JUS- **ONLINE 6/2025**
ISSN 1827-7942
RIVISTA DI SCIENZE GIURIDICHE
a cura della Facoltà di Giurisprudenza dell'Università Cattolica di Milano

INDICE N. 6/2025

VP VITA E PENSIERO

PROGETTI DI RICERCA

***JUS*- ONLINE 6/2025**
ISSN 1827-7942
RIVISTA DI SCIENZE GIURIDICHE
a cura della Facoltà di Giurisprudenza dell'Università Cattolica di Milano

SERENA CACCIATORE - ANNALISA MANGIARACINA - MAR JIMENO BULNES*

Il Regolamento sulla prova "elettronica" prende forma: l'adeguamento da parte dell'Italia e il silenzio della Spagna**

English title: *The Regulation on Electronic Evidence takes shape: Italy's adaptation and Spain's silence*

DOI: 10.26350/18277942_000270

1. Evoluzione tecnologica e processo penale

Negli ultimi decenni, l'evoluzione tecnologica ha profondamente trasformato ogni aspetto della vita quotidiana, rivoluzionando le modalità di interazione sociale e incidendo significativamente anche sul processo penale. Il progresso tecnologico ha infatti generato una quantità sempre più crescente di dati e informazioni suscettibili di essere impiegati come mezzi di prova. In tale contesto, la prova digitale si è affermata come elemento centrale, assumendo un ruolo di grande rilievo già nella fase delle attività investigative[1].

---

*Pur essendo il lavoro frutto di una ricerca collettiva, Serena Cacciatore, Università degli studi di Palermo (serenasabrinaimmacolata.cacciatore@unipa.it), ha redatto i §§ 1, 2, 2.1, 3 e 5; Annalisa Mangiaracina, Università degli studi di Palermo (annalisa.mangiaracina@unipa.it), il § 3.1; Mar Jimeno Bulnes, Universidad de Burgos (mjimeno@ubu.es), il § 4.
** Contributo finanziato dalla Fundación Privada Manuel Serra Domínguez (https://www.manuelserradominguez.org/): X Convocatoria de ayudas para la financiación de actividades propias de la Fundación Privada Manuel Serra Domínguez. El presente trabajo se enmarca dentro del proyecto investigador "Estado de Derecho, justicia sostenible y digitalización en el espacio judicial europeo: preguntas y respuestas" (Ref. PID2024-1565677NB-100) financiado por el Ministerio de Ciencia e Innovación en España.
[1] In argomento, tra i tanti, v. M. HOYOS SANCHO, *La nueva regulación en la Unión Europea sobre obtención transfronteriza de información electrónica en procesos*

Tuttavia, nell'attuale panorama giuridico, tanto a livello interno[2] quanto dell'Unione europea, manca una definizione univoca e condivisa di "prova digitale"[3]. Piuttosto, la dottrina[4] ne ha individuato alcune caratteristiche peculiari, tra le quali spiccano l'immaterialità e la facile alterabilità. Quanto alla prima, essa è connaturata alla natura stessa di tali prove, prive di consistenza fisica e, pertanto, difficilmente riconducibili alla disciplina probatoria tradizionale prevista dagli ordinamenti giuridici nazionali. L'assenza di materialità comporta la possibilità di un rapido trasferimento dei dati da un *server* a un altro, determinando così la transnazionalità delle prove stesse. Tale fenomeno rappresenta una conseguenza diretta della natura "senza frontiere" del cyberspazio e della necessità, da parte dei fornitori di servizi *Internet*, di ottimizzare l'efficienza di *server* collocati in Stati differenti e lo spostamento pressoché continuo dei dati.
Altra caratteristica è quella, come accennato, della facile alterabilità, con il rischio conseguente di perdita, manipolazione o alterazione delle prove digitali: ciò impone l'adozione di cautele specifiche volte a garantirne l'autenticità e l'integrità, assicurando che il giudizio possa fondarsi su elementi probatori genuini e conformi all'originale.
Gli strumenti tradizionali di cooperazione giudiziaria in materia penale — tanto quelli basati sull'assistenza giudiziaria reciproca, quanto quelli fondati sul principio del riconoscimento reciproco (tra tutti l'ordine europeo di indagine) — hanno dimostrato una sostanziale inefficacia rispetto alla gestione delle prove digitali, soprattutto se si considera la rapidità con cui un dato elettronico può essere generato, modificato o

penales análisis y valoración del «e-evidence package», Pamplona, 2024; A. MANGIARACINA, *Nuovi scenari nell'accesso transfrontaliero alla prova "elettronica"*, in *Mobilità, sicurezza e nuove frontiere tecnologiche*, a cura di V. MILITELLO - A. SPENA, Torino, 2018, p. 421 ss.; J. A. MURIEL DIÉGUEZ, *Las órdenes de entrega y conservación de pruebas electrónicas en el proceso penal europeo*, in *Revista de Estudios Europeos*, 83 (2024), p. 172 ss.; M. PITTIRUTI, Digital evidence *e procedimento penale*, Torino, 2017; Á. TINOCO PASTRANA, *Las órdenes europeas de entrega y conservación: la futura obtención transnacional de la prueba electrónica en los procesos penales en la Unión Europea*, in *Cuadernos de política criminal*, 135 (2021), p. 203 ss.

[2] Per quanto concerne il diritto italiano, la mancanza di una definizione precisa di "prova digitale" porta inevitabilmente i giudici ad assumere un ruolo "supplente", attraverso l'impiego di categorie già tipizzate oppure facendo ricorso allo strumento della prova atipica previsto dall'art. 189 c.p.p.

[3] Sulle varianti lessicali v. M. PITTIRUTI, *Digital evidence e procedimento penale*, cit., p. 6 s.

[4] In argomento v. F. SIRACUSANO, *La prova informatica transnazionale: un difficile "connubio" fra innovazione e tradizione*, in *Processo Penale e Giustizia*, 1 (2017), p. 178 ss.; v., altresì, S. SIGNORATO, *Le indagini digitali. Profili strutturali di una metamorfosi investigativa*, Torino, 2018, p. 3 ss.

cancellato. Il disallineamento tra la velocità del fenomeno tecnologico e la lentezza degli strumenti di cooperazione ha posto con forza l'esigenza di un intervento normativo europeo specifico e innovativo, capace di rispondere adeguatamente alle nuove sfide poste dalla dimensione digitale del processo penale contemporaneo.

In questa direzione si colloca il Regolamento (UE) 2023/1543, del 12 luglio 2023, relativo agli ordini europei di produzione e di conservazione di prove elettroniche nei procedimenti penali e all'esecuzione di pene detentive conseguenti a procedimenti penali[5], in vigore dal 18 agosto 2026. Attraverso questo nuovo strumento, l'autorità giudiziaria di uno Stato membro dell'Unione europea potrà richiedere la produzione o la conservazione di dati elettronici (quali comunicazioni *e-mail*, messaggi o altre informazioni digitali) detenuti non già da altre autorità giudiziarie, ma da fornitori di servizi situati in altri Stati membri, al fine di utilizzarli come prove nei procedimenti penali[6]. Dall'*impact assessment*[7] condotto dalla Commissione europea è emerso che le richieste di cooperazione giudiziaria tra Stati membri aventi ad oggetto l'accesso a prove elettroniche ammontano a circa 13.000 all'anno. Le domande indirizzate ai fornitori di servizi – in particolare alle piattaforme globali quali *Google* e *Facebook* – hanno registrato un incremento del 70% nel quadriennio più recente, mentre la percentuale media di riscontro positivo si attesta intorno al 45%[8]. Numeri, questi, significativi.

---

[5] Regolamento n. 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. Al Regolamento si affianca la Direttiva UE 2023/1544, del Parlamento europeo e del Consiglio, del 12 luglio 2023, recante norme armonizzate sulla designazione di stabilimenti designati e sulla nomina di rappresentanti legali ai fini dell'acquisizione di prove elettroniche nei procedimenti penali (da attuare entro il 18 febbraio 2026).

[6] Il considerando n. 10 afferma che il Regolamento «dovrebbe essere applicabile in tutti i casi transfrontalieri in cui il prestatore di servizi ha lo stabilimento designato o il rappresentante legale in un altro Stato membro. Il presente regolamento non pregiudica la facoltà delle autorità nazionali di rivolgersi ai prestatori di servizi stabiliti o rappresentati nel loro territorio affinché ottemperino a misure nazionali dello stesso tipo».

[7] Sul dato empirico v. M. GIALUZ-J. DELLA TORRE, *Lotta alla criminalità nel cyberspazio: la Commissione presenta due proposte per facilitare la circolazione delle prove elettroniche nei processi penali*, in *Diritto penale contemporaneo*, 5 (2018), p. 280 ss.

[8] Cfr. C. MORELLI, E-evidence*, passo avanti: delega al Governo in via di approvazione*, in *Altalex*, 2025, disponibile all'indirizzo https://www.altalex.com/documents/news/2025/03/24/passo-avanti-e-evidence-

Nelle indagini di natura informatica – dove si registra una "frattura" tra il luogo in cui si trovano potenziali elementi probatori e il luogo dal quale essi possono essere legittimamente acquisiti[9] – sorgono delicate questioni interpretative, nonché significative preoccupazioni quanto alla captazione e all'impiego processuale di dati conservati su *server* ubicati all'estero, ovvero di informazioni che, per loro stessa conformazione, sono suscettibili di circolare nello spazio digitale attraverso forme di archiviazione in rete, quali i servizi di *cloud computing*[10].
In ragione dell'immaterialità e della volatilità dei dati digitali, la principale criticità di questa tipologia di investigazioni sta nell'individuazione della normativa applicabile, di fronte all'alternativa tra le norme dello Stato in cui la prova è materialmente reperibile (*lex loci*) e quelle dello Stato in cui essa viene introdotta a fini decisori (*lex fori*). In linea generale, la vigente disciplina in materia di investigazioni transfrontaliere tende a valorizzare la *lex loci*, contemperandola con il rispetto delle «formalità e delle procedure necessarie ai fini dell'utilizzabilità della prova in base alla legge del *locus iudicii*»[11] sempre che queste non siano in conflitto con i principi dell'ordinamento giuridico dello Stato.

2. Il Regolamento (UE) 2023/1543 ("*E-evidence*")

La Commissione europea, nella fase di predisposizione del Regolamento in esame, ha operato nella consapevolezza che lo spazio digitale è, per sua natura, privo di confini e che i servizi online possono essere forniti da qualsiasi luogo, indipendentemente dalla presenza di un'infrastruttura fisica nello Stato in cui tali servizi vengono fruiti. In un numero crescente di procedimenti penali, infatti, le autorità investigative necessitano di accedere a dati conservati al di fuori del proprio territorio, rivolgendosi a fornitori di servizi stabiliti in altri Stati membri o in Paesi terzi.
Per la sua specificità, è opportuno chiarire preliminarmente come il Regolamento non sia destinato a sostituire l'ordine europeo di indagine (di

delega-governo-approvazione (ultimo accesso, come per tutti gli URL citati, il 2 dicembre 2025).
[9] S. SIGNORATO, *Le indagini digitali. Profili strutturali di una metamorfosi investigativa*, cit., p.161.
[10] M. DANIELE, *La vocazione espansiva delle indagini informatica e l'obsolescenza della legge*, in *Processo Penale e Giustizia*, 5 (2018), p. 831 ss.
[11] W. NOCERINO, *I sistemi di controllo da remoto nella legislazione interna e sovranazionale*, in *DPCE online*, 1 (2022), p.76.

seguito: OEI)[12], il quale continuerà a trovare applicazione per l'assunzione delle prove "tradizionali" – ivi incluse quelle precostituite – non elettroniche. A quest'ultimo riguardo, secondo il testo europeo (art. 3 n. 8), per prove elettroniche si intendono: «i dati relativi agli abbonati, i dati sul traffico o i dati relativi al contenuto conservati in formato elettronico da o per conto di un prestatore di servizi al momento della ricezione, di un certificato di ordine europeo di produzione (EPOC) o di un certificato di ordine europeo di conservazione (EPOC-PR)».

La portata della definizione non appare di carattere generale, bensì confinata ai dati effettivamente detenuti dai prestatori di servizi destinatari dell'ordine europeo di produzione e di conservazione delle prove elettroniche[13]. La distinzione tra diverse categorie di dati ha precise implicazioni sul versante dei diritti degli individui posto che non tutti i dati sono contrassegnati dal medesimo grado di intrusività: si passa, infatti, dalla categoria meno invasiva dei dati relativi agli abbonati, c.d. *subscriber data* – quelli forniti dall'utente al momento della registrazione del servizio – e dei dati richiesti al solo scopo di identificare l'utente, a quelle più penetranti dei dati sul traffico, c.d. *traffic data,* e dei dati di contenuto, c.d. *content data*. Questi ultimi, che esprimono il livello massimo di interferenza con i diritti della persona, includono il corpo dei messaggi email, il contenuto delle chat, i file allegati, le foto e i video condivisi, i documenti caricati su servizi di *cloud storage*, i post pubblicati sui *social media*.

Due sono le tipologie di ordini, in relazione alla finalità perseguita, che possono essere emessi: quello di produzione e quello di conservazione dei dati.

Nella versione originaria[14], l'ordine europeo di produzione era definito come la decisione vincolante adottata dall'autorità di emissione di uno

---

[12] Cfr., volendo, S. CACCIATORE, *La aplicación práctica de la orden europea de investigación como mecanismo de obtención transnacional de pruebas*, in *La evolución del Espacio judicial europeo en materia civil y penal: su influencia en el proceso español*, a cura di M. JIMENO BULNES, Valencia, 2022, p. 299 ss.

[13] V. COLAROCCO - T. GROTTO - G. VACIAGO a cura di, *La prova digitale. La casistica civile e penale e gli strumenti di acquisizione in ambito cloud*, Milano, 2020, pp. 1-84.

[14] Art. 2 comma 1 della Proposta di Regolamento del Parlamento europeo e del Consiglio relativo agli ordini europei di produzione e di conservazione di prove elettroniche in materia penale, 17 aprile 2018, COM (2018) 225 finale. Sul testo v. O. CALAVITA, *La proposta di Regolamento sugli ordini di produzione e conservazione europei: Commissione, Consiglio e Parlamento a confronto*, in *La Legislazione Penale*, (2021), p. 1 ss.; R. M. GERACI, *La circolazione transfrontaliera delle prove digitali in U.E.: la proposta di regolamento* e-evidence, in *Cass. pen.*, (2019), p. 1340 ss.

Stato membro, volta a richiedere la produzione di prove elettroniche a un prestatore di servizi che operi nell'Unione e che risulti stabilito o rappresentato in un diverso Stato membro (art. 2, comma 1). Tale definizione è stata tuttavia modificata nel corso dei negoziati: la versione concordata dal Consiglio e Parlamento – orientata a una maggiore precisione – descrive l'ordine di produzione come «la decisione che dispone la produzione di prove elettroniche, emessa o convalidata da un'autorità giudiziaria di uno Stato membro (...), e rivolta a uno stabilimento designato o a un rappresentante legale di un prestatore di servizi che offre servizi nell'Unione, qualora tale stabilimento designato o rappresentante legale sia ubicato in un altro Stato membro vincolato dal presente regolamento» (art. 3, comma 1).
Quanto all'ordine europeo di conservazione, esso consiste nella decisione – anch'essa emessa o convalidata da un'autorità giudiziaria di uno Stato membro – con la quale si impone a un prestatore di servizi l'obbligo di conservare le prove elettroniche, in vista di una successiva richiesta di produzione.
Appare evidente, già dalle definizioni, il cambio di paradigma del Regolamento rispetto ai tradizionali strumenti di assistenza giudiziaria fondati sul "mutuo riconoscimento": la richiesta di accesso ai dati custoditi all'estero è indirizzata non già all'autorità giudiziaria, ma direttamente al prestatore di servizi. Un'innovazione che non ha mancato di sollevare perplessità sui rischi connessi alla tutela dei diritti fondamentali dei soggetti coinvolti.
Analogamente a quanto previsto nella direttiva sull'OEI, anche nel nuovo impianto normativo assume rilievo centrale il principio di proporzionalità[15]. Nello specifico, il Regolamento, tra le condizioni di emissione, tanto dell'ordine di produzione (art. 5) quanto dell'ordine di conservazione (art. 6), stabilisce espressamente che possano essere emessi se necessari e proporzionati; a tal fine, per l'ordine di produzione, si tiene conto dei diritti della persona oggetto di indagini o imputata, e l'emissione può avvenire solo se un ordine dello stesso tipo avrebbe potuto essere emesso alle stesse condizioni in un caso interno analogo (art. 5, comma 2).

[15] Cfr. Regolamento (UE) 2023/1543, in particolare i considerando 2 e 38, nei quali si afferma che gli ordini europei di produzione e conservazione dei dati elettronici devono essere emessi nel rispetto dei principi di necessità e proporzionalità, tenendo conto dell'impatto sui diritti fondamentali delle persone interessate, nonché gli artt. 5, par. 1, lett. b), e 6, par. 1 e 2, che impongono all'autorità emittente di verificare che la misura sia limitata a quanto strettamente necessario e proporzionato allo scopo perseguito nel caso concreto.

Ulteriori condizioni sono correlate alla tipologia di reati per i quali l'ordine può essere adottato e alla categoria di dati.
Come anticipato, per quanto concerne i destinatari della richiesta, gli ordini vanno inoltrati direttamente a uno stabilimento[16] designato o a un rappresentante legale del prestatore di servizi interessato. In via eccezionale, nei casi di emergenza, qualora lo stabilimento designato o il rappresentante legale di un prestatore di servizi non reagisca a un EPOC o a un EPOC-PR entro i termini, i relativi ordini possono essere rivolti a qualsiasi altro stabilimento o rappresentante legale del prestatore di servizi nell'Unione. Quest'ultimo è da intendersi come la persona fisica o giuridica che fornisca uno o più delle seguenti categorie di servizi: «servizi di comunicazione elettronica; servizi di nomi di dominio *internet* e di numerazione IP (...), i registri di nomi di dominio, i *registrars* di nomi di dominio e i connessi servizi per la *privacy* o *proxy (...)*; servizi della società dell'informazione» attraverso i quali gli utenti scambiano comunicazioni e che processano o conservano dati per conto degli utenti, quando la conservazione è componente determinante del servizio offerto.
Una volta ricevuto l'ordine di produzione, il destinatario dovrà preservare i dati fino alla consegna (art. 10). Nel caso in cui venga trasmessa una notifica alle autorità dello Stato di esecuzione e queste non ravvisino alcuna causa di rifiuto entro il termine di 10 giorni, il fornitore di servizi sarà tenuto a trasmettere i dati direttamente all'autorità di emissione allo spirare del suddetto termine[17], caratterizzato dalla particolare brevità. Qualora, invece, l'autorità di esecuzione comunichi, prima del decorso dei 10 giorni, l'assenza di motivi di rifiuto, il destinatario dell'ordine, dovrà procedere alla consegna dei dati senza indugio e, comunque, entro 10 giorni dalla ricezione dell'ordine[18].
Un termine ancora più contenuto – al più tardi entro 8 ore dalla ricezione dell'EPOC – è previsto in caso di "emergenza".
I motivi di rifiuto che l'autorità di esecuzione può opporre all'ordine di produzione, enucleati all'art. 12, sono ben noti, collocandosi sul solco di

[16] Il Regolamento lo definisce come un'entità che esercita effettivamente un'attività economica a tempo indeterminato, con un'infrastruttura stabile a partire dalla quale è svolta l'attività di prestazione di servizi o è gestita l'attività (art. 3, numero 5).
[17] F. LA CHIOMA, *L'ordine di produzione e di conservazione europeo delle prove elettroniche Penale,* in *Magistratura indipendente,* (2019).
[18] V. P. TOPALNAKOS, *Critical Issues in the New EU Regulation on Electronic Evidence in Criminal Proceedings*, in EUCRIM.EU, 2 (2023), p.200; F. PINTO PALACIOS - P. PUJOL CAPILL, *La prueba en la era digital*, Madrid, 2017.

quelli previsti in altri strumenti di assistenza giudiziaria e possono essere così sintetizzati: tutela di immunità o privilegi previsti dall'ordinamento interno, nonché applicazione delle norme a salvaguardia della libertà di stampa o di espressione; circostanze eccezionali in cui sussistano elementi specifici e oggettivi idonei a far ritenere che l'esecuzione dell'ordine determinerebbe una violazione manifesta dei diritti fondamentali, ai sensi dell'art. 6 TUE e della Carta dei diritti fondamentali dell'Unione europea; contrasto con il principio del *ne bis in idem*; mancanza di doppia incriminazione, salvo che il fatto rientri tra quelli elencati nell'Allegato IV e sia punito, nello Stato di emissione, con una sanzione detentiva o misura privativa della libertà della durata massima non inferiore a tre anni.
Prima di far valere un motivo di rifiuto, l'autorità di esecuzione, notificata a norma dell'art. 8, dovrà contattare quella di emissione con qualsiasi mezzo appropriato per avviare un dialogo sulle misure opportune da adottare.
Di rilievo è l'art. 13 del Regolamento, relativo all'onere di informare "senza indebito ritardo" – salvo specifiche esigenze – la persona i cui dati sono richiesti sulla base di un ordine europeo di produzione, incluso il richiamo alle informazioni sui mezzi di ricorso disponibili.
L'art. 16 del Regolamento disciplina la procedura da attivare qualora il fornitore di servizi non ottemperi nei termini all'ordine, senza addurre ragioni ritenute valide dall'autorità di emissione e in assenza di motivi di rifiuto. In tale evenienza, l'autorità di emissione può sollecitare l'intervento dell'autorità di esecuzione, la quale riconosce l'ordine entro cinque giorni, senza ulteriori formalità, e adotta le misure necessarie per dare attuazione agli ordini, salvo che rilevi cause di rifiuto. L'autorità di esecuzione, dunque, intima al *provider* di conformarsi all'ordine, avvertendolo della facoltà di far valere motivi di rifiuto e della possibile irrogazione di sanzioni in caso di mancata cooperazione.
Il quadro sin qui sinteticamente tracciato mostra come il Regolamento in questione miri, attraverso il dialogo tra autorità giudiziaria e fornitore di servizi, da un lato, a garantire certezza giuridica agli operatori coinvolti e, dall'altro, a realizzare un equilibrio tra le esigenze investigative e la tutela dei diritti fondamentali, rafforzando così la fiducia reciproca tra gli Stati membri[19]. Molto però dipenderà dalle modalità con le quali i singoli ordinamenti si adatteranno al testo.

[19] V. le considerazioni di G. TABASCO, *L'acquisizione transfrontaliera delle prove elettroniche* in *Processo Penale e Giustizia*, 4 (2025), p.6 ss.

2.1. Il ruolo della difesa: profili critici

Il ricorso sempre più diffuso alla prova digitale nell'ambito del procedimento penale ha contribuito a ridefinire il ruolo della difesa e la stessa fisionomia del contraddittorio. Nel modello accusatorio delineato dall'art. 111 Cost., la formazione della prova dovrebbe idealmente realizzarsi nel confronto dialettico tra le parti dinanzi al giudice; tuttavia, tale modello entra in crisi quando la prova assume una conformazione tecnica e irripetibile, come nel caso dei dati informatici. La peculiare natura della prova digitale, infatti, impone che la sua acquisizione avvenga quasi sempre nella fase delle indagini preliminari, con la conseguenza di spostare il baricentro del processo al di fuori del dibattimento che, di contro, dovrebbe costituire il momento centrale per la formazione dell'elemento probatorio. Questo "spostamento" determina inevitabilmente un affievolimento delle garanzie partecipative della difesa, la quale spesso non è nelle condizioni di potere intervenire nella fase delicata in cui la prova viene acquisita, preservata o duplicata[20].
In questo contesto, la domanda sul ruolo che la difesa può realmente svolgere nel procedimento, tanto se più se di matrice transnazionale, assume una centralità crescente[21]. L'impossibilità di partecipare agli atti tecnici più delicati – si pensi all'estrazione dei dati, alla creazione della copia forense, all'impiego dei captatori informatici o alla conservazione dei dati volatili – obbliga il difensore a ricollocare la propria funzione su un piano successivo, essenzialmente critico e valutativo. Il contraddittorio, dunque, si realizza, attraverso un controllo *ex post* che diventa una sorta di strumento "compensativo" rispetto alla mancata partecipazione iniziale. Affinché questo possa esplicarsi in modo effettivo, è indispensabile che gli inquirenti adottino tutte le cautele tecniche atte a garantire la genuinità, l'integrità e la non modificabilità del dato acquisito.
La difesa, infatti, svolge la sua funzione di garanzia solo se posta nella condizione di verificare la conformità della copia all'originale, la

[20] V. S. RUGGERI, *Procedimento penale, diritto di difesa e garanzie partecipative nel diritto dell'Unione Europea*, in *Diritto Penale Contemporaneo*, 4 (2015), pp. 1-31.
[21] V. L. LUPARIA- G. ZICCARDI, *Investigazione penale e tecnologia informatica*, Milano, 2007; A. MALACARNE, *Le investigazioni difensive nel prisma delle "nuove" indagini preliminari: per una parità delle armi a vocazione digitale e* ultra fines, in *Archivio Penale*, 3 (2025), p. 1 ss.

correttezza delle procedure adottate e la tracciabilità di ogni attività svolta sul sistema informatico oggetto di indagine.

Sul piano nazionale, risultano di cruciale importanza prescrizioni come quelle contenute negli artt. 254-*bis*[22] e 260, comma 2, c.p.p.[23], che impongono l'utilizzo di supporti idonei ad assicurare la conformità della copia e la sua immodificabilità. Solo il rispetto rigoroso degli standard della *digital forensics* – in particolare la creazione di una *bit-stream image* che riproduca fedelmente il dato senza alterarlo – consentirà al difensore di effettuare una verifica autonoma e scientificamente attendibile della prova[24].

L'attività difensiva, dunque, si ridefinisce come funzione di controllo tecnico-procedurale sull'operato degli inquirenti. Tale funzione assume una rilevanza tanto maggiore quanto più si consideri la particolare fragilità della prova digitale, suscettibile di alterazioni anche minime, intenzionali o accidentali, in grado di comprometterne irrimediabilmente il valore probatorio.

La possibilità di contestare la correttezza delle procedure seguite, la catena di custodia, la conservazione delle copie, il rispetto delle modalità di acquisizione e l'eventuale impiego di strumenti invasivi costituisce, quindi, l'unico spazio residuo in cui la difesa può esercitare efficacemente il proprio ruolo. In questa prospettiva, l'assenza di sanzioni specifiche per il mancato rispetto delle corrette procedure tecniche rappresenta una lacuna significativa del sistema, poiché riduce l'efficacia delle prerogative difensive e rischia di lasciare senza adeguato presidio un ambito probatorio particolarmente sensibile.

---

[22] «1. L'autorità giudiziaria, quando dispone il sequestro, presso i fornitori di servizi informatici, telematici o di telecomunicazioni, dei dati da questi detenuti, compresi quelli di traffico o di ubicazione, può stabilire, per esigenze legate alla regolare fornitura dei medesimi servizi, che la loro acquisizione avvenga mediante copia di essi su adeguato supporto, con una procedura che assicuri la conformità dei dati acquisiti a quelli originali e la loro immodificabilità. In questo caso è, comunque, ordinato al fornitore dei servizi di conservare e proteggere adeguatamente i dati originali».

[23] «2. L'autorità giudiziaria fa estrarre copia dei documenti e fa eseguire fotografie o altre riproduzioni delle cose sequestrate che possono alterarsi o che sono di difficile custodia, le unisce agli atti e fa custodire in cancelleria o segreteria gli originali dei documenti, disponendo, quanto alle cose, in conformità dell'articolo 259. Quando si tratta di dati, di informazioni o di programmi informatici, la copia deve essere realizzata su adeguati supporti, mediante procedura che assicuri la conformità della copia all'originale e la sua immodificabilità; in tali casi, la custodia degli originali può essere disposta anche in luoghi diversi dalla cancelleria o dalla segreteria».

[24] C. MAIOLI, *I "nuovi" mezzi di ricerca della prova fra informatica forense e L. 48/2008*, in *Altalex*, 2012.

Il ruolo assunto dalla difesa nel testo del Regolamento non si differenzia da altri strumenti normativi europei. Al riguardo, l'art. 1, comma 2, prevede che l'emissione di un ordine europeo di produzione o di conservazione possa essere richiesta anche da una persona oggetto di indagini o imputata, ovvero da un avvocato che agisce per conto della suddetta persona, nel quadro dei diritti della difesa applicabili conformemente al diritto processuale penale nazionale.
La formula utilizzata riecheggia quella contenuta nella direttiva sull'OEI[25] e, in linea con quel testo, esclude, senza che possa cogliersi una giustificazione, la persona offesa dal reato dai soggetti che possono sollecitare l'emissione dell'ordine. Al di là della lacuna, la previsione in esame, pur formalmente orientata a rafforzare il ruolo della difesa nelle dinamiche della cooperazione giudiziaria transnazionale, rischia di rivelarsi una "clausola vuota", priva di efficacia, tenuto conto che la sua concreta operatività è rimessa integralmente al diritto interno degli Stati membri, molti dei quali non hanno introdotto a oggi strumenti idonei a consentire alla difesa di attivare autonomamente i meccanismi di assistenza.

3. La legge di delegazione europea

Seppure il Regolamento sarà immediatamente operativo dal 18 agosto 2026, sono subito apparsi necessari alcuni adattamenti a livello interno. Sul versante italiano, l'art. 1 della legge del 13 giugno 2025, n. 91[26] ha conferito al Governo la delega per l'adozione dei decreti legislativi necessari a dare attuazione a taluni atti normativi dell'Unione europea indicati nel testo della legge stessa e, tra questi, figura proprio il Regolamento sulla prova elettronica. La delega, da esercitare entro dodici mesi dalla data di entrata in vigore della legge – ossia a decorrere dal 10 luglio 2025 – è subordinata al previo parere del Garante per la protezione dei dati personali, così da assicurare la coerenza dell'attuazione nazionale con le specifiche prescrizioni del Regolamento in materia di tutela dei dati e garanzie procedurali.

[25] L'art. 1, par. 3, della Direttiva 2014/41/UE prevede che «L'emissione di un OEI può essere richiesta da una persona sottoposta ad indagini o da un imputato, ovvero da un avvocato che agisce per conto di questi ultimi, nel quadro dei diritti della difesa applicabili conformemente al diritto e alla procedura penale nazionale».
[26] Legge 13 giugno 2025, n. 91. Delega al Governo per il recepimento delle direttive europee e l'attuazione di altri atti dell'Unione europea, in *G.U.* n.145 del 25 giugno 2025.

Il comma 2 dell'art. 19 della legge in questione stabilisce che, nell'esercizio della delega, il Governo debba attenersi non solo ai criteri generali di cui all'art. 32 della l. n. 234 del 2012[27], ma anche a una serie di principi e criteri direttivi specifici.
Tra questi, figurano: l'individuazione delle autorità competenti e delle procedure per l'emissione, la convalida e la trasmissione degli ordini europei di produzione e conservazione; il coordinamento delle norme interne con le previsioni del Regolamento, in modo da consentire agli organi di polizia giudiziaria di emettere ordini europei di produzione in situazioni di urgenza; la previsione che il Ministero della giustizia sia l'autorità responsabile della trasmissione amministrativa dei certificati relativi agli ordini di produzione e di conservazione; la disposizione secondo cui, per finalità di coordinamento investigativo, copia dei certificati debba essere trasmessa al Procuratore nazionale antimafia e antiterrorismo quando riferita ai reati previsti dagli artt. 51, commi 3-*bis* e 3-*quater*, e 371-*bis*, comma 4-*bis*, c.p.p., nonché al Procuratore generale presso la Corte d'appello per i procedimenti di cui all'art. 118-*bis* delle disposizioni di attuazione del codice di procedura penale; l'individuazione delle autorità giudiziarie competenti a ricevere le notifiche nell'ambito della procedura speciale di cui all'articolo 8 del Regolamento (UE) 2023/1543; le modalità di informazione della persona interessata dai dati richiesti (...); l'introduzione di sanzioni amministrative efficaci, proporzionate e dissuasive in caso di inosservanza degli obblighi; la definizione delle procedure e delle autorità competenti per l'irrogazione delle sanzioni e la previsione di un ricorso giurisdizionale effettivo per i destinatari delle stesse; l'individuazione delle autorità competenti per l'esecuzione degli ordini, conformemente all'articolo 16 del Regolamento; l'identificazione delle autorità giudiziarie e delle procedure per il riesame delle obiezioni motivate sollevate dai destinatari degli ordini, ai sensi dell'art. 17 del Regolamento (UE) 2023/1543; la previsione di mezzi di impugnazione effettivi a tutela della persona i cui dati siano oggetto di richiesta; l'adozione delle misure necessarie per assicurare la piena operatività del sistema informatico nazionale deputato allo scambio dei certificati e la creazione dei punti di accesso al sistema informatico decentrato europeo, con l'implementazione di adeguati

[27] Legge 24 dicembre 2012, n. 234, Norme generali sulla partecipazione dell'Italia alla formazione e all'attuazione della normativa e delle politiche dell'Unione europea, in *G.U.* n.3 del 4 gennaio 2024. Maggiori informazioni in https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:legge:2012;234~art32.

standard di sicurezza nel trattamento dei dati personali; la determinazione delle lingue dell'Unione europea ammesse per la trasmissione degli ordini; l'obbligo per le autorità competenti di trasmettere periodicamente i dati di monitoraggio al Ministero della giustizia per la loro elaborazione statistica; nonché l'adozione di ogni ulteriore intervento normativo necessario per armonizzare l'ordinamento nazionale con le previsioni del Regolamento europeo.
Il co. 3 dell'art. 19 ha poi fissato un termine più breve, pari a quattro mesi, per l'esercizio della delega limitatamente ad alcuni profili considerati essenziali, quali, in particolare: l'individuazione delle autorità competenti e delle procedure relative all'emissione, convalida e trasmissione degli ordini europei di produzione e conservazione; la designazione delle autorità giudiziarie competenti a ricevere le notifiche nell'ambito della procedura speciale di notifica; l'identificazione delle autorità competenti per l'esecuzione degli ordini, in conformità all'art. 16 del Regolamento; la definizione delle autorità giudiziarie e delle procedure per il riesame delle obiezioni dei destinatari degli ordini, ai sensi dell'art. 17 nonché la specificazione delle lingue dell'Unione accettate ai fini della trasmissione degli ordini.

3. 1. Il decreto legislativo italiano: le autorità competenti

Per dare attuazione alla delega in questa parte, è stato approvato il d.lgs. 30 dicembre 2015, n. 125[28], volto appunto a individuare, anzitutto, le autorità competenti ad emettere gli ordini: profilo, questo, particolarmente delicato, come emerge anche dalle questioni che si sono poste rispetto a strumenti quali il mandato d'arresto e l'ordine di indagine europeo. Il decreto ha poi identificato l'autorità amministrativa centrale nel Ministero della Giustizia (art. 5).

[28] Il decreto relativo alla "individuazione elle autorità competenti di cui all'articolo 31 del regolamento (UE) d 2023/1543 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", è in attesa di pubblicazione in *Gazz. Uff*. Lo stesso giorno è stato approvato il d.lgs. n. 216, di "attuazione della direttiva (UE) 2023/1544, recante norme armonizzate sulla designazione di stabilimenti designati e sulla nomina di rappresentanti legali ai fini dell'acquisizione di prove elettroniche nei procedimenti penali".

Nello specifico, l'art. 2 prevede che, nell'ambito di un procedimento penale – contesto esclusivo di applicazione del Regolamento – quando ricorrono le condizioni di emissione, il pubblico ministero e il giudice che procede possano emettere, nell'ambito delle rispettive attribuzioni, un ordine europeo di produzione di prove elettroniche (comma 1). Questo è emesso dal giudice competente a pronunciarsi nel merito su richiesta del pubblico ministero, formulata anche su istanza della persona offesa o del suo difensore, ovvero su richiesta della persona sottoposta alle indagini, dell'imputato, delle parti private o dei rispettivi difensori (comma 2). Il testo sembra escludere, come già avvenuto in sede di implementazione della direttiva sull'OEI[29], un potere diretto in capo alla difesa, la quale dovrà "canalizzare" la propria richiesta verso il giudice competente; annovera invece la persona offesa tra i soggetti legittimati, così compiendo un evidente passo in avanti rispetto alla disciplina sull'OEI.
Prima dell'esercizio dell'azione penale, provvedono, rispettivamente, in relazione alla natura più o meno "invasiva" dei dati da acquisire, il giudice per le indagini preliminari, se l'ordine riguarda i dati sul traffico e quelli relativi al contenuto, e il pubblico ministero, se l'ordine riguarda dati meno invasivi come quelli relativi agli abbonati e i dati richiesti al solo scopo di identificare l'utente (comma 3)[30]. Tuttavia, nel corso delle indagini preliminari, quando ricorre un caso di "emergenza"[31], prima dell'intervento del pubblico ministero l'ordine – purché finalizzato ad ottenere i soli dati relativi all'abbonato – può essere emesso dagli ufficiali di polizia giudiziaria, i quali, entro quarantotto ore, lo trasmettono al pubblico

[29] Cfr. d.lgs. 21 giugno 2017, n. 108. Sul tema P. SPAGNOLO, *Il procedimento di emissione dell'OEI*, in *L'ordine europeo di indagine penale. Il nuovo volto della raccolta transnazionale delle prove nel d.lgs. n. 108 del 2017*, a cura di M. DANIELE - R. E. KOSTORIS, Torino, 2018, p. 86 ss.
[30] V. considerando n. 36 del Regolamento: «Nel rispetto del diritto a un equo processo, garantito nella Carta dei diritti fondamentali dell'Unione europea e nella Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali, i pubblici ministeri esercitano le loro responsabilità in modo obiettivo, prendendo le loro decisioni circa l'emissione o la convalida di un ordine europeo di produzione o di un ordine europeo di conservazione unicamente sulla base degli elementi fattuali contenuti nel fascicolo e tenendo conto di tutti gli elementi a carico e a discarico».
[31] Secondo l'art. 3, numero 18 del Regolamento, per «caso di emergenza» si intende «una situazione in cui sussiste una minaccia imminente per la vita, l'integrità fisica o la sicurezza di una persona, o per un'infrastruttura critica, quale definita all'articolo 2, lettera a), della direttiva 2008/114/CE, il cui danneggiamento o la cui distruzione comporterebbe una minaccia imminente per la vita, l'integrità fisica o la sicurezza di una persona, anche attraverso un grave danno alla fornitura di beni essenziali alla popolazione o all'esercizio delle funzioni fondamentali dello Stato».

ministero presso il giudice competente. Seguendo le ben note scansioni codicistiche, entro le quarantotto ore successive, il pubblico ministero deciderà sulla convalida con decreto motivato: nel provvedimento in questione occorrerà evidentemente dare atto sia delle condizioni di emissione dell'ordine, sia della sussistenza delle ragioni di urgenza. Se la convalida non intervenga nel termine stabilito, l'ordine è revocato. Del relativo provvedimento è data immediata comunicazione al destinatario e i dati eventualmente acquisiti sono cancellati e, comunque, ne è vietata ogni forma di documentazione e utilizzazione (comma 4).

Come già avviene in materia di ordine europeo di indagine 32, quando l'ordine europeo di produzione sia emesso in relazione ai delitti di cui agli artt. 51, commi 3-*bis* e 3-*quater*, e 371-*bis*, comma 4-*bis*, c.p.p. copia del certificato è trasmessa, ai fini del coordinamento investigativo, al procuratore nazionale antimafia e antiterrorismo; in aggiunta, se si tratta di delitti di cui all'art. 118-*bis* disp. att. c.p.p., occorre informare il procuratore generale presso la corte d'appello (comma 5).

L'autorità giudiziaria che ha emesso l'ordine europeo di produzione provvede nei casi e nei modi previsti dalla legge processuale a dare conoscenza alle parti e ai loro difensori dei dati e della documentazione acquisiti (comma 6). Su tale profilo, vi è evidentemente un richiamo alla disciplina codicistica relativa alla *discovery* degli atti compiuti durante la fase investigativa. Sarebbe forse stato più opportuno definire con precisione le tempistiche e gli avvisi in ordine ai meccanismi di accesso a dati contrassegnati, come detto, da una facile alterabilità, nonché a eventuali richieste di cancellazione degli stessi, compatibilmente con le esigenze di riservatezza delle indagini.

La norma prevede infine, in maniera opportuna, la sanzione dell'inutilizzabilità per i dati acquisiti con un ordine europeo di produzione emesso fuori dai casi o in mancanza delle condizioni previste sia dal regolamento sia dal presente provvedimento (comma 7); nessun dubbio che anche il principio di proporzionalità venga in gioco ai fini di questa valutazione.

Quanto all'ordine di conservazione, ai sensi dell'art. 3 del testo, questo è emesso dal giudice competente a pronunciarsi nel merito su richiesta del pubblico ministero, formulata anche in questo caso su istanza della persona

[32] L'art. 27, comma 2, del d.lgs. 21 giugno 2017, n. 108, recante attuazione della Direttiva 2014/41/UE, relativa all'ordine europeo di indagine penale, prevede l'informativa al procuratore nazionale antimafia e antiterrorismo; v., anche, art. 727, comma 8, c.p.p., relativo alla trasmissione della richiesta di rogatoria all'estero.

offesa o del suo difensore, ovvero su richiesta della persona sottoposta alle indagini, dell'imputato, delle parti private o dei rispettivi difensori. Prima dell'esercizio dell'azione penale, vi provvede il solo pubblico ministero (comma 2) e, nei casi di "urgenza", l'ordine può essere emesso da ufficiali di polizia giudiziaria, i quali, entro quarantotto ore, lo trasmettono al pubblico ministero presso il giudice competente, affinché decida sulla convalida con decreto motivato. La sequenza è quella prima indicata: revoca dell'ordine a fronte della mancanza di convalida nel termine stabilito e immediata comunicazione al destinatario (comma 3). Anche in questa ipotesi, se si sta procedendo per delitti di "criminalità organizzata", copia del certificato di ordine europeo di conservazione (EPOC-PR) di prove elettroniche è trasmessa, ai fini del coordinamento investigativo, rispettivamente al procuratore nazionale antimafia e antiterrorismo e al procuratore generale presso la corte d'appello (comma 4).
L'art. 4 disciplina una procedura "accelerata" a fronte di ragioni di urgenza. Con riguardo all'ordine di produzione per ottenere i dati sul traffico e i dati relativi al contenuto, questo può essere emesso dal pubblico ministero, ma l'efficacia sarà subordinata alla previa convalida del giudice per le indagini preliminari al quale l'ordine è trasmesso entro ventiquattro ore dall'emissione. Se la convalida ha esito positivo, sarà il giudice stesso a trasmettere il certificato di ordine europeo di produzione (EPOC) di prove elettroniche; mentre, l'ordine di produzione per ottenere i dati relativi agli abbonati e quelli richiesti al solo scopo di identificare l'utente può essere emesso da ufficiali di polizia giudiziaria. Anche in questa evenienza, l'efficacia è subordinata alla previa convalida del pubblico ministero.
Nei medesimi casi prima individuati, l'ordine europeo di conservazione può essere emesso da ufficiali di polizia giudiziaria, con efficacia subordinata alla previa convalida del pubblico ministero presso il giudice competente al quale l'ordine è trasmesso entro ventiquattro ore dall'emissione. Se la convalida ha esito positivo, il pubblico ministero trasmetterà il certificato di ordine europeo di conservazione.
L'art. 6 del d.lgs. si occupa delle autorità e delle procedure di esecuzione. La norma, collocandosi in linea con altri strumenti di cooperazione[33], individua quale organo preposto all'esecuzione il procuratore della Repubblica presso il tribunale del capoluogo del distretto nel quale non già

[33] L'art. 4, comma 1, del d.lgs. n. 108 del 2017, individua quale organo chiamato al riconoscimento di un ordine europeo di indagine penale il procuratore della Repubblica presso il tribunale del capoluogo del distretto nel quale devono essere compiuti gli atti richiesti. Allo stesso modo l'art. 724, comma 1, c.p.p., in tema di rogatorie dall'estero.

devono compiersi gli atti, ma si trova lo stabilimento designato o il rappresentante legale nominato ai sensi della direttiva (UE) 2023/154418, destinatari dell'ordine, sono stabiliti o risiedono e il giudice per le indagini preliminari presso il medesimo tribunale. Lo stesso procuratore della Repubblica sarà l'autorità competente ai fini della notifica dell'emissione di un ordine europeo di produzione per l'ottenimento di dati sul traffico o dati relativi al contenuto, nonché ai fini indicati dagli articoli 10 (esecuzione dell'EPOC), 11 (esecuzione dell'EPOC-PR), 12 (motivi di rifiuto degli ordini europei di produzione) e 17 (procedura di riesame in caso di obblighi contrastanti) del medesimo Regolamento, fermo restando quanto previsto dai commi 4, 5 e 6 (comma 2).
Nei casi di notifica, il procuratore della Repubblica informerà, in relazione alla tipologia di reati, il procuratore nazionale antimafia e antiterrorismo o il procuratore generale presso la corte di appello.
Viene altresì previsto che, quando l'autorità di emissione di un altro Stato membro richieda l'esecuzione di un ordine europeo di produzione o di un ordine europeo di conservazione, il procuratore della Repubblica, salvo che sussista un motivo di rifiuto, provveda con decreto motivato al riconoscimento dell'ordine. Se ritiene che il riconoscimento debba essere effettuato da altro ufficio, trasmette immediatamente gli atti all'ufficio del pubblico ministero presso il giudice competente, dandone comunicazione all'autorità di emissione; in caso di contrasto si applicano le disposizioni di cui agli artt. 54, 54 *bis* e 54 *ter* c.p.p. (comma 4) [34].
Se la richiesta di esecuzione riguarda un ordine europeo di produzione per ottenere i dati relativi agli abbonati o i dati richiesti al solo scopo di identificare l'utente o un ordine europeo di conservazione, il procuratore della Repubblica, effettuato il riconoscimento ai sensi del comma 4, dispone l'esecuzione dell'ordine con decreto motivato (comma 5). Se invece la richiesta di esecuzione riguarda un ordine europeo di produzione emesso per ottenere i dati sul traffico o i dati relativi al contenuto, il procuratore della Repubblica, effettuato il riconoscimento ai sensi del comma 4, dovrà trasmettere la richiesta di esecuzione e la documentazione allegata, unitamente al decreto di riconoscimento, al giudice per le indagini preliminari, che prima di autorizzare l'esecuzione dovrà accertare le condizioni per il riconoscimento dell'ordine di produzione (comma 6). Nulla però stabilisce il testo in relazione al procedimento da seguire davanti

[34] Allo stesso modo nel caso di ordine di indagine europeo: art. 4, comma 6, d.lgs. n. 108 del 2017.

all'organo giurisdizionale. Sulla falsariga di quanto previsto sul versante nazionale per l'OEI[35], si potrebbe immaginare il richiamo al disposto di cui all'art. 127 c.p.p. che, comunque, offre la garanzia del contraddittorio.
La norma dispone, infine, che, fermo restando quanto previsto dall'art. 16 (procedura di esecuzione) del Regolamento, il compimento degli atti necessari all'esecuzione è regolato dalla legge italiana (comma 7).
L'art. 7 attribuisce la competenza a pronunciarsi sulla richiesta di riesame dell'ordine di produzione emesso o convalidato dal giudice al tribunale del riesame che ha sede nel capoluogo della provincia in cui si trova l'ufficio che ha emesso il provvedimento (art. 324, comma 5, c.p.p.); se invece "l'obiezione" (termine improprio) motivata riguardi un ordine di produzione adottato dal pubblico ministero, la competenza è del giudice per le indagini preliminari.
L'art. 9 si occupa di raccordare i nuovi strumenti con il testo dell'art. 132, relativo alla "conservazione di dati di traffico per altre finalità", del d.lgs. 30 giugno 2003, n. 196, c.d. codice della privacy. Anzitutto, si estende alle ricerche del latitante, la possibilità di acquisire dati di traffico da parte del pubblico ministero. Sono poi inseriti dei nuovi commi: il comma 3.*bis*.1, prevede che il pubblico ministero possa ordinare con decreto motivato ai fornitori e agli operatori di servizi telefonici, informatici o telematici, di conservare e proteggere, secondo le modalità indicate e per un periodo non superiore a novanta giorni, i dati relativi al traffico telefonico e telematico, esclusi comunque i contenuti delle comunicazioni, nonché i dati relativi alle chiamate senza risposta. Il provvedimento, prorogabile, per motivate esigenze, per una durata complessiva non superiore a sei mesi, può prevedere particolari modalità di custodia dei dati e l'eventuale indisponibilità dei dati stessi da parte dei fornitori e degli operatori di servizi telefonici, informatici o telematici ovvero di terzi; inoltre il comma 3.*bis*.2 esclude l'acquisizione dei dati relativi agli abbonati[36] dall'applicazione delle disposizioni di cui ai succitati commi 3 e 3-*bis*.

[35] V. art. 5, comma 3, d.lgs. n. 108 del 2017.
[36] Per dati relativi agli abbonati si intendono i dati detenuti da un prestatore di servizi relativi all'abbonamento ai suoi servizi, riguardanti: a) l'identità di un abbonato o di un cliente, come il nome, la data di nascita, l'indirizzo postale o geografico, i dati di fatturazione e pagamento, il numero di telefono o l'indirizzo email forniti; b) il tipo di servizio e la sua durata, compresi i dati tecnici e i dati che identificano le misure tecniche correlate o le interfacce usate dall'abbonato o dal cliente o a questo fornite al momento della registrazione o dell'attivazione iniziale e i dati connessi alla convalida dell'uso del servizio, ad esclusione di password o altri mezzi di autenticazione usati al posto di una password, forniti dall'utente o creati a sua richiesta.

Il nuovo comma 3.*bis*.3 dispone che all'acquisizione dei dati relativi agli abbonati provveda il pubblico ministero ovvero la polizia giudiziaria, di propria iniziativa o a seguito di delega del pubblico ministero; il comma 4-*ter*, estende l'oggetto della conservazione ai dati del traffico telefonico e alle chiamate senza risposta e legittima gli ufficiali di polizia giudiziaria alla relativa emissione; con il comma 4-*quater*, si includono tra i destinatari dell'ordine gli operatori di servizi telefonici.
È da evidenziare che il testo normativo introduce un nuovo art. 263-*bis* nel codice di procedura penale, recante la disciplina dell'ordine di conservazione di dati indirizzato a fornitori di servizi "nazionali". Nel corso delle indagini preliminari il pubblico ministero può ordinare, con decreto motivato, ai fornitori e agli operatori di servizi informatici, telematici o di telecomunicazioni, di conservare e proteggere, secondo le modalità indicate e per un periodo non superiore a novanta giorni, i dati da questi detenuti. Il provvedimento, prorogabile, per motivate esigenze, per una durata complessiva non superiore a sei mesi, può prevedere particolari modalità di custodia dei dati e l'eventuale indisponibilità dei dati stessi da parte dei fornitori e degli operatori di servizi informatici, telematici o di telecomunicazioni ovvero di terzi. Si prevede altresì che, quando ricorrono ragioni di urgenza, prima dell'intervento del pubblico ministero, l'ordine di conservazione sia emesso da ufficiali di polizia giudiziaria e sia comunicato per iscritto, senza ritardo e comunque entro quarantotto ore dalla notifica al destinatario, al pubblico ministero del luogo di esecuzione il quale, se ne ricorrono i presupposti, li convalida entro le successive quarantotto ore. In caso di mancata convalida, i provvedimenti assunti perdono efficacia.
Qualche perplessità, del tutto condivisibile, è stata espressa dal Garante per la protezione dei dati[37] riguardo a questa nuova disposizione nella parte in cui non precisa quali siano le tipologie di dati personali oggetto dell'ordine adottato dal pubblico ministero: in linea con il testo europeo, l'ordine dovrebbe essere limitato ai dati che hanno minore incidenza sui diritti dell'indagato.
Il d.lgs. sin qui appena tratteggiato è soltanto un primo passo per adattare il sistema processuale italiano al nuovo strumento di acquisizione delle prove digitali; altri ne dovranno seguire per affrontare profili oltremodo delicati, come quelli attinenti al sistema di garanzie a favore delle persone

[37] Garante per la protezione dei dati personali, provvedimento n. 569, 25 settembre 2025, p. 6. Nello specifico, si pone l'attenzione sull'esigenza di una maggiore determinatezza della norma, per evitare dubbi interpretativi e possibili contestazioni sulla legittimità dell'ordine stesso.

sottoposte a indagini, nonché alle misure da adottare per garantire elevati standard di sicurezza nell'acquisizione dei dati[38].
Come è stato evidenziato[39], il sistema informatico di accesso nazionale, attraverso il quale, in conformità all'art. 25 del Regolamento, deve avvenire lo scambio di dati, deve rispettare «rigorosi requisiti di sicurezza che vanno ben oltre gli standard generici della *cybersecurity*. Tutte le comunicazioni devono essere cifrate utilizzando algoritmi crittografici conformi agli standard dell'ENISA e alle raccomandazioni dell'Agenzia per la Cybersicurezza Nazionale. La gestione delle chiavi crittografiche deve seguire *best practice* consolidate: utilizzo di *Hardware Security Module* per la custodia delle chiavi private, rotazione periodica delle chiavi, segregazione rigorosa dei ruoli tra chi genera, chi custodisce e chi autorizza l'uso delle chiavi». Su questo punto non sono ammesse "disattenzioni".

4. La prospettiva spagnola

A la fecha, salvo error por mi parte y más allá lógicamente de la existencia de cierta regulación sectorial en la materia objeto de adaptación de anteriores Directivas[40], España carece de cualquier normativa en aplicación del Reglamento (UE) 2023/1543 del Parlamento Europeo y del Consejo, de 12 de julio de 2023, sobre las órdenes europeas de producción y las órdenes europeas de conservación a efectos de prueba electrónica en procesos penales y de ejecución de penas privativas de libertad a raíz de procesos penales[41]. Tampoco y aquí con más motivo, se encuentra a la fecha legislación en adaptación de Directiva (UE) 2023/1543 del Parlamento Europeo y del Consejo de 12 de julio de 2023 sobre las órdenes europeas de producción y las órdenes europeas de conservación a efectos de prueba electrónica en procesos penales y de ejecución de penas privativas de

[38] R. DI PIETRA, *Il Regolamento UE sulla* E-Evidence in *Sicurezza e Giustizia*, (2025).
[39] *L'Italia e la* e-evidence: *architettura tecnico giuridica del nuovo ecosistema investigativo transfrontaliero*, in *ICT Security*, (2025).
[40] A modo de ejemplo aquí y ahora Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones, Boletín Oficial del Estado (BOE) n. 251 del 19-10-2007. V. R. LÓPEZ JIMÉNEZ, *El nuevo marco jurídico transfronterizo de las pruebas electrónicas. Las órdenes de entrega y conservación de las pruebas electrónicas*, en *Revista General de Derecho Europeo*, 49 (2019), pp. 307-340, pp. 312 y ss.
[41] Por todos, aquí y ahora, recientemente y entre la literatura española, Á. TINOCO PASTRANA, *Las órdenes de producción y de conservación de prueba electrónica transfronteriza en los procesos penales en la Unión Europea,* cit., pp. 130-158. Otra literatura ya es citada en nota a pie de página n. 3 de este mismo trabajo.

libertad a raíz de procesos penales, la cual complementa el paquete europeo en materia de *e-evidence*[42] o prueba electrónica. Tipología de prueba que como tal prueba o investigación tecnológica es volátil y así "fácilmente manipulable y vulnerable, además de intangible"[43]. Cierto es que la legislación nacional no es necesaria en el primer caso puesto que se trata de un Reglamento y así, recuérdese, acto jurídico de la Unión de "alcance general… obligatorio en todos sus elementos y directamente aplicable en cada Estado miembro" conforme la redacción otorgada por el artículo 288 del Tratado de Funcionamiento de la Unión europea (en adelante TFUE)"[44]. No obstante, aun reconociendo la improcedencia de la adaptación en sede estatal parece siquiera recomendable alguna indicación a este respecto en los distintos Estados miembros. Existe además cierta práctica legislativa al respecto y así España muestra algún ejemplo en este sentido; es así el caso concreto de la Ley Orgánica 9/2021, de 1 de julio, de aplicación del Reglamento (UE) 2017/1939 del Consejo, de 12 de octubre

[42] Desde España y en el marco del proceso penal español recientemente F. ALDAY LÓPEZ-CABELLO, *Tratamiento procesal de las pruebas electrónicas en el proceso penal español,* Madrid, 2025, pp. 127-130; I. GONZÁLEZ PULIDO, *Perspectivas de futuro respecto a la obtención de pruebas electrónicas transfronterizas y a la cooperación con proveedores de servicios: investigación y prueba de los ciberdelitos graves en la Unión*, en *Diario La Ley*, 10266 (2023).

[43] C. GÓMEZ FRÖDE, *La prueba electrónica. Problemas del presente y retos del futuro. El uso de recursos tecnológicos y electrónicos durante la tramitación de procesos jurisdiccionales, en AA.VV. La prueba en el proceso. Evidence in the process. II Conferencia Internacional & XXVI Jornadas Iberoamericanas de Derecho Procesal,* Barcelona, 2018, pp. 367-390, p. 371. Así también, sobre concepto y caracteres de la prueba electrónica y/o tecnológica R. MIGUEL BARRIO, *La prueba tecnológica en el proceso laboral: tendencias y desafíos*, Madrid, 2023, pp. 32 y ss. A todos los efectos aquí y ahora se procede a identificar sendas rúbricas de prueba electrónica y tecnológica.

[44] Sobre las características del Reglamento como fuente de Derecho de la Unión Europea y entonces Comunitario, ya a la fecha, F.J. FONSECA MORILLO, *Reglamento,* en P. BIGLINO CAMPOS, ed., *Diccionario de términos comunitarios,* Madrid, 1997, pp. 382-388; más recientemente J.L. MARTINEZ LÓPEZ-MUÑIZ, *Derecho Comunitario básico de la Unión Europea,* Madrid, 2024, pp. 348-351 en relación con la característica de aplicabilidad inmediata. En relación expresa sobre el uso del Reglamento en este caso en lugar de la acostumbrada Decisión Marco o ahora Directiva empleada desde Bruselas para la regulación de la cooperación judicial en materia penal véase R. M. GERACI, *La circolazione transfrontaliera delle prove digitali in UE: la proposta di regolamento e-evidence*, in *Cass. Pen.,* 59(3) (2019), pp. 1340-1362, pp. 1355 y ss; así también en España M. DE HOYOS SANCHO, *Reflexiones acerca de la Propuesta de Reglamento UE sobre las órdenes europeas de entrega y conservación de pruebas electrónicas a efectos de enjuiciamiento penal, en Revista General de Derecho Procesal*, 58 (2022), pp. 8 y ss.

de 2017, por el que se establece una cooperación reforzada para la creación de la Fiscalía Europea[45].

Ya entonces se advirtió desde la academia la necesidad de incardinar la investigación llevada a cabo por la Fiscalía Europea en el seno del proceso penal nacional y por ello la conveniencia de que cada Estado miembro procediera, en cierta medida y con carácter general, pese a la incorrección aquí del término y trámite, a la "adaptación" (*implementation*) de dicha norma reglamentaria en el respectivo sistema legal[46]. Sería aquí también el caso, por cuanto la ahora regulada prueba electrónica (*e-evidence*) y así, en concreto, el artículo 2.1 del citado Reglamento (UE) 2023/1543 relativo a su ámbito de aplicación, dispone textualmente que "una orden europea de producción o una orden europea de conservación *sólo* podrán emitirse *en el marco y a efectos de procesos penales*" (cursiva es personal) además de los fines de ejecución de pena privativa de libertad o medida de seguridad privativa de libertad con las condiciones allí contempladas.

En consecuencia, la emisión de cualesquiera órdenes de este tipo en solicitud, bien de entrega (orden europea de producción, EPO en inglés) o bien de conservación (orden europea de conservación, EPOC en inglés), en ambos casos de pruebas electrónicas[47], necesitará siempre la pendencia de un proceso penal en la jurisdicción estatal de un Estado miembro; de este modo su emisión podrá tener lugar igualmente, bien en fase de investigación o bien de enjuiciamiento. En la práctica judicial ordinaria el dictado de las mismas tendrá lugar en mayor medida durante la fase de investigación o instrucción siendo éste el supuesto más común por analogía con su "hermana" la orden europea de investigación u OEI[48] de la cual se

---

[45] BOE n. 157 del 2-7-2021. V. S. GUERRERO PALOMARES, ed., *Tratado sobre la Fiscalía Europea y el procedimiento penal especial de la L.O. 9/2021, de 1 de julio,* 3ª ed., Navarra, 2023.

[46] V. M. ENGELHART, *Compliance with EPPO Regulation. Study results on the 'implementation' of Council Regulation (EU) 2017/1939 in the Member States*, in EUCRIM, 1 (2024), pp. 54-58, p. 54; B. VIDAL FERNÁNDEZ, *La actuación de la Fiscalía Europea en el proceso penal español regulada en la LO 9/2021*, in *Revista de Derecho y Proceso Penal,* 66 (2022), pp. 139-173, p. 141.

[47] V. definiciones proporcionadas en ambos casos en arts. 3.1 y 2 Reglamento (UE) 2023/1543. En relación con el objeto y ámbito de aplicación del Reglamento véase M. DE HOYOS SANCHO, *La nueva regulación en la Unión Europea sobre obtención transfronteriza de información electrónica en procesos penales*, cit., pp. 27 y ss.

[48] Directiva 2014/41/CE del Parlamento Europeo y del Consejo, de 3 de abril de 2014, relativa a la orden europea de investigación en materia penal, DOUE n. L 130 del 1-5-2014; V. M. JIMENO BULNES, *Orden europea de investigación en materia penal*, en M. JIMENO BULNES, ed., *Aproximación legislativa versus reconocimiento mutuo en el*

desprende su origen, resultando no en vano ser esta última su antecedente más inmediato. Sin embargo y aun contemplando la OEI también como medida de investigación el acceso a la prueba electrónica, la norma regulatoria en cuestión carece de previsión de disposiciones específicas al respecto considerándose las mismas necesarias dada la singularidad de esta tipología probatoria, todo lo cual justifica el dictado del nuevo acto jurídico por parte de la Unión Europea[49].

Recuérdese además que, a la fecha y aún vaticinada su supresión en los sucesivos intentos de promulgación de nueva legislación procesal penal[50], en España dicha investigación o instrucción es aún de naturaleza judicial a cargo de los Juzgados de Instrucción o ahora Secciones de Instrucción de los Tribunales de Instancia a raíz de la reforma recientemente operada por

desarrollo del espacio judicial europeo: una perspectiva multidisciplinar, Barcelona, 2016, pp. 151-218 así como *La prueba transfronteriza y su incorporación al proceso penal español*, en M.I. GONZÁLEZ CANO (ed.), *Orden europea de investigación y prueba transfronteriza en la Unión Europea*, Valencia, 2019, pp. 719-766 por lo que atañe a su aplicación en España; S. CACCIATORE, *La orden europea de investigación desde una perspectiva comparada y forense*, Valencia, 2025, abordando precisamente perspectivas italiana y española además de la europea.

[49] V. L. GÓMEZ AMIGO, *Prueba penal electrónica en la Unión Europea: las futuras órdenes europeas de entrega y conservación*, en M.I. GONZÁLEZ CANO (ed.), *Orden europea de investigación y prueba transfronteriza en la Unión Europea*, cit., pp. 155-167, p. 156 y *Nuevas perspectivas para la obtención transfronteriza de prueba electrónica en la Unión Europea,* en *Diario La Ley,* 9340 (2019), p. 2 así como *Estudio de las órdenes europeas de producción y conservación: un instrumento eficaz para la obtención transfronteriza de pruebas penales electrónicas*, en *Revista Española de Derecho Europeo*, 92 (2024), pp. 43-91, p. 47; en la misma línea C. CUADRADO SALINAS, *La efectividad de las pruebas penales obtenidas en el marco de la futura normativa europea relativa a la obtención y conservación de pruebas electrónicas*, en *Revista General de Derecho Procesal,* 55 (2021), pp. 7 y ss., Á. TINOCO PASTRANA, *Las órdenes europeas de entrega y conservación: la futura obtención transnacional de la prueba electrónica en los procesos* penales en la Unión Europea, cit., p. 205. Sobre la complementariedad entre ambas, OEI y EPOC, S. TOSZA, *All evidence is equal, but electronic evidence is more equal than any other: the relationship between the European Investigation Order and the European Production Order*, *in New Journal of European Criminal Law*, 11(2) (2020), pp. 161-183 así como *Mutual recognition by private actors in criminal justice? E-evidence regulation and service providers as the new guardians of fundamental rights,* en *Common Market Law Review,* 61(1) (2024), pp. 139-166, pp. 144 y ss; E. LARO GONZÁLEZ, *El Reglamento e-evidence: instrument adicional a la Orden europea de investigación,* en *La Ley Probática,* 3, (2021).

[50] Así Anteproyecto de Ley de Enjuiciamiento Criminal de 2011 y Borrador de Código Procesal Penal de 2013 estando a la espera del resultado del Anteproyecto de Ley de Enjuiciamiento Criminal de 2020, aprobado precisamente por el gobierno español el 28 pasado de octubre de 2025 según información oficial disponible en enlace *https://www.mjusticia.gob.es/es/institucional/gabinete-comunicacion/noticias-ministerio/proyecto-lec*. V. F. JIMÉNEZ CONDE y O. FUENTES SORIANO (eds.), *Reflexiones en torno al Anteproyecto de Ley de enjuiciamiento Criminal de 2020,* Valencia, 2022.

Ley Orgánica 1/2025, de 2 de enero, de medidas en materia de eficiencia del Servicio Público de Justicia[51]. No en vano continúa aún vigente hoy día en España la vetusta Ley de Enjuiciamiento Criminal aprobada por Real Decreto de 14 de septiembre de 1882[52], sucesivamente reformada y parcheada pues, como lógicamente es de imaginar, para nada preveía en su origen cualesquiera tipos de investigación y/o prueba electrónica entre otras muchas ausencias.

En concreto, ha de esperarse a la reforma practicada por la Ley Orgánica 13/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológicas[53] para que en España se ponga de manifiesto "la insuficiencia de un cuadro normativo concebido para tiempos bien distintos" ante el surgimiento de "renovadas formas de delincuencia ligadas al uso de las nuevas tecnologías" conforme reza el propio Preámbulo de la citada norma[54]. De este modo tiene lugar importante reforma de varios preceptos en materia de diligencias de investigación, si bien la principal novedad a este respecto lo constituye la

[51] BOE n. 3 del 3-1-2025, en modificación de la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial y Ley de Enjuiciamiento Criminal, entre muchas otras. Véase al respecto el dossier elaborado por el propio Ministerio de Justicia*, La justicia llega al siglo XXI,* disponible en página web oficial *https://www.mjusticia.gob.es/es/servicio-justicia/nuevo-modelo-organizativo-justicia*. Así también, en relación con la constitución del nuevo modelo organizativo en sede judicial, J.L. DEAÑO RODRIGUEZ, *Ley Orgánica 1/2025: los Tribunales de Instancia,* en *El notario del siglo XXI*, 122 (2025), pp. 55-59, J. DE LAMO RUBIO - E. CAVERO CARRACEDO, *Los Tribunales de Instancia: ¿eficiencia organizativa en justicia?,* en *Práctica de Tribunales: Revista de Derecho Procesal Civil y Mercantil,* 169 (2024).

[52] Gaceta de Madrid n. 260 del 17-9-1882. V. L. BACHMAIER WINTER, *The handling of digital evidence in Spain*, en M. CAIANELLO - A. CAMON, eds., *Digital forensic evidence. Towards common European standards in antifraud administrative and criminal investigations*, Milano, 2021, pp. 165-205, pp. 169 y ss.

[53] BOE n. 239, del 6-10-2015. Por todos, M. DÍAZ MARTINEZ - I. LÓPEZ-BARAJAS PEREA, eds., *La nueva reforma procesal penal. Derechos fundamentales e innovaciones tecnológicas,* Valencia, 2018; F. ALDAY LÓPEZ-CABELLO, *Tratamiento procesal de las pruebas electrónicas en el proceso penal español,* Madrid, 2025.

[54] Aptdo. IV. Entre la bibliografía, R. GARCIMARTÍN MONTERO, *Los medios de investigación tecnológicos en el proceso penal,* Navarra, 2018, pp. 17 y ss. en alusión al "carácter obsoleto de la LECrim; así también F. BUENO DE MATA, *Las diligencias de investigación penal en la cuarta revolución industrial. Principios teóricos y problemas prácticos,* Navarra, 2019, pp. 21 y ss, afirmando que el verdadero origen de la reforma estriba en la jurisprudencia constitucional española y europea del Tribunal Europeo de Derechos Humanos.

introducción de diversos capítulos relativos a la interceptación de comunicaciones electrónicas así como el uso de dispositivos electrónicos y/o informáticos a los fines de la investigación penal en términos generales[55]. La misma regulación parece pretende mantenerse en el hoy todavía discutido Anteproyecto de Ley de Enjuiciamiento Criminal de fecha de 24 de noviembre de 2020, si bien al menos es de esperar mejore la técnica legislativa ofreciendo una regulación más sistemática de la que hoy se contempla[56]. Con todo, en la academia española hay quien considera que la actual regulación de la prueba electrónica en España es aún insuficiente[57], aun cuando a tenor de lo dicho, no parece que la futura pretenda aportar grandes novedades en este sentido, más allá de la proclamada sistematización en su caso.

---

[55]Libro II: Del sumario, Título VIII: De las medidas de investigación limitativas de los derechos reconocidos en el artículo 18 de la Constitución, Capítulo IV: Disposiciones comunes a la interceptación de las comunicaciones telefónicas y telemáticas, la captación y grabación de comunicaciones orales mediante la utilización de dispositivos electrónicos, la utilización de dispositivos técnicos de seguimiento, localización y captación de la imagen, el registro de dispositivos de almacenamiento masivo de información y los registros remotos sobre equipos informáticos (arts. 588 bis a - 588 bis k); Capítulo V: La interceptación de las comunicaciones telefónicas y telemáticas (arts. 588 ter a – 588 ter m); Capítulo VI: Captación y grabación de comunicaciones orales mediante la utilización de dispositivos electrónicos (arts. 588 quater a – 588 quater e); Capítulo VII: Utilización de dispositivos técnicos de captación de la imagen, de seguimiento y de localización (arts. 588 quinquies a – 588 quinquies c); Capítulo VIII: Registro de dispositivos de almacenamiento masivo de información (arts. 588 sexies a – 588 sexies c); Capítulo IX: Registros remotos sobre equipos informáticos (arts. 588 septies a – 588 septies c); Capítulo X: Medidas de aseguramiento (art. 588 octies).

[56] Textualmente se indica en la Exposición de Motivos a este respecto que "la normativa introducida en 2015 es respetada y reproducida en lo esencial, sin perjuicio, no obstante, de introducir en el texto articulado algunas mejoras puntuales de orden técnico o de realizar ciertas alteraciones sistemáticas en beneficio de una mayor coherencia del conjunto" (Aptdo. XLI, 2º párrafo). En concreto su previsión se contempla en el Libro III: De las diligencias de investigación, Título II: Los medios de investigación relativos a la interceptación de las telecomunicaciones y de las conversaciones privadas; Título III: Observaciones y vigilancias físicas y utilización de dispositivos de seguimiento, localización y captación de la imagen; Título IV: Los medios de investigación relativos a la entrada y registro, intervención de libros, papeles y documentos y registros informáticos. V. I. LÓPEZ-BARAJAS PEREA, *Los medios de investigación relativos a la interceptación de las telecomunicaciones y de las conversaciones privadas en el Anteproyecto de LECrim de 2020: análisis crítico*, en *Revista de la Asociación de Profesores de Derecho Procesal de las Universidades Españolas*, 4 (2021), pp. 123-148, pp. 133 y ss.

[57] Cfr. M. E. LARO GONZÁLEZ, *Prueba electrónica: situación actual en el proceso penal y perspectivas de futuro,* en J. CONDE FUENTES - G. SERRANO HOYO, eds., *La justicia digital en España y la Unión Europea,* Barcelona, 2019, pp. 239-250, p. 246, afirmando que "la regulación en España de la prueba electrónica sigue siendo una imperiosa necesidad que aún está por llegar".

Finalmente conviene recordar que, si resulta aconsejable el dictado de normativa nacional para la aplicación del Reglamento (UE) 2023/1543, en el caso la Directiva (UE) 2023/1543 esta promulgación es además obligatoria al tratarse de una Directiva[58]. Aun cuando el plazo de transposición establecido para el próximo 18 de febrero de 2026 conforme su art. 7.1 aún no ha precluído a la fecha que se redactan estas líneas, el tiempo que resta parece ya exiguo para España que a la fecha carece de iniciativa legislativa en este sentido, más allá de la previsión hecha por el gobierno español en el Plan Anual Normativo de 2025 en el que se contempla una denominada *Ley de transposición de Directivas europeas y otras disposiciones para la adaptación de la legislación procesal y sustantiva al ordenamiento de la Unión Europea*[59]*;* en suma, dicho plan prevé no sólo la obligatoria adaptación de la Directiva sino también la preconizada "aplicación" del Reglamento (UE) 2023/1543. Tendrá que darse prisa en todo caso España a riesgo de la invocación del efecto directo de la directiva en cuestión ante los órganos jurisdiccionales españoles[60].

5. Sviluppi e limiti dell'attuale cooperazione giudiziaria

Il quadro che emerge dall'introduzione del Regolamento (UE) 2023/1543 e dalla parallela evoluzione degli ordinamenti nazionali evidenzia un momento di profonda trasformazione dell'assistenza giudiziaria in materia

---

[58] Norma obligatoria "en cuanto al resultado que deba conseguirse, dejando, sin embargo, a las autoridades nacionales la elección de la forma y los medios" según el anterior art. 288.III TFUE. Cfr. J.F. DUQUE DOMÍNGUEZ, *Directiva*, en P. BIGLINO, ed., *Diccionario de términos comunitario*s, cit., pp. 154-163.

[59] Ministerio de la Presidencia, Justicia y Relaciones con las Cortes*, Plan Anual Normativo 2025*, abril 2025, p. 93, disponible en el Portal de transparencia del gobierno de España, disponible en enlace *https://transparencia.gob.es/publicidad-activa/por-materias/normativa-otras-disposiciones/plan-anual*. Cabe añadir que la mesa de la Sección de Derecho Procesal que tuvo lugar en las últimas jornadas celebradas por la Comisión General de Codificación versaron precisamente sobre prueba electrónica sin que se añadiera nada a este respecto; así *II Jornadas de la Comisión General de Codificación. Inteligencia artificial y ordenamiento jurídico: su incidencia en la codificación. Resumen de las mesas,* Palacio de Parcent, 12 y 13 de diciembre de 2024, *Mesa Redonda 5. Sección de Derecho Procesal. La prueba electrónica*, pp. 24-28, documento disponible en enlace *https://www.mjusticia.gob.es/es/areas-actuacion/actividad-legislativa/comision-general-codificacion/noticias-interes/celebracion-ii-jornadas-comision-general-codificacion*.

[60] V. F. RASSU, *L'invocabilité des directives européennes et son incidence sur l'ordre juridique italien,* en *Revue de Droit de l'Union Européenne*, 4 (2017), pp. 167-193; P. PESCATORE, *The doctrine of "direct effect": an infant disease of Communiry Law,* en *European Law Review,* 2 (2015), pp. 135-153.

di prova elettronica. Il nuovo sistema europeo si propone di superare la frammentazione normativa, da un lato, e gli ostacoli strutturali derivanti dalla dimensione territoriale delle indagini nell'era digitale, dall'altro, costruendo un modello inedito fondato sul rapporto diretto tra autorità giudiziaria e prestatore di servizi. Questo passaggio rappresenta un'evoluzione necessaria rispetto ai meccanismi tradizionali di assistenza giudiziaria – lenti, se parametrati alla volatilità del dato informatico – ma, allo stesso tempo, porta nuove tensioni sul piano delle garanzie processuali e dell'equilibrio fra poteri pubblici e soggetti privati.

Nel confronto tra Italia e Spagna emergono traiettorie differenti. L'Italia si è avviata verso un adattamento tempestivo e strutturato: la legge di delegazione europea 2024 e il decreto legislativo approvato delineano la volontà di adattamento delle previsioni regolamentari, individuando autorità competenti, procedure, meccanismi di riesame e un sistema sanzionatorio coerente con gli obblighi europei. Si tratta di un approccio che, pur non esente da criticità – si pensi alla necessità di coordinare l'innovazione tecnologica con le garanzie difensive, alla perdurante assenza di standard forensi uniformi e all'urgenza di garantire un adeguato sistema informatico nazionale – mostra una volontà di integrazione normativa e operativa utile a evitare frizioni applicative.

Di contro, la Spagna si colloca in una fase di maggiore incertezza. L'assenza, allo stato attuale, di interventi legislativi specifici relativi, anzitutto, al Regolamento, può incidere sul funzionamento del nuovo meccanismo. Sebbene il testo sarà direttamente applicabile, la letteratura spagnola ha evidenziato la necessità – già sperimentata in occasione dell'istituzione della Procura europea – di predisporre norme di coordinamento che garantiscano l'inserimento delle nuove competenze investigative nel tessuto procedurale nazionale.

A ciò si aggiunge un ulteriore elemento di complessità: la disciplina spagnola del processo penale, ancora fondata sulla *Ley de Enjuiciamiento Criminal* del 1882 e su un modello di istruzione giudiziale, mostra una limitata capacità di recepire organicamente le esigenze derivanti dalla prova digitale, nonostante le riforme settoriali del 2015 e gli interventi più recenti in materia di investigazioni tecnologiche.

Il bilancio complessivo mostra, dunque, un'Europa che si muove verso una cooperazione giudiziaria più rapida, diretta e tecnologicamente adeguata, nella quale la reale efficacia del nuovo sistema dipenderà dalla capacità degli Stati membri di assicurare un dialogo coerente tra fonti europee e discipline interne. L'Italia sembra avviata verso un'integrazione

relativamente tempestiva, mentre la Spagna fronteggia un percorso più incerto, condizionato sia da ritardi legislativi sia da una struttura processuale meno flessibile rispetto alle esigenze dell'*e-evidence*.
Restano aperte alcune sfide comuni: la definizione di criteri tecnico-forensi condivisi, il rafforzamento delle garanzie difensive nella fase di acquisizione del dato digitale, la gestione dei conflitti tra diritti fondamentali e poteri investigativi, e la costruzione di infrastrutture informatiche sicure e interoperabili. In definitiva, lo sviluppo della cooperazione giudiziaria europea in materia di prova elettronica appare oggi segnato da un duplice movimento: da un lato, la progressiva uniformazione del quadro normativo sovranazionale; dall'altro, la persistente eterogeneità dei sistemi processuali nazionali, che richiede un costante lavoro di allineamento per evitare che l'innovazione si traduca in nuove asimmetrie e in potenziali deficit di tutela. Solo attraverso un equilibrio consapevole tra efficienza investigativa e diritti fondamentali il modello europeo potrà realizzare pienamente la propria ambizione di uno spazio giudiziario comune realmente efficace anche nell'ambiente digitale.

Abstract: In the frame of criminal proceedings, a significant role is currently played by digital evidence. At the European level, in order to facilitate the gathering of this type of evidence, Regulation (EU) 2023/1543 on European Production Orders and European Preservation Orders for electronic evidence has been adopted. Although the Regulation is directly applicable within national legal systems, in Italy a first Legislative Decree has been approved to adapt the domestic legal framework; by contrast, no such initiative has been undertaken in Spain. This contribution aims to analyse the impact that the Regulation may have in Italy and Spain, with particular regard to the rights of the person under investigation.

Key words: Electronic evidence – E-evidence Regulation – judicial cooperation – fundamental rights.