

FRANCESCO CAMBIANO* LORENZO RAPISARDA**

DIGITALIZZAZIONE DEL CRIMINE E COOPERAZIONE GIUDIZIARIA: GLI ORDINI DI PRODUZIONE E CONSERVAZIONE NEL REGOLAMENTO SULL'E-EVIDENCE***

SOMMARIO: 1. Premessa – 2. Il fenomeno della c.d. digitalizzazione del crimine – 3. La disciplina delineata dal Regolamento UE 2023/1543 e dalla Direttiva UE 2023/1544. – 4. Una nuova frontiera per il mutuo riconoscimento nel settore penalistico. – 5. Cifratura e decrittazione: criticità applicative del nuovo Regolamento. – 6. I prestatori di servizi digitali nello scacchiere della cooperazione giudiziaria. – 7. Conclusioni.

1. *Premessa*

È ormai evidente che il tradizionale rapporto dicotomico tra dimensione *on-line* e *off-line* risulta poco adatto – se non addirittura inadeguato – a descrivere la condizione attuale dell'agire umano. Le nostre vite si svolgono in un contesto profondamente trasformato dall'incessante interconnessione tra immateriale e materiale¹.

L'epoca in cui viviamo si caratterizza per il progressivo utilizzo e per la natura totalizzante delle tecnologie digitali, le quali da un lato hanno radicalmente trasformato la produzione di informazioni – da analogiche a digitali – e dall'altro lato hanno mutato le modalità con le quali queste ultime vengono modificate, scambiate e archiviate. Si assiste, da alcuni anni, all'emersione di nuove forme di condotte penalmente rilevanti, rendendosi necessario un riassetto delle categorie proprie del diritto penale sostanziale e del diritto processuale penale.

In considerazione al secondo tra i due aspetti poc'anzi evidenziati, la pervasività degli strumenti digitali ha determinato una crescente rilevanza – ed una contestuale notevole incidenza – della prova elettronica all'interno dei procedimenti penali.

La *e-evidence* può assumere forme eterogenee – dai metadati ai dati di traffico, dalle comunicazioni telematiche ai contenuti pubblicati sui *social media* – e presenta caratteristiche peculiari, quali la volatilità, la dispersione transnazionale e la dipendenza da soggetti privati terzi e spesso localizzati al di fuori della giurisdizione dell'autorità inquirente. Tali

* Dottorando di ricerca in *Pluralismi giuridici. Prospettive antiche ed attuali* presso l'Università degli Studi di Palermo in co-tutela con la Rijksuniversiteit Groningen.

** Dottorando di ricerca in *Giurisprudenza* presso l'Università degli Studi di Catania..

*** Lo scritto riproduce, con note e integrazioni, l'intervento svolto in occasione del convegno su *Tutela del "terzo" e giustizia penale transnazionale: la prospettiva eurounitaria*, organizzato nell'ambito progetto PRIN 2022 su *Criminal proceedings and the protection of third parties: old and new challenges in the digital era*, Università di Palermo, 13 marzo 2025. Inoltre, il contributo è frutto di un sinergico confronto tra i due autori; tuttavia, a F. CAMBIANO può essere attribuita la redazione dei paragrafi 1, 2, 5 e 7, mentre a L. RAPISARDA dei paragrafi 3, 4 e 6.

¹ Autorevolmente, sul punto, L. FLORIDI, *The Onlife Manifesto. Being Human in a hyperconnected Era*, Cham, 2014, il quale utilizza l'interessante e pertinente neologismo '*onlife*' per descrivere la crescente inscindibilità tra le due realtà, virtuale e reale.

caratteristiche pongono inedite sfide operative e giuridiche in ordine all'acquisizione, alla conservazione e all'utilizzabilità della prova in sede processuale.

L'attuale sistema di cooperazione giudiziaria, fondato in larga parte su meccanismi 'tradizionali' di assistenza giudiziaria, si dimostra inefficace a contrastare la velocità e la complessità delle indagini digitali. Anche lo stesso OEI (ordine europeo d'indagine), pur rappresentando un passo avanti nella logica del principio del mutuo riconoscimento, non sembra in grado di affrontare adeguatamente le criticità operative descritte, specialmente per quanto riguarda i Paesi – come l'Irlanda – in regime di *opt-out*.

Al fine di rispondere positivamente a tali esigenze, nell'ordinamento dell'Unione europea sono stati recentemente introdotti due nuovi strumenti: l'ordine europeo di produzione (noto anche con l'acronimo EPO, derivante dalla denominazione inglese *European Production Order*) e l'ordine europeo di conservazione (EPrO, sempre secondo la denominazione inglese: *European Preservation Order*) mediante un pacchetto normativo che si compone di un Regolamento e di una Direttiva².

2. Il fenomeno della c.d. digitalizzazione del crimine

La digitalizzazione, in parte consolidata e in parte in continua evoluzione³, ha contribuito a un impiego esponenziale di sistemi elettronici nelle attività quotidiane, sia lecite sia illecite.

Relativamente a tale ultima dimensione, le autorità giudiziarie e le forze dell'ordine si trovano ad affrontare nuovi e impegnativi ostacoli, soprattutto qualora si adotti una concezione ampia del termine 'crimine', svincolata e indipendente dal tipo di reato commesso o, ancora, da commettere. Particolare rilievo assume la gestione delle prove digitali, in termini di accesso, lettura e utilizzo delle stesse nei procedimenti penali. Infatti, al di là delle attività probatorie che possono già contare su una più compiuta esperienza – si pensi, fra le molteplici, all'analisi del DNA – le prove elettroniche o, appunto, digitali sono utilizzate con maggiore frequenza, non solo in relazione a reati direttamente o intrinsecamente connessi al mondo digitale⁴, ma anche con riguardo a una vasta gamma di fattispecie in cui, anche indirettamente, sistemi avanzati e non ancora consueti rivestono un ruolo significativo durante l'intero procedimento penale.

La natura trasformativa delle tecnologie digitali ha rivoluzionato le attività criminali, ampliandone in modo esponenziale lo spettro di operatività e influenzando su vari aspetti

² Si tratta del Regolamento UE 2023/1543 del Parlamento europeo e del Consiglio, 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 penale, nonché della Direttiva UE 2023/1544 del Parlamento europeo e del Consiglio, recante Norme armonizzate sulla designazione di stabilimenti designati e sulla nomina di rappresentanti legali ai fini dell'acquisizione di prove elettroniche nei procedimenti penali.

³ Si pensi, in riferimento al nostro Paese, alle ingenti risorse stanziare nell'ambito del piano Nazionale di Rilancio e Resilienza per la transizione digitale delle pubbliche amministrazioni. Per informazioni maggiormente dettagliate sul piano di ripartizione delle somme di cui sopra, si rinvia al seguente *link*: <https://www.mim.it/gov/it/pnrr/piano>.

⁴ La categoria potrebbe ricomprendere tutti quegli illeciti penalmente rilevanti contraddistinti, sin dalla loro denominazione, dal prefisso “-cyber”. Si assiste, infatti, al passaggio da fattispecie di reato “contemporanee ma residuali” quali ad esempio il bullismo o il terrorismo, a quelle “contemporanee ma primarie”, quali il cyberbullismo e il cyberterrorismo.

strutturali. Il fenomeno in questione non è intervenuto solamente sulla genesi di nuovi illeciti penalmente rilevanti di particolare complessità e di difficile individuazione, accertamento e repressione, ma ha altresì ridefinito la configurazione di fattispecie tradizionali, al punto da condizionare tanto le modalità di commissione quanto l'impatto delle condotte illecite.

In tale prospettiva, si propone la formulazione di un nuovo concetto funzionale a esprimere il cambiamento epocale di paradigma: 'digitalizzazione del crimine'. Attraverso tale locuzione risulta possibile superare il classico dualismo crimine-tecnologia, circoscritto meramente ai *cybercrimes* in senso stretto, riconoscendo la piena integrazione degli strumenti digitali in una molteplicità di altre fattispecie delittuose.

Se, appunto, i *cybercrimes* – come gli attacchi *hacker* ai sistemi informatici, il furto d'identità virtuale, le frodi *online* o, ancora, l'utilizzo di *ransomware* – si caratterizzano per lo sfruttamento della tecnologia quale mezzo indefettibile ovvero senz'altro necessario attraverso cui si realizza la condotta criminosa, l'analisi evolutiva di altri reati è in grado di dimostrare come il digitale si sia innestato, con intensità naturalmente variabile a seconda della singola fattispecie in esame, anche su comportamenti delittuosi non direttamente, o quantomeno non originariamente, legati al mondo *tech*.

Per comprendere adeguatamente la portata del fenomeno della c.d. digitalizzazione del crimine, appare opportuno considerare, seppur brevemente e per sommi capi, l'evoluzione di alcuni fenomeni criminali in grado di dimostrare l'accelerazione in tal senso avvenuta negli ultimi anni.

Tra le manifestazioni più evidenti del fenomeno menzionato rientrano le metamorfosi subite dai reati a sfondo sessuale, i quali hanno trovato nelle piattaforme multimediali, da un canto, un nuovo terreno fertile per la loro commissione e, dall'altro, un vettore di diffusione dei relativi contenuti. Infatti, la rete e le applicazioni di messaggistica istantanea, specialmente quelle dotate di sistemi crittografati *end-to-end*, costituiscono oggi i principali strumenti attraverso cui vengono perpetrate forme di violenza e sfruttamento sessuale. A tal riguardo, è possibile menzionare una figura in crescente diffusione, ossia quella del c.d. *revenge porn*, consistente – in breve – nella divulgazione – spesso su gruppi chiusi, *forum* criptati o applicazioni anonime – di materiale multimediale a contenuto sessuale senza il consenso della persona ritratta. Le caratteristiche strutturali delle piattaforme utilizzate a tale scopo, come l'anonimato degli utenti e l'impossibilità di tracciarne le interazioni in tempo reale, rendono estremamente complesso l'accertamento della responsabilità penale degli autori delle condotte in esame e il reperimento delle relative prove digitali. Accanto alla pratica appena descritta, si segnala sempre a titolo esemplificativo un progressivo aumento della produzione e diffusione di contenuti sessuali 'in diretta' – *live streaming* – aventi ad oggetto l'esibizione di minori o altri individui particolarmente vulnerabili. In tali casi, l'autore della condotta mira a due possibili obiettivi: da un lato, l'influenza ed il 'potere sociale' all'interno di specifiche comunità digitali e, dall'altro, l'accrescimento del proprio patrimonio economico⁵.

Analogamente, i canali di facile comunicazione a noi contemporanei – come i *social media* e le moderne piattaforme di corrispondenza e messaggistica⁶ – vengono sempre con maggiore frequenza utilizzati nelle fasi di adescamento, reclutamento e sfruttamento delle vittime di tratta di esseri umani. Nonostante i continui interventi da parte delle società proprietarie delle piattaforme in questione, per limitarne gli usi inappropriati, cresce l'utilizzo di queste ultime da parte di soggetti che intendono creare rapporti di fiducia manipolativa ed

⁵ La monetizzazione del contenuto può avvenire, di norma, mediante circuiti di pagamento integrati all'interno delle stesse piattaforme ove avviene la realizzazione e la diffusione del contenuto.

⁶ Tra le tante è possibile menzionare le più diffuse quali *WhatsApp*, *Telegram*, *Discord* ovvero anche *Instagram*.

esercitare pressioni funzionali al successivo sfruttamento sessuale, lavorativo ovvero ancora criminale. Inoltre, l'impiego di pseudonimi e profili falsi rende difficoltose l'identificazione degli autori e la raccolta tempestiva dei dati rilevanti ai casi in questione, ostacolando – non poco – le indagini, soprattutto se si considera che le informazioni utili a livello investigativo si trovano memorizzate, spesso, su banche dati collocate in Paesi terzi ovvero soggette a brevissimi termini di conservazione che ne rendono praticamente impossibile l'acquisizione *ex post*.

Ancora, il *deep web* si è ormai affermato come il principale mercato illecito per il commercio di una serie di “prodotti” – materiale pedopornografico, stupefacenti, armi, beni culturali, ma anche piante e animali – che vengono scambiati a fronte del pagamento sotto forma, spesso, di criptovalute, le quali garantiscono transazioni anonime e difficilmente rintracciabili, rendendo estremamente complesse le attività di contrasto da parte delle autorità competenti. Perfino il fenomeno del terrorismo internazionale ha trovato nel mondo digitale un potente alleato. Le organizzazioni estremiste approfittano degli strumenti tecnologici per le attività preliminari di propaganda, indottrinamento e radicalizzazione, oltre che per la diffusione di ‘manuali d’istruzione’ e coordinamento operativo. Proprio tale ultimo livello rappresenta, da un punto di vista investigativo e repressivo, una delle frontiere più complesse: la possibilità di coordinare condotte illecite attraverso piattaforme digitali consente alle organizzazioni terroristiche di adottare una struttura reticolare in cui cellule autonome operano in maniera sincronica, pur in assenza di una direzione gerarchica, secondo comuni principi ideologici. Si assiste, di conseguenza, a una decentralizzazione delle operazioni che compromette l'efficacia dei tradizionali strumenti di contrasto.

La descritta evoluzione del crimine impone necessariamente una riflessione sullo strumento di maggiore rilievo per l'accertamento dei fatti nel contesto investigativo contemporaneo: la prova digitale.

Se, per un verso, risulta un dato incontrovertibile che la tecnologia abbia agevolato la proliferazione di nuove modalità di realizzazione degli illeciti, dall'altro appare indubbio che abbia contribuito alla formazione di nuove tracce che possono rivelarsi determinanti per le indagini⁷. Le informazioni, spesso sommerse nella vastità dei dati digitali generati quotidianamente, costituiscono una fonte preziosa per le autorità investigative, consentendo la ricostruzione di dinamiche criminali e l'individuazione dei responsabili.

In particolare, la prova digitale può assumere diverse forme, a seconda della sua natura e del contesto in cui viene raccolta⁸. I dati di traffico, quali indirizzi IP, cronologie di connessione e comunicazioni telematiche, permettono di tracciare le attività *online* e di stabilire, ove esistenti, eventuali legami tra soggetti coinvolti in attività illecite. I *metadati* – contenenti informazioni relativi alla creazione, alla modifica e alla localizzazione del *file* – offrono dettagli ‘invisibili’ nel contenuto stesso del documento, ma essenziali per l'analisi forense. Le transazioni finanziarie digitali, che includono pagamenti elettronici, operazioni in criptovaluta e movimenti bancari sospetti, rivestono un ruolo chiave nella ricerca di schemi di riciclaggio di denaro, frodi e finanziamenti illeciti. Anche l'attività compiuta attraverso i *social media* può rappresentare una fonte di prova significativa, con la possibilità di acquisire

⁷ Cfr. M. DANIELE, *La prova digitale nel processo penale*, in *Rivista di diritto processuale*, 2007, p. 283, il quale, correttamente, sottolinea che per tali ragioni le prove digitali «hanno un ambito operativo potenzialmente illimitato».

⁸ Cfr. F. SALIMI, *Legal Challenges in Dealing with Electronic Evidence in Criminal Proceedings*, in L. BACHMAIER WINTER, F. SALIMI (a cura di), *Admissibility of Evidence in EU Cross-Border Criminal Proceedings: Electronic Evidence, Efficiency and Fair Trial Rights*, Oxford, 2024, pp. 50-51.

post, messaggi privati, dati di geolocalizzazione e interazione tra gli utenti, spesso cruciali per ricostruire la preparazione e l'esecuzione di condotte criminali.

Una caratteristica distintiva della prova digitale, tuttavia, è la sua volatilità: a differenza delle prove fisiche, i dati elettronici possono essere facilmente modificati, cancellati o resi inaccessibili, rendendo necessaria un'acquisizione tempestiva e conforme a procedure forensi rigorose. Altresì – ed è anche questo aspetto di fondamentale importanza – la prova digitale pone dei notevoli problemi rispetto alla sua localizzazione: a differenza delle prove materiali, che si trovano in un luogo specifico e tangibile, essa può venire memorizzata in *server* soggetti a giurisdizioni diverse, risultando distribuita tra più Paesi o conservata in sistemi di *cloud computing*, con la conseguente difficoltà di risalire alla sua effettiva collocazione⁹.

La gestione e, in molti casi, la conservazione degli elementi che possono costituire prove digitali rimangono di dominio esclusivo dei *digital service providers*, terzi rispetto al procedimento penale, la cui collaborazione¹⁰ non risulta solamente auspicabile quanto necessaria ed essenziale per la trasmissione dei dati memorizzati sui loro *server* alle autorità giudiziarie richiedenti.

Tradizionalmente, l'ottenimento di queste informazioni da uno Stato all'altro avveniva attraverso meccanismi di assistenza giudiziaria piuttosto lenti e burocratici.

Neppure l'ordine europeo d'indagine (OEI), introdotto nel 2014¹¹, è riuscito a sopperire a queste difficoltà, tenendo conto del dato secondo cui il Paese membro dell'Unione europea all'interno del quale hanno sede i principali *digital service providers*, cioè l'Irlanda, si trova in regime di *opt-out* rispetto al menzionato strumento di mutuo riconoscimento¹².

Per superare i limiti della disciplina vigente, «le autorità nazionali hanno iniziato a contattare direttamente i *service providers* situati in altri Stati (appartenenti all'Unione o terzi), senza coinvolgere le autorità del Paese di esecuzione, creando canali di comunicazione su base “volontaria”»¹³ e ricercando, dunque, una collaborazione da parte dei *service providers* assolutamente non coercibile in caso di rifiuto.

All'esito di un percorso travagliato, all'interno dell'Unione europea sono stati recentemente introdotti due nuovi strumenti: l'ordine europeo di produzione (noto anche con l'acronimo EPO, derivante dalla denominazione inglese *European Production Order*) e l'ordine europeo di conservazione (EPrO, sempre secondo la denominazione inglese:

⁹ Cfr. T. CHRISTAKIS, *From Mutual Trust to the Gordian Knot of Notifications. The EU e-evidence Regulation and Directive*, in V. FRANSSSEN, S. TOSZA (a cura di), *The Cambridge Handbook of Digital Evidence in the Criminal Investigations*, Cambridge, 2025, p. 175. Altresì, sul punto, S. TOSZA, *Electronic Evidence after E-evidence Package's Adoption: Challenges for Application and Unresolved Problems*, in *Studia Iuridica Lublinsia*, 2024, 5, p. 240: «the current legal framework, rooted in the principle that enforcement jurisdiction is confined to a state's territory, restricts law enforcement's ability to access data stored abroad. This territorial limitation clashes with the borderless nature of the Internet».

¹⁰ J. RINCEANU, *Verso una forma di polizia private nello spazio digitale? L'inedito ruolo dei provider nella disciplina tedesca dei social network*, in *Sistema penale*, 2021.

¹¹ Direttiva UE 2014/41 del Parlamento Europeo e del Consiglio, relativa all'ordine europeo d'indagine penale.

¹² Cfr. S. SIGNORATO, *Le indagini digitali. Profili strutturali di una metamorfosi investigativa*, Torino, 2018, p. 173 ss; altresi, V. FRANSSSEN, *Cross-border gathering of electronic evidence in the EU: towards more direct cooperation under the e-Evidence Regulation*, in V. MITSILEGAS, M. BERGSTRÖM, T. QUINTEL (a cura di), *Research Handbook on EU Criminal Law*, II ed., Cheltenham, 2024, pp. 186-187.

¹³ 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*, 2018, 5, p. 281.

European Preservation Order) mediante un pacchetto normativo che si compone di un Regolamento e di una Direttiva¹⁴.

Alla luce delle considerazioni fin qui esposte, emerge con chiarezza come la c.d. digitalizzazione del crimine imponga un completo ripensamento delle strategie di contrasto alla criminalità, richiedendo strumenti investigativi aggiornati e un quadro normativo adeguato alla complessità dell'attuale contesto tecnologico. In tale scenario, la prova digitale non rappresenta soltanto un elemento imprescindibile per le indagini penali, ma costituisce altresì un banco di prova per l'evoluzione della cooperazione giudiziaria nella lotta alla criminalità nell'era digitale.

3. La disciplina delineata dal Regolamento UE 2023/1543 e dalla Direttiva UE 2023/1544

Il pacchetto normativo in tema di *e-evidence* trae origine da una proposta della Commissione europea, presentata ad aprile del 2018¹⁵, sostenuta da un approfondito studio d'impatto dell'intervento legislativo (283 pagine)¹⁶. L'approvazione definitiva del Regolamento e della Direttiva, all'esito di un lungo *iter* che ha coinvolto i due co-legislatori, Consiglio e Parlamento europeo, è giunta soltanto cinque anni dopo, il 12 luglio 2023. Sebbene la normativa sia già in vigore, la sua applicabilità è prevista a partire da agosto 2026, essendo necessari, tra l'altro, dei congrui termini per l'attuazione della Direttiva da parte degli Stati membri.

All'interno del Regolamento è disciplinato il funzionamento dei due istituti di nuova introduzione.

Lo strumento principe è indubbiamente l'ordine europeo di produzione, che consente alle autorità giudiziarie di uno Stato membro di richiedere direttamente a un fornitore di servizi digitali, situato in un altro Stato membro (concetto estremamente vago in questi termini, che verrà elaborato più dettagliatamente nel prosieguo, trattando della Direttiva), la consegna di dati sugli utenti, estremamente utili all'interno di un procedimento penale per il loro valore probatorio.

Le condizioni e le modalità di emissione ed esecuzione di un ordine di produzione variano a seconda della tipologia di dati che vengono richiesti. Infatti, il Regolamento distingue fra tre categorie di dati: dati relativi agli abbonati, dati relativi al traffico e dati relativi al contenuto¹⁷.

¹⁴ Si tratta del Regolamento UE 2023/1543 del Parlamento europeo e del Consiglio, 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 penale, e della Direttiva UE 2023/1544 del Parlamento europeo e del Consiglio, recante norme armonizzate sulla designazione di stabilimenti designati e sulla nomina di rappresentanti legali ai fini dell'acquisizione di prove elettroniche nei procedimenti penali.

¹⁵ *European Commission, Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters*, COM/2018/225 final; *European Commission, Proposal for a Directive of the European Parliament and of the Council laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings*, COM/2018/226 final.

¹⁶ [Commission Staff Working Document Impact Assessment, SWD\(2018\) 118 final](#).

¹⁷ È, dunque, evidente che «[the] approach is based on the assumption that different levels of protection, based on the sensitive nature of the data and the corresponding degree of invasiveness of the production order, should apply» (M. CORHAY, *Private Life, Personal Data Protection and the Role of Service Providers: The EU E-evidence proposal*, in *European Papers*, 2021, p. 447).

Per i dati relativi agli abbonati e per quelli di traffico, purché questi ultimi siano necessari per la sola identificazione dell'autore del reato, l'ordine di produzione può essere emesso per qualsiasi reato oggetto d'indagine, oppure per eseguire una condanna a una pena o ad una misura di sicurezza di tipo detentivo non inferiori a quattro mesi¹⁸.

Diversamente, per l'acquisizione dei dati di contenuto e per quelli di traffico diversi dai precedenti, i requisiti sono maggiormente stringenti: l'ordine può essere emesso solo per reati puniti con una pena detentiva non inferiore a tre anni nel massimo edittale; tuttavia, se l'ordine è finalizzato all'esecuzione di una condanna o di una misura di sicurezza detentive, può essere emesso quando queste ultime non sono inferiori a quattro mesi¹⁹; infine, l'ordine può essere emesso anche per alcuni reati armonizzati da Direttive europee, specificamente e tassativamente individuati, quando commessi, in tutto o in parte, attraverso un sistema informatico²⁰.

In ogni caso – indipendentemente dalla tipologia di dato richiesto – l'emissione dell'ordine è subordinata al rispetto dei requisiti di necessità e proporzionalità, nonché alla possibilità che un simile ordine sia adottabile, in condizioni identiche, in un procedimento meramente interno²¹.

Le differenze attengono, tuttavia, anche agli aspetti strettamente procedurali.

Invero, per i dati relativi agli abbonati e per quelli di traffico necessari per la sola identificazione dell'autore del reato, secondo la formulazione del Regolamento, l'ordine di produzione può essere emesso da «un giudice, un organo giurisdizionale, un magistrato inquirente o un pubblico ministero»²², ovvero convalidato da uno di questi, se l'ordinamento dello Stato d'emissione attribuisce la competenza a emettere l'ordine ad altra «autorità inquirente nel procedimento penale [...] competente a disporre l'acquisizione di prove in conformità del diritto nazionale»²³.

Destinatario dell'ordine è unicamente l'*internet service provider*²⁴, che dovrà tempestivamente darvi esecuzione – a meno che non ravvisi la sussistenza di uno dei *grounds of refusal* tassativamente indicati dal Regolamento – entro i successivi dieci giorni²⁵. In ipotesi d'urgenza, peraltro, i termini per l'esecuzione sono ridottissimi: il prestatore di servizi, infatti, dovrà dare riscontro all'autorità emittente entro otto ore dalla ricezione dell'ordine di produzione²⁶. Nell'eventualità in cui l'*internet service provider* non dia esecuzione all'ordine di produzione entro il termine imposto (sia esso quello ordinario o quello d'emergenza), senza

Lo stesso legislatore europeo, nel considerando n. 31, specifica che la suddivisione dei dati in queste categorie è conforme a quanto già previsto nella Direttiva CE 2002/58 nella Convenzione di Budapest e dalla giurisprudenza della Corte di giustizia. Il Regolamento, comunque, offre una definizione delle categorie di dati all'art. 3, numeri 9), 10) e 11). Sul punto, inoltre, v. A. SACHOULIDOU, *Cross-border access to electronic evidence in criminal matters: The new EU legislation and the consolidation of a paradigm shift in the area of "judicial" cooperation*, in *New Journal of European Criminal Law*, 2024, p. 261.

¹⁸ Art. 5, paragrafo 3, del Regolamento.

¹⁹ Art. 5, paragrafo 4, lett. a) e d) del Regolamento.

²⁰ Art. 5, paragrafo 4, lett. b) e c) del Regolamento.

²¹ Art. 5, paragrafo 2, del Regolamento. Per un'efficace disamina dei requisiti di necessità e proporzionalità – comuni anche alla Direttiva UE 2014/41 sull'ordine europeo d'indagine penale – si rinvia a O. CALAVITA, *L'ordine europeo di indagine penale. Presente e futuro della cooperazione probatoria nell'Unione europea*, Milano, 2025, pp. 24-38.

²² Art. 4, paragrafo 1, lett. a) del Regolamento.

²³ Art. 4, paragrafo 1, lett. b) del Regolamento.

²⁴ Art. 7, paragrafo 1, del Regolamento.

²⁵ Art. 10, paragrafo 3, del Regolamento.

²⁶ Art. 10, paragrafo 4, del Regolamento.

addurre una ragione di rifiuto accettata dall'autorità d'emissione, l'autorità giudiziaria del Paese membro in cui vi è il destinatario dell'ordine, assumerà le vesti di autorità d'esecuzione²⁷: in questa eventualità, dunque, si ripristina lo schema classico della cooperazione giudiziaria, che vede due autorità giudiziarie ai due poli.

Per i dati di contenuto e per quelli di traffico diversi dai precedenti, invece, il legislatore europeo ha voluto apprestare maggiori garanzie, data la maggiore sensibilità di queste informazioni.

In primo luogo, è imposto un previo vaglio giurisdizionale al momento dell'emissione dell'ordine di produzione. Sul punto, però, la versione italiana del Regolamento presenta alcune ambiguità testuali: è indicato che l'ordine di produzione debba essere emesso da «un giudice, un organo giurisdizionale o un magistrato inquirente»²⁸. Però, in alternativa, questi ultimi, possono effettuare un previo vaglio sulle richieste provenienti da qualsiasi altra autorità competente all'emissione, secondo l'ordinamento dello Stato d'emissione, che agisce in qualità di autorità inquirente nel procedimento penale e sia competente a disporre l'acquisizione di prove in conformità del diritto nazionale²⁹. Così, peraltro, parrebbe che anche il pubblico ministero possa essere organo emanante, atteso che nell'ordinamento italiano esso è il magistrato inquirente. Eppure, come visto, la figura del pubblico ministero è esplicitamente e distintamente ricompresa tra i soggetti che possono esclusivamente emanare un ordine di produzione per dati relativi agli abbonati o dati di traffico utili per la sola identificazione dell'autore del reato. Forse, allora, quella adottata dalla versione italiana del Regolamento è una terminologia tesa a includere il *juge d'instruction* tra i soggetti competenti per l'emissione (circostanza che sembra confermata dalla versione in lingua francese del Regolamento), ma non certo il pubblico ministero.

In secondo luogo, l'ordine di produzione inerente a queste tipologie di dati deve essere notificato all'autorità giudiziaria dello Stato in cui si trova lo stabilimento o il rappresentante del prestatore di servizi, affinché anch'essa eserciti un controllo sulle condizioni di emissione ed esecuzione, entrando fin da subito nel circuito della cooperazione per l'acquisizione della *e-evidence*; la notificazione, infatti, è contestuale alla trasmissione dell'ordine³⁰. Vi è, peraltro, un'eccezione, che sarà relevantissima sotto il punto di vista dell'incidenza statistica: non vi è alcun obbligo di notificazione se, al momento dell'emissione dell'ordine, l'autorità emittente abbia fondato motivo di ritenere che il reato sia stato commesso, sia in atto o sia suscettibile di essere commesso nello Stato di emissione, oppure se la persona i cui dati sono richiesti risieda nello Stato di emissione³¹.

Infine, cambiano i tempi di esecuzione. Dato che la notificazione all'autorità giudiziaria d'esecuzione è contestuale alla trasmissione dell'ordine di produzione al prestatore di servizi, quest'ultimo non deve eseguire l'ordine immediatamente; al contrario, l'art. 8, paragrafo 4, del Regolamento parla esplicitamente di un effetto sospensivo sugli obblighi dell'*internet service provider*, a meno che non si versi in un caso d'esecuzione in via d'urgenza. Il prestatore di servizi deve, quindi, attendere un sostanziale nulla osta da parte dell'autorità giudiziaria notificata, che può anche essere tacito: l'ordine di produzione andrà, infatti, eseguito se non

²⁷ Art. 16, paragrafo 1, del Regolamento.

²⁸ Art. 4, paragrafo 2, lett. a) del Regolamento.

²⁹ Art. 4, paragrafo 2, lett. b) del Regolamento.

³⁰ Art. 8, paragrafo 1, del Regolamento.

³¹ Art. 8, paragrafo 2, del Regolamento. Il peso di quest'eccezione dipende naturalmente dal fatto che la transnazionalità, nella stragrande maggioranza dei casi, attiene esclusivamente al piano della singola prova digitale da acquisire, essendo, per tutto il resto, *purely domestic cases*.

dovesse pervenire alcun motivo di rifiuto entro dieci giorni dalla notificazione. Nelle more, comunque, l'*internet service provider* dovrà preservare quei dati, così da trovarsi nelle condizioni di eseguire l'ordine entro dieci giorni da quando perviene l'assenso dell'autorità giudiziaria notificata (o comunque alla scadenza del termine dato a quest'ultima per fare valere ragioni di rifiuto dell'ordine di produzione)³². In ipotesi d'urgenza, peraltro, l'autorità giudiziaria a cui è stato notificato l'ordine può, se decide di far valere un motivo di rifiuto, al più tardi entro quattro giorni dalla ricezione della notifica, notificare all'autorità di emissione e al destinatario la propria opposizione all'uso dei dati ovvero imporre un utilizzo dei dati solo alle condizioni da essa specificate; tuttavia, se in caso di rifiuto i dati sono già stati trasmessi all'autorità di emissione, quest'ultima cancella i dati o ne limita in altro modo l'uso oppure rispetta le condizioni d'impiego dei dati, nel caso in cui l'autorità di esecuzione abbia specificato condizioni³³.

Attraverso l'ordine europeo di conservazione, invece, non viene imposto ai fornitori di servizi di consegnare immediatamente i dati, bensì, si prescrive loro di preservarli, evitando che vengano definitivamente rimossi o alterati prima che le autorità possano richiederli. Il Regolamento stabilisce un periodo di conservazione dei dati di sessanta giorni³⁴.

Questo strumento è particolarmente utile nei casi in cui i dati dell'utente non occorrono subito, ma è possibile che diventino rilevanti per le indagini successivamente; oppure, altra ipotesi, è quella per cui l'autorità che procede con le investigazioni si trovi in attesa della previa autorizzazione di un giudice, qualora quest'ultima sia necessaria per la tipologia di dati di cui si intende chiedere la produzione (quindi, per i dati di contenuto e i dati di traffico, quando questi ultimi non vengano richiesti per la sola identificazione dell'autore del reato); in questi casi, inoltre, il Regolamento prevede anche la possibilità di estendere il periodo di conservazione di ulteriori trenta giorni³⁵.

Per l'ordine di conservazione il Regolamento non prevede limitazioni sull'autorità emittente, neppure per i dati di traffico e di contenuto; inoltre, non vi è notificazione all'autorità giudiziaria dello Stato in cui si trova lo stabilimento o il rappresentante del prestatore di servizi digitali. La ragione, evidentemente, risiede nella minore intrusività e lesività di questo strumento, posto che non vi è una divulgazione dei dati dell'utente, collocati presso i server dell'*internet service provider*, il quale, semplicemente, li "congela" in attesa di una – del tutto eventuale – futura richiesta di produzione. Anche per tali ragioni, un ordine di conservazione – non importa a quale tipologia di dati esso si riferisca – può essere emesso in presenza dei medesimi presupposti che rendono legittima l'emissione di un ordine di produzione per dati relativi agli abbonati e per dati di traffico richiesti per la sola identificazione dell'autore del reato.

Come si è accennato, il pacchetto normativo si compone, altresì di una Direttiva. Quest'ultima, che andrà recepita dagli Stati membri entro il 18 febbraio 2026, impone (*rectius*: imporrà) ai *providers* che operano nell'Unione – anche se sono stabiliti in Paesi terzi e indipendentemente dalla localizzazione dei loro server – di designare un proprio stabilimento, ovvero, alternativamente, di nominare un rappresentante legale all'interno dell'UE. Questi ultimi saranno i destinatari degli ordini di produzione e di conservazione e dovranno, quindi, riscontrare alle richieste provenienti dalle autorità giudiziarie dei Paesi

³² Art. 10, paragrafo 2, del Regolamento.

³³ Art. 10, paragrafo 4, del Regolamento.

³⁴ Art. 11, paragrafo 1, del Regolamento.

³⁵ Estensione temporale, su richiesta dell'autorità emittente, sempre prevista dall'art. 11, paragrafo 1, del Regolamento.

membri, dandovi esecuzione, consegnando i dati in loro possesso, suscettibili di configurarsi come prove elettroniche in un procedimento penale.

La Direttiva semplifica l'operato delle autorità giudiziarie nazionali e agevola l'acquisizione transfrontaliera della prova digitale, poiché rende esplicitamente non determinante il luogo in cui siano conservati i dati: se l'*internet service provider* è un prestatore di servizi all'interno dell'Unione, allora deve designare un proprio stabilimento o nominare un proprio rappresentante nel territorio UE³⁶.

Sempre secondo la Direttiva (art. 2, nn. 2 e 3), tale obbligo sorge quando l'*internet service provider* consente alle persone fisiche o giuridiche in almeno uno Stato membro di usufruire dei propri servizi, oppure se ha un collegamento sostanziale, basato su specifici criteri di fatto, con almeno uno Stato membro. Sul punto, specifica ulteriormente la Direttiva, che un collegamento sostanziale con uno Stato membro si considera esistente quando il fornitore di servizi ha una sede stabile in quello Stato; oppure, se non dispone di un vero e proprio stabilimento, il collegamento può comunque essere riscontrato, se il servizio ha un numero significativo di utenti o se le sue attività sono chiaramente rivolte verso quel Paese membro.

Presupposto di applicabilità del Regolamento, come è ovvio, è la transnazionalità della ricerca dell'*e-evidence*. Ciò significa che – in un caso diametralmente opposto – se l'*internet service provider* dovesse avere sede, stabilimento, o rappresentante nel Paese in cui si trova l'autorità investigativa che necessita dei dati, si applicherebbe la disciplina nazionale³⁷.

4. Una nuova frontiera per il mutuo riconoscimento nel settore penalistico

Si discute se gli ordini europei di conservazione e di produzione possano considerarsi operanti sulla base del principio del mutuo riconoscimento, lo stesso che orienta altri meccanismi di cooperazione giudiziaria in ambito UE, tra cui, in particolare, il mandato d'arresto europeo e l'ordine europeo d'indagine penale. Questo dibattito ha anche messo in dubbio la congruità della base legale su cui è stata, in un primo momento, avanzata la proposta di Regolamento e Direttiva e quella su cui è stata, successivamente, approvata la disciplina finale.

Secondo una sintetica definizione – che è certamente parziale e approssimativa, ma che deriva dallo sviluppo dello stesso principio in materia penale – il mutuo riconoscimento implica che a una decisione assunta da un'autorità giudiziaria in un Paese membro dell'Unione europea debbano essere dati riconoscimento e applicazione dall'autorità giudiziaria di un altro Stato membro, senza che quest'ultima possa opporre motivi di rifiuto al riconoscimento e/o all'esecuzione, se non per ragioni tassativamente indicate per i singoli strumenti di cooperazione giudiziaria³⁸.

La disciplina sugli ordini di produzione e conservazione va oltre questa dinamica, perché, come già si è ampiamente sottolineato, attraverso il suo schema procedimentale ordinario, consente all'autorità emittente dello Stato membro A di rivolgere l'ordine direttamente all'*internet service provider*, quindi a un soggetto privato, che ha il proprio

³⁶ Cfr. V. FRANSSEN, *Cross-border gathering of electronic evidence in the EU: towards more direct cooperation under the e-Evidence Regulation*, cit., p. 195.

³⁷ *Ibidem*.

³⁸ Cfr. J. R. SPENCER, *The Principle of Mutual Recognition*, in R. E. KOSTORIS (a cura di), *Handbook of European Criminal Procedure*, Cham, 2018, pp. 281-282.

stabilimento oppure che ha designato un proprio rappresentante legale – secondo quanto stabilito dalla Direttiva – in altro Paese membro dell'Unione (Stato B). Viene, dunque, a mancare l'interlocuzione con un'altra autorità giudiziaria, perché destinatario dell'ordine è direttamente il prestatore di servizi³⁹.

A questo proposito, è interessante confrontare gli ordini di produzione e conservazione con l'ordine europeo di indagine penale – strumento il cui utilizzo, sempre nel campo dell'acquisizione di prove, è già ampiamente consolidato nel panorama della cooperazione giudiziaria europea – al fine di sottolinearne le principali differenze.

Mediante l'OIE si consente a un'autorità giudiziaria di uno Stato membro di chiedere all'autorità giudiziaria di un altro Paese membro di compiere uno o più atti investigativi, come perquisizioni, sequestri o intercettazioni, oppure per ottenere prove già nella disponibilità delle autorità competenti dello Stato di esecuzione (il caso Encrochat è probabilmente il più importante esempio di ordine europeo d'indagine emesso per tale finalità⁴⁰). A differenza dell'ordine di produzione, che consente di ottenere dati direttamente da un fornitore di servizi, l'ordine europeo d'indagine richiede sempre l'intervento dell'autorità giudiziaria dello Stato di esecuzione.

Rispetto all'OIE, pertanto, gli ordini di produzione e conservazione determinano un passo ulteriore verso una cooperazione diretta e immediata tra autorità giudiziarie e fornitori di servizi privati, localizzati presso un Paese membro conformemente a quanto previsto dalla Direttiva; rappresentano, dunque, un fondamentale tassello nell'evoluzione della cooperazione giudiziaria in materia penale, nello specifico settore dell'acquisizione transfrontaliera della prova digitale, traendo ispirazione dalle forme di attuazione del principio del mutuo riconoscimento, già sperimentate con strumenti come l'OIE e il MAE, ma sviluppandole ulteriormente.

Nel corso dell'iter legislativo, peraltro, più voci hanno messo in dubbio che, così concepiti, gli ordini di produzione e conservazione fossero strumenti di mutuo riconoscimento; conseguentemente, incertezze erano state rilevate anche rispetto alla congruità dell'art. 82, paragrafo 1, lett. a) e d) TFUE, inizialmente assunto come base legale nella proposta della Commissione europea⁴¹. Invero, un argomento cardine nelle critiche risiedeva proprio nell'assenza di un'autorità giudiziaria coinvolta nel riconoscimento, poiché ciò condurrebbe all'adozione di un modello di «*direct public-private cooperation [that] cannot be framed as a form of judicial cooperation under EU law as foreseen in Article 82 of the TFEU*»⁴².

Le obiezioni appaiono parzialmente corrette. È certamente vero che la lett. d) del primo paragrafo dell'art. 82 TFUE, volto a facilitare la cooperazione tra le autorità giudiziarie degli Stati membri, è poco calzante rispetto a istituti per i quali, secondo lo schema procedimentale base, non è previsto l'intervento di un'autorità giudiziaria preposta al riconoscimento e all'esecuzione di una decisione giudiziaria, se non in limitate ipotesi.

³⁹ Cfr. S. TOSZA, *Mutual recognition by private actors in criminal justice? E-evidence Regulation and service providers as the new guardians of fundamental rights*, in *Common Market Law Review*, 2024, p. 155.

⁴⁰ CGUE, *Grande Chambre*, Sent. 30/04/2024, Causa C-670/22, M.N. (Encrochat).

⁴¹ Sul punto, v. E. SELLIER, A. WEYEMBERGH, *Criminal procedural laws across the European Union – A comparative analysis of selected main differences and the impact they have over the development of EU legislation*, Study requested by the LIBE committee of the EU Parliament, 2018, p. 31 (disponibile su europarl.europa.eu); altresì, M. BÖSE, *An assessment of the Commission's proposals on electronic evidence*, Study requested by the LIBE committee of the EU Parliament, 2018, p. 36 (disponibile su europarl.europa.eu).

⁴² S. CARRERA, M. STEFAN, V. MITSILEGAS, *Cross-border data access in criminal proceedings and the future of digital justice. Navigating the current legal framework and exploring ways forward within the EU and across the Atlantic*, in CEPS, 2020, p. 58.

Sulla scorta di tali considerazioni, la versione finale del Regolamento – senza addentrarsi in alcuna pericolosa specificazione – individua la propria base legale nell’art. 82, paragrafo 1, TFUE nella sua interezza.

Peraltro, le residuali perplessità sulla congruità complessiva dell’art. 82 TFUE – e, in particolare, sulla lett. a) del paragrafo 1 –, che fanno leva su una discussa riconducibilità degli istituti in esame al principio di mutuo riconoscimento, sono superabili. Infatti, come correttamente si è osservato, «*the principle of mutual recognition as a basis for cooperation in criminal matters, does not have a formal definition in the Treaty*»⁴³. Trattandosi, piuttosto, di un principio estremamente duttile – nato in origine per favorire la circolazione dei beni e delle merci – è assolutamente accettabile che si presti alle stesse evoluzioni cui è andato incontro proprio nel settore commerciale e in ambito civilistico, dove decisioni di un’autorità giudiziaria di un Paese membro sono già eseguibili dai soggetti privati di un altro Stato membro cui sono indirizzate. Pertanto, superata questa rigidità, disancorata da precise prescrizioni contenute nelle fonti di diritto primario eurounitarie, è indubbio che la disciplina introdotta con il Regolamento UE 1543/2023 ambisca a facilitare la circolazione e il riconoscimento delle decisioni giudiziarie dei Paesi membri; lo fa attraverso l’introduzione di due nuovi strumenti, il cui funzionamento si basa su una fiducia tra gli ordinamenti così elevata da non essere neppure necessario l’intervento di un’autorità giudiziaria in sede di riconoscimento. In questi termini, ne deriva la piena coerenza con l’art. 82, paragrafo 1, lett. a) TFUE.

Questi strumenti, dunque, transcendendo il modello classico di mutuo riconoscimento, adottano una forma di riconoscimento tacito strutturale, in cui l’efficacia della decisione giudiziaria straniera è presupposta e operativa *ab initio*, senza alcun coinvolgimento necessario dell’autorità giudiziaria dello Stato di esecuzione (quantomeno nelle ipotesi maggiormente incidenti dal punto di vista statistico).

L’intervento del legislatore europeo era particolarmente atteso e la fase di negoziazione del pacchetto legislativo è stata particolarmente lunga ed elaborata⁴⁴. Tuttavia, la semplificazione procedimentale porta con sé alcune criticità. Se da un lato offre maggiori possibilità di accesso ai dati elettronici necessari già nelle fasi preliminari delle indagini, con tempistiche certamente più celeri ed esiti di riscontro meno incerti, dall’altro pone nuove sfide in termini di bilanciamento tra efficienza investigativa e tutela dei diritti dei soggetti coinvolti.

5. Cifratura e decrittazione: criticità applicative del nuovo Regolamento

Le riflessioni esposte appaiono sufficienti a evidenziare come il Regolamento 2023/1543/UE costituisca certamente un passo significativo in materia di raccolta e trasmissione transfrontaliera delle prove digitali. Tuttavia, persistono criticità applicative non marginali, soprattutto con riferimento alla trasparenza e all’effettiva utilità operativa delle procedure di acquisizione, decifrazione e verifica dei dati oggetto di richiesta.

L’era digitale, tra le molteplici innovazioni, porta con sé innegabili vantaggi tecnici e operativi, come ad esempio la possibilità, già menzionata, di utilizzare protocolli di messaggistica crittografati. Numerose aziende private attive nel settore delle

⁴³ Cfr. S. TOSZA, *Mutual recognition by private actors in criminal justice? E-evidence Regulation and service providers as the new guardians of fundamental rights*, cit., p. 158.

⁴⁴ I passaggi chiave dell’iter legislativo sono disponibili sul [sito del Parlamento europeo](#).

telecomunicazioni hanno già sviluppato – o stanno perfezionando – meccanismi avanzati di cifratura e trasmissione dei dati con l'obiettivo di incrementare e rafforzare la sicurezza delle conversazioni tra gli utenti.

La crescente diffusione della cifratura nelle comunicazioni elettroniche, da un lato, rappresenta una garanzia imprescindibile per la tutela della riservatezza dei dati e della sicurezza informatica; dall'altro lato, introduce barriere tecniche che rendono complessa l'attività investigativa e di contrasto, come dimostrano in maniera emblematica i casi *SkyECC*⁴⁵ e *Encrochat*⁴⁶. In relazione a tali casi, le autorità giudiziarie europee hanno affrontato ostacoli, *in primis*, all'accesso e, *in secundis*, all'utilizzo ai fini dell'accertamento penale di tali comunicazioni protette.

I dispositivi elettronici di nuova generazione, infatti, integrano nativamente sistemi di cifratura per i dati memorizzati e molte applicazioni, scaricabili facilmente da un utente medio, impiegano protocolli *end-to-end* in grado di rendere l'intercettazione o l'estrazione di dati intellegibili tecnicamente complessa e di difficile realizzazione⁴⁷.

In uno scenario così variegato, lo squilibrio tra l'evoluzione tecnologica e gli strumenti giuridici di contrasto alla criminalità crea un divario evidente e incolmabile, con il rischio concreto di una notevole compromissione delle attività investigative. Ad ogni modo, ogni intervento in materia deve continuare a rispettare i principi fondamentali del giusto processo, primo fra tutti la presunzione di innocenza, cardine irrinunciabile dello Stato di diritto.

Sul punto risulta interessante esaminare nel dettaglio un considerando del Regolamento, in particolare il n. 20, che, in poche battute, sintetizza ed evidenzia un problema che resta irrisolto. Il dettato si apre con il seguente periodo «l'applicazione del presente regolamento non dovrebbe pregiudicare l'uso della cifratura da parte dei prestatori di servizi o dei loro utenti»⁴⁸.

Innanzitutto, la Commissione dimostra di essere pienamente cosciente del ruolo cruciale che la crittografia riveste tanto in un'ottica squisitamente economica – cioè con riguardo all'interesse dei prestatori di servizi a offrire sul mercato prodotti in grado di garantire la segretezza delle comunicazioni tra i privati – quanto di tutela dei diritti fondamentali e della sicurezza cibernetica dei cittadini, dei governi, dell'industria e, più in generale, della società.

Di contro, risulta problematica – sotto il profilo pratico – la clausola finale del considerando in esame, secondo la quale «i dati richiesti per mezzo di un ordine europeo di produzione o di un ordine europeo di conservazione dovrebbero essere forniti o conservati a prescindere dal fatto che siano criptati o meno. Tuttavia, il presente regolamento non dovrebbe stabilire alcun obbligo per i prestatori di servizi di decifrare i dati».

L'assenza di un obbligo di decifrazione a carico dei prestatori di servizi comporta un significativo *vulnus* sul piano probatorio. La mera trasmissione di un dato cifrato, non intellegibile o non tecnicamente decifrabile, rischia di svuotare di contenuto, e non poco, l'efficacia dell'EPO – ma lo stesso dicasi per l'EPrO –, riducendolo a una formalità priva di valore funzionale.

⁴⁵ Cass. Sez. Un., sent. 29 febbraio-14 giugno 2024, n. 23755 e Cass. Sez. Un., sent. 29 febbraio-14 giugno 2024, n. 23756.

⁴⁶ CGUE, *Grande Chambre*, Sent. 30/04/2024, Causa C-670/22, M.N. (*Encrochat*), cit.

⁴⁷ Sul punto vedi F. CARLI, *La crittografia: cos'è, come funziona e perché è alleata della sicurezza informatica*, in *Network Digital* 360, 2022.

⁴⁸ Considerando 20 del Regolamento.

Ci si chiede allora su quali strumenti e metodologie debba fare affidamento l'autorità inquirente per accedere ai contenuti protetti: sebbene il pubblico ministero possa contare, di norma, su risorse – economiche e di “forza-lavoro” – notevolmente o comunque di misura superiore rispetto a quelle proprie della difesa, la questione dell'accessibilità, lettura e verificabilità delle prove digitali resta centrale.

In particolare, tra le varie problematiche, una sembra primeggiare, soprattutto in considerazione di quanto sopraindicato in termini di preservazione della presunzione di innocenza: si tratta del diritto della difesa di verificare l'integrità e la genuinità del dato digitale, specialmente in assenza – rispetto all'accusa – di un'analoga capacità tecnica di analisi e decodifica.

La Corte di Giustizia dell'Unione Europea, nella già citata sentenza *Encrochat* del 30 aprile 2024⁴⁹, ha ribadito che, sebbene la cooperazione giudiziaria si fondi sul principio di fiducia reciproca tra gli Stati membri, resta ferma la responsabilità dei giudici nazionali di garantire che le prove digitali acquisite nel contesto transfrontaliero rispettino pienamente i diritti della difesa e gli *standard* del giusto processo. La Corte ha sottolineato la necessità estrema di garantire almeno dei livelli minimi procedurali, che implicino la produzione di relazioni tecniche dettagliate, certificazioni di autenticità e documentazione dell'intera catena di custodia dei dati, al fine di consentire agli accusati e ai loro difensori un controllo effettivo sulla legittimità e sulla genuinità della prova digitale.

Più nello specifico, la CGUE ha chiarito che un OEI finalizzato alla trasmissione di prove già detenute dallo Stato di esecuzione – nel caso di specie la Francia – può essere emesso anche dal pubblico ministero purché sussistano specifiche condizioni, le quali non necessariamente devono essere una riproduzione integrale di quelle previste per la raccolta delle prove nello Stato di emissione.

Ciò che rileva – e costituisce proprio uno degli aspetti più significativi del provvedimento in esame relativamente al tema del presente paragrafo – è la necessità che sia sempre garantita la possibilità di un controllo giurisdizionale successivo sul rispetto dei diritti fondamentali delle persone coinvolte. In questa prospettiva, la Corte sembra orientarsi verso un equilibrio tra le esigenze di efficienza investigativa e la tutela giurisdizionale, riconoscendo come irrinunciabile – anche in assenza di un vaglio preventivo – almeno un controllo *ex post* sul rispetto dei diritti fondamentali.

Tornando all'ordine europeo di produzione, laddove non sia possibile prevedere un controllo preventivo sul materiale acquisito, è imprescindibile che all'imputato sia riconosciuta la possibilità di esercitare un controllo successivo. In linea con quanto affermato dalla CGUE nella pronuncia sopra richiamata, tale controllo deve includere la possibilità di sottoporre a nuova verifica le operazioni di decrittazione e di valutare in modo autonomo la catena di custodia dei dati.

In tal senso, risulta particolarmente rilevante quanto affermato dalla Corte europea dei diritti dell'uomo nella sentenza *Yuksel Yalcinkaya c. Turchia*⁵⁰, del 2023, secondo la quale la «la violazione del diritto alla conoscenza è compensata dalla valutazione successiva del contenuto probatorio con altre garanzie». Seppur maturato in un diverso contesto processuale, l'orientamento della Corte EDU risulta perfettamente coerente con l'impostazione della CGUE nella sentenza C-670/22: in assenza di un controllo preventivo sull'acquisizione probatoria, è essenziale garantire alla difesa un controllo successivo pieno,

⁴⁹ CGUE, *Grande Chambre*, Sent. 30/04/2024, Causa C-670/22, M.N. (*Encrochat*), cit.

⁵⁰ Corte eur. [GC], 26 settembre 2023, *Yuksel Yalcinkaya c. Turchia*. ric. 15669/20.

effettivo e tecnicamente idoneo, finalizzato alla verifica dell'integrità, autenticità e affidabilità del dato digitale.

Alla luce delle criticità evidenziate e degli orientamenti giurisprudenziali riportati, ci si potrebbe legittimamente interrogare sull'opportunità di prevedere – quantomeno in presenza di determinate garanzie giudiziarie – un obbligo, e non una mera attività discrezionale, a carico dei prestatori di servizi, di fornire alle autorità richiedenti le chiavi di cifratura o altri strumenti tecnici idonei a rendere accessibili in maniera effettiva i dati richiesti. È certo che una simile scelta normativa, sebbene suscettibile di influire negativamente sulla competitività tra aziende e sull'attrattività commerciale delle piattaforme digitali – soprattutto di quelle che fanno della cifratura un elemento distintivo della propria affidabilità – avrebbe potuto contribuire in modo più efficace alla velocità di intervento e al riequilibrio tra le parti processuali, rafforzando la concretezza del principio di parità delle armi.

In particolare, l'accesso diretto ai dati cifrati, reso possibile dall'ipotetico obbligo – non introdotto – avrebbe evitato alle autorità giudiziarie costosi e complessi procedimenti di decrittazione, con un impatto positivo in termini di risparmio di risorse e di efficienza investigativa. Allo stesso tempo, la trasmissione alla difesa della medesima chiave di cifratura – o comunque di strumenti tecnici equivalenti – le avrebbe consentito di decifrare autonomamente i contenuti o di verificare *ex post*, in modo pieno e indipendente, la correttezza e la completezza delle operazioni di decrittazione eseguite dall'accusa.

Forse, ed è soltanto un'idea di stimolo per una riflessione futura anche in vista di ciò che accadrà in seguito all'entrata in vigore del Regolamento, l'introduzione di un siffatto obbligo avrebbe permesso di superare molte delle criticità segnalate, restituendo equilibrio al confronto processuale e rafforzando, in modo concreto ed effettivo, la tutela dei diritti fondamentali coinvolti.

6. I prestatori di servizi digitali nello scacchiere della cooperazione giudiziaria

L'inedito ruolo assunto dai *digital service providers* nella disciplina sugli ordini di produzione e conservazione è il presupposto per la formulazione di una serie di interrogativi inediti nel panorama della cooperazione giudiziaria.

I fornitori di servizi digitali, che nella stragrande maggioranza dei casi sono dei veri e propri colossi (Alphabet, Apple, Meta, Microsoft, Twitter, ecc.), sono dei soggetti privati; dunque, puntano, prima di tutto, alla crescita delle proprie attività e alla massimizzazione dei profitti; non nascono come autorità pubbliche deputate alla tutela di interessi della collettività. È, altresì, possibile affermare che – in linea di principio – rispetto al procedimento penale che si svolge nello Stato d'emissione dell'ordine essi siano dei soggetti terzi.

Il Regolamento sugli ordini di produzione e conservazione della prova digitale rimette in discussione tutto ciò, essendosi in proposito parlato – già a partire dalla Proposta della Commissione europea – di «*re-allocation of protective functions*»⁵¹. Agli internet service providers, invero, quali destinatari ed esecutori degli ordini, spetta anche il compito di verificare che

⁵¹ M. BÖSE, *An assessment of the Commission's proposals on electronic evidence*, Study requested by the LIBE committee of the EU Parliament, cit., p. 41.

siano rispettati i diritti fondamentali dei soggetti cui la richiesta si riferisce, spingendo gli *internet service providers* «*more towards the public sphere, constituting a true paradigm shift*»⁵².

Ebbene, ci si deve in primo luogo interrogare sulla capacità dei prestatori di servizi digitali di offrire un'effettiva tutela dei diritti fondamentali, posto che, a tutti gli effetti, essi divengono «*il perno centrale del sistema*»⁵³. Come verrà meglio esplicitato in seguito, è possibile affermare che le scelte tradottesi nella versione definitiva del Regolamento offrono delle prospettive di tutela – senza trascurare le esigenze di efficienza del sistema – ben più appaganti delle soluzioni alternative avanzate nel corso dell'*iter* legislativo.

La Commissione europea, nella sua proposta, era orientata verso l'attribuzione di un ruolo estremamente marginale all'autorità giudiziaria del Paese membro in cui si trova l'*internet service provider*, non contemplando neppure il ricorso alla notificazione. Il Consiglio aveva edulcorato questa impostazione, prevedendo una notificazione, priva di effetti sospensivi, per le richieste di dati di contenuto riguardanti soggetti non residenti nello Stato d'emissione. Si discostava moltissimo, invece, la soluzione offerta dal Parlamento europeo, mosso dall'idea, marcatamente in antitesi, per cui «*the responsibility for protecting human rights should not be shifted from states to service providers*»⁵⁴. Proprio a causa di ciò, si proponeva un utilizzo massiccio dello strumento della notificazione, per ordini di produzione relativi a ogni tipologia di dato e persino per gli ordini di conservazione; si differenziava, tuttavia, tra notificazioni con effetti sospensivi degli obblighi dei prestatori di servizi e notificazioni prive di tali effetti. La versione finale del Regolamento, come spesso accade, rappresenta un accomodamento tra queste posizioni antitetiche, ma opta anche per un regime astrattamente bilanciato alla luce di alcune considerazioni.

Rispetto a questo tema, infatti, è fondamentale sottolineare che l'Irlanda si trova in regime di *opt-in* per il Regolamento e la Direttiva sull'*e-evidence*. Ebbene, il cuore del problema risiede proprio in ciò: se la quasi totalità dei più importanti *internet service providers* ha stabilito la propria sede nello stesso Paese, cioè proprio l'Irlanda, principalmente per ragioni fiscali, un controllo da parte dell'autorità giudiziaria di questo Stato, come autorità sempre e comunque notificata, su ogni richiesta e per tutte le tipologie di dati, sarebbe assolutamente inefficace oltre che inefficiente.

Invero, già da alcuni numeri del sistema attuale, ancora basato sulla cooperazione volontaria da parte dei principali *internet service providers*⁵⁵, si ricava che il numero di richieste di trasmissione dati ogni anno è elevatissimo, nell'ordine delle decine di migliaia⁵⁶; soprattutto, si evince che le richieste hanno principalmente ad oggetto dati diversi dai dati di contenuto e che destinatari del 90% delle richieste sono cinque grandi fornitori di servizi

⁵² S. TOSZA, *Internet service providers as law enforcers and adjudicators. A public role for private actors*, in *Computer Law & Security Review*, 2021, 43, p. 12.

⁵³ O. POLLICINO, M. BASSINI, *La proposta di Regolamento e-Evidence: osservazioni a caldo e possibili sviluppi*, in *Medialaws.net*, 26 ottobre 2018, p. 11.

⁵⁴ T. CHRISTAKIS, *From Mutual Trust to the Gordian Knot of Notifications. The EU e-evidence Regulation and Directive*, cit., p. 189. L'autore ha svolto un'esaustiva analisi di tutte le differenti proposte susseguitesi nel corso del complesso *iter* legislativo in punto di notificazione degli ordini di produzione ad autorità giudiziaria diversa da quella emittente; al suo ricchissimo contributo, dunque, si rinvia per ogni approfondimento.

⁵⁵ Per la consultazione dei quali si rinvia alle pagg. 13-15 dell'*impact assessment* della Commissione europea (v. nota n. 14).

⁵⁶ Sul punto, v. T. CHRISTAKIS, *From Mutual Trust to the Gordian Knot of Notifications. The EU e-evidence Regulation and Directive*, cit., pp. 194-195, che, richiamando i dati forniti da Europol, SIRIUS EU Digital Evidence Situation Report: Cross-Border Access to Electronic Evidence, The Hague, 20 December 2019, mette in luce che «*in 2018 Facebook received and examined a total of 53.841 data requests, Google received 47.011, Apple 43.480 and Microsoft 22.919*».

digitali, già precedentemente citati, tutti localizzati nella regione di Dublino. Ipotizzando che i numeri rimangano invariati anche in futuro ed essendo verosimile che questi prestatori di servizi indichino i propri stabilimenti in Irlanda anche ai fini della Direttiva, ne deriverebbe un volume di ordini di produzione notificati alla sola autorità giudiziaria irlandese assolutamente non compatibile con la capacità di effettuare un vaglio degli stessi a tutela dei diritti fondamentali dei soggetti coinvolti⁵⁷.

Il rischio connesso a una scelta legislativa che preveda l'obbligatorietà della notificazione per ogni tipologia di dato – con conseguente esame degli ordini da parte dell'autorità giudiziaria notificata – diverrebbe quello di una trasformazione della tutela dei diritti fondamentali dei soggetti coinvolti in un mero manifesto ideologico, un simulacro, del tutto avulso dalla realtà fattuale. Al contrario, è il contesto in cui si inserisce il pacchetto legislativo sull'*e-evidence* a consentire di affermare che è proprio il singolo prestatore di servizi a trovarsi nella posizione migliore per offrire una tutela effettiva dei suoi utenti e dei loro dati, eventualmente attraverso l'istituzione di unità operative deputate all'esecuzione o al rifiuto all'esecuzione degli ordini di produzione e conservazione. Dunque, è una scelta bilanciata quella di prevedere un intervento dell'autorità giudiziaria dello Stato membro in cui ha sede il prestatore di servizi, quale autorità notificata, solo per quelle richieste che si contraddistinguono per elevata intrusività, cioè, principalmente, per le ipotesi che riguardano acquisizioni di dati di contenuto⁵⁸.

Per quanto strettamente connessa a quella fin qui analizzata, è questione distinta quella attinente al tipo di approccio che il Regolamento adotta nei confronti degli *internet service providers*, dopo avere posto in capo a questi ultimi una funzione pubblicistica di particolare sensibilità. Anche in questo caso, anticipando le conclusioni, si deve osservare che, proprio su questo terreno, si riscontrano alcuni aspetti problematici all'interno del Regolamento, i quali rischiano di compromettere il complessivo sistema di tutela, in nome dell'efficienza "a ogni costo".

Come autorevole dottrina ha fin da subito messo in luce, invero, il Regolamento trasmette chiaramente l'idea che la cooperazione tra autorità giudiziaria emanante e prestatore di servizi digitali non avvenga affatto su un piano paritario⁵⁹.

Il primo elemento da cui ciò si evince è il controverso art. 15 del Regolamento, che si compone di due paragrafi. Il primo paragrafo istituisce un sistema di sanzioni pecuniarie "effettive, proporzionate e dissuasive", azionabili in caso di violazione delle norme sull'esecuzione degli ordini di produzione e conservazione; la determinazione di queste sanzioni è, peraltro, rimessa ai singoli Stati membri, con la sola previsione di un tetto massimo del 2% del fatturato mondiale annuo del prestatore di servizi. Il secondo paragrafo, all'opposto, crea una sorta di scudo per gli *internet service providers*, i quali non sono ritenuti

⁵⁷ Autorevolmente sul punto S. TOSZA, *Mutual recognition by private actors in criminal justice? E-evidence Regulation and service providers as the new guardians of fundamental rights*, cit., secondo cui, «if the volume of issued orders becomes significant, Irish authorities may simply not have the necessary resources to examine all of the transmitted orders» (p. 151); l'Autore sottolinea, altresì, che «if notification was to be made obligatory for any type of data, it would simply insert even more additional bureaucracy without any real effect on the rights of affected persons» (p. 159).

⁵⁸ In senso critico, M. DANIELE, *L'acquisizione delle prove digitali dai service provider: un preoccupante cambio di paradigma nella cooperazione internazionale*, in *Revista Brasileira de Direito Processual Penal*, 2019, 3, pp. 1290-1291, il quale sostiene che la natura privatistica degli *internet service providers* e la loro esigenza di tutelare i propri interessi non si riesca bene a coniugare con il dovere di agire come organi pubblici in posizione di imparzialità, essendo gli stessi, in linea di principio, del tutto estranei all'esito del vaglio delle richieste.

⁵⁹ Il riferimento, sul punto, è a V. MITSILEGAS, *The privatisation of mutual trust in Europe's area of criminal justice: The case of e-evidence*, in *Maastricht Journal of European and Comparative Law*, 2018, p. 263 ss.

responsabili per eventuali pregiudizi causati agli utenti o ai terzi, che derivino esclusivamente da un'ottemperanza in buona fede a un ordine di produzione o di conservazione.

Vi è un ulteriore dato, di natura strettamente linguistica ma altrettanto emblematico, che emerge non tanto dalla versione in lingua italiana del Regolamento, bensì da quella inglese: l'autorità giudiziaria notificata, quindi l'autorità giudiziaria dello Stato in cui si trovano stabilimento o rappresentante del prestatore di servizi – come era stato evidenziato in dottrina ben prima dell'approvazione definitiva del Regolamento⁶⁰ – non è denominata *executing authority*, ma *enforcing authority*, così creandosi le basi per una netta differenza di approccio alla cooperazione, rispetto a quanto previsto per l'ordine europeo d'indagine penale.

Insomma, si espone certamente a critiche un sistema che, da un lato, attribuisce a degli enti privati una funzione di protezione dei diritti fondamentali dei soggetti coinvolti e, dall'altro lato, ponendoli in una posizione di subordinazione, li rende passibili di sanzioni economiche, in ipotesi di rifiuto all'esecuzione non gradite all'autorità emanante.

Vi è poi da notare che tra prestatore di servizi e autorità giudiziaria notificata vi è una parziale divergenza dei motivi di rifiuto all'esecuzione, indicati, rispettivamente agli artt. 10 e 12 del Regolamento. Il riferimento critico, nello specifico, è rivolto al mancato inserimento delle (manifeste) violazioni di un diritto fondamentale sancito dall'art. 6 TUE e dalla Carta di Nizza tra le ragioni di rifiuto che può fare valere il prestatore di servizi. Peraltro, questa specifica ragione di rifiuto era presente nell'originaria Proposta della Commissione europea, ma è stata successivamente rimossa dal testo e oggi figura soltanto tra i motivi di rifiuto che può fare valere l'*enforcing authority*⁶¹. Anche questo punto del Regolamento, dunque, appare assolutamente distonico rispetto alla funzione attribuita ai prestatori di servizi.

Al contrario, rappresenta un elemento di grande plauso l'inserimento dell'interferenza con le immunità o i privilegi o con le limitazioni della responsabilità penale relative alla libertà di stampa o alla libertà di espressione nello Stato d'esecuzione come comune motivo di rifiuto. L'introduzione è parecchio opportuna alla luce delle derive autoritarie (già in atto o allo stato soltanto temute) in alcuni Paesi membri dell'UE, nei quali potrebbe divenire rischiosa anche la sola espressione di pensieri politicamente dissenzienti su account social, attraverso l'uso di pseudonimi. A causa degli stessi timori, era di assoluto interesse la proposta del Parlamento europeo (non confluita nel testo finale) d'inserire un meccanismo di trasmissione dell'ordine, da parte del prestatore di servizi all'autorità giudiziaria del Paese in cui lo stesso ha sede, con effetti sospensivi dei propri obblighi d'esecuzione, nell'eventualità in cui autorità giudiziaria emittente fosse quella di uno Stato membro nei confronti del quale fosse in corso una procedura *ex art. 7 TUE*⁶².

7. Conclusioni

Il fenomeno della c.d. digitalizzazione del crimine e la crescente dematerializzazione della prova nel procedimento penale rappresentano due traiettorie convergenti che hanno

⁶⁰ M. CORHAY, *Private Life, Personal Data Protection and the Role of Service Providers: The EU E-evidence proposal*, cit., p. 461.

⁶¹ Cfr. S. TOSZA, *Mutual recognition by private actors in criminal justice?*, cit., pp. 151-152.

⁶² Sul punto, v. T. CHRISTAKIS, *From Mutual Trust to the Gordian Knot of Notifications*, cit., p. 196.

imposto una revisione articolata e profonda degli strumenti di cooperazione giudiziaria in ambito europeo.

Il Regolamento UE 2023/1543 costituisce una svolta normativa di particolare interesse, destinata a incidere in modo strutturale sul rapporto tra investigazione e spazio digitale. L'introduzione dei due nuovi istituti – ordine europeo di produzione e ordine europeo di conservazione – segna il superamento, o quantomeno un aggiornamento, delle tradizionali logiche di assistenza giudiziaria. Ne deriva la nascita di un nuovo modello, diretto e immediato, che mira a garantire una risposta più efficace alle sfide poste dalla criminalità in rete.

Sul piano sistematico, le novità sono molteplici.

Innanzitutto, i nuovi strumenti coinvolgono in maniera diretta nella giustizia penale transfrontaliera dei soggetti privati, ovvero i *digital service providers*. La loro posizione di terzietà rispetto al procedimento penale viene, dunque, ridiscussa, a causa dell'assunzione di un ruolo di particolare delicatezza, derivante dall'attribuzione di una funzione di carattere pubblicistico, che integra il fulcro del sistema di cooperazione. Il sistema così sviluppato, altresì, segna un inedito mutamento di paradigma nel funzionamento della cooperazione giudiziaria orizzontale nel settore penalistico, fondata sul principio (e sul metodo) del mutuo riconoscimento.

In secondo luogo, si assiste a una ridefinizione degli equilibri tra efficienza dell'azione investigativa e tutela dei diritti fondamentali dell'indagato, in linea con i principi elaborati dalla giurisprudenza della CGUE e della Corte EDU in materia di accesso ai dati personali, riservatezza delle comunicazioni e garanzie difensive. In particolare, il rischio di una compressione eccessiva del diritto al contraddittorio e della parità delle armi impone di monitorare con attenzione le ricadute del nuovo impianto sul piano processuale.

Alcune scelte appaiono meno convincenti. Tra queste, l'assenza di un obbligo per i prestatori di servizi di consegnare le chiavi di cifratura rischia di pregiudicare l'efficacia degli ordini emessi, vanificando la finalità stessa della disciplina. In un contesto in cui le comunicazioni cifrate rappresentano il centro degli interessi, sicuramente di quelli economici, di molte piattaforme, tale omissione costituisce un *vulnus* rilevante che potrebbe depotenziare l'intero sistema.

In conclusione, se da un lato il Regolamento sulla prova digitale delinea un modello potenzialmente virtuoso e 'al passo coi tempi', dall'altro lato resta ancora incerto il bilanciamento effettivo tra le esigenze di celerità ed efficienza investigativa e la tutela dei diritti fondamentali dei soggetti coinvolti, primo fra tutti il diritto di difesa. Sarà il futuro – e, auspicabilmente, anche l'intervento chiarificatore delle Corti nazionali e sovranazionali – a stabilire se tale ambizioso impianto si consoliderà come strumento di cooperazione efficace al pari, ad esempio, del MAE ovvero anche dell'OEI, o si rivelerà un compromesso fragile tra istanze, purtroppo, inevitabilmente divergenti.

ABSTRACT: *Digitalisation of Crime and Judicial Cooperation: the European Production and Preservation Order Framed by the E-Evidence Regulation*

The notion of digitalisation of offences captures a paradigm shift in the criminal matters: digital tools are no longer merely instrumental to specific offences, but increasingly permeate a wide range of traditional criminal behaviours. In this framework, digital evidence

has become central, yet its peculiar features – volatility, cross-border dispersion, dependence on service providers – challenge the effectiveness of traditional mechanisms of judicial cooperation. Even the European Investigation Order has proved insufficient. Regulation (EU) 2023/1543, introducing the European Production Order (EPO) and the European Preservation Order (EPrO), constitutes a significant step towards a more direct and efficient model of cooperation. Nevertheless, unresolved issues remain – most notably the absence of decryption obligations for service providers and the attribution to the latter of a fundamental rights protection role – raising concerns on the actual balance between investigative efficiency and the protection of fundamental rights.