Il Regolamento UE sulla E-Evidence

di Renzo Di Pietra[1]

Il 28 luglio 2023 sono stati pubblicati sulla Gazzetta Ufficiale dell'Unione europea i due atti preposti alla regolamentazione dell'accesso "transfrontaliero" delle prove digitali (c.d. E-Evidence). Il regolamento (UE) 2023/1543 relativo agli ordini europei di produzione e di conservazione di prove elettroniche nei procedimenti penali è entrato in vigore subito, il 18 agosto 2023. La direttiva (UE) 2023/1544, recante norme armonizzate sulla designazione di stabilimenti designati e sulla nomina di rappresentanti legali ai fini dell'acquisizione di prove elettroniche nei procedimenti penali, dovrà essere recepita il 18 febbraio del 2026.

Sommario

1 https://www.sicurezzaegiustizia.com/renzo-di-pietra/

1) L'accesso transfrontaliero delle prove digitali

Al termine di un percorso lungo 5 anni, caratterizzato da un'intensa opera di collaborazione tra tutte le parti coinvolte, hanno visto luce, con la pubblicazione sulla Gazzetta Ufficiale dell'Unione europea del 28 luglio 2023, L. 191, due atti preposti alla regolamentazione dell'accesso "transfrontaliero" delle prove digitali (c.d. E-Evidence):

- la direttiva (UE) 2023/1544 del Parlamento europeo e del Consiglio, del 12 luglio 2023, recante norme armonizzate sulla designazione di stabilimenti designati e sulla nomina di rappresentanti legali ai fini dell'acquisizione di prove elettroniche nei procedimenti penali;
- e il regolamento (UE) 2023/1543 del Parlamento europeo e del Consiglio, del 12 luglio 2023, relativo agli ordini europei di produzione e di conservazione di prove elettroniche nei procedimenti penali.

Il termine fissato dalla direttiva per il recepimento è il 18 febbraio del 2026, mentre il Regolamento entrerà in vigore a far data dal 18 agosto dello stesso anno.

I regolamenti e le direttive sono atti normativi di diritto derivato adottabili dall'Unione.

Consistono in atti tipici, in quanto disciplinati rispettivamente dai paragrafi 1 e 2 dell'art. 288 [1] del TFUE (trattato sul funzionamento dell'Unione europea), possono essere emanati come atti legislativi e provocano effetti giuridici obbligatori, seppur parzialmente diversi, nei confronti dei loro destinatari.

Il Regolamento, infatti, ha portata generale, è vincolante in tutti i suoi elementi ed è direttamente applicabile negli Stati membri dell'Unione senza la necessità (anzi, vietando) l'emanazione di un atto recettivo da parte dello Stato.

La Direttiva invece, si caratterizza per la sua portata meno vincolante, obbliga il destinatario (o i destinatari) in termini di obiettivi da raggiungere per il tramite della stessa e, di norma, fissa il termine entro il quale questi debbano essere raggiunti, lasciando agli Stati membri ampio margine di discrezionalità per quanto concerne le modalità e gli strumenti da adoperare per il loro raggiungimento (es. atto legislativo nazionale, regolamento, ecc.).

La base giuridica del Regolamento sulle prove elettroniche, si poggia sull'articolo 82 paragrafo 1 del TFUE, relativo alla cooperazione giudiziaria in materia penale, che dispone:

"1. La cooperazione giudiziaria in materia penale nell'Unione è fondata sul principio di riconoscimento reciproco delle sentenze e delle decisioni giudiziarie e include il ravvicinamento delle disposizioni legislative e regolamentari degli Stati membri nei settori di cui al paragrafo 2 e all'articolo 83. Il Parlamento europeo e il Consiglio, deliberando secondo la procedura legislativa ordinaria, adottano le misure intese a: a) definire norme e procedure per assicurare il riconoscimento in tutta l'Unione di qualsiasi tipo di sentenza e di decisione giudiziaria; b) prevenire e risolvere i conflitti di giurisdizione tra gli Stati membri; c) sostenere la formazione dei magistrati e degli operatori giudiziari; d) facilitare la cooperazione tra le autorità giudiziarie o autorità omologhe degli Stati membri in relazione all'azione penale e all'esecuzione delle decisioni."

Come sottolineato dalla Commissione nella valutazione d'impatto che ha accompagnato le proposte

di Regolamento, <<l'articolo 82, paragrafo 1, specifica che la cooperazione giudiziaria in materia penale deve basarsi sul principio del riconoscimento reciproco. Tale base giuridica si applicherebbe all'eventuale legislazione in materia di cooperazione diretta con i prestatori di servizi, nell'ambito della quale l'autorità dello Stato membro di emissione si rivolgerebbe direttamente a un'entità (il prestatore di servizi) nello Stato di esecuzione imponendole di assolvere a determinati obblighi. Ciò introdurrebbe una nuova dimensione nel riconoscimento reciproco, che va oltre la cooperazione giudiziaria tradizionale nell'Unione, attualmente basata su procedure che coinvolgono due autorità giudiziarie, una nello Stato di emissione e l'altra nello Stato di esecuzione>>. [0]

1.1) Cenni sulla Direttiva

La direttiva costituisce uno strumento essenziale ai fini dell'applicazione del futuro regolamento relativo agli ordini europei di produzione e di conservazione di prove elettroniche in materia penale, in quanto è volta a definire le norme concernenti la nomina dei rappresenti legali dei prestatori di servizi, le cui figure assurgeranno al ruolo di incaricati a ricevere e rispondere a tali ordini. La creazione di tali figure si è rivelata necessaria a causa della mancanza di un obbligo giuridico generale in capo ai prestatori di servizi non UE di essere fisicamente presenti nell'Unione nonostante prestino servizi al suo interno.

Il presente articolo, si propone di prendere in esame i profili più significativi del Regolamento di maggior impatto nei confronti del prestatore di servizi, legati all'accesso transfrontaliero della prova digitale.
Nel correlato articolo "Il regolamento E-Evidence – I principali impatti per i TELCO", si forniscono alcune valutazioni riguardanti gli impatti del Regolamento verso gli Operatori di Telecomunicazioni.

2) I lavori della Commissione

Il principale obiettivo perseguito dai lavori della Commissione che ha portato al termine dell'iter legislativo alla promulgazione dei due su citati atti, è quello richiesto a gran voce dai ministri della giustizia e degli affari interni per il Consiglio GAI e dai rappresentanti delle altre istituzioni dell'Unione, di poter consentire alle Autorità Giudiziarie di procedere agevolmente e velocemente all'accesso delle prove digitali, che rivestono particolare importanza per combattere le gravi forme di criminalità e del terrorismo, tema da sempre ritenuto di primaria importanza e stimolato ulteriormente dagli attentati di Bruxelles del 2016.
La Commissione, partendo dal presupposto che l'accesso alle prove elettroniche da parte delle Autorità Giudiziarie dell'Unione, allo stato attuale, si riveli un processo lungo e complicato (e spesso infruttuoso) data la collocazione delle stesse in un altro paese membro, sommato al fatto che lo siano anche le sedi dei prestatori di servizi che le detengono (in alcune ipotesi in paesi terzi), ha individuato la necessità di porre in essere un processo che, viceversa, necessiti di maggiore velocità e flessibilità.

Nel contesto attuale, infatti, l'acquisizione delle prove elettroniche da parte delle Autorità Giudiziarie risulta esperibile per il tramite di una procedura farraginosa, in quanto soggetta ad una disciplina disorganica e frammentata, causata dalla numerosità delle norme attualmente vigenti in materia di cooperazione giudiziaria (vedasi ad esempio OEI, Convenzione di Bruxelles in materia di assistenza giudiziaria del 2000, Rogatoria, ecc.).
Inoltre, l'assenza di un obbligo legale armonizzato circa i tempi di conservazione (c.d. data retention) di svariate tipologie di dati, consente ai prestatori di servizi di poter cancellare quelli in loro possesso nel minor tempo possibile, rendendo più difficoltosa la raccolta delle prove da parte delle Autorità Giudiziarie nel contesto di un procedimento penale.
Infatti, il più delle volte, tali tempistiche (spesso arbitrariamente adottate dai prestatori dei servizi) si rilevano non compatibili con il ricorso agli ordinari istituti di cooperazione giudiziaria.
Nell'aprile 2018, a seguito delle richieste del Consiglio europeo di migliorare i processi di acquisizione delle prove elettroniche, convogliandoli all'interno di una disciplina olistica (in luogo di quella attuale, come già evidenziato, frammentata ed eterogenea) la Commissione ha proposto, al fine di facilitare e velocizzare l'accesso, che quest'ultimo potesse essere espletato indipendentemente dall'ubicazione dei dati e dello stabilimento del prestatore che fornisce servizi nell'ambito dell'Unione Europea, prevedendo nuove norme volte a consentire alle Autorità Giudiziarie di un paese UE, di richiedere direttamente l'accesso alle prove elettroniche conservate da qualsiasi prestatore di servizi che operi nell'Unione europea, senza passare per l'Autorità Giudiziaria del Paese di esecuzione, favorendo così un meccanismo agile e soprattutto veloce [0].
La normativa proposta era composta da due atti legislativi:

1. un regolamento relativo agli ordini europei di produzione e di conservazione di prove elettroniche;
2. una direttiva recante norme armonizzate sulla nomina di rappresentanti legali ai fini dell'acquisizione di prove elettroniche.

3) Cosa sono le prove elettroniche?

Stando alla definizione del Consiglio Europeo per prove elettroniche si intendono l'insieme dei dati digitali utilizzati per indagare e perseguire i reati.
Tali prove includono:

- e-mail;
- SMS o contenuti provenienti dalle applicazioni di messaggistica;
- contenuti audiovisivi;
- informazioni sull'account online degli utenti.

Questi dati possono essere utilizzati per identificare una persona od ottenere maggiori informazioni sulle sue attività.

La definizione di "prova elettronica", inoltre, si ravvisa nello stesso Regolamento, essendo questa

contenuta nell'art. 3 (Definizioni) al paragrafo 8, mentre nei successivi paragrafi (da 9 a 12) ne sono disciplinati i dettagli:

8) «prove elettroniche»: i dati relativi agli abbonati, i dati sul traffico o i dati relativi al contenuto conservati in formato elettronico da o per conto di un prestatore di servizi al momento della ricezione, di un certificato di ordine europeo di produzione (EPOC) o di un certificato di ordine europeo di conservazione (EPOC-PR);

9) «dati relativi agli abbonati»: i dati detenuti da un prestatore di servizi relativi all'abbonamento ai suoi servizi, riguardanti:

a) l'identità di un abbonato o di un cliente, come il nome, la data di nascita, l'indirizzo postale o geografico, i dati di fatturazione e pagamento, il numero di telefono o l'indirizzo e-mail forniti;

b) il tipo di servizio e la sua durata, compresi i dati tecnici e i dati che identificano le misure tecniche correlate o le interfacce usate dall'abbonato o dal cliente o a questo fornite al momento della registrazione o dell'attivazione iniziale e i dati connessi alla convalida dell'uso del servizio, ad esclusione di password o altri mezzi di autenticazione usati al posto di una password, forniti dall'utente o creati a sua richiesta;

10) «dati richiesti al solo scopo di identificare l'utente»: gli indirizzi IP e, se necessario, le porte sorgenti e le marche temporali pertinenti, vale a dire la data e l'ora, o gli equivalenti tecnici di tali identificativi e le informazioni connesse, se richiesto dalle autorità di contrasto o dalle autorità giudiziarie al solo scopo di identificare l'utente in una specifica indagine penale;

11) «dati sul traffico»: i dati riguardanti la fornitura di un servizio offerto da un prestatore di servizi, che servono per fornire informazioni di contesto o supplementari sul servizio e che sono generati o trattati da un sistema di informazione del prestatore di servizi, come la fonte e il destinatario di un messaggio o altro tipo di interazione, sull'ubicazione del dispositivo, la data, l'ora, la durata, le dimensioni, il percorso, il formato, il protocollo usato e il tipo di compressione, e altre comunicazioni elettroniche e i dati, diversi dai dati relativi agli abbonati, relativi all'inizio e alla fine di una sessione di accesso utente a un servizio, come la data e l'ora d'uso, la connessione al servizio (log-in) e la disconnessione (log-off) dal medesimo;

12) «dati relativi al contenuto»: qualsiasi dato in formato digitale, come testo, voce (n.d.r. no voce intercettazione), video, immagini o suono, diverso dai dati relativi agli abbonati o dai dati sul traffico.

Estendendo l'analisi alla restante parte del Regolamento, si rileva che la tipologia dei dati oggetto del Regolamento viene definita anche all'interno del "Considerando", precipuamente al n° 31, il quale sancisce che:

(31) Il presente regolamento dovrebbe comprende le seguenti categorie di dati: dati relativi agli abbonati, dati relativi al traffico e dati relativi al contenuto. Tale categorizzazione è conforme agli ordinamenti giuridici di molti Stati membri e al diritto dell'Unione, in particolare alla direttiva 2002/58/CE e alla giurisprudenza della Corte di giustizia, come pure al diritto internazionale, segnatamente la Convenzione di Budapest.

Si badi come la definizione in oggetto, non menziona in alcun modo l'intercettazione delle conversazioni (telefoniche né, tanto meno, telematiche) le quali, pertanto, si ritiene che debbano rimanere assolutamente

escluse dalla applicabilità del Regolamento.

Concetto quest'ultimo peraltro avvalorato anche dal disposto del Considerando 19:
(19) Il presente regolamento dovrebbe disciplinare l'acquisizione dei dati conservati dal prestatore di servizi solamente al momento della ricezione di un ordine europeo di produzione o di un ordine europeo di conservazione. Non dovrebbe imporre un obbligo generale di conservazione dei dati per i prestatori di servizi e non dovrebbe avere l'effetto di comportare una conservazione generalizzata e indifferenziata dei dati. Il presente regolamento non dovrebbe inoltre autorizzare l'intercettazione di dati o l'ottenimento di dati che sono conservati dopo la ricezione di un ordine europeo di produzione o di un ordine europeo di conservazione.

Ovviamente, ciò non significa che per le Autorità Giudiziarie resti esclusa la possibilità di avvalersi dell'istituto dell'intercettazione, il quale continuerà a poter essere richiesto ad esempio, per il tramite del noto meccanismo dell'OEI (Ordine Europeo d'Indagine) [2].
Altro concetto importante, e che il Regolamento tratta dati precostituiti e quindi già conservati dal prestatore di servizio, al momento in cui riceve l'Ordine (EPOC o EPOC-PR).
Tale fattispecie è rilevabile dal citato art. 3 (Definizioni) paragrafo 8) che nel definire le prove elettroniche, sancisce che sono "i dati relativi… conservati ….. al momento della ricezione ….".

4) Principi fondamentali del Regolamento - il Prestatore di servizi

Analizzando il testo del Regolamento, è possibile ricavarne una serie di principi fondamentali, i quali, oltre ad aver costituito la fonte di ispirazione dei lavori della Commissione, rappresentano una novità assoluta in tema di accesso alle prove.
Tale innovazione introdotta dal Regolamento, infatti, è senza dubbio rappresentata dalla facoltà concessa all'Autorità richiedente di poter accedere alle prove richiedendole direttamente al fornitore di servizio, prescindendo dal luogo in cui fisicamente questi risieda o dove abbia conservato i dati, senza dover passare dall'Autorità Giudiziaria del paese di esecuzione.
Tale facoltà è concessa alle Autorità comunitarie in ordine al principio della reciproca fiducia tra Paesi membri, ricavabile dal disposto contenuto nel Considerando 12 [3] attraverso il quale il Regolamento "…. consente alle autorità nazionali competenti di inviare tali ordini direttamente ai prestatori di servizio" senza passare dall'Autorità Giudiziaria del Paese di esecuzione.
Tale meccanismo, dunque, permetterà un significativo accorciamento dei tempi di acquisizione, consentendo all'Autorità di emissione di concentrare in un'unica richiesta la produzione di dati [0].
Dalla lettura combinata del Considerando 26 [4] e del Considerando 21 [5], si evince l'ambito di applicazione del Regolamento in oggetto, i quale si applicherà a tutti i prestatori che offrono servizi nell'Unione, a prescindere dall'ubicazione della loro sede o stabilimento. Ne deriva, quindi, che nei casi in cui un prestatore operante all'interno dell'Unione non abbia uno stabilimento (sede) all'interno di essa, dovrà nominare almeno un Rappresentante legale (vedi anche art. 7 paragrafo 1 [6]) per assolvere

agli obblighi previsti dal Regolamento. Pertanto, in tali casi, ossia se lo stabilimento del prestatore di servizio o il luogo dove questi conserva i dati non siano ubicati nell'Unione, fermo restando che questi offra servizi in uno o più paesi comunitari (Vedi Considerando 26 [4] e art. 2 paragrafo 1 [7]), dovrà necessariamente nominare un Rappresentante legale al quale potranno essere notificati gli Ordini di produzione e di conservazione per la loro esecuzione.
La definizione di prestatore di servizio, invece, la si rileva dall'art. 3 (Definizioni) paragrafo 3 [8] e in specie dal Considerando 27 [9].
L'art. 3 paragrafo 3, identifica 3 categorie di prestatori di servizio che forniscono:

- servizi di comunicazione elettronica;
- servizi di domini internet e di numerazioni IP;
- altri servizi della società dell'informazione, che non possono essere considerati prestatori di servizi di comunicazione elettronica ma offrono agli utenti la possibilità di comunicare tra loro oppure servizi che possono essere utilizzati per memorizzare o altrimenti trattare dati per loro conto.

Nel Considerando 27 [9], invece, si è voluto estendere l'area di intervento del Regolamento, ai «servizi cloud e altri servizi di hosting che forniscono una vasta gamma di risorse informatiche, quali reti, server o altre infrastrutture, mezzi di conservazione, app e servizi che permettono di conservare dati a diversi scopi».
Lo stesso Considerando prevede altresì l'esclusione di alcune categorie, quali i prestatori di servizi della società dell'informazione quando non offre ai propri utenti la possibilità di comunicare tra loro, ma solo con il prestatore di servizi, o non offre la possibilità di memorizzare o altrimenti trattare dati, ovvero se la conservazione di dati non costituisce una componente propria, ovvero una parte essenziale del servizio fornito agli utenti, quali i servizi giuridici, di ingegneria architettonica e contabili forniti online a distanza, esso non dovrebbe rientrare nella definizione di «prestatore di servizi» di cui al presente regolamento, anche se i servizi forniti da tale prestatore sono servizi della società dell'informazione ai sensi della direttiva (UE) 2015/1535.

5) Ordini di produzione e di conservazione

Le tipologie di ordini che, a norma del Regolamento l'Autorità di emissione potrà adottare sono due:

- Ordini di Produzione di prove elettroniche – EPOC
- Ordini di Conservazione di prove elettroniche – EPOC-PR

Attraverso tali ordini, come già detto, viene consentito alle Autorità di accedere direttamente ai dati conservati dal fornitore del servizio, indipendentemente dal luogo in questi si trovino.
Gli ordini di produzione (EPOC) permetteranno alle Autorità Giudiziarie di uno Stato membro di chiedere direttamente l'accesso alle prove elettroniche conservate da un prestatore di servizi stabilito o rappresentato in un altro Stato membro.
Quest'ultimo dovrà rispondere entro il termine massimo di 10 giorni dalla richiesta (notifica) o, in caso di emergenza, entro 8 ore.

Gli ordini di conservazione (EPOC-PR), invece, sono finalizzati ad impedire la cancellazione delle prove elettroniche da parte del prestatore di servizi durante il trattamento dell'Ordine di produzione, per un periodo max di 60 giorni (prorogabili di altri 30).
Le prove sottoposte a tale regime imposto dall'Ordine di conservazione, inoltre, potranno essere acquisite successivamente solamente a seguito di un Ordine di produzione.

6) Ordine Europeo – Condizioni per l'emissione

6.1) L'EPOC

L'Ordine di produzione è definito dall'art. 3 (Definizioni) paragrafo 1 del Regolamento:
1) «ordine europeo di produzione»: (EPOC) la decisione che dispone la produzione di prove elettroniche, emessa o convalidata da un'autorità giudiziaria di uno Stato membro (n.d.r. di emissione) a norma dell'articolo 4, paragrafi 1, 2, 4 e 5, e rivolta a uno stabilimento designato o a un rappresentante legale di un prestatore di servizi che offre servizi nell'Unione, qualora tale stabilimento designato o rappresentante legale sia ubicato in un altro Stato membro vincolato dal presente regolamento;
Le condizioni necessarie per l'emissione dell'EPOC sono sancite dall'articolo 5 del Regolamento, rubricato, appunto, Condizioni di emissione dell'ordine europeo di produzione [10], a norma del quale è richiesta:

- garanzia delle condizioni sancite dall'art. 5;
- che l'Ordine sia necessario e proporzionato ai fini del procedimento;
- che sia emesso solo se possibile emettere analogo provvedimento per casi interni analoghi.

Le condizioni di emissione dell'Ordine sancite dall'articolo 5 paragrafo 3 [10] (vedi anche Considerando 40 [11] e 41 [12] è che l'EPOC, per la richiesta di dati relativi agli abbonati o per ottenere dati richiesti al solo scopo di identificare l'utente, quali definiti all'articolo 3, paragrafo 10, si basano alternativamente sia sul profilo quantitativo del reato da perseguire, che sul profilo qualitativo, a seconda dell'oggetto dell'Ordine stesso.
Sotto il primo profilo, quello quantitativo, può essere emesso un EPOC o un EPOC-PR per qualsiasi reato e per l'esecuzione di una pena o di una misura di sicurezza detentiva di almeno quattro mesi mentre, per la richiesta di dati di traffico o di contenuti (Art. 5 paragrafo 4 [10]), considerata la natura più sensibile di questa tipologia, si devono autorizzare l'emissione di ordini europei di produzione nei procedimenti penali solo per reati punibili con una pena detentiva della durata massima di almeno 3 anni, fatta eccezione per i reati informatici per i quali si prevede la possibilità di richiedere l'EPOC per tali reati, anche qualora comportino una pena detentiva della durata massima inferiore a 3 anni.
Sono posti sotto il secondo profilo, quello qualitativo, i reati connessi al terrorismo ai sensi della direttiva (UE) 2017/541 del Parlamento europeo e del Consiglio, come pure i reati relativi all'abuso e allo sfruttamento sessuale dei minori di cui alla direttiva 2011/93/UE del Parlamento europeo e del Consiglio, per i quali non è richiesta la soglia minima della pena edittale (durata massima di 3 anni) ma ciò che rileva è la tipologia del reato da perseguire.

Completando l'analisi dell'articolo 5 del Regolamento, si ritiene opportuno porre l'attenzione su due ulteriori condizioni che rivestono una posizione parzialmente diversa rispetto alle precedenti e che, per tale motivo, si rilevano elementi di specificità:
Il Paragrafo 8 prevede, infatti, che per i dati conservati per una autorità pubblica, questi possono essere richiesti tramite Ordine solo se la quest'ultima è situata nel luogo di emissione,
8. Qualora i dati siano conservati o altrimenti trattati nell'ambito di un'infrastruttura fornita da un prestatore di servizi a un'autorità pubblica, è possibile emettere un ordine europeo di produzione solo se l'autorità pubblica per la quale i dati sono conservati o altrimenti trattati si trova nello Stato di emissione.

Anche il Considerando 44 conferma tale disciplina:
(44) Qualora i dati siano conservati o trattati nell'ambito di un'infrastruttura fornita da un prestatore di servizi a un'autorità pubblica, dovrebbe essere possibile emettere un ordine europeo di produzione o un ordine europeo di conservazione solo se l'autorità pubblica per la quale i dati sono conservati o altrimenti trattati è situata nello Stato di emissione.
Se ne ricava, quindi, che la produzione di dati appartenenti ad una autorità pubblica sarà possibile solo qualora questa sia situata nello Stato di emissione.

Il paragrafo 5 dell'art. 10 [12 b] disciplina, invece, i casi di "immunità o privilegi" rilevati dal destinatario (prestatore di servizi), prevedendo una procedura di informazione del destinatario verso l'Autorità di esecuzione e di emissione, volta alla verifica della possibilità di fornire o meno i dati oggetto di "immunità o privilegi".

6.2) L'EPOC-PR

La definizione dell'Ordine di produzione è riscontrabile nell'art. 3 (Definizioni) paragrafo 2 del Regolamento:
2) «ordine europeo di conservazione»: (EPOC-PR) la decisione che dispone la conservazione di prove elettroniche ai fini di una richiesta di produzione successiva, e che è emessa o convalidata da un'autorità giudiziaria di uno Stato membro (n.d.r. di emissione) a norma dell'articolo 4, paragrafi 3, 4 e 5, e rivolta a uno stabilimento designato o a un rappresentante legale di un prestatore di servizi che offre servizi nell'Unione, qualora tale stabilimento designato o rappresentante legale sia ubicato in un altro Stato membro vincolato dal presente regolamento.

Nell'art. 6 (Condizioni di emissione dell'ordine europeo di produzione) paragrafo 2 e 3 [14] del Regolamento, sono esplicitate le condizioni necessarie per poter procedere all'emissione di un EPOC-PR, che sono:

- deve essere necessario e proporzionato al fine di impedire la rimozione, la cancellazione o la modifica di dati in vista della presentazione di una successiva richiesta di produzione dei medesimi

tramite l'assistenza giudiziaria, un ordine europeo d'indagine (OEI) o un Ordine europeo di produzione, tenendo conto dei diritti della persona oggetto di indagini o imputata;

- che sia emesso solo se possibile emettere analogo provvedimento per casi interni analoghi;
- può essere emesso per tutti i reati (art. 6 paragrafo 3 [14]).

Immunità e Privilegi

Il paragrafo 4 dell'art. 11 [15] disciplina, i casi di "immunità e privilegi" che possono essere rilevati dal destinatario (prestatore di servizi).

7) Ordine europeo - Esecuzione

7.1) L'EPOC

Analizzando maggiormente nel dettaglio l'Ordine di produzione, come già accennato si ravvisano due tipologie di EPOC che possono essere emessi, alternativamente, a secondo la categoria di dati che si richiedono:

- Dati di traffico e contenuti;
- Dati relativi agli abbonati o per ottenere dati richiesti al solo scopo di identificare l'utente, quali definiti all'articolo 3, paragrafo 10). [16]

L'Art. 4 (Autorità di emissione) paragrafi 1 e 2, disciplina quale Autorità possa emettere un EPOC.

1. Per la prima categoria di dati sopra indicata, l'organo preposto all'emissione dell'EPOC può essere, un organo giurisdizionale (inteso, quest'ultimo, secondo la definizione comunitaria), un magistrato inquirente competente nel caso interessato o qualsiasi altra Autorità competente definita dallo Stato di emissione, previo esame di un giudice, un organo giurisdizionale o un magistrato inquirente nello Stato di emissione;
2. Per la seconda categoria di dati, l'EPOC può essere emesso da un giudice, un organo giurisdizionale, un magistrato inquirente o un pubblico ministero competente nel caso interessato.

Come si nota, per i dati di traffico e dei contenuti, non è prevista la possibilità per il pubblico ministero di emettere l'EPOC (Vedi anche Considerando 36 [16 b]).

Per la seconda categoria di dati, l'EPOC può essere emesso sia da un giudice, un organo giurisdizionale, un magistrato inquirente che da un pubblico ministero competente nel caso interessato.

7.1.1) La Cifratura

Un aspetto di sicuro rilievo che, come tale, merita di essere evidenziato, è l'utilizzo di un sistema di cifratura, richiamato dal Considerando 20 [21].

Tale Considerando dispone esplicitamente che il Regolamento non debba pregiudicare, il prestatore di servizio, nell'attivare meccanismi di cifratura dei dati e che questi dovranno essere forniti a prescindere dall'uso di questo meccanismo, ferma restando la totale assenza di obblighi in capo al prestatore di decifrare tali dati.

Quest'ultima specifica rappresenta una novità rispetto alle prime versioni di proposta del Regolamento, nelle quali il Considerando 19 sanciva:
(19) Il presente regolamento disciplina l'acquisizione solo dei dati conservati, ossia dei dati detenuti dal prestatore di servizi al momento della ricezione di un certificato di ordine europeo di produzione o di conservazione. Non impone un obbligo generale di conservare i dati né autorizza l'intercettazione di dati o l'ottenimento di dati che saranno conservati dopo la ricezione del certificato di ordine di produzione o di conservazione. I dati devono essere forniti a prescindere dal fatto che siano criptati o meno.
Dalla comparazione dei due testi, si rileva che il vecchio disposto (Considerando 19) si limitava a specificare che i dati si sarebbero dovuti fornire a prescindere dal fatto che essi fossero o meno soggetti a cifratura, potendo sottintendere, in questo modo, un obbligo per il prestatore di servizio di fornirli in chiaro.

7.2) L'EPOC-PR

Parzialmente diversa risulta la disciplina riguardante L'EPOC-PR, il quale può essere emesso per qualsiasi categoria di dati.
Tale disciplina è contenuta all'interno dell'Art. 4 (Autorità di emissione) paragrafo 3 [18], il quale si occupa di fornire anche indicazioni, relative all'Autorità autorizzata all'emissione di un EPOC-PR.
Nello specifico, tale Ordine, può essere emesso da un giudice, un organo giurisdizionale o un magistrato inquirente competente nel caso interessato, o qualsiasi altra Autorità competente definita dallo Stato di emissione, previo esame di un giudice, un organo giurisdizionale o un magistrato inquirente o un pubblico ministero nello Stato di emissione.
Scopo dell'EPOC-PR è quindi quello di impedire la rimozione, la cancellazione o la modifica dei dati, in attesa di richiederne l'acquisizione successivamente tramite un EPOC. È indubbio il carattere strumentale teso a congelare i dati in un determinato momento e evitare così che vengano cancellati in attesa dell'emissione dell'EPOC.

7.3) EPOC, EPOC-PR - Negazione all'esecuzione

Nell'art. 16 ai paragrafi 4 e 5, è previsto per il prestatore di servizi, di negare l'esecuzione dell'EPOC e EPOC-PR solo se:

- non è stato emesso o convalidato da un'autorità di emissione conformemente al regolamento;
- non è stato emesso in relazione a un reato previsto di cui all'articolo 5, paragrafo 4;
- il destinatario non ha potuto ottemperare per impossibilità materiale dovuta a circostanze che non possono essergli imputate, o perché l'ordine contiene errori manifesti;
- l'ordine non riguarda dati conservati dal prestatore di servizi o per suo conto al momento della ricezione dell'ordine;
- il servizio esula dall'ambito di applicazione del regolamento;
- i dati richiesti sono protetti da immunità o privilegi concessi a norma del diritto dello Stato di esecuzione o i dati richiesti sono disciplinati da norme sulla determinazione o la limitazione della

responsabilità penale relative alla libertà di stampa o alla libertà di espressione in altri mezzi di comunicazione, che impediscono l'esecuzione o l'applicazione dell'ordine;

- in situazioni eccezionali, dalle sole informazioni contenute nell'ordine risulta che sussistono fondati motivi per ritenere che l'esecuzione dell'ordine comporterebbe una violazione manifesta di un diritto fondamentale pertinente sancito dall'articolo 6 TUE e dalla Carta.

L'autorità di esecuzione decide se eseguire o meno l'ordine sulla base di qualsiasi informazioni fornite dal destinatario e dopo aver consultato l'autorità di emissione.

8) EPOC – La notifica all'Autorità di esecuzione (dati di traffico e Contenuti)

Per la categoria di dati inerenti al traffico e i contenuti, l'art. 8 (Notifica all'Autorità di emissione) paragrafo 1, prevede una procedura consistente in un contestuale notifica dell'EPOC, da parte dell'Autorità di emissione, sia prestatore di servizio che all'Autorità di esecuzione (del Paese di emissione), disponendo:

1. Qualora un ordine europeo di produzione sia emesso per ottenere dati sul traffico, fatta eccezione per i dati richiesti al solo scopo di identificare l'utente ai sensi dell'articolo 3, punto 10), o per ottenere dati relativi al contenuto, l'autorità di emissione ne dà notifica all'autorità di esecuzione trasmettendole l'EPOC contestualmente alla trasmissione dell'EPOC al destinatario conformemente all'articolo 9, paragrafi 1 e 2.

Tale procedura "rafforzata" prevista per l'acquisizione dei dati di traffico e dei contenuti risalta il principio della delicatezza ed è finalizzata a costituire un regime più articolato per l'accesso a quest'ultimi, rispetto alle altre tipologie di dati. La possibilità di accedere a tali dati, tra l'altro, è soggetta anche ad un'altra limitazione, di tipo qualitativo, circa i reati da perseguire, come abbiamo avuto modo di evidenziare nel cap.6.

La notifica all'Autorità di esecuzione, inoltre, risulta rivestita di forza sospensiva, ai sensi del paragrafo 4 dello stesso articolo 8, il quale sancisce che:

4. La notifica all'autorità di esecuzione di cui al paragrafo 1 del presente articolo ha effetto sospensivo sugli obblighi del destinatario di cui all'articolo 10, paragrafo 2, tranne nei casi di emergenza quali definiti all'articolo 3, punto 18).

9) Termini per adempiere

9.1) EPOC

Ulteriore aspetto che si ritiene meritevole di un'analisi maggiormente particolareggiata, è quello rappresentato dai termini stabiliti dal Regolamento entro i quali i prestatori di servizi dovranno adempiere agli ordini ricevuti.

A tal proposito, l'art. 10 paragrafo 2 [19] (Esecuzione dell'EPOC) prevede una tempistica max di 10 giorni (salvo condizione di urgenza per le quali il termine per adempiere viene ridotto a 8 ore).

Va considerato, tuttavia, che la notifica all'Autorità di esecuzione (per le richieste di traffico e contenuti), come già accennato, è dotata di effetto sospensivo, e ciò comporta che il prestatore di servizio dovrà

attendere la valutazione dell'Autorità di esecuzione ai sensi dell'art. 10 paragrafo 2) [19].
Se ne ricava una disposizione suscettibile di interpretazioni contrastanti circa l'individuazione del corretto computo dei termini previsti per adempiere.
A parere dello scrivente, tale disposizione va interpretata nel senso che, qualora l'Autorità di esecuzione non faccia valere entro 10 giorni motivi di rifiuto, il prestatore di servizi sarà tenuto ad adempiere all'Ordine dell'Autorità di emissione a far data dall'11° giorno, in quanto deve attendere la scadenza del periodo di 10 giorni concessi all'Autorità di esecuzione per fornire una valutazione (l'Autorità di esecuzione potrebbe infatti rispondere il 10 giorno e casomai nel tardo pomeriggio/sera).
Tale disposizione, a causa della (a mio avviso) infelice forma con cui sia stata espressa, si presta a ingenerare un'evidente sovrapposizione dei termini finali, anche se un aiuto parziale ci viene fornito dall'articolo 10 paragrafo 2) [19] nella parte in cui recita: il destinatario provvede affinché i dati richiesti siano trasmessi…….. al termine di tale periodo di 10 giorni..." dove la locuzione al termine va interpretata dopo lo scadere delle ore 24:00 del decimo giorno.

Come già anticipato, lo stesso articolo 10, al paragrafo 4 disciplina un regime emergenziale, volto ad accelerare ulteriormente il processo di acquisizione dei dati, riducendo i termini di esecuzione da 10 gg a 8 ore:
4. In caso di emergenza, il destinatario trasmette i dati richiesti senza indebito ritardo, al più tardi entro otto ore dalla ricezione dell'EPOC. Qualora sia prevista una notifica all'autorità di esecuzione a norma dell'articolo 8, quest'ultima può, se decide di far valere un motivo di rifiuto a norma dell'articolo 12, paragrafo 1, senza indugio e al più tardi entro 96 ore dalla ricezione della notifica, notificare all'autorità di emissione e al destinatario che essa si oppone all'uso dei dati o che i dati possono essere utilizzati solo alle condizioni da essa specificate. Se l'autorità di esecuzione fa valere un motivo di rifiuto e se i dati sono già stati trasmessi dal destinatario all'autorità di emissione, quest'ultima cancella i dati o ne limita in altro modo l'uso oppure, nel caso in cui l'autorità di esecuzione abbia specificato condizioni, rispetta tali condizioni quando utilizza i dati.
L'articolo 3 paragrafo 18, prova a definire i casi di emergenza:
18) «caso di emergenza»: una situazione in cui sussiste una minaccia imminente per la vita, l'integrità fisica o la sicurezza di una persona, o per un'infrastruttura critica, quale definita all'articolo 2, lettera a), della direttiva 2008/114/CE, il cui danneggiamento o la cui distruzione comporterebbe una minaccia imminente per la vita, l'integrità fisica o la sicurezza di una persona, anche attraverso un grave danno alla fornitura di beni essenziali alla popolazione o all'esercizio delle funzioni fondamentali dello Stato;
Il paragrafo, pur definendo tale regime, non menziona specificatamente le casistiche per le quali si possa definire una situazione di emergenza, lasciando quindi ampia discrezionalità all'Autorità di emissione di emanare un Ordine emergenziale, al quale i prestatori dovranno adempiere in un lasso di tempo molto limitato.

Non è ravvisabile nel Regolamento, alcuna disciplina specifica, circa il criterio relativo al computo

dei termini; ne deriva, quindi, che si debba applicare le disposizioni previste dal Regolamento (CEE, Euratom) n. 1182/71 del Consiglio del 3 giugno 1971 (Vedi in particolare Art. 3 Paragrafo 2 lett. b).
L'unica eccezione è quella rappresentata dall'art. 17 (Procedura di riesame in caso di obblighi contrastanti) paragrafo 9, il quale prevede che:
….
9. Ai fini delle procedure di cui al presente articolo (n.d.r. Riesame), i termini sono calcolati in conformità del diritto nazionale dell'autorità di emissione
Interpretando letteralmente la disposizione contenuta all'interno del Paragrafo, se ne ricava la necessità, in capo al prestatore di servizi di conoscere i termini stabiliti dal diritto interno del Paese di emissione.
Si ritiene che tale presupposto rappresenti una criticità nell'economia del processo di fornitura dei dati, in quanto la sua osservazione richiederebbe la conoscenza delle norme di settore di tutti i Paesi membri.
Da ultimo, si ritiene opportuno evidenziare, alla luce di quanto già accennato in precedenza, che i dati che i prestatori di servizi saranno chiamati a fornire saranno solo quelli disponibili (sino) alla data di notifica dell'Ordine di produzione (quindi non quelli successivi).
Pertanto, particolare attenzione dovrà essere prestata dal prestatore dei servizi (anche attuando, ove necessario, specifici sviluppi sui sistemi di retention e di specifiche policy) nel "congelare" i dati memorizzati alla data di notifica dell'Ordine.

9.2) EPOC-PR

Per quanto riguarda l'Ordine di conservazione (EPOC-PR), la disciplina dei termini di esecuzione è affidata all'art. 11 (Esecuzione dell'EPOC-PR) paragrafo 1[20], il quale prevede una tempistica max di 60 giorni prorogabili di altri 30.
Come già menzionato nei capitoli precedenti, per l'acquisizione dei dati conservati si rileverà necessario un successivo Ordine di produzione, ai sensi dell'articolo 11 par.1 [20]
Qualora l'Autorità di emissione informi il prestatore di servizi circa l'emissione di un Ordine di Produzione, questi dovrà garantire la conservazione dei dati sino a che l'EPOC non sia stato notificato (art. 11 paragrafo 2).
2. Qualora, durante il periodo di conservazione di cui al paragrafo 1 l'autorità di emissione confermi che è stata emessa una successiva richiesta di produzione, il destinatario conserva i dati per tutto il tempo necessario per la loro produzione una volta ricevuta la successiva richiesta di produzione.
Il Paragrafo 3 disciplina la casistica della cancellazione dei dati qualora l'Autorità di emissione informi il prestatore di servizi che i dati non siano più necessari.
3. Qualora la conservazione non fosse più necessaria, l'autorità di emissione ne informa il destinatario senza indebito ritardo e l'obbligo di conservazione sulla base dell'ordine europeo di conservazione cessa di sussistere.

10) Rimborso spese

Il Considerando 68 e l'art. 14 (Rimborso spese) prevedono rimborsi verso il prestatore di servizi, qualora analoga possibilità sia prevista dall'ordinamento nazionale.

Art. 14

1. Laddove tale possibilità sia prevista dal diritto nazionale dello Stato di emissione per gli ordini interni in situazioni analoghe, il prestatore di servizi può chiedere allo Stato di emissione il rimborso delle sue spese, conformemente al diritto nazionale di tale Stato. Gli Stati membri comunicano le proprie norme interne di rimborso alla Commissione, che le rende pubbliche.

2. Il presente articolo non si applica al rimborso dei costi del sistema informatico decentrato di cui all'articolo 25.

11) Sanzioni

Il Considerando 69 e l'art. 15 (Sanzioni), dispone che la competenza dell'attuazione del regime sanzionatorio spetti a ciascuno Stato membro.

Art. 15

1. Fatti salvi i diritti nazionali che prevedono l'irrogazione di sanzioni penali, gli Stati membri stabiliscono le norme relative alle sanzioni pecuniarie applicabili in caso di violazione degli articoli 10 e 11 e dell'articolo 13, paragrafo 4, in conformità dell'articolo 16, paragrafo 10, e adottano tutte le misure necessarie per assicurarne l'applicazione. Le sanzioni pecuniarie previste devono essere effettive, proporzionate e dissuasive. Gli Stati membri garantiscono che possano essere imposte sanzioni pecuniarie pari fino al 2% del fatturato mondiale totale annuo del prestatore di servizi nell'esercizio precedente. Gli Stati membri notificano tali norme e misure alla Commissione senza ritardo e provvedono poi a dare immediata notifica delle eventuali modifiche successive.

2. Fatti salvi gli obblighi in materia di protezione dei dati, i prestatori di servizi non sono ritenuti responsabili negli Stati membri per il pregiudizio causato agli utenti o a terzi derivanti esclusivamente dall'ottemperanza in buona fede a un EPOC o a un EPOC-PR.

12) Esecuzione forzata - Riesame

Gli artt. 16 e 17 del Regolamento disciplinano, rispettivamente, i casi di mancata esecuzione dell'Ordine (da parte del prestatore di servizio) e quello del riesame.

Nell'art. 16 è disciplinato il procedimento di esecuzione "forzata" che l'Autorità di emissione richiede all'Autorità di esecuzione in caso di inottemperanza del prestatore di servizio.

Da questo istituto nasce, in capo all'Autorità di esecuzione, la facoltà di decidere se negare la prosecuzione dell'Ordine proveniente dall'Autorità di emissione o se ingiungere al prestatore di servizio di eseguire l'Ordine.

L'art. 17 tratta, invece, l'istituto del Riesame:

art. 17 Paragrafo 1. Se ritiene che l'ottemperanza all'ordine europeo di produzione sia in contrasto con un obbligo previsto dal diritto applicabile di un paese terzo, il destinatario informa l'autorità di emissione e

l'autorità di esecuzione dei motivi per non eseguire l'ordine europeo di produzione, conformemente alla procedura di cui all'articolo 10, paragrafi 8 e 9, utilizzando il modulo di cui all'allegato III («obiezione motivata»).
In ordine a questo paragrafo, cioè che si ritiene possa avere effetti gravosi per i prestatori di servizio concerne la valutazione sul "… contrasto con obbligo previsto dal diritto... di un paese terzo...", i quali dovrebbero così essere tenuti a conoscere la legislazione applicabile di qualsiasi Paese terzo e a valutare se l'Ordine si ponga in contrasto con la stessa.
Questo potrebbe indurre un comportamento di "massima" tutela del prestatore di servizio, richiedendo il riesame per tutte le richieste in specie o eseguire le richieste senza valutazione alcuna.
Per meglio comprendere lo scenario, facciamo l'esempio di questa triangolazione:
EPOC emesso da un'Autorità francese, con prestatore di servizio italiano per reati commessi da un Argentino nel territorio francese.
In questo caso il prestatore italiano dovrebbe verificare se l'Ordine francese sia compatibile con il diritto argentino.
Processo che si renderebbe alquanto complicato da adempiere correttamente da parte del Prestatore di servizi, considerando anche i tempi brevi per adempiere che potrebbero far vanificare eventuali verifiche intraprese.

13) Sistemi Informativi

Il Capo V disciplina il sistema informativo che dovrebbe essere dedicato alla gestione delle richieste degli Ordini e dell'invio dei dati e per tutte le attività di comunicazione. Ogni prestatore di servizio dovrà, infatti, essere collegato al sistema informatico decentrato.
Art. 19 paragrafo 1
1. La comunicazione scritta tra le autorità competenti e gli stabilimenti designati o i rappresentanti legali a norma del presente regolamento, compresi lo scambio di moduli previsti dal presente regolamento e i dati richiesti tramite un ordine europeo di produzione o un ordine europeo di conservazione, ha luogo tramite il sistema informatico decentrato sicuro e affidabile («sistema informatico decentrato»)

Gli Stati membri sostengono le spese per i punti di accesso al sistema informatico decentrato:
Art. 23 paragrafo 1
1. Ciascuno Stato membro sostiene i costi di installazione, funzionamento e manutenzione dei punti di accesso al sistema informatico decentrato per i quali lo Stato membro è responsabile.
I prestatori di servizio dovranno, viceversa, sostenere i costi per l'accesso al sistema informatico.

Art. 23 paragrafo 5
5. I prestatori di servizi sostengono tutti i costi necessari per potersi integrare con successo nel sistema informatico decentrato o interagire con esso in altro modo.

All'art. 25 (Atti di esecuzione) paragrafo 3, viene sancito che gli atti di esecuzione di cui al paragrafo 1, sono adottati entro il 18 agosto 2025.
Paragrafo 1
a) le specifiche tecniche che definiscono i metodi di comunicazione per via elettronica ai fini del sistema informatico decentrato;
b) le specifiche tecniche per i protocolli di comunicazione;
c) gli obiettivi in materia di sicurezza delle informazioni e le pertinenti misure tecniche che garantiscono le norme minime di sicurezza delle informazioni e un livello elevato di cybersicurezza per il trattamento e la comunicazione delle stesse nell'ambito del sistema informatico decentrato;
d) gli obiettivi minimi di disponibilità e i possibili requisiti tecnici correlati per i servizi forniti dal sistema informatico decentrato.

Il 19 ottobre 2023, a Bruxelles, è avvenuto il Kik-Off meeting dell'"Expert group on the E-Evidence decentralised IT system", che avrà il compito di definire quanto previsto dal su citato articolo 25.

14) Monitoraggi - Reporting

Nell'art. 28 sono previste le attività di monitoraggio e reporting delle richieste.
I prestatori di servizio dovranno adottare un sistema di reportistica (art. 28 paragrafo 4) inerente alle richieste degli Ordini.
Le statistiche raccolte dell'anno civile precedente, potranno essere trasmesse alla Commissione entro il 31 marzo.

15) I moduli per le richieste

Il Regolamento prevede, infine, anche una serie di modulistica da utilizzare per i vari casi disciplinati (es. richiesta, riesame, impossibilità ad eseguire l'Ordine, ecc.).
Da evidenziare che nei moduli di richiesta (sia EPOC che EPOC-PR) per quanto riguarda il dato di traffico, è previsto il solo traffico mobile (voce e dati).

16) Valutazione della Commissione

Entro il 18 agosto 2029, la Commissione effettuerà una valutazione del presente regolamento.
La Commissione dovrà stilare una relazione di valutazione al Parlamento europeo, al Consiglio, al Garante europeo della protezione dei dati e all'Agenzia dell'Unione europea per i diritti fondamentali, che dovrà includere una valutazione dell'applicazione del presente regolamento e dei risultati conseguiti in relazione ai suoi obiettivi nonché una valutazione dell'impatto del presente Regolamento sui diritti fondamentali.

NOTE

[0]
Parere del Comitato 23/2018 sulle proposte della Commissione relative agli ordini europei di produzione e di conservazione di prove elettroniche in materia penale (articolo 70, paragrafo 1, lettera b) Adottato il 26 settembre 2018. https://edpb.europa.eu/sites/default/files/files/file1/edpb-2018-09-26-eevidence_it.pdf

[1]
Art. 288
Per esercitare le competenze dell'Unione, le istituzioni adottano regolamenti, direttive, decisioni, raccomandazioni e pareri.
Il regolamento ha portata generale. Esso è obbligatorio in tutti i suoi elementi e direttamente applicabile in ciascuno degli Stati membri.
La direttiva vincola lo Stato membro cui è rivolta per quanto riguarda il risultato da raggiungere, salva restando la competenza degli organi nazionali in merito alla forma e ai mezzi.
La decisione è obbligatoria in tutti i suoi elementi. Se designa i destinatari è obbligatoria soltanto nei confronti di questi.
Le raccomandazioni e i pareri non sono vincolanti.

[2]
artt. 23-24 e 43-44 del decreto legislativo del 21 giugno 2017, n. 108 di attuazione della Direttiva sull'OEI, in materia di "ordine di intercettazione"

[3]
Considerando 12
Il meccanismo dell'ordine europeo di produzione e dell'ordine europeo di conservazione per le prove elettroniche nei procedimenti penali si basa sul principio della fiducia reciproca tra gli Stati membri e sulla presunzione di conformità da parte degli Stati membri al diritto dell'Unione, allo Stato di diritto e, in particolare, ai diritti fondamentali, che sono elementi essenziali dello spazio di libertà, di sicurezza e di giustizia dell'Unione. Tale meccanismo consente alle autorità nazionali competenti di inviare tali ordini direttamente ai prestatori di servizi.

[4]
Considerando 26
Il presente regolamento dovrebbe applicarsi ai prestatori di servizi che offrono servizi nell'Unione, e dovrebbe essere possibile emettere gli ordini di cui al presente regolamento in relazione ai dati riguardanti servizi offerti nell'Unione. I servizi offerti esclusivamente al di fuori dell'Unione non dovrebbero

rientrare nell'ambito di applicazione del presente regolamento, anche se il prestatore di servizi è stabilito nell'Unione. Pertanto, il presente regolamento non dovrebbe consentire l'accesso a dati diversi dai dati relativi ai servizi offerti all'utente nell'Unione da tali prestatori di servizi

[5]
Considerando 21
In molti casi i dati non sono più conservati o altrimenti trattati nel dispositivo dell'utente ma sono messi a disposizione su un'infrastruttura cloud che consente l'accesso da qualsiasi luogo. Per fornire tali servizi i prestatori non hanno bisogno di essere stabiliti o di avere server in una specifica giurisdizione. Pertanto l'applicazione del presente regolamento non dovrebbe dipendere dal luogo effettivo in cui sono stabiliti il prestatore di servizi o la struttura per il trattamento o la conservazione dei dati.

[6]
Articolo 7 (Destinatari degli ordini europei di produzione e degli ordini europei di conservazione) paragrafo 1
1. Gli ordini europei di produzione e gli ordini europei di conservazione sono rivolti direttamente a uno stabilimento designato o a un rappresentante legale del prestatore di servizi interessato.

[7]
art. 2 (Ambito di applicazione) al paragrafo 1:
Il presente regolamento si applica ai prestatori di servizi che offrono servizi nell'Unione.
[8]
Art. 3 (Definizioni) paragrafo 3
3) «prestatore di servizi»: la persona fisica o giuridica che fornisce una o più delle seguenti categorie di servizi, ad eccezione dei servizi finanziari di cui all'articolo 2, paragrafo 2, lettera b), della direttiva 2006/123/CE del Parlamento europeo e del Consiglio:
a) servizi di comunicazione elettronica quali definiti all'articolo 2, punto 4), della direttiva (UE) 2018/1972;
b) servizi di nomi di dominio internet e di numerazione IP, quali l'assegnazione di indirizzi IP, i servizi di registri di nomi di dominio, di registrar di nomi di dominio e i servizi per la privacy o proxy connessi ai nomi di dominio;
c) altri servizi della società dell'informazione di cui all'articolo 1, paragrafo 1, lettera b), della direttiva (UE) 2015/1535 che:
i) consentono ai loro utenti di comunicare fra di loro; o
ii) rendono possibile la conservazione o il trattamento di dati per conto degli utenti ai quali è fornito il servizio, quando la conservazione dei dati è una componente propria del servizio fornito all'utente;

[9]
Considerando 27
I prestatori di servizi più pertinenti per l'acquisizione di prove nei procedimenti penali sono i prestatori di servizi di comunicazione elettronica e specifici prestatori di servizi della società dell'informazione che facilitano l'interazione tra utenti. Pertanto, entrambi i gruppi dovrebbero rientrare nell'ambito di applicazione del presente regolamento. I servizi di comunicazione elettronica sono definiti nella direttiva (UE) 2018/1972 del Parlamento europeo e del Consiglio e comprendono i servizi di comunicazioni interpersonali, quali Voice over IP (VoIP), la messaggistica istantanea e i servizi di posta elettronica. Il presente regolamento dovrebbe essere applicabile anche a prestatori di servizi della società dell'informazione ai sensi della direttiva (UE) 2015/1535 del Parlamento europeo e del Consiglio che non possono essere considerati prestatori di servizi di comunicazione elettronica ma offrono agli utenti la possibilità di comunicare tra loro oppure servizi che possono essere utilizzati per memorizzare o altrimenti trattare dati per loro conto. Ciò sarebbe in linea con i termini utilizzati nella Convenzione del Consiglio d'Europa sulla criminalità informatica (STC n. 185) («Convenzione di Budapest»), firmata a Budapest il 23 novembre 2001 («convenzione di Budapest»). Il trattamento dei dati dovrebbe essere inteso nel senso tecnico di creazione o manipolazione di dati, vale a dire di operazioni tecniche volte a produrre o modificare dati attraverso la potenza di elaborazione informatica. Le categorie di prestatori di servizi che rientrano nel presente regolamento dovrebbero includere, ad esempio, i mercati online che offrono ai consumatori e alle imprese la possibilità di comunicare tra loro e altri servizi di hosting, anche quando il servizio è fornito attraverso cloud computing, nonché le piattaforme di gioco online e le piattaforme di gioco d'azzardo online. Se un prestatore di servizi della società dell'informazione non offre ai propri utenti la possibilità di comunicare tra loro, ma solo con il prestatore di servizi, o non offre la possibilità di memorizzare o altrimenti trattare dati, ovvero se la conservazione di dati non costituisce una componente propria, ovvero una parte essenziale del servizio fornito agli utenti, quali i servizi giuridici, di ingegneria architettonica e contabili forniti online a distanza, esso non dovrebbe rientrare nella definizione di «prestatore di servizi» di cui al presente regolamento, anche se i servizi forniti da tale prestatore sono servizi della società dell'informazione ai sensi della direttiva (UE) 2015/1535.

[10]
Articolo 5 (Condizioni di emissione dell'ordine europeo di produzione)
1. L'autorità di emissione può emettere un ordine europeo di produzione laddove siano soddisfatte le condizioni stabilite dal presente articolo.
2. L'ordine europeo di produzione è necessario e proporzionato ai fini del procedimento di cui all'articolo 2, paragrafo 3, tenuto conto dei diritti della persona oggetto di indagini o imputata, e può essere emesso solo se un ordine dello stesso tipo avrebbe potuto essere emesso alle stesse condizioni in un caso interno analogo.
3. L'ordine europeo di produzione per ottenere dati relativi agli abbonati o per ottenere dati richiesti al

solo scopo di identificare l'utente, quali definiti all'articolo 3, punto 10), può essere emesso per qualsiasi reato e per l'esecuzione di una pena o di una misura di sicurezza detentiva di almeno quattro mesi, a seguito di un procedimento penale, irrogata con decisione non pronunciata in contumacia, nei casi in cui la persona condannata è latitante.
4. Un ordine europeo di produzione per ottenere dati sul traffico, ad eccezione dei dati richiesti al solo scopo di identificare l'utente, quali definiti all'articolo 3, punto 10), del presente regolamento, o per ottenere dati relativi al contenuto è emesso solo:
……..

[11]
Considerando 40
Considerata la natura più sensibile dei dati relativi al traffico, ad eccezione dei dati richiesti al solo scopo di identificare l'utente ai sensi del presente regolamento, e dei dati relativi al contenuto, occorre effettuare una distinzione per quanto riguarda l'ambito di applicazione materiale del presente regolamento. Dovrebbe essere possibile emettere un ordine europeo di produzione per ottenere i dati relativi agli abbonati o per ottenere i dati richiesti al solo scopo di identificare l'utente, ai sensi del presente regolamento, per qualsiasi reato; mentre un ordine europeo di produzione per ottenere dati relativi al traffico, ad eccezione dei dati richiesti al solo scopo di identificare l'utente ai sensi del presente regolamento, o per ottenere dati relativi al contenuto dovrebbe essere soggetto a requisiti più severi, a causa del carattere più sensibile di questi dati. Il presente regolamento dovrebbe prevedere una soglia in relazione al suo ambito di applicazione, consentendo un approccio più proporzionato, insieme a una serie di altre condizioni e garanzie ex ante ed ex post per assicurare il rispetto della proporzionalità e dei diritti degli interessati. Tale soglia non dovrebbe però limitare l'efficacia del presente regolamento e il suo uso da parte degli operatori. Autorizzare l'emissione di ordini europei di produzione nei procedimenti penali solo per reati punibili con una pena detentiva della durata massima di almeno 3 anni limiterà l'ambito di applicazione del presente regolamento ai reati più gravi senza compromettere eccessivamente le possibilità di uso dello stesso da parte degli operatori. Tale limitazione escluderebbe dall'ambito di applicazione del presente regolamento un numero significativo di reati che gli Stati membri considerano meno gravi e puniscono con una pena massima inferiore. Tale limitazione offrirà inoltre il vantaggio di essere facilmente applicabile nella pratica.

[12]
Considerando 41
Esistono reati specifici per i quali le prove sono tipicamente disponibili esclusivamente in formato elettronico, per natura particolarmente effimero. Si tratta dei reati connessi all'informatica, anche quando non sono considerati gravi di per sé ma potrebbero causare un danno esteso o considerevole, in particolare

i reati che comportano un effetto individuale scarso ma un danno complessivo di elevato volume. Per la maggior parte dei reati commessi a mezzo di un sistema d'informazione, l'applicazione della stessa soglia fissata per gli altri tipi di reato comporterebbe l'impunità nella maggior parte dei casi. Questa considerazione giustifica l'applicazione del presente regolamento per tali reati anche qualora comportino una pena detentiva della durata massima inferiore a 3 anni. Anche i reati connessi al terrorismo ai sensi della direttiva (UE) 2017/541 del Parlamento europeo e del Consiglio, come pure i reati relativi all'abuso e allo sfruttamento sessuale dei minori di cui alla direttiva 2011/93/UE del Parlamento europeo e del Consiglio, non dovrebbero richiedere la soglia minima di una pena detentiva della durata massima di 3 anni.

[12 b]
Art. 10 (Esecuzione dell'EPOC)
5. Qualora il destinatario ritenga, sulla base delle sole informazioni contenute nell'EPOC, che l'esecuzione dell'EPOC possa interferire con le immunità o i privilegi o con le norme sulla determinazione o la limitazione della responsabilità penale relative alla libertà di stampa o alla libertà di espressione in altri mezzi di comunicazione, a norma del diritto dello Stato di esecuzione, ne informa l'autorità di emissione e l'autorità di esecuzione utilizzando il modulo di cui all'allegato III.
Qualora non abbia avuto luogo alcuna notifica all'autorità di esecuzione a norma dell'articolo 8, l'autorità di emissione tiene conto delle informazioni di cui al primo comma del presente paragrafo e decide, di propria iniziativa o su richiesta dell'autorità di esecuzione, se ritirare, adattare o mantenere l'ordine europeo di produzione.
Qualora abbia avuto luogo una notifica all'autorità di esecuzione a norma dell'articolo 8, l'autorità di emissione tiene conto delle informazioni di cui al primo comma del presente paragrafo e decide se ritirare, adattare o mantenere l'ordine europeo di produzione. L'autorità di esecuzione può decidere di far valere i motivi di rifiuto di cui all'articolo 12.

[14]
Art. 6 (Condizioni di emissione dell'ordine europeo di conservazione)
2. Un ordine europeo di conservazione deve essere necessario e proporzionato al fine di impedire la rimozione, la cancellazione o la modifica di dati in vista della presentazione di una successiva richiesta di produzione dei medesimi tramite l'assistenza giudiziaria, un ordine europeo d'indagine (OEI) o un ordine europeo di produzione, tenendo conto dei diritti della persona oggetto di indagini o imputata.
3. Un ordine europeo di conservazione può essere emesso per tutti i reati, laddove avrebbe potuto essere emesso alle stesse condizioni in un caso interno analogo, e per l'esecuzione di una pena o di una misura di sicurezza detentiva di almeno quattro mesi, a seguito di un procedimento penale, irrogata con decisione non pronunciata in contumacia, nei casi in cui la persona condannata è latitante.

[15]

Art. 11 (Esecuzione dell'EPOC-PR)
4. Qualora ritenga, sulla base delle sole informazioni contenute nell'EPOC-PR, che l'esecuzione dell'EPOC-PR possa interferire con le immunità o i privilegi o con le norme sulla determinazione o la limitazione della responsabilità penale relative alla libertà di stampa o alla libertà di espressione in altri mezzi di comunicazione, a norma del diritto dello Stato di esecuzione, il destinatario ne informa l'autorità di emissione e l'autorità di esecuzione usando il modulo di cui all'allegato III.

[16]
Art. 3 (Definizioni)
10) «dati richiesti al solo scopo di identificare l'utente»: gli indirizzi IP e, se necessario, le porte sorgenti e le marche temporali pertinenti, vale a dire la data e l'ora, o gli equivalenti tecnici di tali identificativi e le informazioni connesse, se richiesto dalle autorità di contrasto o dalle autorità giudiziarie al solo scopo di identificare l'utente in una specifica indagine penale;

[16 b]
Considerando 36
È opportuno che nel processo di emissione o di convalida di un ordine europeo di produzione o di un ordine europeo di conservazione intervenga sempre un'autorità giudiziaria. Considerata la natura più sensibile dei dati relativi al traffico, ad eccezione dei dati richiesti al solo scopo di identificare l'utente ai sensi del presente regolamento, e dei dati relativi al contenuto, l'emissione o la convalida di un ordine europeo di produzione per ottenere tali categorie di dati richiede il riesame da parte di un giudice. Poiché i dati relativi agli abbonati e i dati richiesti al solo scopo di identificare l'utente ai sensi del presente regolamento sono meno sensibili, un ordine europeo di produzione per ottenere tali dati può essere emesso o convalidato anche da un pubblico ministero competente.
……

[18]
Art. 4 (Autorità di emissione)
3. Un ordine europeo di conservazione relativo a dati di qualsiasi categoria può essere emesso solamente da:
a) un giudice, un organo giurisdizionale, un magistrato inquirente o un pubblico ministero competente nel caso interessato; o
b) qualsiasi altra autorità competente, definita dallo Stato di emissione che, nel caso di specie, agisca in qualità di autorità inquirente nel procedimento penale e sia competente a disporre l'acquisizione di prove in conformità del diritto nazionale; in tal caso, l'ordine europeo di conservazione è convalidato, previo esame della sua conformità alle condizioni di emissione di un ordine europeo di conservazione ai sensi del presente regolamento, da un giudice, un organo giurisdizionale, un magistrato inquirente o un pubblico ministero nello Stato di emissione.

[19]
Art. 10 (Esecuzione dell'EPOC)
Qualora sia prevista una notifica all'autorità di esecuzione a norma dell'articolo 8 e tale autorità non abbia fatto valere alcun motivo di rifiuto a norma dell'articolo 12 entro 10 giorni dalla ricezione dell'EPOC, il destinatario provvede affinché i dati richiesti siano trasmessi direttamente all'autorità di emissione o alle autorità di contrasto, come indicato nell'EPOC, al termine di tale periodo di 10 giorni. Se l'autorità di esecuzione conferma all'autorità di emissione e al destinatario, già prima della scadenza di tale termine di 10 giorni, che non farà valere motivi di rifiuto, il destinatario agisce quanto prima dopo tale conferma e al più tardi al termine del periodo di 10 giorni"

[20]
Art. 11 (Esecuzione dell'EPOC-PR)
1. Quando riceve un EPOC-PR il destinatario provvede, senza indebito ritardo, a conservare i dati richiesti. L'obbligo di conservare i dati cessa dopo 60 giorni, a meno che l'autorità di emissione confermi, usando il modulo di cui all'allegato V, che è stata emessa una successiva richiesta di produzione. Durante tale periodo di 60 giorni l'autorità di emissione, usando il modulo di cui all'allegato VI, può prorogare la durata dell'obbligo di conservare i dati di un ulteriore periodo di 30 giorni, se necessario per consentire l'emissione di una successiva richiesta di produzione.

[21]
Considerando 20
L'applicazione del presente regolamento non dovrebbe pregiudicare l'uso della cifratura da parte dei prestatori di servizi o dei loro utenti. 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.

FONTI

- https://www.magistraturaindipendente.it/lordine-di-produzione-e-di-conservazione-europeo-delle-prove-elettroniche.htm
- https://www.consilium.europa.eu/it/policies/e-evidence/
- https://www.consilium.europa.eu/it/press/press-releases/2019/03/08/e-evidence-package-council-agrees-its-position-on-rules-to-appoint-legal-representatives-for-the-gathering-of-evidence/
- Oscar Calavita,"La proposta di regolamento sugli ordini di produzione e conservazione europei: Commissione, Consiglio e Parlamento a confronto - in "La legislazione penale" 30/03/2021