **riesame** secondo un criterio coerente con la struttura del procedimento interno. Nei casi contemplati dall'art. 17 Reg., la decisione spetta al tribunale del capoluogo del distretto nel quale ha sede l'ufficio che ha emesso

[36] Sul conflitto tra ordini di accesso ai dati e normative extraterritoriali, cfr.: S. CARRERA, M. STEFAN, V. MITSILEGAS, *Cross-border data access in criminal proceedings and the future of digital justice*, CEPS/QMUL Task Force Report, 2020; J. DASKAL, *The CLOUD Act and Cross-Border Data Requests*, in *Harvard National Security Journal*, vol. 10, n. 2, 2019, p. 447 e ss.

o convalidato l'ordine, ai sensi dell'art. 324, comma 5, cod. proc. pen., quando l'ordine europeo di produzione sia stato emesso o convalidato dal giudice; qualora, invece, l'ordine sia stato emesso o convalidato dal pubblico ministero, la decisione compete al giudice per le indagini preliminari.

La soluzione richiama consapevolmente il modello dei controlli sulle misure reali e, in particolare, il sistema del riesame dei provvedimenti di sequestro, assicurando una verifica giurisdizionale rapida e concentrata, compatibile con le esigenze dell'attività investigativa.

L'autorità giudiziaria che ha emesso o convalidato l'ordine, qualora intenda confermarlo, deve trasmettere, entro dieci giorni dalla ricezione dell'obiezione, l'ordine, l'obiezione motivata e la relativa documentazione all'autorità investita del riesame, la quale decide entro i successivi dieci giorni, adottando le determinazioni previste dall'art. 17, par. 8, Reg. Nei casi disciplinati dal par. 7 del medesimo articolo, ossia quando il conflitto riguarda diritti fondamentali o interessi essenziali del Paese terzo, in particolare connessi alla sicurezza o alla difesa nazionale, l'autorità giurisdizionale può richiedere informazioni all'autorità competente di tale Paese e il termine per la decisione decorre dalla ricezione delle informazioni richieste.

La possibilità di interlocuzione con l'autorità del Paese terzo non reintroduce un modello di cooperazione giudiziaria internazionale in senso tradizionale, ma costituisce uno strumento informativo diretto ad accertare la concreta esistenza del conflitto dedotto, restando la decisione finale concentrata nello Stato di emissione. Il fulcro del meccanismo è, dunque, rappresentato dalla fase di riesame giurisdizionale.

Il giudice chiamato a pronunciarsi non è incaricato di un sindacato sul merito dell'attività investigativa sottesa all'emissione dell'ordine, ma deve verificare la concreta sussistenza del conflitto normativo e procedere a un bilanciamento tra l'interesse investigativo perseguito dall'autorità di emissione e gli obblighi giuridici derivanti dal diritto del Paese terzo.

Tale valutazione deve essere compiuta secondo i criteri ricavabili dall'art. 17 Reg., come precisati dai considerando 61-66, tenendo conto della natura e della sensibilità dei dati richiesti, dell'intensità dell'ingerenza nei diritti fondamentali e del grado di collegamento territoriale della vicenda con l'Unione europea. I considerando richiamati precisano che il bilanciamento deve essere condotto nel rispetto degli artt. 7 e 8 CDFUE e della normativa europea in materia di protezione dei dati personali, evitando sia applicazioni automatiche dell'ordine europeo sia il rischio opposto di paralisi investigativa derivante da conflitti meramente astratti o ipotetici.

La disciplina dei conflitti normativi si collega, inoltre, ai criteri che definiscono l'ambito soggettivo di applicazione del Regolamento. L'assoggettamento dei prestatori agli obblighi previsti dal Regolamento non dipende, infatti, dal luogo della sede principale, ma dall'offerta di servizi nel mercato dell'Unione. Anche i prestatori stabiliti in Paesi terzi rientrano, pertanto,

nell'ambito di applicazione dello strumento europeo, dovendo designare un rappresentante legale nell'Unione incaricato di ricevere e dare esecuzione agli ordini[37].

Va precisato che il decreto legislativo **non** prevede un **ricorso diretto per cassazione** avverso la decisione adottata nel procedimento di riesame. Tuttavia, la questione potrà essere riproposta nel corso del giudizio di merito, ove i dati acquisiti siano introdotti nel fascicolo e la parte che vi abbia interesse dovesse contestarne l'utilizzabilità. In tale sede, il giudice del processo sarà chiamato a verificare la corretta applicazione del Regolamento e delle garanzie procedurali, e la relativa decisione potrà essere sottoposta al vaglio anche della Corte di cassazione. Fuori dal procedimento di riesame, il prestatore di servizi non ha più titolo per intervenire: l'eventuale contestazione sull'utilizzabilità dei dati resta, quindi, rimessa alle parti del procedimento che abbiano interesse.

11. La clausola di inutilizzabilità e il regime processuale della prova acquisita mediante ordine europeo (art. 2, comma 7, d.lgs. n. 215 del 2025).

Il d.lgs. n. 215 del 2025 introduce una specifica clausola di inutilizzabilità destinata a incidere direttamente sul regime probatorio dei dati acquisiti mediante ordine europeo di produzione. L'art. 2, comma 7, dispone, infatti, che «i dati acquisiti con un ordine europeo di produzione emesso fuori dai casi o in mancanza delle condizioni previste dal regolamento e dal presente decreto non sono utilizzabili».

La norma stabilisce un nesso diretto tra il rispetto delle condizioni di emissione dell'ordine europeo e il regime di utilizzabilità dei dati acquisiti, inserendosi nel sistema dell'art. 191 cod. proc. pen., ma secondo una tecnica normativa peculiare, poiché la sanzione processuale non è ancorata alla violazione di singole prescrizioni formali, bensì al difetto delle condizioni sostanziali che legittimano l'emissione dell'ordine europeo. In questo modo, i presupposti stabiliti dal Regolamento e dalla normativa di adattamento diventano i limiti dell'acquisizione probatoria e la loro inosservanza si riflette direttamente sull'utilizzabilità.

11.1. La clausola di inutilizzabilità condiziona le modalità attraverso le quali il controllo di legalità dell'acquisizione probatoria viene esercitato nel processo penale. In assenza di un sistema di impugnazioni autonome dell'ordine europeo di produzione nella fase genetica – ferma restando la procedura attivabile a seguito delle obiezioni del prestatore di servizi –, la verifica della conformità dell'acquisizione alle condizioni previste dal diritto unionale e nazionale può emergere principalmente nel momento dell'utilizzazione processuale dei dati.

Il vaglio di utilizzabilità postula che le condizioni di emissione dell'ordine europeo risultino verificabili nel processo attraverso la documentazione dell'attività investigativa, secondo le regole proprie del sistema processuale interno. Il giudice del procedimento nel quale la prova viene introdotta è, quindi, chiamato a verificare, nel contraddittorio tra le parti, la sussistenza

[37] Il criterio adottato riproduce una logica funzionale già presente in altri strumenti del diritto dell'Unione, tra cui il regolamento (UE) 2016/679 in materia di protezione dei dati personali, che estende l'applicazione della disciplina anche ai prestatori stabiliti fuori dall'Unione quando offrano servizi nel mercato europeo.

dei presupposti sostanziali richiesti dal diritto dell'Unione e dalla disciplina nazionale, tra cui la riconducibilità del caso alle ipotesi consentite, il rispetto dei criteri di necessità e proporzionalità e la corretta individuazione delle categorie di dati acquisibili.

Il sindacato giurisdizionale si posiziona nella fase valutativa della prova, senza subire attenuazioni sul piano delle garanzie. La deducibilità dell'inutilizzabilità secondo le regole generali dell'art. 191 cod. proc. pen. consente alle parti di contestare la legittimità dell'acquisizione e al giudice di rilevare anche d'ufficio eventuali violazioni delle condizioni di emissione dell'ordine europeo. Il controllo della Corte di cassazione assume carattere successivo e mediato e può essere sollecitato mediante i motivi di impugnazione relativi all'utilizzazione della prova.

In questa prospettiva, si colloca anche la sentenza della Grande Sezione 30 aprile 2024, M.N. (EncroChat), causa C-670/22, che ha chiarito come il principio di reciproco riconoscimento non possa tradursi in una compressione del diritto di difesa tale da impedire un controllo effettivo sulla prova posta a fondamento dell'accusa.

11.2. L'art. 2, comma 7, d.lgs. n. 215 del 2025 solleva alcune questioni interpretative con riguardo all'individuazione delle "condizioni" cui la norma collega l'inutilizzabilità.

A tal fine, assume rilievo preliminare il tema della **documentazione dell'ordine europeo e** della **sua effettiva conoscibilità nel processo**. Il controllo sull'utilizzabilità presuppone, infatti, che gli atti relativi all'emissione e all'esecuzione dell'ordine confluiscano nel fascicolo del pubblico ministero secondo le regole generali di documentazione dell'attività investigativa previste dagli artt. 357 e 373 cod. proc. pen., divenendo accessibili al giudice e alle parti attraverso i meccanismi ordinari di *discovery*.

La natura transnazionale delle procedure previste dal Regolamento introduce, tuttavia, un profilo peculiare, poiché una parte significativa dell'attività esecutiva si realizza attraverso comunicazioni standardizzate con il prestatore di servizi e flussi informatici non coincidenti con gli atti investigativi tradizionali.

Occorre, pertanto, individuare un nucleo documentale idoneo a consentire un controllo effettivo sulla legittimità dell'acquisizione.

Il corretto funzionamento del sindacato giurisdizionale risulta, dunque, strettamente connesso alla tracciabilità procedimentale dell'intero ciclo di acquisizione del dato digitale.

Profili ulteriori di possibile incidenza sull'utilizzabilità possono derivare da criticità di natura linguistica nella redazione e trasmissione dell'ordine europeo, quando imprecisioni terminologiche o traduttive incidano sulla qualificazione dei dati richiesti o sui presupposti giuridici dell'acquisizione (cfr. *infra*, § 14.1).

Resta, inoltre, aperta la questione relativa alla **rilevanza della competenza dell'autorità che ha emesso l'ordine europeo**. Nel sistema processuale interno, l'incompetenza non comporta ordinariamente inutilizzabilità della prova, salvo che determini la violazione di garanzie essenziali o l'elusione di controlli giurisdizionali imposti dalla legge. Trasposta nel contesto dell'*e-evidence*, tale impostazione induce a ritenere che solo le violazioni lesive, in modo sostanziale, delle garanzie previste dal Regolamento possano determinare l'inutilizzabilità, mentre le

irregolarità attinenti alla mera distribuzione interna delle competenze non sembrano automaticamente idonee a produrre il medesimo effetto.

11.3. Ulteriori interrogativi emergono con riferimento al **rapporto tra illegittimità dell'ordine europeo e successiva riemissione di provvedimenti validi**.

Qualora un ordine europeo di conservazione risulti illegittimo, ma abbia comunque determinato la preservazione dei dati, può porsi il problema della successiva acquisizione mediante un nuovo ordine legittimo. Poiché la conservazione non comporta accesso conoscitivo alle informazioni, appare astrattamente configurabile una successiva acquisizione fondata su un autonomo titolo valido; più problematico risulta, invece, il caso in cui la disponibilità del dato derivi causalmente dall'ordine illegittimo, ad esempio quando esso abbia impedito una cancellazione altrimenti inevitabile.

Diversamente, con riguardo all'ordine europeo di produzione, l'inutilizzabilità colpisce l'acquisizione già effettuata e non è suscettibile di sanatoria retroattiva; resta, tuttavia, possibile una nuova acquisizione dei medesimi dati mediante un ordine validamente emesso, purché fondato su un autonomo titolo legittimo e non meramente riproduttivo dell'atto invalido.

La clausola di inutilizzabilità pone interrogativi anche con riguardo alle **procedure accelerate e** ai **meccanismi di urgenza**, nei quali l'attività acquisitiva può precedere il controllo giurisdizionale pieno. Nel processo penale interno, l'illegittimità dell'atto investigativo urgente non si riflette automaticamente sull'utilizzabilità della prova, come emerge nella disciplina dei sequestri probatori, ove la giurisprudenza ha distinto tra invalidità del provvedimento ablativo e statuto probatorio degli elementi acquisiti[38]. Tali esperienze interpretative suggeriscono che l'anticipazione dei controlli non determini di per sé la perdita di utilizzabilità dei dati, salvo che il vizio incida direttamente sulle garanzie difensive o sui diritti fondamentali coinvolti.

11.4. La portata della **clausola di inutilizzabilità** risulta più chiaramente delimitata se si considera che una analoga previsione **non** è **dettata per** gli **ordini europei di conservazione**. Tale scelta appare coerente con la diversa funzione dell'istituto, che non comporta acquisizione conoscitiva del dato né introduzione immediata di elementi probatori nel processo.

L'eventuale illegittimità dell'ordine di conservazione sembra, pertanto, destinata a tradursi nell'inefficacia della misura e nel venir meno dell'obbligo di mantenimento dei dati, senza determinare di per sé conseguenze sul piano dell'utilizzabilità probatoria.

11.5. La clausola di inutilizzabilità introdotta dall'art. 2, comma 7, d.lgs. n. 215 del 2025 costituisce il principale punto di raccordo tra il modello europeo di acquisizione diretta delle prove elettroniche e il sistema processuale penale interno.

[38] In argomento, cfr. Sez. 2, n. 4887 del 20/01/2017, Aslo, Rv. 268991-01, secondo cui l'annullamento del provvedimento di sequestro probatorio impedisce il mantenimento del vincolo sul bene, ma non l'utilizzabilità degli elementi acquisiti ai fini dell'emissione di un successivo decreto di sequestro preventivo, i quali non possono ritenersi prove illegittimamente acquisite ai sensi dell'art. 191cod. proc. pen. Conf. Sez. 3, n. 8762 del 19/12/2002, Raddino, Rv. 223739-01.

Essa proietta nel giudizio sulla prova il rispetto delle condizioni di emissione dell'ordine europeo, facendo della loro osservanza il presupposto della sua efficacia probatoria nel processo.

12. Il coordinamento tra sistema *e-evidence* e disciplina nazionale della conservazione dei dati: adeguamento della *data retention* e introduzione dell'ordine di conservazione processuale (art. 9, comma 1, d.lgs. n. 215 del 2025; art. 132 d.lgs. n. 196 del 2003).

L'art. 9, comma 1, d.lgs. n. 215 del 2025 opera sull'assetto interno della conservazione dei dati, in funzione di coordinamento con il sistema e-*evidence*.

La disposizione opera su due piani. Da un lato, modifica l'art. 132 d.lgs. 30 giugno 2003, n. 196 (di seguito: codice *privacy*), adeguando, almeno in parte, la disciplina della conservazione dei dati di traffico alle esigenze derivanti dal nuovo quadro europeo; dall'altro, introduce nel codice di procedura penale l'art. 263-*bis*, che tipizza un autonomo ordine di conservazione nel corso delle indagini preliminari.

Non ci troviamo in presenza di un adeguamento formale delle disposizioni, bensì di un intervento che ridefinisce la funzione della conservazione del dato digitale, spostandola stabilmente sul piano investigativo, secondo una linea già emersa nel quadro eurounitario. La conservazione non è più soltanto effetto di obblighi legali generalizzati, ma diviene oggetto di attivazione selettiva, funzionale alla successiva acquisizione probatoria.

12.1. Per quel che concerne il rapporto tra la disciplina nazionale della conservazione dei dati di traffico e il sistema europeo degli ordini di conservazione, il coordinamento non si realizza mediante sovrapposizione di modelli, ma attraverso la differenziazione funzionale degli strumenti.

La disciplina di cui all'art. 132 codice *privacy* continua a operare sul piano della conservazione generalizzata imposta *ex lege*, mentre il sistema *e-evidence* e l'intervento interno introdotto dall'art. 9 si collocano sul piano della conservazione mirata, attivata in relazione a un procedimento penale determinato.

La *retention* legale assicura la disponibilità generalizzata dei dati entro limiti temporali predeterminati, mentre gli strumenti di conservazione mirata consentono di intervenire su dati specificamente individuati, per evitarne la dispersione in funzione dell'indagine.

Quando i dati siano ancora soggetti all'obbligo di conservazione previsto dalla disciplina nazionale, l'ordine europeo non incide sui termini legali, ma consente di vincolare in concreto i dati rilevanti per il procedimento, anche quando il termine di conservazione sia prossimo alla scadenza, evitando che essi vengano cancellati nel momento in cui emerge l'esigenza investigativa.

Diversa è l'ipotesi in cui il termine di conservazione previsto dalla disciplina nazionale sia già decorso. In tal caso, l'ordine europeo non è idoneo a determinare la ricostituzione di dati ormai cancellati, ma può spiegare effetti solo ove i dati siano ancora materialmente presenti

presso il prestatore di servizi, imponendone la conservazione per un periodo ulteriore, nei limiti e alle condizioni previste dalla disciplina unionale.

Si tratta, dunque, di due regimi distinti: uno, di carattere generale e preventivo, fondato su termini predeterminati; l'altro, specifico e funzionale al singolo procedimento, attivato dall'autorità giudiziaria in presenza di concrete esigenze investigative.

Questa distinzione rappresenta il punto di equilibrio del coordinamento tra disciplina interna e sistema eurounitario, evitando sovrapposizioni e mantenendo separati i rispettivi ambiti funzionali.

12.2. L'art. 9 d.lgs. n. 215 del 2025, mediante la modifica dell'art. 132 codice *privacy*, ristruttura la disciplina interna della conservazione dei dati, ampliandone la portata funzionale e operativa.

Il legislatore estende le finalità legittimanti l'acquisizione dei dati, includendovi anche le ricerche del latitante, attraverso l'inserimento di un espresso riferimento nei commi 3 e 3-*bis* del citato art. 132. L'utilizzo degli strumenti di conservazione e acquisizione dei dati di traffico, pertanto, non è più circoscritto alla repressione di fatti già accertati, ma può operare anche in funzione di ricerca e localizzazione del soggetto ricercato, in linea con la crescente centralità investigativa del dato digitale.

Di maggiore impatto è l'introduzione dei nuovi commi 3-*bis*.1, 3-*bis*.2 e 3-*bis*.3, attraverso i quali viene tipizzata una misura di conservazione dei dati distinta dall'acquisizione probatoria. Il pubblico ministero può, infatti, ordinare, con decreto motivato, ai fornitori e agli operatori di servizi telefonici, informatici o telematici di conservare e proteggere, per un periodo non superiore a novanta giorni – prorogabile sino a un massimo complessivo di sei mesi – i dati relativi al traffico telefonico e telematico, nonché quelli concernenti le chiamate senza risposta, restando esclusi i contenuti delle comunicazioni.

Il sistema si articola così in tre livelli tra loro coordinati, nei quali la conservazione generalizzata convive con forme di conservazione mirata attivabili in funzione investigativa e con la successiva fase acquisitiva probatoria, soggetta alle garanzie giurisdizionali previste per l'accesso conoscitivo.

La misura introdotta dai commi 3-*bis*.1 e seguenti opera sul solo piano della conservazione e non comporta accesso ai dati.

Assume rilievo la scelta di delineare una disciplina autonoma per i dati relativi agli abbonati, escludendo espressamente l'applicazione delle procedure autorizzatorie previste dai commi 3 e 3-*bis* e attribuendo l'acquisizione al pubblico ministero o alla polizia giudiziaria ai sensi dell'art. 348 cod. proc. pen. (art. 132, comma 3-*bis*.2, codice *privacy*). Tale previsione si correla al minore grado di intrusività proprio dei dati identificativi rispetto ai dati di traffico.

La novella rafforza, dunque, il segmento della preservazione preventiva del dato digitale, in linea con il sistema europeo dell'*e-evidence* e con la natura deperibile delle informazioni telematiche.

All'interno dell'art. 132 codice *privacy* convivono forme di conservazione generalizzata e modalità di conservazione mirata attivabili in funzione di uno specifico procedimento.

In tale contesto, la separazione tra conservazione e accesso rappresenta una scelta strutturale del sistema, che consente di anticipare la tutela della disponibilità del dato senza anticiparne l'utilizzazione probatoria.

Tale configurazione evidenzia non solo un problema di coordinamento interno tra i diversi livelli della disciplina, ma anche una tensione strutturale con il diritto dell'Unione, legata al progressivo superamento del modello della conservazione generalizzata dei dati di traffico.

Le tensioni sistemiche trovano già riscontro nella prassi giudiziaria.

Con ordinanza del giudice per le indagini preliminari presso il Tribunale di Catania è stata sollevata questione pregiudiziale dinanzi alla CGUE in ordine alla compatibilità della disciplina nazionale della conservazione dei dati di traffico con i principi affermati dalla giurisprudenza eurounitaria[39]. Il giudice del rinvio ha chiesto, in particolare, alla CGUE di chiarire se i dati costituiti dai *file* di *log*, ove utilizzati esclusivamente al fine di identificare l'autore di una condotta illecita, possano essere esclusi dalla nozione di "dati di traffico" ai sensi dell'art. 15 direttiva 2002/58/UE ovvero, in via subordinata, se, qualora ricondotti a tale nozione, sia comunque consentito l'accesso a tali dati anche al di fuori delle ipotesi di criminalità grave, quando essi risultino indispensabili ai fini dell'identificazione dell'autore del reato[40]. La struttura del rinvio evidenzia come il giudice nazionale abbia prospettato una soluzione interpretativa articolata su piani tra loro graduati, privilegiando, in via principale, una lettura restrittiva della nozione di "dati di traffico" e, solo in via subordinata, una rimodulazione del requisito della gravità del reato quale presupposto per l'accesso ai dati. Tale impostazione riflette il tentativo di ricondurre la disciplina interna entro i limiti tracciati dalla giurisprudenza eurounitaria, salvaguardando, al contempo,

[39] GIP Catania, ord. 26 giugno 2025, proc. n. 5030/2025 R.G. G.I.P. Ignoti, in *Sist. pen.*, 24 luglio 2025.

[40] Testualmente, le questioni pregiudiziali sono così articolate:

1. se l'articolo 15, paragrafo 1, della direttiva 2002/58/CE del Parlamento europeo e del Consiglio del 12 luglio 2002, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche, modificata dalla direttiva 2009/136/CE del Parlamento europeo e del Consiglio, del 25/11/2009, letto alla luce degli articoli 7, 8, 11 e 52 della Carta dei diritti fondamentali dell'Unione europea e nel quadro della nuova disciplina della prova elettronica (artt. 3, 5 Regolamento 1543/2023), può essere interpretato nel senso che l'accesso delle autorità pubbliche ai dati telematici definibili come *file* di *log*, consistenti in accessi ed uscite (*log-in* e *log-out*) di un utente del sistema o applicazione con relativi indirizzi IP e marche temporali (ossia relativi a un certo arco temporale) e ove questi mirino soltanto a identificare l'autore di un reato – in materia di prevenzione, ricerca, accertamento e perseguimento dei reati –, comporti un'ingerenza nei diritti fondamentali dei soggetti ai quali i dati si riferiscono, che – diversamente dai dati di traffico e geolocalizzazione – non presenti una gravità tale da dover limitare il suddetto accesso alla lotta contro la criminalità grave, potendo invece estendersi alla generalità dei reati;
2. in subordine, laddove la Corte ritenga che l'accesso ai file di *log* (consistenti in accessi ed uscite, ovvero *log-in* e *log-out*, di un utente del sistema o applicazione con relativi indirizzi IP e marche temporali), sebbene questi siano mirati al solo scopo di identificare l'autore di un reato, possa comportare un'ingerenza grave nei diritti fondamentali dei soggetti ai quali i dati si riferiscono, come sanciti dalla Carta dei diritti fondamentali, se l'articolo 15 della Direttiva 2002/58/UE possa essere interpretato nel senso che l'esigenza di accertare e perseguire i reati commessi attraverso la rete telematica – laddove l'autore possa essere identificato unicamente mediante l'acquisizione di dati telematici, quali i citati file di *log*, e tenuto conto della tipica anonimizzazione della rete – sia idonea a giustificare l'accesso ai dati personali trattati dai *service providers* (compresi i dati di traffico e localizzazione), a prescindere dalla "gravità" di detti reati, come definita dagli Stati, e dunque se una legislazione nazionale che ciò preveda possa ritenersi appropriata, proporzionata allo scopo perseguito e necessaria in una società democratica, anche avuto riguardo alla salvaguardia del diritto alla riservatezza e alla identità delle vittime di detti reati.

l'effettività dell'azione investigativa nei contesti caratterizzati dall'uso esclusivo di strumenti digitali.

La pendenza della questione conferma l'attualità del problema interpretativo e la sua immediata rilevanza applicativa.

13. L'introduzione dell'ordine di conservazione nel processo penale (art. 9, comma 2, d.lgs. n. 215 del 2025; art. 263-*bis* c.p.p.).

Accanto alle modifiche di coordinamento apportate alla disciplina della conservazione amministrativa dei dati, il legislatore ha introdotto nel codice di rito l'art. 263-*bis*, che tipizza un autonomo ordine di conservazione destinato a operare nel corso delle indagini preliminari (art. 9, comma 2, d.lgs. n. 215 del 2025).

La disposizione, collocando stabilmente la conservazione mirata tra gli strumenti di indagine, recepisce sul piano processuale il modello europeo, nel quale la conservazione del dato è configurata come attività distinta e logicamente anteriore rispetto alla sua acquisizione probatoria.

13.1. L'art. 263-*bis* cod. proc. pen. attribuisce al pubblico ministero il potere di ordinare, con decreto motivato, ai fornitori e agli operatori di servizi informatici, telematici o di telecomunicazioni di conservare e proteggere i dati detenuti per un periodo non superiore a novanta giorni, prorogabile, per motivate esigenze, entro un limite massimo complessivo di sei mesi. Il provvedimento può, inoltre, prevedere specifiche modalità di custodia e l'eventuale indisponibilità dei dati da parte dei gestori o di terzi, ponendo un vincolo giuridico volto a impedirne l'alterazione o la cancellazione durante il periodo di conservazione (art. 263-*bis*, comma 1, cod. proc. pen.).

La norma solleva **interrogativi interpretativi**, a cominciare dalla delimitazione del **contenuto dell'ordine di conservazione**. È, infatti, stabilito che il pubblico ministero «può ordinare (…) di conservare e proteggere, secondo le modalità indicate e per un periodo non superiore a novanta giorni» i dati detenuti dal prestatore, ma non è precisato se l'indicazione delle modalità di custodia e della durata costituisca elemento necessario o eventuale del provvedimento[41].

[41] Sul contenuto necessario degli atti investigativi limitativi di diritti fondamentali, la giurisprudenza di legittimità ha costantemente valorizzato l'esigenza di determinatezza del comando giudiziario quale corollario del principio di legalità processuale e della verificabilità successiva dell'atto. A titolo puramente esemplificativo, si vedano: Sez. 6, n. 38260 del 08/10/2025, Bevilacqua, Rv. 288923-01, ove si precisa che, in tema di intercettazioni, il decreto autorizzativo di operazioni da effettuarsi con captatore informatico, relativo a reati diversi da quelli previsti dall'art. 266, comma 2-*bis*, cod. proc. pen., deve indicare i luoghi di privata dimora suscettibili di captazione, le ragioni per cui si ritiene fondatamente che vi si stia svolgendo l'attività criminosa e i tempi di attivazione del microfono, essendo, invece, irrilevante l'inserimento di ulteriori condizioni eccedenti i limiti normativamente previsti, la cui violazione non inficia, pertanto, l'utilizzabilità dei risultati dell'attività captativa. (In applicazione del principio, la Corte ha ritenuto utilizzabili le captazioni effettuate nell'abitazione di un indagato, valutando prive di effetti le condizioni afferenti alla predeterminazione dei frangenti e delle modalità dell'azione criminosa, inserite nel decreto autorizzativo, valutate eccentriche rispetto ai limiti legislativamente stabiliti); Sez. 5, n. 9797 del 04/03/2025, R., 287778-02, per la quale, in tema di sequestro probatorio di documenti informatici e telematici contenenti dati sensibili, l'obbligo motivazionale del provvedimento ablatorio può dirsi adempiuto qualora, tenuto conto del momento processuale in cui è stato adottato, nonché delle peculiari esigenze di accertamento del reato, il pubblico ministero abbia indicato in maniera specifica, ancorché concisa, le ragioni determinanti la necessità di una limitazione temporanea alla disponibilità esclusiva dei dati da parte del destinatario del provvedimento ablatorio.

Con riferimento alle **modalità di custodia**, la previsione di legge sembra attribuire al pubblico ministero un potere conformativo sulle tecniche di conservazione, consentendo l'imposizione di cautele dirette a garantire l'integrità, la non alterazione e la tracciabilità del dato, anche mediante vincoli di indisponibilità operativa nei confronti del prestatore o di terzi. Resta, tuttavia, dubbio se l'omessa indicazione di prescrizioni puntuali incida sulla validità dell'ordine: qualora si ritenga che l'indicazione delle modalità di custodia costituisca elemento necessario del provvedimento, la loro mancanza potrebbe incidere sulla validità dell'ordine di conservazione; se, invece, tale indicazione è intesa come meramente eventuale, l'ordine dovrebbe ritenersi comunque valido anche in assenza di prescrizioni specifiche, con conseguente applicazione degli *standard* tecnici ordinariamente adottati dal prestatore per la conservazione dei dati.

Analoghe perplessità riguardano la determinazione della **durata** della misura. Il limite massimo di novanta giorni non chiarisce se l'ordine debba necessariamente indicare il termine di efficacia oppure se, in mancanza di una specifica determinazione temporale, operi automaticamente il limite legale. Quest'ultima opzione esegetica rischierebbe di trasformare il termine massimo in durata ordinaria della misura, attenuando la funzione di garanzia connessa alla valutazione di proporzionalità nel caso concreto.

Il riferimento alle **«particolari modalità di custodia» e** all'**eventuale indisponibilità del dato** attribuisce all'autorità procedente un potere conformativo che incide non soltanto sull'*an* della conservazione, ma anche sulle modalità tecniche di attuazione della misura all'interno delle infrastrutture del prestatore di servizi.

Le prescrizioni possono riguardare, ad esempio, l'adozione di misure idonee a garantire integrità e immutabilità del dato, la segregazione logica[42] delle informazioni rispetto ai sistemi ordinari di gestione, la tracciabilità degli accessi e delle operazioni (*logging*), nonché la sospensione dei processi automatici di cancellazione o sovrascrittura. La possibilità di imporre l'indisponibilità del dato nei confronti del prestatore o di terzi evidenzia come la misura possa incidere sulla sfera di controllo tecnico del gestore, introducendo un vincolo giuridico di custodia che comporta una temporanea indisponibilità funzionale del dato.

L'esecuzione dell'ordine avviene, tuttavia, integralmente all'interno dei sistemi del prestatore, senza la presenza dell'autorità giudiziaria. La verifica del rispetto delle modalità imposte non può, quindi, fondarsi su un controllo diretto, ma dipende dalla documentazione tecnica e dalle attestazioni fornite dal destinatario dell'ordine. La tracciabilità dell'attività di conservazione e la completezza della documentazione riversata nel fascicolo costituiscono, pertanto, elementi essenziali della verifica.

13.2. Ulteriori questioni interpretative derivano dalla formulazione dell'**oggetto dell'ordine**, riferito ai **«dati da questi detenuti»**. L'espressione appare significativamente più

[42] Con l'espressione "segregazione logica" si indica, nel linguaggio informatico, l'isolamento dei dati all'interno del sistema informativo mediante misure *software* o configurazioni di accesso che ne limitano l'utilizzo e ne impediscono la modifica o la cancellazione, pur senza comportarne la separazione materiale dai sistemi del prestatore, diversamente dalla "segregazione fisica", che implica la collocazione dei dati su supporti o sistemi separati. Sul tema, cfr.: ISO/IEC 27002, *Information security controls*; ENISA, *Cloud Security Guidelines*; ID., *Cloud Computing Risk Assessment*.

ampia rispetto alle formule tradizionalmente utilizzate dal codice di rito, normalmente riferite a cose determinate o comunque determinabili. La disposizione non chiarisce se l'ordine debba individuare categorie di dati, utenze, *account* o periodi temporali specifici, ovvero se possa estendersi all'intero patrimonio informativo detenuto dal prestatore.

Una lettura meramente letterale finirebbe per avvicinare la conservazione processuale a forme di *retention* investigativa generalizzata, in contrasto con l'orientamento della Corte di giustizia che esclude modelli di conservazione indiscriminata dei dati comunicativi.

La delimitazione dell'oggetto deve, pertanto, emergere dalla motivazione del provvedimento, quale sede nella quale si realizza il controllo di necessità e proporzionalità, così da evitare che la misura assuma carattere generalizzato.

13.3. In presenza di ragioni di **urgenza**, l'ordine può essere anticipato dagli ufficiali di polizia giudiziaria, con obbligo di comunicazione al pubblico ministero entro quarantotto ore e successiva convalida nelle quarantotto ore successive; in mancanza di convalida, il provvedimento perde efficacia (art. 263-*bis*, comma 2, cod. proc. pen.).

La valutazione dell'urgenza sembra dover essere ricondotta ai criteri elaborati nel sistema processuale interno per gli atti investigativi anticipati, fondati sul rischio concreto che il ritardo determini la perdita o l'irreversibile alterazione della fonte di prova. Nel contesto digitale, tale rischio risulta strettamente connesso alla rapida deperibilità dei dati e ai meccanismi automatici di cancellazione o sovrascrittura propri dei sistemi informatici.

Il modello presenta affinità con quello previsto per altri atti urgenti incidenti su diritti fondamentali – quali, ad esempio, le intercettazioni disposte in via d'urgenza dal pubblico ministero –, pur collocandosi su un piano di minore intensità intrusiva, in quanto l'ordine di conservazione non comporta accesso conoscitivo al contenuto delle comunicazioni. I presupposti dell'urgenza, pur richiedendo una verifica concreta e motivata, risultano, quindi, meno stringenti rispetto a quelli richiesti per gli strumenti acquisitivi.

L'urgenza si configura, dunque, come anticipazione funzionale della tutela del dato rispetto al rischio di dispersione, coerente con la natura della misura.

13.4. La previsione secondo cui, **in caso di mancata convalida, il provvedimento perde efficacia** solleva interrogativi circa la sorte dei dati già conservati nel periodo intercorrente tra l'adozione dell'ordine urgente e il controllo dell'autorità giudiziaria.

La disciplina non chiarisce se la perdita di efficacia imponga l'eliminazione dei dati conservati o comporti soltanto la cessazione dell'obbligo di ulteriore conservazione. Non risulta, inoltre, regolata l'eventuale incidenza della mancata convalida sulla successiva acquisizione probatoria di dati la cui disponibilità sia stata resa possibile proprio dall'attivazione della misura urgente.

La situazione presenta profili analoghi a quelli del sequestro probatorio disposto d'iniziativa dalla polizia giudiziaria e successivamente non convalidato, nel quale la caducazione dell'atto elimina gli effetti ablativi per il futuro, senza neutralizzare automaticamente le conseguenze

fattuali già prodotte[43]. Trasposta nel contesto dell'ordine di conservazione, tale impostazione induce a interrogarsi sulla possibilità di una successiva acquisizione dei medesimi dati mediante un autonomo ordine di produzione e sulla rilevanza, sul piano della legittimità, della disponibilità dell'informazione resa possibile da un provvedimento non convalidato.

Il problema si riflette, in particolare, sulla legittimità della successiva acquisizione probatoria dei dati, qualora la loro disponibilità risulti causalmente riconducibile all'attivazione di una misura di conservazione adottata in assenza dei presupposti di legge.

La misura consente di intervenire su dati specificamente individuati, anche al fine di evitarne la cancellazione in prossimità della scadenza dei termini di conservazione legale, determinando un effetto di prolungamento della loro disponibilità.

Tale effetto opera nei limiti della persistente esistenza materiale dei dati presso il prestatore e non comporta la ricostituzione di informazioni già cancellate.

La conservazione si configura, dunque, come fase funzionalmente prodromica rispetto all'acquisizione probatoria.

14. Monitoraggio dell'attuazione e obblighi informativi nel sistema *e-evidence* (art. 8 d.lgs. n. 215 del 2025).

Accanto al controllo giurisdizionale esercitato nel singolo procedimento, il d.lgs. n. 215 del 2025 introduce un ulteriore livello di controllo, affidato a meccanismi di monitoraggio istituzionale su scala europea.

L'art. 8 attribuisce al Ministero della giustizia il compito di raccogliere e trasmettere le informazioni relative all'applicazione degli ordini europei. Il Ministero cura la registrazione e l'elaborazione dei dati statistici previsti dall'art. 28, par. 2, Reg., relativi al numero e alla tipologia degli ordini emessi, alle categorie di dati richiesti, ai reati interessati, ai tempi di esecuzione e agli esiti delle procedure, alle ipotesi di mancata esecuzione o ritardo[44], nonché la loro

[43] Cfr. Sez. 6, n. 4328 del 02/03/1999, Abate, Rv. 213659-01, per la quale la mancata convalida del sequestro operato dalla polizia giudiziaria – *ex* art. 355 cod. proc. pen. – non incide sull'utilizzazione a fini probatori delle cose sequestrate, ma soltanto sulla possibilità di mantenimento del sequestro stesso: la convalida – i cui eventuali vizi devono essere fatti valere con le impugnazioni previste dagli art. 324 ss. cod. proc. pen. – ha, infatti, la funzione di legittimare la sottrazione del bene sottoposto a sequestro alla sfera di appartenenza del proprietario o di chi ne abbia la disponibilità e non già di permettere l'utilizzazione processuale del bene sottoposto alla misura cautelare. Conf. Sez. 4, n. 14854 del 27/02/2003, Ghezzi, Rv. 224391-01.

[44] Nello specifico, a mente dell'art, 28, par. 2, i dati inviati alla Commissione includono:

a) il numero di EPOC e EPOC-PR emessi, per tipo di dati richiesti, destinatari e situazione (di emergenza o meno);
b) il numero di EPOC emessi nell'ambito di deroghe per casi di emergenza;
c) il numero di EPOC e EPOC-PR adempiuti e non adempiuti, per tipo di dati richiesti, destinatari e situazione (di emergenza o meno);
d) il numero di notifiche alle autorità di esecuzione a norma dell'articolo 8 e il numero di EPOC rifiutati, per tipo di dati richiesti, destinatari e situazione (di emergenza o meno), nonché i motivi addotti per il rifiuto;
e) per gli EPOC adempiuti, il periodo medio che intercorre tra il momento dell'emissione dell'EPOC e il momento in cui i dati sono ottenuti, per tipo di dati richiesti, destinatari e situazione (di emergenza o meno);
f) per gli EPOC-PR adempiuti, il periodo medio che intercorre tra il momento dell'emissione dell'EPOC-PR e il momento dell'emissione della successiva richiesta di produzione, per tipo di dati richiesti e destinatari;
g) il numero di ordini europei di produzione o di ordini europei di conservazione trasmessi a uno Stato di esecuzione e da questo ricevuti ai fini dell'esecuzione, per tipo di dati richiesti, destinatari e situazione (di emergenza o meno), e il numero di tali ordini adempiuti;

trasmissione alla Commissione europea e l'effettuazione delle notifiche previste dagli artt. 31, par. 1, e 32, par. 2, Reg.

L'autorità giudiziaria trasmette al Ministero i dati necessari alla raccolta statistica, secondo un modello accentrato di gestione dei dati. La concentrazione delle funzioni di raccolta ed elaborazione presso il Ministero della giustizia assicura l'uniformità dei flussi informativi provenienti dagli uffici giudiziari e consente di individuare un unico punto nazionale di interlocuzione con le istituzioni dell'Unione europea.

Il sistema europeo di valutazione dell'applicazione della disciplina assegna alla Commissione il compito di effettuare una verifica periodica del funzionamento degli strumenti di acquisizione delle prove elettroniche e dei risultati conseguiti, anche con riguardo all'impatto sui diritti fondamentali, sulla base delle informazioni fornite dagli Stati membri (art. 33 Reg.).

L'elaborazione dei dati provenienti dai diversi ordinamenti nazionali consente di individuare eventuali criticità applicative e tendenze interpretative[45]. Le informazioni, pur non incidendo sulla validità del singolo ordine europeo né costituendo parametro immediato di giudizio nel processo penale, contribuiscono alla ricostruzione del contesto applicativo del diritto dell'Unione e favoriscono la formazione di orientamenti interpretativi comuni nella prassi istituzionale europea.

L'art. 28, par. 2, Reg. prevede una scansione temporale del flusso informativo verso la Commissione, stabilendo che, a decorrere dal 18 agosto 2026, gli Stati membri trasmettano annualmente, entro il 31 marzo, i dati relativi all'anno civile precedente.

Il sistema sarà ulteriormente specificato dal programma di monitoraggio che la Commissione è chiamata a istituire entro il 18 agosto 2026, il quale definirà i mezzi di raccolta dei dati, nonché la periodicità delle acquisizioni e le misure che gli Stati membri devono adottare nella raccolta e nell'analisi delle informazioni.

---

h) il numero di ricorsi proposti contro gli ordini europei di produzione nello Stato di emissione e nello Stato di esecuzione, per tipo di dati richiesti;

i) il numero di casi in cui non è stata concessa la convalida ex post a norma dell'articolo 4, paragrafo 5;

j) una panoramica delle spese dichiarate dai prestatori di servizi per l'esecuzione degli EPOC e degli EPOC-PR e delle spese rimborsate dalle autorità di emissione.

[45] Tecniche analoghe di monitoraggio applicativo sono state adottate in altri strumenti di cooperazione giudiziaria europea fondati sul reciproco riconoscimento, quali il mandato di arresto europeo (di seguito: MAE) e l'OEI.
Con specifico riferimento al MAE, i periodici *report* della Commissione europea sull'attuazione della decisione quadro 2002/584/GAI (tra cui COM(2005) 63, COM(2007) 407, COM(2011) 175 e, da ultimo, COM(2020) 270, reperibili in eur-lex.europa.eu) hanno evidenziato, sulla base dei dati trasmessi dagli Stati membri, fenomeni di utilizzo disomogeneo dello strumento e criticità applicative ricorrenti, quali, in particolare, problemi di proporzionalità nell'emissione dei mandati, divergenze interpretative tra ordinamenti e difficoltà connesse alla tutela dei diritti fondamentali. A tali rilievi sono seguiti interventi correttivi e di coordinamento a livello unionale, tra cui l'adozione di strumenti di *soft law*, in particolare, l'*Handbook* della Commissione, e iniziative di valutazione istituzionale, quale la risoluzione del Parlamento europeo del 20 gennaio 2021 sull'attuazione del MAE.
Analogamente, con riferimento all'OEI, la Commissione europea ha avviato attività di monitoraggio dell'attuazione della direttiva 2014/41/UE (v. relazione COM(2021) 409 *final*, reperibile in eur-lex.europa.eu), dalle quali sono emerse difficoltà operative e applicazioni non uniformi dello strumento, con particolare riguardo ai tempi di esecuzione, alla completezza delle richieste e al coordinamento tra autorità giudiziarie. Anche in questo caso, alle criticità rilevate sono seguiti interventi di supporto e armonizzazione, attraverso linee guida operative e il ruolo di coordinamento svolto da organismi quali *Eurojust* e la Rete giudiziaria europea.
Tali esperienze confermano come, nel diritto dell'Unione, il funzionamento degli strumenti di cooperazione giudiziaria sia affidato a un modello dinamico, fondato sulla sequenza attuazione–monitoraggio–correzione, nel quale la raccolta sistematica dei dati applicativi costituisce il presupposto per l'elaborazione di interventi interpretativi e, ove necessario, normativi.

La previsione di una raccolta e trasmissione periodica dei dati pone un problema di coordinamento con il segreto investigativo di cui all'art. 329 cod. proc. pen.

Le informazioni oggetto di comunicazione, pur essendo tipizzate dal Regolamento e non riguardando il contenuto delle comunicazioni né gli elementi probatori acquisiti, potrebbero, infatti, se considerate nel loro insieme, consentire l'individuazione indiretta di procedimenti specifici ovvero rivelare l'esistenza e lo stato di attività investigative in corso.

Il rischio di disvelamento non deriva, pertanto, dal contenuto intrinseco delle singole informazioni, ma dalla loro possibile combinazione, idonea a restituire un quadro conoscitivo significativo delle modalità di utilizzo dello strumento e, in taluni casi, delle strategie investigative adottate, soprattutto nei contesti territoriali di dimensioni ridotte o con riferimento a indagini caratterizzate da particolare riservatezza.

Il coordinamento tra obblighi informativi e tutela del segreto investigativo impone l'adozione, sul piano applicativo, di modalità di raccolta e trasmissione dei dati idonee a evitare la riconducibilità delle informazioni a specifici procedimenti.

A tal fine, l'aggregazione su base temporale e territoriale comporta la riconduzione dei dati a periodi di riferimento determinati (ad es., su base annuale o semestrale) e ad ambiti geografici sufficientemente ampi (ad es., distrettuali o sovradistrettuali), evitando la trasmissione di informazioni riferite al singolo procedimento o a unità organizzative di dimensioni ridotte, così da ridurre il rischio di identificazione indiretta.

Ove necessario, si affiancano le tecniche di anonimizzazione o pseudonimizzazione delle informazioni trasmesse. Le prime consistono nella eliminazione irreversibile di ogni elemento idoneo a consentire l'identificazione diretta o indiretta del procedimento o dei soggetti coinvolti, mediante la rimozione degli identificativi specifici e la riconduzione delle informazioni a categorie aggregate. La pseudonimizzazione si realizza, invece, attraverso la sostituzione degli elementi identificativi con codici o altri identificatori indiretti, che non consentono l'immediata individuazione del procedimento, ma che restano, in linea di principio, reversibili da parte del soggetto che detiene la chiave di collegamento. Nel sistema delineato dal Regolamento, destinato al monitoraggio su scala unionale e non alla gestione del singolo procedimento, l'anonimizzazione appare, in linea generale, la soluzione maggiormente coerente, in quanto idonea a garantire un più elevato livello di tutela del segreto investigativo, ferma restando la necessità di evitare una perdita di dettaglio tale da compromettere l'utilità delle informazioni.

La concreta individuazione delle modalità di raccolta e trasmissione dei dati, ivi compresi i mezzi di acquisizione delle informazioni e l'articolazione della loro periodicità, è affidata, da un lato, all'organizzazione interna degli Stati membri e, dall'altro, al programma di monitoraggio che la Commissione è chiamata a definire ai sensi dell'art. 28, par. 1, Reg., scelte che incidono direttamente sull'equilibrio tra esigenze di monitoraggio e tutela del segreto investigativo, in ragione del grado di standardizzazione, automazione e dettaglio delle informazioni richieste.

In tale prospettiva, la circolazione delle informazioni continua a svolgere una funzione di garanzia indiretta del sistema, contribuendo alla costruzione di un quadro conoscitivo

complessivo idoneo a consentire verifiche di coerenza applicativa e a prevenire utilizzi disomogenei dello strumento nei diversi ordinamenti, purché le modalità di raccolta e trasmissione dei dati siano strutturate in modo da non compromettere la riservatezza delle indagini.

14.2. Su un piano distinto, relativo ai flussi informativi interni, le disposizioni contenute negli artt. 2, commi 5 e 6, 3, comma 4, 4, comma 3, e 6, comma 3, d.lgs. n. 215 del 2025 prevedono, a fini di coordinamento investigativo, la trasmissione della copia dell'ordine europeo, rispettivamente, al Procuratore nazionale antimafia e antiterrorismo e al Procuratore generale presso la Corte d'appello.

La comunicazione non si esaurisce nella mera notizia dell'emissione o dell'esecuzione dello strumento, ma comporta la trasmissione dell'atto nei suoi elementi essenziali, quali la qualificazione giuridica del fatto, le categorie di dati richiesti e il contesto investigativo.

La previsione normativa appare funzionale a consentire alle autorità destinatarie di esercitare in modo effettivo le rispettive attribuzioni di coordinamento e controllo, che presuppongono una conoscenza non meramente formale, ma sostanziale dell'attività investigativa in corso.

La trasmissione dell'ordine, in quanto atto selettivo e già definito nei suoi contenuti essenziali, consente un flusso informativo mirato, senza comportare la circolazione dell'intero compendio investigativo.

La scelta legislativa si inserisce in un assetto ordinamentale che già consente forme di circolazione interna delle informazioni tra uffici del pubblico ministero, in funzione di coordinamento e raccordo investigativo.

PARTE III.
Le ricadute organizzative e le prospettive di sistema.

15. Prime ricadute sull'organizzazione degli uffici giudiziari.

Il nuovo assetto dei rapporti tra autorità giudiziaria e prestatori di servizi, la compressione dei tempi procedimentali e la necessità di una puntuale qualificazione delle informazioni impongono una **revisione delle modalità operative** degli uffici giudiziari, sia sul versante requirente sia su quello giudicante.

In primo luogo, va considerata la **gestione dei flussi comunicativi con i prestatori di servizi e con le autorità degli altri Stati membri**. La centralità del pubblico ministero distrettuale nella fase passiva e la concentrazione delle competenze presso specifici uffici richiedono modelli organizzativi idonei a garantire continuità operativa, tempestività e tracciabilità degli atti, evitando sovrapposizioni o ritardi incompatibili con la natura volatile delle informazioni digitali.

Un ulteriore aspetto attiene alla **specializzazione**. La complessità tecnica delle categorie di dati, il raccordo con la giurisprudenza eurounitaria e la gestione dei conflitti normativi con ordinamenti terzi suggeriscono l'opportunità di sviluppare competenze dedicate e nuclei di riferimento interni agli uffici, capaci di garantire uniformità applicativa e qualità delle decisioni.

Infine, si pone l'**esigenza di coordinamento con il Ministero della giustizia** per quanto attiene ai profili statistici, ai rapporti con la Commissione europea e al monitoraggio dell'impatto applicativo del nuovo sistema. L'*e-evidence* introduce, infatti, una dimensione di responsabilità organizzativa che trascende il singolo procedimento e si proietta sul piano dell'efficienza complessiva del servizio giustizia.

Le ricadute organizzative mostrano che l'attuazione del Regolamento non si esaurisce in un adattamento procedurale, ma implica una rimodulazione delle modalità di funzionamento degli uffici giudiziari, chiamati a integrare efficienza operativa, presidio delle garanzie e competenze tecniche specialistiche nell'ambito di una cooperazione europea diretta.

15.1. Il sistema delineato dal Regolamento impone che gli ordini europei di produzione e di conservazione siano redatti mediante **certificato standardizzato in una lingua accettata** dallo Stato membro nel quale è stabilito o designato il prestatore di servizi. Ciò non esclude, tuttavia, che il certificato debba risultare agli atti del procedimento anche in lingua italiana, in conformità al principio stabilito dall'art. 109 cod. proc. pen., secondo cui gli atti del procedimento penale sono compiuti nella lingua dello Stato.

Nel rapporto con il prestatore di servizi, la lingua del certificato non è rimessa alla discrezionalità dell'autorità emittente, ma è vincolata alle dichiarazioni rese dagli Stati membri, con la conseguenza che un ordine redatto in lingua non accettata può non essere eseguito.

Il Regolamento non disciplina le modalità della traduzione né individua il soggetto competente a curarla, lasciando all'ordinamento interno il compito di colmare la lacuna sul piano organizzativo. La traduzione dell'ordine non integra un'attività peritale ai sensi del codice di procedura penale né richiede forme di asseverazione, trattandosi di atto di cooperazione giudiziaria e non di mezzo di prova. Tuttavia, l'accuratezza linguistica assume rilievo sostanziale, poiché imprecisioni nella qualificazione dei dati o nella descrizione del presupposto giuridico possono incidere sull'esecuzione dell'ordine e, indirettamente, sulla validità dell'acquisizione.

La questione impone, pertanto, una riflessione sull'organizzazione degli uffici giudiziari. L'affidamento della traduzione a conoscenze linguistiche personali del magistrato o del personale amministrativo, pur teoricamente possibile, espone a rischi di disomogeneità e di errore tecnico. Appare, invece, coerente con l'impianto del sistema l'individuazione di soluzioni stabili e dedicate, quali nuclei linguistici specializzati presso gli uffici distrettuali, convenzioni con traduttori qualificati o forme di supporto centralizzato.

Il profilo linguistico, lungi dall'essere un elemento meramente formale, si posiziona al crocevia tra effettività della cooperazione e garanzia della legalità e rappresenta una delle prime e più concrete sfide organizzative poste dall'attuazione del nuovo sistema europeo.

La redazione dell'ordine in lingua non accettata dallo Stato membro interessato si ripercuote sull'effettività della cooperazione, potendo legittimare il prestatore a non eseguire l'ordine o a sollevare obiezione; la criticità resta, in tal caso, confinata alla fase genetica del procedimento cooperativo.

Una traduzione imprecisa o incompleta può integrare un'irregolarità formale priva di incidenza sostanziale, ove non alteri l'oggetto dell'ordine né il titolo giuridico dell'acquisizione; anche in tale ipotesi, non si configura un vizio idoneo a determinare inutilizzabilità.

Qualora, invece, l'errore linguistico incida sulla qualificazione della tipologia dei dati richiesti, sul perimetro dell'acquisizione o sulla base giuridica dell'ordine, determinando un ampliamento o una modifica non consentita dei presupposti sostanziali previsti dal Regolamento, il vizio non riguarda più la mera forma linguistica, ma investe la legittimazione dell'accesso al dato, potendo riflettersi sulla validità dell'acquisizione e incidere sull'utilizzabilità della prova ai sensi dell'art. 2, comma 7, d.lgs. n. 215/2025.

La questione linguistica si colloca, dunque, su una linea di confine tra organizzazione e garanzia: l'errore produce effetti patologici sul piano probatorio, solo ove si traduca in una deviazione dai presupposti sostanziali dell'ordine europeo.

15.2. Il nuovo sistema impone un controllo rigoroso delle **scansioni temporali** previste per l'emissione, la convalida e la trasmissione degli ordini europei, nonché per l'attivazione delle procedure di emergenza o di riesame. La compressione dei termini, specie nei casi di urgenza, richiede strumenti organizzativi di tracciabilità idonei a monitorare le fasi del procedimento cooperativo.

La gestione degli ordini mediante certificati standardizzati e canali di trasmissione dedicati implica l'adozione di protocolli informatici chiari, idonei a garantire sicurezza, integrità e verificabilità degli atti. L'adeguamento organizzativo investe non solo la fase decisionale, ma anche la conservazione e l'archiviazione digitale dei provvedimenti, che devono essere facilmente individuabili e ricostruibili, anche in vista di eventuali contestazioni processuali.

La corretta gestione dei termini non assume un rilievo solo amministrativo, ma si inserisce nel circuito delle garanzie: eventuali ritardi nella convalida o nella trasmissione possono incidere sull'efficacia dell'atto e sulla stabilità dell'acquisizione.

15.3. La **distinzione tra dati** relativi agli abbonati, dati di accesso, dati di traffico e dati di contenuto incide sul riparto delle competenze e sul livello delle garanzie richieste, sicché errori di qualificazione possono determinare incertezze applicative e divergenze interpretative, soprattutto nella fase iniziale di attuazione del sistema, e riflettersi sulla corretta individuazione dell'autorità competente e sul regime dei controlli giurisdizionali.

Si manifesta, pertanto, un'esigenza di coordinamento e di progressiva uniformazione delle prassi, diretta a prevenire frammentazioni applicative tra uffici e a garantire coerenza nell'impiego di uno strumento destinato a operare in un contesto europeo integrato. L'elaborazione di linee guida condivise e il confronto sistematico tra uffici assumono un ruolo

centrale nel consolidamento del nuovo modello, favorendo un'applicazione omogenea delle categorie normative e una più stabile definizione dei relativi confini interpretativi.

15.4. L'art. 10 d.lgs. n. 215 del 2025, recante le disposizioni finanziarie relative all'attuazione del decreto, non limita la propria funzione al piano meramente contabile, ma presenta evidenti implicazioni organizzative.

La norma autorizza uno stanziamento specifico destinato all'attuazione delle disposizioni concernenti l'ordine europeo di conservazione, la procedura accelerata e la fase passiva di ricezione ed esecuzione degli ordini europei, ossia proprio agli ambiti nei quali il legislatore ha concentrato le principali innovazioni operative e i maggiori carichi organizzativi per gli uffici giudiziari. La selettività dell'intervento finanziario evidenzia che l'impatto del nuovo modello si manifesta soprattutto nelle attività caratterizzate da maggiore urgenza procedimentale e da più intensa necessità di coordinamento tra autorità giudiziarie, prestatori di servizi e strutture amministrative.

Al contempo, la previsione secondo cui le amministrazioni interessate provvedono agli adempimenti ulteriori con le risorse umane, strumentali e finanziarie disponibili a legislazione vigente conferma la scelta di innestare il sistema dell'*e-evidence* all'interno dell'organizzazione giudiziaria esistente, senza la creazione di strutture autonome o di un apparato dedicato, affidando l'effettività della cooperazione diretta con i prestatori di servizi e il rispetto delle scansioni temporali previste dal diritto dell'Unione alla capacità dei singoli uffici di riorganizzare e gestire l'esistente più che all'apporto di nuove risorse.

16. Osservazioni conclusive.

L'introduzione dell'*e-evidence package* non costituisce un semplice aggiornamento tecnico degli strumenti di cooperazione giudiziaria, ma un mutamento di paradigma nell'acquisizione della prova digitale. L'intervento unionale ridefinisce la struttura del modello probatorio penale, incidendo sul rapporto tra potere investigativo, garanzie difensive e dimensione sovranazionale dell'azione giudiziaria.

Per lungo tempo, il diritto penale, sostanziale e processuale, è rimasto ai margini dell'integrazione europea rispetto ad altri settori dell'ordinamento. Oggi, invece, l'accesso alla prova digitale e la cooperazione transnazionale costituiscono ambiti nei quali l'influenza del diritto dell'Unione e della giurisprudenza della Corte di giustizia si manifesta in modo sistemico, riflettendosi non solo sui presupposti di utilizzazione della prova, ma anche sulla distribuzione delle competenze e sulle modalità del sindacato giurisdizionale.

Il nuovo quadro normativo configura il dato elettronico come oggetto giuridicamente tipizzato, attorno al quale si sviluppa un regime articolato di presupposti, competenze e verifiche, che regola l'accesso al dato digitale secondo criteri di proporzionalità, prevedibilità e controllabilità ed estende il controllo di legalità all'intero ciclo di formazione della prova.

L'effettività dell'adattamento interno dell'*e-evidence* – costruito su un delicato equilibrio tra integrazione europea e categorie processuali nazionali – dipende ora anche dall'elaborazione

giurisprudenziale e dalla capacità degli uffici giudiziari di assicurare uniformità applicativa e qualità del controllo.
La disciplina esaminata evidenzia come, anche nell'era della prova digitale, l'effettività dell'azione penale e la tutela delle garanzie non costituiscano termini antitetici, ma poli di un equilibrio che il diritto è chiamato a mantenere stabile, verificabile e coerente con i principi dello spazio europeo di giustizia penale.

Il Redattore: Caterina Brignone

Il Vice Direttore
Antonio Corbo

Il Direttore
Alberto Giusti