

L'Italia e le E-Evidence: architettura tecnico- giuridica del nuovo ecosistema investigativo transfrontaliero



Quando si parla di acquisizione transfrontaliera di prove digitali nei procedimenti penali, ci troviamo di fronte a una delle sfide più complesse che il diritto processuale penale europeo abbia mai affrontato. Non si tratta semplicemente di armonizzare procedure: stiamo ridisegnando il rapporto tra sovranità nazionale, tutela dei diritti fondamentali e necessità investigative in un ecosistema digitale dove i dati non rispettano confini geografici e i *provider* di servizi possono trovarsi a migliaia di chilometri dalla giurisdizione richiedente.

Gli schemi di decreto legislativo attualmente all'esame delle Commissioni parlamentari italiane – l'Atto del Governo n. 303 e l'Atto del Governo n. 330 – rappresentano il tentativo italiano di dare attuazione a questo nuovo paradigma normativo. Ma al di là della mera trasposizione tecnica delle norme europee, questi provvedimenti sollevano questioni che toccano il cuore stesso della *digital forensics*, della cooperazione investigativa e della tutela dei diritti nella società dell'informazione.

Dal sistema tradizionale alla rivoluzione E-Evidence: un cambio

di paradigma

Per comprendere appieno la portata innovativa del pacchetto E-Evidence, è necessario inquadrarlo nel più ampio sistema di cooperazione internazionale in materia di *cybercrime*. La Convenzione di Budapest del 2001 ha rappresentato per oltre vent'anni il principale strumento di cooperazione, introducendo meccanismi di assistenza giudiziaria reciproca specificamente pensati per i reati informatici.

Il Secondo Protocollo Addizionale alla Convenzione, adottato dal Comitato dei Ministri del Consiglio d'Europa il 17 novembre 2021 e aperto alla firma il 12 maggio 2022, ha tentato di modernizzare questi strumenti, introducendo procedure accelerate e contatti diretti tra autorità. Tuttavia, anche questi aggiornamenti non hanno risolto il problema strutturale che affligge l'investigazione digitale transfrontaliera: i tempi della cooperazione giudiziaria tradizionale, spesso nell'ordine di mesi, collidono frontalmente con la volatilità delle prove elettroniche, che possono essere cancellate in pochi secondi o automaticamente sovrascritte da *retention policies* aggressive.

L'Ordine Europeo di Indagine, introdotto dalla Direttiva 2014/41/UE e recepito in Italia con il decreto legislativo 21 giugno 2017, n. 108, ha semplificato le procedure tra Stati membri dell'UE sostituendo il sistema delle rogatorie con uno strumento più agile basato sul principio del riconoscimento reciproco. Eppure, anche l'OEI mantiene il modello della cooperazione «verticale» attraverso le autorità giudiziarie dello Stato di esecuzione, con i conseguenti tempi di tramitazione che, per quanto ridotti rispetto alle rogatorie tradizionali, rimangono incompatibili con l'urgenza di molte investigazioni digitali.

Il Regolamento UE 2023/1543 e la Direttiva UE 2023/1544, pubblicati nella Gazzetta Ufficiale dell'Unione Europea il 28

luglio 2023, rappresentano un salto paradigmatico che alcuni studiosi hanno definito «post-westfaliano» perché mette in discussione il principio tradizionale della territorialità della giurisdizione penale. Per la prima volta, viene introdotta la cooperazione «orizzontale», permettendo alle autorità giudiziarie di rivolgersi direttamente ai prestatori di servizi stabiliti in altri Stati membri, bypassando il necessario coinvolgimento preventivo dell'autorità giudiziaria dello Stato di esecuzione. Questa innovazione solleva interrogativi profondi sul bilanciamento tra efficienza investigativa e tutela dei diritti fondamentali, tra necessità di rapidità e garanzie processuali, tra cooperazione europea e sovranità nazionale.

L'architettura del sistema italiano: autorità, procedure e governance

La decisione del Consiglio dei Ministri dell'8 ottobre 2025 ha designato il Ministero della Giustizia quale autorità centrale per la gestione del sistema E-Evidence sul territorio nazionale, ma l'architettura operativa che emerge dalla bozza dell'Atto del Governo n. 303 è significativamente più complessa e stratificata. Il primo nodo da sciogliere riguarda l'individuazione delle autorità di emissione competenti, una questione che il regolamento europeo affronta attraverso una graduazione basata sulla tipologia e sull'invasività dei dati richiesti.

La tassonomia dei dati e le implicazioni per le autorità competenti

Quando parliamo di prove digitali, la distinzione tra le diverse categorie di dati non è meramente accademica ma ha profonde implicazioni forensi, probatorie e, soprattutto, in

termini di tutela dei diritti fondamentali. I dati relativi agli abbonati, quelli che il regolamento definisce come *subscriber data*, comprendono le informazioni fornite dall'utente al momento della registrazione del servizio: nome, cognome, *alias* o *username*, indirizzo email, numero di telefono, indirizzo postale, data di nascita, informazioni di pagamento come le ultime quattro cifre della carta di credito o l'IBAN, data di creazione dell'account e stato dello stesso.

Questi dati, considerati relativamente poco invasivi perché già condivisi volontariamente dall'utente con il *provider*, possono essere richiesti tramite un ordine emesso o convalidato da un pubblico ministero. Il loro valore investigativo risiede principalmente nell'identificazione del soggetto e nella possibilità di correlare identità digitali multiple che una stessa persona può utilizzare su piattaforme diverse.

I dati di accesso, o *access data*, rappresentano un salto qualitativo in termini di invasività. Si tratta delle informazioni tecniche relative alle connessioni: indirizzo IP di connessione, *timestamp* precisi di *login* e *logout*, *user agent* che rivela il *browser* e il sistema operativo utilizzato, eventuale geolocalizzazione se disponibile, tipo di dispositivo, identificativi di sessione.

Questi dati, generati automaticamente dai sistemi al momento dell'accesso, permettono di ricostruire la *timeline* di attività dell'utente, di determinare la sua geolocalizzazione approssimativa attraverso l'analisi degli indirizzi IP e di identificare i dispositivi specifici utilizzati. Dal punto di vista forense, sono particolarmente preziosi ma anche estremamente volatili, spesso conservati per periodi limitati in base alle *data retention policies* dei *provider*. Anche per questi dati, il regolamento consente che l'autorità di emissione sia il pubblico ministero.

La situazione si complica quando entriamo nel territorio dei

dati relativi alle operazioni, i *transactional data* che la giurisprudenza della Corte di Giustizia dell'Unione Europea considera altamente invasivi anche se non includono il contenuto effettivo delle comunicazioni. Nel caso delle email, si tratta degli *header* completi che rivelano mittente, destinatari in chiaro, in copia e in copia nascosta, l'oggetto del messaggio, i *timestamp* precisi e il *route* seguito dal messaggio attraverso i server. Per le chiamate VoIP, comprendono i numeri del chiamante e del chiamato, la durata della conversazione e i *timestamp*.

Per i servizi di messaggistica, si tratta dell'elenco delle comunicazioni con tutti i metadati ma senza il contenuto dei messaggi. Questi dati permettono di mappare le reti di contatti, di identificare possibili complici, di ricostruire *pattern* comunicativi che possono essere rivelatori quanto il contenuto stesso delle comunicazioni. La Corte di Giustizia, nelle celebri sentenze *Digital Rights Ireland* e *Tele2 Sverige*, ha equiparato l'accesso massivo a questi dati a una forma di sorveglianza che può rivelare informazioni intime sulla vita privata delle persone. Per questo motivo, il regolamento richiede garanzie più elevate.

Infine, i *content data* rappresentano il livello massimo di invasività: 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*. Si tratta del contenuto effettivo delle comunicazioni private, che richiede le tutele più stringenti. Per questi dati, il regolamento impone che l'autorità di emissione sia un giudice, un tribunale o un giudice istruttore, escludendo esplicitamente la competenza del pubblico ministero.

Il decreto italiano deve mappare con precisione chirurgica le autorità nazionali su questo schema europeo, e qui emergono le peculiarità del nostro ordinamento processuale penale. Il pubblico ministero italiano è magistrato inquirente ma non

organo giurisdizionale, una distinzione che diventa cruciale soprattutto per i dati relativi alle operazioni e ai contenuti, dove la giurisprudenza europea ha stabilito standard elevati di tutela che richiedono un controllo genuinamente giurisdizionale. Il riferimento naturale per i dati più invasivi sarebbe al giudice per le indagini preliminari, ma il decreto dovrà chiarire se in fase dibattimentale la competenza passi al giudice del dibattimento o rimanga comunque al GIP.

Il caso delle emergenze e la questione della polizia giudiziaria

L'articolo 7 del regolamento prevede che, in casi di urgenza debitamente accertati, gli ordini europei di produzione possano essere emessi da «qualsiasi altra autorità competente» purché seguiti da convalida giudiziaria entro ventiquattro ore. La formulazione è volutamente ampia per consentire agli Stati membri di adattarla ai propri ordinamenti, ma solleva questioni delicate quando si tratta di attribuire questo potere alla polizia giudiziaria. La legge di delegazione europea 2024 prevede che il Governo coordini le disposizioni nazionali per consentire agli organi di polizia giudiziaria di emettere ordini europei di produzione in casi di emergenza.

Questa previsione rappresenta un'innovazione significativa nel nostro sistema processuale, dove la polizia giudiziaria opera tradizionalmente sotto la direzione e il controllo del pubblico ministero ai sensi dell'articolo 109 della Costituzione e degli articoli 347-348 del codice di procedura penale. Un EPOC emesso autonomamente dalla polizia giudiziaria, anche con successiva convalida, configura uno spazio di autonomia operativa che necessita di essere circoscritto con parametri rigorosi.

Il decreto dovrà probabilmente limitare questa facoltà a situazioni di reale necessità e urgenza: pericolo imminente di

perdita irreparabile delle prove, situazioni di pericolo di vita, indagini su atti di terrorismo o criminalità organizzata transnazionale dove ogni ora può essere decisiva. La convalida giudiziaria entro ventiquattro ore dovrà essere effettiva e non meramente formale, con l'obbligo per l'autorità giudiziaria di verificare non solo i presupposti sostanziali dell'ordine ma anche la sussistenza delle condizioni di urgenza che hanno giustificato l'emissione da parte della polizia giudiziaria.

Il coordinamento con la Direzione Nazionale Antimafia: un tassello cruciale

Un aspetto che potrebbe apparire marginale a una lettura superficiale, ma che rivela la sua importanza strategica nell'ottica del coordinamento investigativo nazionale, è l'obbligo di trasmettere copia dei certificati EPOC ed EPOC-PR al Procuratore Nazionale Antimafia quando si riferiscono a procedimenti per i delitti indicati all'articolo 51, comma 3-*bis* e 3-*quater* del codice di procedura penale. Si tratta dei delitti di criminalità organizzata, terrorismo, criminalità transnazionale, traffico di stupefacenti, armi ed esseri umani.

La *ratio* di questa previsione, inserita nella legge di delegazione, risponde a logiche di coordinamento investigativo fondamentali nel contrasto alla criminalità organizzata: la Direzione Nazionale Antimafia deve avere contezza in tempo reale delle indagini transfrontaliere che potrebbero interconnettersi con altre investigazioni in corso su organizzazioni criminali, permettendo di individuare collegamenti, di evitare sovrapposizioni o conflitti tra procedimenti, di coordinare strategie investigative complesse che coinvolgono più procure.

Dal punto di vista tecnico, questo significa che il sistema informatico decentrato dovrà prevedere meccanismi

automatizzati di *routing* delle comunicazioni verso la DNA, con adeguate misure di sicurezza e tracciabilità. La sfida tecnica è garantire che questa trasmissione avvenga in tempo reale o *near-real-time*, senza creare colli di bottiglia procedurali che rallenterebbero l'intero meccanismo.

Il sistema informatico decentrato: l'infrastruttura critica invisibile

L'articolo 25 del Regolamento 2023/1543 prevede l'istituzione di un sistema informatico decentrato per la comunicazione sicura e lo scambio di dati tra le autorità competenti e i prestatori di servizi. La terminologia tecnica e burocratica rischia di oscurare la portata di questa infrastruttura: non si tratta di un semplice sistema di messaggistica ma dell'infrastruttura critica su cui poggia l'intero meccanismo E-Evidence. Senza un sistema affidabile, sicuro e interoperabile, anche le norme più sofisticate rimangono lettera morta.

L'architettura del sistema si basa su un modello decentrato dove ogni Stato membro mantiene il proprio punto di accesso nazionale, interconnesso con gli altri punti di accesso attraverso una rete sicura. Questa scelta architettonica, preferita rispetto a un sistema centralizzato, risponde a multiple esigenze: sovranità nazionale, perché ogni Stato mantiene il controllo sul proprio nodo e sui dati che transitano; resilienza, perché il fallimento di un nodo non compromette l'intero sistema; scalabilità, perché nuovi Stati membri possono essere aggiunti senza riprogettare l'architettura complessiva. Il modello ricorda quello adottato per e-CODEX, il sistema utilizzato per lo scambio di informazioni giudiziarie in ambito civile, che ha dimostrato nel corso degli anni una buona tenuta operativa.

Il decreto italiano deve garantire che il punto di accesso nazionale rispetti 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. L'autenticazione degli operatori deve basarsi su meccanismi multi-fattore, con certificati digitali rilasciati e gestiti secondo gli standard eIDAS che garantiscono l'identità digitale certificata degli operatori.

Un aspetto cruciale per la *digital forensics* è la tracciabilità completa di ogni operazione sul sistema. Ogni emissione, ricezione, modifica, accesso ai dati deve essere tracciata in *log* immutabili con *timestamp* certificato. Questa tracciabilità non risponde solo a esigenze di sicurezza informatica ma è fondamentale per garantire la *chain of custody* digitale delle prove: in un eventuale processo, deve essere possibile ricostruire esattamente chi ha avuto accesso a quali dati, quando, da quale terminale, con quale autorizzazione. I *log* devono essere protetti contro manomissioni attraverso tecniche di firma digitale o *blockchain*, e conservati per periodi congrui che permettano verifiche *ex post*.

La segregazione dei dati sensibili contenuti negli EPOC e nelle risposte deve essere implementata attraverso controlli di accesso granulari basati su *Role-Based Access Control*. Non basta un semplice sistema di permessi: ogni operatore deve avere accesso esclusivamente ai procedimenti per i quali è specificamente autorizzato, con meccanismi automatici che impediscano accessi non autorizzati anche accidentali. Il sistema deve inoltre garantire *availability* del 99,9%, il che significa al massimo circa otto ore di *downtime* all'anno.

Considerando che gli EPOC in emergenza devono essere eseguiti entro otto ore, anche poche ore di interruzione del sistema potrebbero tradursi nella perdita di prove critiche. Questo richiede sistemi ridondanti, *backup* geograficamente distribuiti, procedure di *disaster recovery* testate periodicamente attraverso simulazioni realistiche.

L'intero sistema deve essere progettato secondo i principi di *privacy by design* e *privacy by default*, con una *Data Protection Impact Assessment* obbligatoria che coinvolga attivamente il Garante per la protezione dei dati personali. Ma c'è un ulteriore livello di complessità: il punto di accesso nazionale non può essere un sistema isolato.

Deve interfacciarsi con il sistema OEI nazionale per garantire coordinamento e complementarietà tra i due strumenti, evitando che gli investigatori si trovino a dover scegliere tra procedure diverse senza criteri chiari. Deve dialogare con il Sistema Informativo della Cognizione Penale per la gestione dei procedimenti penali, con i sistemi Eurojust e della rete giudiziaria europea per lo scambio di informazioni complementari, con il portale europeo e-Justice per l'accesso alle informazioni pubbliche sul sistema.

Il rischio concreto è creare l'ennesimo sistema a sé stante, un'isola tecnologica che richiede *login* separati, interfacce diverse, flussi di lavoro ridondanti. L'integrazione con i sistemi esistenti è cruciale non solo per l'efficienza operativa ma anche per garantire che gli strumenti vengano effettivamente utilizzati dagli operatori sul campo. La legge di delegazione impone al Governo di provvedere all'adozione delle misure necessarie a garantire la piena funzionalità del sistema informatico nazionale, il che significa investimenti significativi non solo in *hardware* e *software* ma anche in formazione degli operatori. La *governance* del sistema dovrà coinvolgere Ministero della Giustizia, Agenzia per la Cybersicurezza Nazionale, AGID, con ruoli e responsabilità chiaramente definiti e meccanismi di coordinamento efficaci.

Procedure di riesame e tutela dei diritti: il difficile equilibrio

Uno degli aspetti più delicati del sistema E-Evidence, che solleva le maggiori perplessità tra i garantisti e gli esperti di diritti fondamentali, riguarda i meccanismi di riesame e tutela dei diritti. Il modello «orizzontale» che bypassa l'autorità giudiziaria dello Stato di esecuzione rischia di indebolire le garanzie processuali se non viene adeguatamente bilanciato attraverso altri meccanismi di controllo. Il regolamento cerca questo equilibrio attraverso un sistema articolato di obiezioni, notifiche e ricorsi, ma l'efficacia concreta dipenderà dalle scelte implementative degli Stati membri.

L'articolo 14 del regolamento prevede che i prestatori di servizi possano sollevare obiezioni motivate all'esecuzione di un EPOC in diverse circostanze: quando l'ordine non è stato emesso o convalidato da un'autorità competente secondo il regolamento; quando l'ordine è manifestamente al di fuori dell'ambito di applicazione del regolamento, ad esempio perché richiede dati per finalità non penali; quando l'ordine viola manifestamente la Carta dei diritti fondamentali dell'UE o è manifestamente arbitrario; quando esistono conflitti con obblighi previsti dalla legislazione di paesi terzi dove i dati sono fisicamente conservati.

Quest'ultimo caso è particolarmente delicato: se un *provider* americano conserva dati su server negli Stati Uniti e riceve un EPOC che richiede quei dati, potrebbe trovarsi in conflitto tra gli obblighi europei e le disposizioni del CLOUD Act americano.

Il decreto italiano deve individuare l'autorità giudiziaria competente per il riesame di queste obiezioni ai sensi dell'articolo 17 del regolamento. La scelta più logica appare essere il Tribunale del Riesame, già competente per questioni

analoghe in ambito interno relative al sequestro e all'acquisizione di prove, ma il decreto potrebbe anche prevedere un giudice specializzato considerata la complessità tecnico-giuridica delle questioni. Un giudice chiamato a valutare un'obiezione basata su un conflitto con la legislazione di un paese terzo deve avere competenze che vanno oltre il tradizionale diritto processuale penale: deve comprendere i principi di diritto internazionale privato, le questioni di giurisdizione extraterritoriale, gli aspetti tecnici di localizzazione dei dati in architetture *cloud* distribuite.

Parallelamente, l'articolo 15 del regolamento impone che la persona i cui dati sono stati richiesti sia informata della richiesta, salvo quando la notifica possa compromettere l'indagine. Il decreto deve definire con precisione le tempistiche per la notifica quando non differita, il contenuto dell'informativa specificando quali elementi devono essere comunicati, i meccanismi di ricorso effettivo dinanzi alle autorità giudiziarie dello Stato di emissione, le procedure per l'accesso, la rettifica e la cancellazione dei dati compatibilmente con le esigenze investigative.

Questo diritto all'informazione è fondamentale perché permette alla persona interessata di attivarsi per la tutela dei propri diritti, ma al contempo può compromettere l'efficacia dell'indagine se esercitato prematuramente. Il bilanciamento tra questi interessi confliggenti richiede criteri oggettivi e verificabili, non rimessi alla mera discrezionalità dell'autorità inquirente.

Un ultimo livello di garanzia è rappresentato dal sistema di notifica agli Stati membri previsto per i dati più invasivi. Per i dati relativi alle operazioni e ai contenuti, salvo casi specifici dove è evidente che il reato è stato commesso nel paese di emissione o la persona interessata risiede in quel territorio, lo Stato di emissione deve notificare l'EP0C allo Stato di esecuzione dove si trova lo stabilimento designato o

il rappresentante legale del *provider*.

Lo Stato di esecuzione ha dieci giorni per sollevare eventuali motivi di rifiuto: immunità o privilegi secondo il proprio diritto, rischio per la sicurezza nazionale o per altri interessi essenziali, *ne bis in idem* se la persona è già stata giudicata per gli stessi fatti, conflitto con principi fondamentali del proprio ordinamento costituzionale. Questo meccanismo rappresenta un residuo di cooperazione «verticale» all'interno del modello orizzontale, una valvola di sicurezza per proteggere gli interessi fondamentali degli Stati membri. Il decreto italiano deve definire quale autorità nazionale gestisce queste notifiche in arrivo e valuta l'eventuale sollevazione di motivi di rifiuto, con procedure rapide che non vanifichino l'obiettivo di celerità del sistema ma che garantiscano al contempo una valutazione seria e approfondita.

L'obbligo di rappresentanza: ridisegnare la presenza dei *provider* nell'UE

La Direttiva UE 2023/1544, che l'Atto del Governo 330 deve recepire entro il 18 febbraio 2026, introduce un obbligo che può apparire tecnico ma che ha implicazioni profonde sul modo in cui i *provider* globali operano nel mercato europeo. I prestatori di servizi che offrono servizi nell'Unione Europea, anche se non fisicamente stabiliti sul territorio, devono designare uno «stabilimento designato» o nominare un «rappresentante legale» in almeno uno Stato membro dell'UE. Questa previsione ribalta il principio tradizionale per cui un'impresa non stabilita in un territorio non è soggetta alla giurisdizione di quel territorio: qui si impone un obbligo di presenza, sia pure attraverso un rappresentante, come condizione per operare nel mercato europeo.

Il perimetro applicativo della direttiva è ampio. Rientrano nell'obbligo i fornitori di reti e servizi di comunicazione elettronica, dai tradizionali operatori telefonici ai *provider*

di servizi internet, dai servizi VoIP come Skype o WhatsApp ai servizi di messaggistica istantanea. Sono inclusi i prestatori di servizi della società dell'informazione: *social media* come Facebook, Twitter, Instagram; piattaforme di *video-sharing* come YouTube o TikTok; servizi di *cloud storage* come Dropbox, Google Drive, OneDrive; *provider* di email come Gmail o Outlook.com; piattaforme e-commerce come Amazon o eBay. Infine, ricadono nell'obbligo i prestatori di servizi finanziari: banche *online*, servizi di pagamento elettronico come PayPal o Stripe, piattaforme di *trading*, servizi di *wallet* digitale per criptovalute.

Le esclusioni sono significative e rispondono a logiche di proporzionalità. Sono esentate le micro-imprese con meno di dieci dipendenti e fatturato annuo inferiore a due milioni di euro, una soglia che esclude le *startup* in fase iniziale e i piccoli progetti ma che non offre riparo ai *player* consolidati.

Sono esclusi i prestatori puramente nazionali che offrono servizi esclusivamente all'interno di un singolo Stato membro, anche se la verifica di questo requisito può essere complessa nell'era di internet dove anche un servizio pensato per un mercato locale può essere tecnicamente accessibile da qualsiasi parte del mondo. Infine, sono esclusi i servizi dove la conservazione dei dati è puramente accessoria rispetto all'attività principale, come nel caso di professionisti quali avvocati, architetti, ingegneri o contabili che forniscono servizi *online* ma la cui attività principale non è digitale.

La sfida per il decreto italiano sarà applicare queste categorie a modelli di *business* ibridi o innovativi che non rientrano facilmente nelle classificazioni tradizionali. Un *influencer* con milioni di *follower* che monetizza contenuti attraverso una piattaforma proprietaria è un prestatore di servizi della società dell'informazione? Un'applicazione di *dating* con funzionalità di messaggistica integrata rientra nell'obbligo perché offre un servizio di comunicazione

elettronica? Una piattaforma di *gaming online* con chat tra giocatori deve nominare un rappresentante legale? Il decreto dovrà fornire criteri interpretativi chiari, possibilmente attraverso esempi concreti o una casistica di riferimento, per evitare incertezze che potrebbero tradursi in contenziosi.

Rappresentante legale vs stabilimento designato: una scelta strategica

La direttiva lascia ai prestatori la scelta tra due modalità di adempimento dell'obbligo. Lo stabilimento designato è un'entità del *provider* già presente nell'UE – una filiale, una succursale, un ufficio – che viene formalmente designata come punto di contatto per ricevere e dare seguito agli ordini europei. Questa opzione presenta vantaggi in termini di integrazione con la struttura aziendale esistente e di accesso diretto ai sistemi e alle banche dati del *provider*, ma presuppone che il *provider* abbia già una presenza fisica significativa nell'UE, il che non è scontato per molti *player* extra-europei.

L'alternativa è la nomina di un rappresentante legale, una persona fisica o giuridica distinta dal *provider* che viene incaricata di fungere da interfaccia. Può essere un grande studio legale specializzato in diritto digitale e cooperazione giudiziaria internazionale, un *service provider* dedicato che offre servizi di rappresentanza legale per conto di multipli clienti, un consulente esterno con le competenze necessarie. Questa opzione offre flessibilità ed è particolarmente adatta per *provider* extra-UE senza presenza fisica, ma solleva interrogativi sulla reale capacità del rappresentante di dare seguito agli ordini se non ha accesso diretto ai sistemi del *provider*.

Ed è proprio qui che la direttiva introduce una previsione cruciale: l'articolo 3, paragrafo 4, impone che il rappresentante legale o lo stabilimento designato abbiano «i

poteri e le risorse necessari per ottemperare» agli ordini europei. Non si tratta quindi di una semplice nomina formale, di una casella postale o di un *front office* che inoltra le richieste alla casa madre. Il rappresentante deve avere accesso tecnico effettivo ai sistemi del *provider* per recuperare i dati richiesti, il che implica accordi contrattuali dettagliati, interfacce tecniche sicure, credenziali di accesso privilegiate.

Deve disporre di competenza tecnico-legale, con personale esperto sia in *digital forensics* e *data management* che in diritto processuale penale e *data protection*. Deve avere capacità operativa H24/7 per gestire le richieste di emergenza che richiedono risposta entro otto ore, il che significa turni continui, reperibilità costante, processi organizzativi rodati e testati. Deve avere risorse finanziarie adeguate per sostenere i costi operativi non trascurabili di un sistema di questo tipo.

Il decreto italiano deve chiarire gli standard minimi richiesti per considerare adeguati i poteri e le risorse del rappresentante. Un rappresentante legale che dichiara formalmente di avere i poteri necessari ma che nella pratica non riesce ad accedere ai dati o che impiega settimane per ottenere risposte dalla casa madre rende l'intero meccanismo inefficace. Potrebbe essere opportuno prevedere un sistema di accreditamento o certificazione dei rappresentanti legali, con verifiche periodiche della loro effettiva capacità operativa. D'altra parte, standard troppo stringenti potrebbero scoraggiare i *provider* dall'offrire servizi nel mercato europeo o spingere verso soluzioni di *compliance* meramente formali.

Responsabilità solidale: un meccanismo controverso ma necessario

Uno degli aspetti più discussi della direttiva è la previsione

di responsabilità solidale tra il prestatore di servizi e il rappresentante legale o lo stabilimento designato per l'inottemperanza agli obblighi. L'articolo 3, paragrafo 5, stabilisce che entrambi possono essere ritenuti responsabili e che non può essere invocata «la mancanza di procedure interne adeguate» tra *provider* e rappresentante come giustificazione dell'inottemperanza. Questa previsione risponde a un'esigenza pratica comprensibile: evitare che *provider* e rappresentanti si «scarichino» reciprocamente la responsabilità, con il *provider* che sostiene di aver fornito tutti i dati al rappresentante e il rappresentante che afferma di non aver ricevuto collaborazione dal *provider*, mentre l'autorità inquirente rimane senza le prove necessarie.

Tuttavia, la responsabilità solidale solleva questioni complesse che il decreto italiano dovrà affrontare. Come si coordina questo meccanismo con i principi costituzionali di personalità della responsabilità penale e amministrativa? Se il rappresentante legale è uno studio legale esterno che ha adempiuto diligentemente ai propri obblighi contrattuali ma il *provider*, che ha sede in un paese extra-UE, si rifiuta di fornire i dati, è giusto sanzionare anche il rappresentante? Viceversa, se il *provider* ha fornito tempestivamente tutti i dati richiesti ma il rappresentante, per negligenza o incapacità organizzativa, non li trasmette all'autorità richiedente, il *provider* deve subire le conseguenze?

La soluzione probabilmente risiede in una graduazione della responsabilità basata sull'effettivo controllo sulla situazione e sulla possibilità concreta di adempiere. Il rappresentante legale dovrebbe rispondere pienamente quando l'inottemperanza dipende da inefficienze nella sua organizzazione o da sua negligenza, ma dovrebbe avere la possibilità di dimostrare di aver fatto tutto il possibile per ottenere i dati dal *provider*. Simmetricamente, il *provider* dovrebbe rispondere pienamente quando si rifiuta di collaborare con il proprio rappresentante o quando le

«procedure interne» sono volutamente farragginose per rendere difficile l'esecuzione degli ordini. La responsabilità dovrebbe essere effettivamente solidale solo quando entrambi hanno contribuito all'inottemperanza o quando non è possibile determinare dove risieda la responsabilità principale.

Il regime sanzionatorio disegnato dal regolamento 2023/1543 prevede sanzioni pecuniarie fino al due per cento del fatturato mondiale annuo totale dell'esercizio precedente per i *provider* che non rispettano gli ordini europei, mentre la direttiva 2023/1544 richiede sanzioni «effettive, proporzionate e dissuasive» per la violazione degli obblighi di designazione o nomina e per l'inottemperanza. Per comprendere la portata di queste cifre, si consideri che per un gigante tecnologico come Meta il due per cento del fatturato mondiale può significare oltre due miliardi di dollari. Si tratta di sanzioni potenzialmente devastanti, pensate per essere realmente deterrenti anche per i *player* globali che potrebbero essere tentati di ignorare le richieste europee.

Il decreto italiano deve definire diversi aspetti fondamentali di questo regime sanzionatorio. Innanzitutto, la natura delle sanzioni: saranno puramente amministrative o si configureranno reati in casi particolarmente gravi, ad esempio quando l'inottemperanza è dolosa e finalizzata a favorire attività criminali? In secondo luogo, l'autorità competente per l'irrogazione: il Garante per la protezione dei dati personali, che ha già esperienza con sanzioni significative in ambito GDPR? L'autorità giudiziaria che ha emesso l'EPOC non eseguito? Un'autorità amministrativa dedicata?

La graduazione delle sanzioni dovrà tenere conto della gravità della violazione, distinguendo tra ritardi nella risposta e rifiuti espliciti, tra prime violazioni e comportamenti reiterati, tra situazioni di impossibilità oggettiva debitamente documentata e mancanza di collaborazione. Dovranno essere previste circostanze attenuanti per situazioni di reale

impossibilità tecnica, per i casi di prima violazione quando seguita da immediata correzione, per i *provider* che dimostrano piena cooperazione anche se non riescono a fornire tutti i dati richiesti nei tempi previsti.

Infine, e questo è cruciale per la legittimità del sistema, devono essere garantiti il diritto di difesa e meccanismi di ricorso effettivo. Un *provider* sanzionato deve avere la possibilità di contestare la sanzione dinanzi a un giudice indipendente, di dimostrare l'impossibilità di esecuzione, di fornire elementi a propria discolta. Il rischio, altrimenti, è che sanzioni tanto elevate vengano considerate sproporzionate dalla giurisprudenza europea, rendendo l'intero sistema inefficace.

Impatto operativo: costi, opportunità e trasformazioni di mercato

L'implementazione del sistema E-Evidence comporta costi significativi per i prestatori di servizi che vanno ben oltre l'aspetto meramente finanziario, incidendo sull'organizzazione aziendale, sui processi operativi, sulle strategie di mercato. I costi di *setup* iniziale includono la nomina o designazione del rappresentante legale o stabilimento designato, con tutti gli adempimenti legali e contrattuali connessi. Occorre sviluppare interfacce tecniche con il sistema informatico decentrato, il che significa progetti di integrazione *software* complessi che devono garantire sicurezza, affidabilità e conformità agli standard europei.

I sistemi interni di *data retention* e *retrieval* devono essere adeguati per permettere l'estrazione rapida ed efficiente dei dati nelle categorie previste dal regolamento, con particolare attenzione alla capacità di rispettare i tempi stringenti di otto ore per le emergenze. Il personale deve essere formato non solo sugli aspetti tecnici ma anche su quelli giuridici, perché chi gestisce le richieste deve essere in grado di

comprendere le implicazioni legali di ogni categoria di dati e di valutare la legittimità formale degli ordini ricevuti.

I costi ricorrenti sono altrettanto rilevanti. Ogni richiesta richiede analisi legale per verificare la conformità formale dell'ordine, estrazione tecnica dei dati che può essere semplice per i *subscriber data* ma estremamente complessa per ricostruzioni di dati storici o per dati conservati in architetture distribuite, preparazione delle risposte in formati strutturati e sicuri. Il mantenimento della disponibilità H24/7 implica costi di personale significativi, con turni di reperibilità e procedure di escalation. Gli aggiornamenti tecnici e normativi sono continui in un settore in rapidissima evoluzione, e il sistema deve essere costantemente adeguato. Infine, le attività di *auditing* e *compliance* per dimostrare la conformità agli obblighi richiedono risorse dedicate.

Per i grandi *provider* questi costi sono sostenibili e probabilmente già parzialmente ammortizzati attraverso le strutture esistenti per gestire richieste di autorità nazionali attraverso canali tradizionali. Google, Meta, Microsoft, Amazon hanno già team dedicati alla *law enforcement compliance* con processi consolidati, anche se dovranno adeguarli alle specificità del sistema E-Evidence. Per *provider* medio-piccoli, invece, questi costi possono rappresentare una barriera significativa che potrebbe scoraggiarli dall'offrire servizi nel mercato europeo o spingerli verso modelli di *business* che eludono formalmente l'applicazione della direttiva. Il rischio concreto è un effetto di concentrazione di mercato, dove i *player* dominanti vengono ulteriormente rafforzati perché hanno le risorse per gestire la *compliance* mentre i concorrenti più piccoli vengono marginalizzati.

Questo scenario potrebbe però aprire opportunità di *business* interessanti. Si sta già sviluppando un mercato di «E-Evidence *Compliance as a Service*», con società specializzate che

offrono servizi di rappresentanza legale e gestione delle richieste per conto di multiple *provider*.

Il modello è simile a quello dei *Data Protection Officer as a Service* emerso con il GDPR: un *provider* specializzato che mette a disposizione le competenze, le infrastrutture, i processi necessari serve multiple clienti, distribuendo i costi fissi e rendendo la *compliance* accessibile anche a realtà più piccole.

Questo modello potrebbe abbassare significativamente le barriere all'ingresso, ma solleva questioni di qualità del servizio e di tutela dei dati, perché i *provider* delegano al fornitore esterno l'accesso a dati potenzialmente molto sensibili dei propri utenti.

***Digital forensics* transfrontaliera: l'anello critico della catena probatoria**

***Chain of custody* in ambiente transfrontaliero: preservare l'integrità attraverso i confini**

Quando parliamo di prove digitali acquisite attraverso un EPOC, uno degli aspetti più critici da un punto di vista forense è la preservazione della *chain of custody* attraverso passaggi multipli e giurisdizioni diverse. In ambito nazionale, la catena di custodia delle prove digitali segue protocolli consolidati: dal momento del sequestro o dell'acquisizione, ogni passaggio deve essere documentato, ogni persona che ha avuto accesso ai dati deve essere identificata, ogni operazione sui dati deve essere tracciata, ogni trasferimento deve essere accompagnato da verbali di consegna. Gli standard internazionali come l'ISO/IEC 27037

forniscono linee guida dettagliate per l'identificazione, la raccolta, l'acquisizione e la preservazione di prove digitali.

Il sistema E-Evidence introduce una complessità aggiuntiva perché la prova digitale attraversa confini giurisdizionali senza che l'autorità richiedente abbia controllo diretto sul processo di estrazione. I dati vengono estratti dai sistemi del *provider*, nello Stato di esecuzione, da personale del *provider* o del rappresentante legale che opera secondo procedure proprie, possibilmente diverse da quelle dello Stato richiedente. I dati vengono quindi trasmessi attraverso il sistema informatico decentrato, subendo processi di crittografia, trasferimento su reti, decrittografia. Infine, arrivano all'autorità richiedente che deve verificarne l'autenticità e l'integrità prima di utilizzarli nel procedimento.

Come garantire che in questo processo articolato le prove mantengano le caratteristiche di genuinità, autenticità e integrità richieste per la loro utilizzabilità processuale? La risposta risiede in una combinazione di misure tecniche e procedurali.

Dal punto di vista tecnico, l'utilizzo di funzioni di *hash* crittografiche come SHA-256 o SHA-3 permette di generare un'impronta digitale univoca dei dati al momento dell'estrazione. Questa impronta viene allegata ai dati trasmessi e l'autorità ricevente può ricalcolarla sui dati ricevuti: se le due impronte coincidono, è matematicamente certo che i dati non sono stati alterati durante la trasmissione. Il *timestamping* certificato, basato su servizi di *timestamping* qualificati ai sensi del regolamento eIDAS, permette di provare che i dati esistevano in una certa forma in un momento specifico, rendendo impossibile retrodatazioni o modifiche.

I *metadata* originali dei file devono essere preservati integralmente perché possono contenere informazioni forensi

cruciali: data e ora di creazione, data e ora di ultima modifica, autore del documento, versioni precedenti, dati EXIF per le immagini che includono informazioni sulla fotocamera e sulla geolocalizzazione. Il formato di trasmissione deve essere *forense-friendly*, preferibilmente formati aperti e documentati che permettano verifiche indipendenti. Le firme digitali apposte dal sistema informatico decentrato ad ogni passaggio creano una catena di autenticazione verificabile.

Dal punto di vista procedurale, è fondamentale che ogni attore della catena documenti dettagliatamente le proprie operazioni. Il *provider* o il rappresentante legale che estrae i dati deve generare un *report* tecnico che descriva: quali sistemi sono stati interrogati, quali *query* sono state eseguite, in quale formato sono stati estratti i dati, quali *hash* sono stati calcolati, chi ha effettuato materialmente l'estrazione, quando è avvenuta l'operazione. Il sistema informatico decentrato deve generare *log* completi che documentino ogni passaggio della trasmissione. L'autorità ricevente deve verificare formalmente l'integrità dei dati ricevuti ricalcolando gli *hash*, controllando le firme digitali, validando i *timestamp*, e deve documentare queste verifiche in un verbale che entrerà a far parte del fascicolo processuale.

La sfida è standardizzare queste procedure tra Stati membri con tradizioni processuali diverse. Un investigatore italiano deve poter fidarsi che i dati estratti da un *provider* secondo le procedure tedesche o francesi o svedesi rispettino standard forensi equivalenti a quelli italiani. Questo richiede un lavoro di armonizzazione che va oltre le norme giuridiche e coinvolge le *best practice* tecniche, la formazione degli operatori, la certificazione dei processi.

I tempi di risposta come variabile critica: tra efficienza e qualità

Il regolamento stabilisce tempi di risposta stringenti: dieci

giorni per un EPOC standard, riducibili a otto ore in caso di emergenza debitamente accertata. Questi tempi rappresentano un drammatico miglioramento rispetto ai mesi necessari per le rogatorie tradizionali o alle settimane dell'OEI, ma introducono tensioni con le esigenze di accuratezza e completezza proprie della *digital forensics*. Un'estrazione di dati frettolosa, eseguita sotto la pressione di una scadenza di otto ore, può comportare errori, omissioni, perdita di *metadata*, contaminazione di prove.

Le otto ore per le emergenze sono pensate per situazioni dove il pericolo di perdita delle prove è imminente: un sospetto di terrorismo che potrebbe rendersi conto di essere sotto investigazione e cancellare tutti i suoi *account*; una vittima di sequestro di persona dove le comunicazioni del sequestratore potrebbero fornire indizi sulla localizzazione; un attacco informatico in corso dove i *log* potrebbero essere cancellati. In questi casi, la velocità è effettivamente prioritaria rispetto alla perfezione forense, secondo il principio che una prova imperfetta è meglio di nessuna prova. Ma questa logica non può essere estesa indiscriminatamente: l'emergenza deve essere reale, documentata, verificabile *ex post*.

I dieci giorni per le richieste standard rappresentano un compromesso più ragionevole che dovrebbe permettere estrazioni accurate, ma anche qui ci sono criticità. Per dati semplici come *subscriber data* o *access data* limitati nel tempo, dieci giorni sono abbondanti.

Ma se l'EPOC richiede, ad esempio, tutti i contenuti di un *account* email attivo da anni con decine di migliaia di messaggi, o tutti i file conservati in un *account* di *cloud storage* che contiene terabyte di dati, o una ricostruzione completa delle comunicazioni di un utente su un *social network* nell'arco di mesi, dieci giorni possono essere insufficienti per un'estrazione completa e accurata. Il regolamento prevede la possibilità per il *provider* di chiedere una proroga in casi

di impossibilità tecnica, ma questa deve essere motivata e documentata, e non è detto che venga concessa.

Un aspetto spesso sottovalutato riguarda la qualità dei dati ricevuti. Non basta che il *provider* trasmetta dei dati entro i termini: i dati devono essere completi, accurati, utilizzabili. Se arrivano dati parziali, o in formati proprietari non facilmente analizzabili, o senza adeguata documentazione tecnica che permetta di interpretarli correttamente, l'utilità investigativa è compromessa.

Il regolamento non specifica in dettaglio i requisiti tecnici per il formato di trasmissione dei dati, rimandando a standard che dovranno essere sviluppati nell'ambito del sistema informatico decentrato. Questa standardizzazione è cruciale: un investigatore che riceve un file di *log* di accesso deve sapere come interpretare ogni campo, quale *timezone* sia utilizzato per i *timestamp*, come siano codificati gli indirizzi IP se compressi, quale sia il significato di eventuali *flag* o codici.

Competenze richieste: oltre il tradizionale perito informatico

L'utilizzo efficace del sistema E-Evidence richiede competenze che vanno ben oltre quelle del tradizionale investigatore o del perito informatico. Gli organi investigativi devono sviluppare capacità di formulare richieste tecnicamente precise, il che significa comprendere a fondo la distinzione tra le diverse categorie di dati e le loro implicazioni. Non è più sufficiente chiedere genericamente «tutti i dati relativi all'utente X»: bisogna specificare se si richiedono *subscriber data*, *access data*, *transactional data*, *content data*, e per ciascuna categoria quali elementi specifici sono rilevanti per l'indagine.

Un investigatore che sta seguendo un caso di frode *online* potrebbe aver bisogno dei *subscriber data* per identificare il

titolare dell'*account*, degli *access data* per determinare da dove e quando l'*account* è stato utilizzato, dei *transactional data* per ricostruire le comunicazioni con le vittime, dei *content data* per acquisire i messaggi in cui è stata perfezionata la truffa. Ma deve sapere che richiedere i *content data* comporta un livello di tutela più elevato, tempi potenzialmente più lunghi, maggiori possibilità di obiezioni. Deve valutare se i *transactional data*, che possono già rivelare molto sulla rete di contatti, siano sufficienti per quella fase dell'indagine, lasciando eventualmente i *content data* a una richiesta successiva quando ci saranno elementi più solidi.

La competenza tecnica deve estendersi alla comprensione delle architetture dei servizi investigati. I dati su un servizio di email tradizionale sono strutturati diversamente da quelli su un servizio di messaggistica *end-to-end encrypted*.

Un *social network* organizza i dati in modi che riflettono la sua particolare architettura: post pubblici, post condivisi con gruppi specifici, messaggi privati, reazioni, commenti, *metadata* di geolocalizzazione, connessioni tra utenti. Un servizio di *cloud storage* può conservare non solo i file attuali ma anche versioni precedenti, file cancellati ancora presenti in cestini o *backup*, *metadata* di condivisione. Richiedere «tutti i dati» senza specificare può portare a ricevere una massa enorme di informazioni difficile da analizzare, oppure a ricevere solo una parte dei dati effettivamente rilevanti perché il *provider* interpreta la richiesta in senso restrittivo.

Questa complessità implica necessità formative significative. Gli investigatori devono essere formati non solo sugli aspetti giuridici del sistema E-Evidence ma anche sugli aspetti tecnici dei servizi digitali più comuni. I magistrati che devono convalidare gli EPOC o valutare le obiezioni dei *provider* devono avere competenze che vanno oltre il diritto processuale penale tradizionale, includendo elementi di

diritto digitale, *data protection*, giurisdizione internazionale, tecnologie informatiche. I periti e i consulenti tecnici che analizzano i dati ricevuti devono avere familiarità con i formati di *export* dei principali *provider* e con le tecniche di analisi forense di grandi volumi di dati digitali.

E-Evidence e OEI: complementarità o sovrapposizione?

Una delle questioni operative più delicate riguarda il rapporto tra il sistema E-Evidence e l'Ordine Europeo di Indagine. Entrambi gli strumenti sono destinati a coesistere, ma con ambiti di applicazione e logiche diverse che possono creare confusione negli operatori. L'OEI è uno strumento generalista che copre qualsiasi atto di indagine penale in ambito transfrontaliero: intercettazioni in tempo reale, perquisizioni e sequestri, assunzioni di testimoni, accertamenti tecnici, e ovviamente anche l'acquisizione di prove digitali. Il sistema E-Evidence è invece uno strumento specialistico focalizzato esclusivamente sull'acquisizione di prove digitali già conservate dai *provider* di servizi.

La logica dell'OEI rimane quella della cooperazione verticale tra autorità giudiziarie: l'autorità di emissione invia l'OEI all'autorità di esecuzione che lo esegue secondo le proprie procedure nazionali. Questo significa che l'autorità di esecuzione mantiene un controllo sull'esecuzione dell'atto investigativo, può sollevare motivi di rifiuto, può ricorrere a atti di indagine diversi da quello richiesto se permettono di ottenere lo stesso risultato con mezzi meno intrusivi. Il sistema E-Evidence introduce invece la cooperazione orizzontale dove l'autorità richiedente si rivolge direttamente al *provider*, bypassando l'autorità giudiziaria dello Stato di esecuzione salvo il meccanismo di notifica per i dati più invasivi.

In teoria, la scelta tra i due strumenti dovrebbe basarsi sulla natura dell'atto investigativo richiesto. Se si tratta di acquisire prove digitali già conservate da un *provider* che ha uno stabilimento designato o un rappresentante legale nell'UE, lo strumento appropriato è l'EPOC. Se invece l'atto investigativo richiede un'attività materiale sul territorio dello Stato di esecuzione – una perquisizione di locali fisici, un sequestro di dispositivi *hardware*, un'intercettazione in tempo reale di comunicazioni – lo strumento appropriato rimane l'OEI. Se l'obiettivo è acquisire prove digitali da un soggetto che non è un *provider* di servizi rientrante nell'ambito della direttiva 2023/1544 – ad esempio, acquisire i dispositivi informatici di un'azienda sospettata di frode – l'OEI rimane lo strumento necessario.

Tuttavia, nella pratica le situazioni possono essere più ambigue. Si consideri il caso di un'indagine su un reato commesso utilizzando un servizio di *cloud storage*. L'investigatore potrebbe voler acquisire sia i file conservati sul *cloud* (accessibili tramite EPOC) sia il dispositivo fisico da cui l'utente accedeva al servizio (che richiederebbe un OEI per la perquisizione e il sequestro nello Stato dove si trova il dispositivo). Oppure un'indagine su traffico di stupefacenti potrebbe richiedere sia i messaggi scambiati su un'app di messaggistica (EPOC) sia le intercettazioni in tempo reale delle comunicazioni future (OEI). La complementarità dei due strumenti richiede coordinamento: l'autorità inquirente deve sviluppare strategie investigative integrate che utilizzino entrambi gli strumenti in modo sinergico.

C'è poi una zona grigia rappresentata dai casi in cui sarebbe tecnicamente possibile utilizzare entrambi gli strumenti. Se un'autorità italiana vuole acquisire i contenuti dell'*account* email di un indagato, e l'email *provider* ha un rappresentante legale in Germania, può emettere un EPOC indirizzato direttamente al rappresentante legale.

Ma potrebbe anche, in teoria, emettere un OEI verso l'autorità

giudiziaria tedesca chiedendo di acquisire quegli stessi dati. Quale strumento dovrebbe essere preferito? La logica del sistema E-Evidence suggerisce che, quando applicabile, l'EPOC dovrebbe essere lo strumento primario perché più rapido ed efficiente. Ma ci potrebbero essere situazioni in cui l'autorità richiedente preferisce passare attraverso l'OEI perché ritiene importante il controllo dell'autorità giudiziaria dello Stato di esecuzione, ad esempio in casi particolarmente delicati o controversi.

Il decreto italiano dovrebbe fornire linee guida operative su questi aspetti, possibilmente attraverso circolari interpretative o manuali operativi destinati ai pubblici ministeri e agli investigatori. Dovrebbe chiarire che il sistema E-Evidence non sostituisce l'OEI ma lo affianca per una categoria specifica di prove, che la scelta tra i due strumenti deve basarsi sulla natura dell'atto investigativo e sul soggetto da cui si vogliono acquisire le prove, che in situazioni complesse è possibile e anzi auspicabile utilizzare entrambi gli strumenti in modo coordinato.

Un aspetto procedurale importante riguarda la gestione dei casi in cui un EPOC non produce i risultati attesi: se il *provider* non è in grado di fornire i dati richiesti, o se fornisce dati parziali o inadeguati, l'autorità richiedente può «convertire» la richiesta in un OEI rivolgendosi all'autorità giudiziaria dello Stato di esecuzione per un'azione più invasiva? Il coordinamento tra i due sistemi deve essere fluido per evitare che le inefficienze di uno strumento non possano essere compensate dall'altro.

Privacy, GDPR e proporzionalità: il bilanciamento necessario

Il rapporto tra il sistema E-Evidence e il Regolamento Generale sulla Protezione dei Dati è uno dei nodi più delicati e potenzialmente conflittuali dell'intera architettura

normativa. Il regolamento 2023/1543 non deroga al GDPR ma stabilisce una base giuridica specifica per il trattamento dei dati personali nell'ambito dei procedimenti penali, richiamando l'articolo 23 del GDPR che permette limitazioni dei diritti degli interessati quando necessarie per la prevenzione, l'indagine e il perseguimento di reati. Tuttavia, anche quando opera questa base giuridica, rimangono fermi i principi fondamentali della protezione dati: necessità, proporzionalità, finalità limitata, minimizzazione dei dati, conservazione limitata nel tempo.

Ogni EPOC deve rispettare il principio di necessità, nel senso che i dati richiesti devono essere effettivamente necessari per l'indagine in corso e non acquisibili con mezzi meno invasivi.

Non è legittimo richiedere «tutti i dati» disponibili su un *account* per poi selezionare *a posteriori* quelli rilevanti: la richiesta deve essere specifica e mirata. Il principio di proporzionalità richiede che l'invasività della richiesta sia bilanciata con la gravità del reato investigato. Il regolamento stesso incorpora questo principio prevedendo che gli EPOC per i dati più invasivi (*transactional* e *content data*) possano essere emessi solo per reati punibili con pena detentiva massima di almeno tre anni, o per specifici reati informatici, di terrorismo o contro la sicurezza cibernetica indipendentemente dalla pena prevista.

Il principio di finalità limitata impone che i dati acquisiti tramite EPOC possano essere utilizzati esclusivamente per il procedimento penale per cui sono stati richiesti, e non per altri scopi. Se durante l'analisi dei dati emergono indizi di reati diversi da quello per cui è stato emesso l'EPOC, la loro utilizzabilità come prova per questi altri reati è questione delicata che richiederà l'intervento della giurisprudenza. In ambito nazionale, la Corte di Cassazione ha elaborato la dottrina delle «scoperte fortuite» nel contesto delle intercettazioni, ma l'applicazione di questi principi ai dati

acquisiti tramite EPOC presenta specificità che dovranno essere chiarite.

La minimizzazione dei dati richiede che vengano acquisiti solo i dati strettamente necessari. Se è sufficiente conoscere con chi un indagato ha comunicato e quando (*transactional data*), non è proporzionato richiedere anche il contenuto delle comunicazioni. Se è sufficiente sapere da quale indirizzo IP un *account* è stato utilizzato (*access data*), non è necessario richiedere tutti i file conservati nell'*account*. Questo principio pone oneri significativi sulle autorità richiedenti che devono formulare richieste precise e giustificate, ma anche sui *provider* che dovrebbero avere la capacità tecnica di estrarre selettivamente solo i dati richiesti senza fornire automaticamente insiemi di dati più ampi.

Il diritto all'informazione dell'interessato, previsto dall'articolo 15 del regolamento E-Evidence, deve essere effettivo e non meramente formale. La persona deve essere informata in termini comprensibili di quali dati sono stati acquisiti, per quale procedimento, con quale base giuridica, con quali diritti di ricorso. L'informazione può essere differita quando potrebbe pregiudicare l'indagine, ma non può essere negata indefinitamente. Il decreto italiano deve stabilire criteri oggettivi per decidere quando differire l'informazione e per quanto tempo, evitando che il differimento diventi la regola piuttosto che l'eccezione.

I diritti di accesso, rettifica e cancellazione dell'interessato, previsti dal GDPR, devono essere compatibilizzati con le esigenze investigative. Un indagato ha diritto di accedere ai propri dati acquisiti dall'autorità inquirente? In linea generale, questo diritto si realizza attraverso il diritto di accesso agli atti del procedimento secondo le norme processuali penali, non attraverso i meccanismi del GDPR.

Ma ci possono essere fasi in cui l'interessato non è ancora

formalmente indagato e quindi non ha accesso agli atti: in questi casi, il GDPR potrebbe offrire tutele aggiuntive. Il diritto alla cancellazione è particolarmente problematico: non può essere invocato per cancellare prove di reato, ma potrebbe applicarsi a dati non rilevanti che sono stati acquisiti ma non sono utilizzati nel procedimento. Il decreto dovrebbe prevedere procedure di revisione periodica dei dati conservati per cancellare quelli non più necessari.

Prospettive critiche e rischi sistemici

Sarebbe ingenuo pensare che il sistema E-Evidence risolverà magicamente tutti i problemi dell'acquisizione transfrontaliera di prove digitali. Diverse questioni strutturali rimangono aperte e potrebbero minare l'efficacia del sistema o generare conseguenze indesiderate.

La prima incognita riguarda l'effettiva volontà di *compliance* dei *provider*, specialmente quelli extra-europei. I giganti tecnologici americani hanno già team dedicati alla *law enforcement compliance* e probabilmente si adegueranno, anche se non senza tensioni politiche. Ma *provider* cinesi, russi, o di altre giurisdizioni con cui l'UE ha rapporti difficili, potrebbero essere meno cooperativi. Un *provider* che decide di non nominare un rappresentante legale nell'UE tecnicamente viola la direttiva e dovrebbe essere sanzionato, ma come imporre concretamente la sanzione a un'entità che non ha presenza fisica nell'UE e che potrebbe semplicemente ignorare le richieste europee? L'unica leva reale sarebbe il *blocking* del servizio, ma questo solleva questioni di proporzionalità e di impatto sugli utenti europei che utilizzano legittimamente quel servizio.

La frammentazione geografica dei dati pone sfide tecniche e giuridiche. Molti *provider* globali utilizzano architetture *cloud* distribuite dove i dati degli utenti sono replicati su

server in diverse giurisdizioni per ragioni di *performance* e affidabilità. Un utente italiano che utilizza un servizio americano potrebbe avere i propri dati conservati contemporaneamente su server in Irlanda, negli Stati Uniti, a Singapore. Quale copia dei dati viene fornita in risposta a un EPOC? Cosa succede se le diverse copie non sono perfettamente sincronizzate? Il *provider* è tenuto a fornire tutte le copie o solo una? E se diverse giurisdizioni reclamano obblighi contrastanti su quegli stessi dati?

Il rischio di *weaponization* politica del sistema E-Evidence è concreto. Stati membri con standard democratici indeboliti potrebbero utilizzare gli EPOC per perseguire oppositori politici, giornalisti, attivisti. Il sistema di garanzie previsto dal regolamento dovrebbe proteggere contro questi abusi, ma la storia insegna che le garanzie formali non sempre sono sufficienti quando manca la volontà politica di applicarle. I *provider* potrebbero trovarsi nella difficile posizione di dover valutare se un EPOC formalmente legittimo nasconda in realtà un abuso politico, una valutazione che richiede giudizi delicati su sistemi giuridici stranieri.

La standardizzazione tecnica tra Stati membri richiederà tempo e investimenti che non tutti i paesi sono egualmente preparati a sostenere. Il rischio è che il sistema funzioni efficacemente tra un nucleo di Stati con infrastrutture avanzate e competenze consolidate, mentre altri Stati rimangano ai margini. Questo potrebbe creare una cooperazione giudiziaria a più velocità, dove gli Stati tecnologicamente avanzati cooperano efficacemente tra loro attraverso E-Evidence mentre gli altri rimangono ancorati a strumenti tradizionali più lenti.

La pressione sui tempi di risposta potrebbe compromettere la qualità delle prove. L'enfasi sulla velocità, comprensibile date le esigenze investigative, potrebbe creare incentivi perversi a sacrificare accuratezza e completezza sull'altare dell'efficienza. Un'estrazione frettolosa eseguita per

rispettare il termine di otto ore potrebbe perdere *metadata* cruciali, omettere dati rilevanti, o introdurre errori che compromettono l'utilizzabilità processuale. Serve un bilanciamento delicato, e la cultura forense deve evolversi per incorporare protocolli di qualità anche in contesti di emergenza.

Conclusioni: verso un ecosistema investigativo maturo

L'attuazione del pacchetto E-Evidence attraverso gli schemi di decreto legislativo attualmente all'esame parlamentare rappresenta un passaggio epocale per il diritto processuale penale europeo e italiano. Non si tratta di una semplice aggiunta di strumenti tecnici alla cassetta degli attrezzi investigativi, ma di un ripensamento profondo di come lo Stato esercita la giurisdizione penale in un mondo digitalizzato dove i confini territoriali hanno perso gran parte del loro significato pratico.

Per gli operatori del diritto, questo significa acquisire competenze nuove che incrociano diritto processuale, *data protection*, tecnologie informatiche, cooperazione internazionale. Per le forze di *law enforcement*, significa riorganizzare processi investigativi consolidati, formare personale specializzato, investire in infrastrutture tecnologiche. Per i CISO e i professionisti della *cybersecurity* dei *provider*, significa costruire processi di *compliance* complessi che bilanciano obblighi legali, tutela della *privacy* degli utenti, efficienza operativa, rischi reputazionali. Per gli esperti di *digital forensics*, significa sviluppare metodologie che funzionino in contesti transfrontalieri dove il controllo diretto sull'acquisizione delle prove è limitato.

Ma soprattutto, per tutti gli attori dell'ecosistema, significa mantenere alta la vigilanza sui diritti fondamentali. L'efficienza investigativa è un valore

importante in una società che deve proteggersi dalla criminalità, sempre più organizzata su scala transnazionale e sempre più sofisticata nell'uso delle tecnologie. Ma questa efficienza non può mai tradursi in un sacrificio ingiustificato della *privacy*, della libertà di espressione, del diritto alla difesa, delle garanzie processuali che definiscono una democrazia liberale. Il sistema E-Evidence funzionerà veramente solo se saprà essere al contempo efficace nel dare alle autorità gli strumenti per investigare e garantista nel proteggere i diritti delle persone.

L'Italia ha l'opportunità, attraverso gli schemi di decreto attualmente in discussione, di contribuire a costruire un sistema che sia modello di questo equilibrio. Le scelte implementative che verranno fatte nelle prossime settimane e mesi – quali autorità designare, come strutturare i processi di riesame, quali standard di sicurezza imporre al sistema informatico, come graduare le sanzioni, come formare gli operatori – determineranno se il sistema E-Evidence italiano sarà un esempio di cooperazione giudiziaria efficace e rispettosa dei diritti, o se si rivelerà un'altra occasione mancata.

Il dibattito tecnico e politico che accompagna l'esame parlamentare degli schemi di decreto deve essere all'altezza della posta in gioco. Non può limitarsi a questioni formali di conformità alle norme europee, ma deve affrontare le questioni sostanziali di come vogliamo che la giustizia penale funzioni nell'era digitale, di quali garanzie consideriamo irrinunciabili, di come bilanciare esigenze investigative e tutela dei diritti, di come costruire fiducia reciproca tra Stati membri e tra Stati e cittadini. Ridefinire il rapporto tra giustizia penale e spazio digitale nell'Europa del ventunesimo secolo è la sfida che ci troviamo di fronte. Gli strumenti normativi ci sono, l'infrastruttura tecnica si sta costruendo. Ora serve la saggezza di usarli bene.

Condividi sui Social Network:

<https://www.ictsecuritymagazine.com/articoli/e-evidence/>