Consiglio dell'Unione europea

Bruxelles, 18 aprile 2018
(OR. en)

8110/18

Fascicolo interistituzionale: 2018/0108 (COD)

JAI 323
COPEN 104
CYBER 66
DROIPEN 53
JAIEX 27
ENFOPOL 171
TELECOM 94
DAPIX 106
EJUSTICE 27
MI 269
IA 101
CODEC 577

PROPOSTA

Origine:	Jordi AYET PUIGARNAU, Direttore, per conto del Segretario Generale della Commissione europea
Data:	18 aprile 2018
Destinatario:	Jeppe TRANHOLM-MIKKELSEN, Segretario Generale del Consiglio dell'Unione europea
n. doc. Comm.:	COM(2018) 225 final
Oggetto:	Proposta di REGOLAMENTO DEL PARLAMENTO EUROPEO E DEL CONSIGLIO relativo agli ordini europei di produzione e di conservazione di prove elettroniche in materia penale

Si trasmette in allegato, per le delegazioni, il documento COM(2018) 225 final.

All.: COM(2018) 225 final

COMMISSIONE
EUROPEA

Strasburgo, 17.4.2018
COM(2018) 225 final

2018/0108 (COD)

Proposta di

REGOLAMENTO DEL PARLAMENTO EUROPEO E DEL CONSIGLIO

relativo agli ordini europei di produzione e di conservazione di prove elettroniche in materia penale

{SWD(2018) 118 final} - {SWD(2018) 119 final}

RELAZIONE

1. CONTESTO DELLA PROPOSTA

• Motivi e obiettivi della proposta

Usare i social media, la posta elettronica, i servizi di messaggistica e le applicazioni ("app") per comunicare, lavorare, socializzare e ottenere informazioni è ormai prassi comune in molte parti del mondo. Questi servizi interconnettono centinaia di milioni di utenti e contribuiscono notevolmente al loro benessere economico e sociale in tutta l'Unione e al suo esterno. Tuttavia possono anche essere usati impropriamente come strumenti per commettere o facilitare reati, compresi reati gravi come gli attentati terroristici. In questi casi, tali servizi e app sono spesso l'unico posto in cui gli inquirenti possono trovare indizi per scoprire l'autore di un reato e ottenere prove utilizzabili in giudizio.

Dato che internet non conosce frontiere, tali servizi possono essere prestati da qualsiasi luogo del mondo e non richiedono necessariamente un'infrastruttura fisica né la presenza di un'azienda o di personale negli Stati membri in cui sono offerti o nel mercato interno nel suo insieme. Non richiedono nemmeno un luogo specifico in cui conservare i dati: spesso il prestatore di servizi sceglie tale luogo in base a considerazioni legittime quali la sicurezza dei dati, le economie di scala e la rapidità di accesso. Di conseguenza, in un numero crescente di procedimenti penali riguardanti qualsiasi tipo di reato[1], le autorità degli Stati membri richiedono l'accesso ai dati che potrebbero servire da prove e che sono conservati al di fuori del loro paese e/o da prestatori di servizi situati in altri Stati membri o in paesi terzi.

Per trattare i casi in cui le prove o il prestatore di servizi si trovano all'estero, vari decenni fa sono stati elaborati meccanismi per la cooperazione tra paesi[2]. Nonostante le riforme periodiche, tali meccanismi di cooperazione subiscono una pressione crescente a causa della sempre maggiore necessità di accedere tempestivamente alle prove elettroniche a livello transfrontaliero. Per risolvere tale problema un certo numero di Stati membri e di paesi terzi ha deciso di ampliare gli strumenti nazionali. La frammentazione giuridica che ne è conseguita genera tuttavia incertezza giuridica e obblighi contrastanti, e solleva dubbi circa la protezione dei diritti fondamentali e delle garanzie procedurali delle persone interessate da tali richieste.

Nel 2016 il Consiglio ha esortato a intraprendere azioni concrete sulla base di un approccio comune dell'UE per rendere più efficiente l'assistenza giudiziaria, migliorare la cooperazione tra le autorità degli Stati membri e i prestatori di servizi aventi sede in paesi terzi e proporre soluzioni al problema della determinazione e della competenza di esecuzione[3] nel ciberspazio[4]. Analogamente, il Parlamento europeo ha messo in rilievo le sfide che l'attuale quadro giuridico frammentato può creare per i prestatori di servizi che intendono soddisfare le

---

1 Cfr. sezioni 2.1.1 e 2.3 della valutazione d'impatto.

2 Nell'Unione i meccanismi di riconoscimento reciproco attualmente si basano sull'ordine europeo di indagine, mentre con i paesi terzi sull'assistenza giudiziaria.

3 Ai fini del presente documento, per "competenza esecutiva" s'intende la competenza delle autorità pertinenti a compiere un atto di indagine.

4 Conclusioni del Consiglio dell'Unione europea sul miglioramento della giustizia penale nel ciberspazio, ST9579/16.

richieste dei servizi di contrasto, e ha invitato a mettere a punto un quadro giuridico europeo che comprenda anche garanzie per i diritti e le libertà di tutti gli interessati[5].

La presente proposta affronta il problema specifico dalla natura volatile delle prove elettroniche e della loro dimensione internazionale. Essa mira ad adattare i meccanismi di cooperazione all'era digitale, fornendo alle autorità giudiziarie e di contrasto gli strumenti per stare al passo con le attuali modalità di comunicazione dei criminali e combattere le forme moderne di criminalità. Tali strumenti sono subordinati alla condizione di essere soggetti a forti meccanismi di tutela dei diritti fondamentali. La presente proposta intende migliorare la certezza del diritto per le autorità, i prestatori di servizi e le persone interessate e mantenere uno standard elevato per le richieste delle autorità di contrasto, garantendo così la protezione dei diritti fondamentali, la trasparenza e la responsabilità. Essa inoltre rende più rapido il processo per assicurare ed ottenere prove elettroniche conservate e/o detenute da prestatori di servizi stabiliti in un'altra giurisdizione. Lo strumento proposto si affiancherà agli attuali strumenti di cooperazione giudiziaria, che rimangono pertinenti e possono essere usati dalle autorità competenti quando lo ritengono appropriato. Parallelamente, la Commissione si sta adoperando per rafforzare gli attuali meccanismi di cooperazione giudiziaria attraverso misure quali la creazione di una piattaforma sicura per lo scambio rapido di richieste tra le autorità giudiziarie dell'Unione e l'investimento di 1 milione di EUR nella formazione dei professionisti di tutti gli Stati membri dell'UE in materia di assistenza giudiziaria e cooperazione, in particolare con gli Stati Uniti, che sono il paese terzo che riceve il maggior numero di richieste dall'UE[6].

Per la notifica e l'esecuzione degli ordini emessi ai sensi dello strumento proposto, le autorità dovrebbero avvalersi del rappresentante legale designato dai prestatori di servizi. La Commissione presenta oggi una proposta volta a garantire che tali rappresentanti legali siano effettivamente designati. Offre una soluzione comune a tutta l'UE per rivolgere gli ordini ai prestatori di servizi per mezzo di un rappresentante legale.

- **Coerenza con il quadro giuridico dell'UE in vigore nel settore e con la convenzione di Budapest del Consiglio d'Europa**

L'attuale quadro giuridico dell'UE si compone, da un lato, degli strumenti di cooperazione dell'Unione in materia penale, quali la direttiva 2014/41/UE relativa all'ordine europeo di indagine penale[7] (direttiva OEI), la convenzione relativa all'assistenza giudiziaria in materia penale tra gli Stati membri dell'Unione europea[8], la decisione 2002/187/GAI del Consiglio che istituisce l'Eurojust[9], il regolamento (UE) 2016/794 su Europol[10], la decisione quadro

5 P8_TA(2017)0366.

6 https://ec.europa.eu/home-affairs/sites/homeaffairs/files/docs/pages/20170522_non-paper_electronic_evidence_en.pdf

7 Direttiva 2014/41/UE del Parlamento europeo e del Consiglio, del 3 aprile 2014, relativa all'ordine europeo di indagine penale (GU L 130 dell'1.5.2014, pag. 1).

8 Atto del Consiglio del 29 maggio 2000 che stabilisce, conformemente all'articolo 34 del trattato sull'Unione europea, la convenzione relativa all'assistenza giudiziaria in materia penale tra gli Stati membri dell'Unione europea.

9 Decisione 2002/187/GAI del Consiglio, del 28 febbraio 2002, che istituisce l'Eurojust per rafforzare la lotta contro le forme gravi di criminalità. Nel 2013 la Commissione ha adottato una proposta di regolamento per riformare Eurojust (proposta di regolamento del Parlamento europeo e del Consiglio che istituisce l'Agenzia dell'Unione europea per la cooperazione giudiziaria penale (Eurojust), COM/2013/0535 final).

2002/465/GAI del Consiglio relativa alle squadre investigative comuni[11], e, dall'altro, degli accordi bilaterali tra l'Unione e paesi terzi, quali gli accordi sull'assistenza giudiziaria con gli USA[12] e con il Giappone[13].

Introducendo l'ordine europeo di produzione e l'ordine europeo di conservazione, la proposta rende più facile, nell'ambito di un procedimento penale, assicurare e raccogliere prove elettroniche conservate o detenute da prestatori di servizi in un'altra giurisdizione. La direttiva OEI, che ha in larga misura sostituito la convenzione relativa all'assistenza giudiziaria in materia penale, riguarda qualsiasi atto d'indagine[14]. Copre quindi anche l'accesso alle prove elettroniche, ma non contiene disposizioni specifiche su questo tipo di prove[15]. Il nuovo strumento non sostituirà l'OEI per l'ottenimento di prove elettroniche, ma fornirà alle autorità un ulteriore strumento. In alcune situazioni l'OEI risulta preferibile per le autorità pubbliche, ad esempio quando devono essere compiuti diversi atti d'indagine nello Stato membro di esecuzione. Poiché l'ottenimento di prove elettroniche presenta problematiche specifiche che non riguardano gli altri atti d'indagine contemplati dalla direttiva OEI, anziché modificare la direttiva OEI si è deciso di creare un nuovo strumento per tali prove.

Per agevolare la raccolta di prove elettroniche, il nuovo strumento si baserà sui principi del reciproco riconoscimento. Ai fini della notifica e dell'esecuzione dell'ordine non occorrerà coinvolgere direttamente l'autorità del paese in cui si trova il destinatario dell'ordine, tranne se il destinatario non vi ottempera spontaneamente, nel qual caso l'ordine sarà fatto eseguire e sarà necessario l'intervento dell'autorità competente del paese in cui si trova il rappresentante. Lo strumento richiede pertanto una serie di solide garanzie e disposizioni, come la convalida da parte di un'autorità giudiziaria in ogni singolo caso. Ad esempio, l'ordine europeo di produzione riguardante dati relativi alle operazioni o al contenuto (ma non dati relativi agli abbonati o agli accessi) può essere emesso solo per reati punibili nello Stato di emissione con una pena detentiva della durata massima di almeno 3 anni o per specifici reati contro la sicurezza cibernetica, favoriti dall'uso del ciberspazio o connessi al terrorismo, specificati nella proposta.

I dati personali rientranti nell'ambito di applicazione del regolamento proposto sono protetti e possono essere trattati solo in conformità con il regolamento generale sulla protezione dei dati[16] e la direttiva sulla protezione dei dati nelle attività di polizia e giustizia[17]. Il

---

10 Regolamento (UE) 2016/794 del Parlamento europeo e del Consiglio, dell'11 maggio 2016, che istituisce l'Agenzia dell'Unione europea per la cooperazione nell'attività di contrasto (Europol) e sostituisce e abroga le decisioni del Consiglio 2009/371/GAI, 2009/934/GAI, 2009/935/GAI, 2009/936/GAI e 2009/968/GAI.

11 Decisione quadro 2002/465/GAI del Consiglio, del 13 giugno 2002, relativa alle squadre investigative comuni.

12 Decisione 2009/820/PESC del Consiglio, del 23 ottobre 2009, relativa alla conclusione, a nome dell'Unione europea, dell'accordo sull'estradizione tra l'Unione europea e gli Stati Uniti d'America e dell'accordo sulla mutua assistenza giudiziaria tra l'Unione europea e gli Stati Uniti d'America.

13 Decisione 2010/616/UE del Consiglio, del 7 ottobre 2010, relativa alla conclusione dell'accordo tra l'Unione europea e il Giappone sull'assistenza giudiziaria reciproca in materia penale

14 Ad esclusione delle squadre investigative comuni (cfr. articolo 3 della direttiva OEI); non tutti gli Stati membri partecipano alla direttiva OEI (Irlanda e Danimarca).

15 Fatto salvo un riferimento - all'articolo 10 paragrafo 2, lettera e) - all'individuazione di persone titolari di un indirizzo IP, per le quali la doppia incriminabilità non può essere fatta valere come motivo di rifiuto del riconoscimento o dell'esecuzione della richiesta.

16 Regolamento (UE) n. 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera

regolamento generale sulla protezione dei dati entra in applicazione il 25 maggio 2018, mentre la direttiva deve essere recepita dagli Stati membri entro il 6 maggio 2018.

La convenzione di Budapest del Consiglio d'Europa sulla criminalità informatica (STCE n. 185), ratificata dalla maggior parte degli Stati membri dell'UE, stabilisce meccanismi internazionali di cooperazione contro la criminalità informatica[18]. Essa riguarda i reati commessi tramite internet e altre reti informatiche. Fa obbligo alle parti di definire i poteri e le procedure per ottenere prove elettroniche e prestarsi assistenza giudiziaria, non solo in relazione ai reati informatici. In particolare, la convenzione impone alle parti di istituire ordini di produzione per ottenere dati informatici da prestatori di servizi presenti sul loro territorio e dati relativi agli abbonati da prestatori di servizi che offrono servizi sul loro territorio. Prevede inoltre la possibilità di ordinare la conservazione di dati qualora sussistano motivi per ritenere che i dati informatici siano particolarmente a rischio di perdita o modificazione. La notificazione e l'esecutività degli ordini nazionali di produzione nei confronti di prestatori stabiliti al di fuori del territorio di una delle parti sollevano problematiche. A tale proposito, sono attualmente all'esame ulteriori misure per migliorare l'accesso transfrontaliero alle prove elettroniche[19].

- **Sintesi del regolamento proposto**

Il regolamento proposto istituisce ordini europei di produzione e di conservazione vincolanti. Entrambi gli ordini devono essere emessi o convalidati da un'autorità giudiziaria di uno Stato membro. Un ordine può essere emesso per chiedere di conservare o produrre dati che sono conservati da un prestatore di servizi situato in un'altra giurisdizione e che sono necessari come prova in indagini o procedimenti penali. Tali ordini possono essere emessi solo se una misura dello stesso tipo è disponibile per lo stesso reato in una situazione nazionale comparabile nello Stato di emissione. Entrambi gli ordini possono essere notificati ai prestatori di servizi di comunicazione elettronica, alle reti sociali, ai mercati online, ad altri prestatori di servizi di hosting e ai fornitori di infrastrutture internet quali l'indirizzo IP e registri di nomi di dominio, o ai loro rappresentanti legali, se esistenti. L'ordine europeo di conservazione, analogamente all'ordine europeo di produzione, è rivolto al rappresentante legale al di fuori della giurisdizione dello Stato membro di emissione affinché provveda alla conservazione di dati in vista di una successiva richiesta di produzione dei medesimi, ad esempio tramite i canali di assistenza giudiziaria in caso di paesi terzi o attraverso un OEI tra gli Stati membri partecipanti. A differenza delle misure di sorveglianza e degli obblighi legali di conservazione dei dati, che non sono previsti dal presente regolamento, l'ordine europeo di

---

circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati).

17 Direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio.

18 Nella Strategia dell'Unione europea per la cibersicurezza del 2013, la convenzione di Budapest è stata riconosciuta come il principale quadro multilaterale per la lotta alla criminalità informatica — comunicazione congiunta della Commissione e del vicepresidente della Commissione/alto rappresentante dell'Unione per gli affari esteri e la politica di sicurezza "Strategia dell'Unione europea per la cibersicurezza: un ciberspazio aperto e sicuro", JOIN(2013)1 final.

19 Durante la 17ª sessione (giugno 2017) la commissione per la convenzione sulla criminalità informatica (T-CY) ha adottato il mandato per la preparazione di un secondo protocollo addizionale alla convenzione ("secondo protocollo addizionale"), che dovrà essere elaborato e ultimato dalla T-CY entro dicembre 2019. L'obiettivo è prescindere dal luogo di conservazione dei dati.

conservazione è un ordine emesso o convalidato da un'autorità giudiziaria in un procedimento penale previa valutazione della proporzionalità e necessità nel singolo caso. Al pari dell'ordine europeo di produzione, esso si riferisce a specifici autori, noti o sconosciuti, di un reato che è già stato commesso. L'ordine europeo di conservazione consente di chiedere la conservazione solo di dati che sono già conservati al momento della ricezione dell'ordine, e non di accedere a dati in una fase successiva alla ricezione dell'ordine.

Entrambi gli ordini possono essere usati solo nell'ambito di un procedimento penale, dalla fase preprocessuale delle indagini preliminari fino alla chiusura del procedimento con sentenza o altra decisione. Gli ordini per la produzione di dati relativi agli abbonati o agli accessi possono essere emessi per qualsiasi reato, mentre quelli per la produzione di dati relativi alle operazioni o al contenuto possono essere emessi solo per reati punibili nello Stato di emissione con una pena detentiva della durata massima di almeno 3 anni o per specifici reati precisati nella proposta e se vi è un collegamento specifico con gli strumenti elettronici e i reati rientranti nel campo di applicazione della direttiva (UE) 2017/541 sulla lotta contro il terrorismo.

Tenuto conto dei diversi livelli di invasività delle misure imposte in relazione ai dati ricercati, la proposta stabilisce una serie di condizioni e garanzie, tra cui l'obbligo di una convalida ex ante dell'ordine da parte di un'autorità giudiziaria. La proposta si applica solo ai dati conservati. Esulano dal suo ambito di applicazione le intercettazioni in tempo reale delle telecomunicazioni. La misura è limitata a quanto necessario e proporzionato ai fini del procedimento penale cui l'ordine si riferisce. Essa consente ai prestatori di servizi di ottenere chiarimenti dalle autorità di emissione, se necessario. Se i problemi sollevati non possono essere risolti e l'autorità di emissione decide di far eseguire l'ordine, il prestatore di servizi può avvalersi degli stessi motivi per opporsi all'esecuzione da parte delle proprie autorità. Inoltre, è istituita una procedura specifica per i casi in cui l'obbligo di fornire i dati contrasta con un obbligo derivante dal diritto di un paese terzo.

La legislazione dell'UE tutela i diritti degli indagati e degli imputati nei procedimenti penali, e vi sono già norme che proteggono i dati personali. Tuttavia, per le persone i cui dati sono ricercati, le garanzie supplementari previste nella proposta riconoscono diritti procedurali sia all'interno che all'esterno del procedimento penale, come la possibilità di contestare la legittimità, la necessità o la proporzionalità dell'ordine, che vanno ad aggiungersi ai motivi di impugnazione previsti dal diritto nazionale. I diritti riconosciuti dalla legge dello Stato di esecuzione sono pienamente rispettati poiché i privilegi e le immunità che proteggono i dati ricercati nello Stato membro del prestatore di servizi devono essere presi in considerazione nello Stato di emissione. È il caso, in particolare, di quando la legge dello Stato di esecuzione garantisce una protezione maggiore rispetto a quella garantita dalla legge dello Stato di emissione.

Gli ordini emessi ai sensi del regolamento proposto sono eseguiti allo stesso modo degli ordini nazionali comparabili nella giurisdizione in cui il prestatore di servizi riceve l'ordine. Il regolamento proposto prevede che gli Stati membri devono poter irrogare sanzioni efficaci e proporzionate.

2. BASE GIURIDICA, SUSSIDIARIETÀ E PROPORZIONALITÀ

• Base giuridica

La base giuridica per le azioni in questo settore è l'articolo 82, paragrafo 1, del trattato sul funzionamento dell'Unione europea, che autorizza l'adozione, secondo la procedura

legislativa ordinaria, di misure intese a definire norme e procedure per assicurare il riconoscimento in tutta l'Unione di qualsiasi tipo di sentenza e decisione giudiziaria, e di misure intese a facilitare la cooperazione tra le autorità giudiziarie o autorità omologhe degli Stati membri in relazione all'azione penale e all'esecuzione delle decisioni.

Tale base giuridica si applica ai meccanismi di cui al regolamento proposto. L'articolo 82, paragrafo 1, garantisce il riconoscimento reciproco delle decisioni con cui l'autorità giudiziaria dello Stato di emissione si rivolge a una persona giuridica in un altro Stato membro e le impone obblighi, senza il previo intervento dell'autorità giudiziaria di tale altro Stato membro. L'ordine europeo di produzione o di conservazione può comportare l'intervento dell'autorità giudiziaria dello Stato di esecuzione ove necessario per far eseguire la decisione.

- **Scelta dell'atto giuridico**

L'articolo 82, paragrafo 1, del TFUE consente al legislatore dell'Unione di adottare regolamenti e direttive.

Poiché la proposta riguarda procedure transfrontaliere, per le quali sono necessarie norme uniformi, non occorre lasciare un margine agli Stati membri per recepirle. Il regolamento è direttamente applicabile, offre chiarezza e maggiore certezza giuridica e consente di evitare interpretazioni divergenti negli Stati membri e altri problemi di recepimento incontrati dalle decisioni quadro sul riconoscimento reciproco delle sentenze e delle decisioni giudiziarie. Inoltre permette che lo stesso obbligo sia imposto in modo uniforme in tutta l'Unione. Pertanto la forma più appropriata per questo strumento di riconoscimento reciproco è il regolamento.

- **Sussidiarietà**

A causa della dimensione transfrontaliera dei problemi da affrontare, le misure contenute nella proposta devono essere adottate a livello di Unione per conseguire gli obiettivi. I reati per i quali esistono prove elettroniche spesso riguardano casi in cui il quadro giuridico nazionale, all'interno o all'esterno dell'Unione, applicabile all'infrastruttura in cui le prove elettroniche sono conservate e al prestatore di servizi che gestisce l'infrastruttura è diverso da quello applicabile alla vittima e all'autore del reato. Di conseguenza, può essere difficile e laborioso per il paese competente accedere effettivamente alle prove elettroniche oltre frontiera senza norme minime comuni. In particolare, gli Stati membri da soli avrebbero difficoltà ad affrontare le seguenti questioni:

- la frammentazione dei quadri giuridici degli Stati membri, che è stata identificata come un grosso problema per i prestatori di servizi che intendono ottemperare alle richieste sulla base di leggi nazionali diverse;
- migliori opportunità di cooperazione giudiziaria sulla base del diritto dell'UE in vigore, in particolare tramite l'OEI.

In considerazione della varietà di approcci giuridici, del numero di settori interessati (sicurezza, diritti fondamentali, compresi i diritti procedurali e la protezione dei dati personali, aspetti economici) e dell'ampia gamma di parti interessate, un atto legislativo dell'Unione è lo strumento più idoneo per affrontare i problemi individuati.

- **Proporzionalità**

La proposta stabilisce norme che consentono a un'autorità competente di uno Stato membro di ordinare a un prestatore di servizi che offre servizi nell'Unione e che non è stabilito nello stesso Stato membro di produrre o conservare prove elettroniche. Gli elementi principali della proposta, quali l'ambito di applicazione materiale dell'ordine europeo di produzione, le condizioni che garantiscono la cortesia internazionale, il meccanismo sanzionatorio e il sistema di garanzie e mezzi di ricorso, limitano la proposta a quanto è necessario per conseguire i suoi principali obiettivi. In particolare, la proposta è limitata alle richieste di dati già conservati (l'intercettazione in tempo reale delle telecomunicazioni è esclusa dall'ambito di applicazione) e agli ordini emessi nell'ambito di un procedimento penale per un reato specifico per il quale sono in corso indagini. Essa non riguarda quindi la prevenzione della criminalità né altri tipi di procedimenti o violazioni (come i procedimenti amministrativi per violazione di norme giuridiche) e non impone ai prestatori di servizi di raccogliere o conservare sistematicamente più dati di quanto non facciano per motivi aziendali o per rispettare altri obblighi di legge. Inoltre, mentre gli ordini per la produzione di dati relativi agli abbonati o agli accessi possono essere emessi per qualsiasi reato, quelli per la produzione di dati relativi alle operazioni o al contenuto possono essere emessi solo per reati punibili nello Stato di emissione con una pena detentiva della durata massima di almeno 3 anni o per specifici reati contro la sicurezza cibernetica, favoriti dall'uso del ciberspazio o connessi al terrorismo, specificati nella proposta. Infine, la proposta chiarisce le norme procedurali e le garanzie applicabili all'accesso transfrontaliero alle prove elettroniche ma non si spinge ad armonizzare le misure nazionali. Essa si limita a quanto è necessario e proporzionato per rispondere alle esigenze delle autorità giudiziarie e di contrasto nell'era digitale.

3. RISULTATI DELLE VALUTAZIONI EX POST, DELLE CONSULTAZIONI DEI PORTATORI DI INTERESSI E DELLE VALUTAZIONI D'IMPATTO

- **Consultazioni dei portatori di interessi**

Nel corso di un anno e mezzo la Commissione ha consultato tutti i portatori di interessi per individuare i problemi e le possibili soluzioni, organizzando una consultazione pubblica aperta e sondaggi mirati presso le autorità pubbliche pertinenti, riunioni di gruppi di esperti e riunioni bilaterali per discutere i potenziali effetti della normativa dell'UE e conferenze sull'accesso transfrontaliero alle prove elettroniche per raccogliere contributi per l'iniziativa.

In generale, i partecipanti alla consultazione ritengono che il crescente uso dei servizi dell'informazione ponga problemi alle autorità di contrasto, che sono spesso male equipaggiate per trattare prove online. Uno dei principali ostacoli è la lunghezza dell'iter per ottenere le prove. Altri aspetti problematici evidenziati dalle autorità pubbliche sono la mancanza di cooperazione affidabile con i prestatori di servizi, la mancanza di trasparenza e l'incertezza giuridica circa la competenza giurisdizionale per gli atti di indagine. La cooperazione transfrontaliera diretta tra le autorità di contrasto e i prestatori di servizi digitali dovrebbe aggiungere valore alle indagini penali. I prestatori di servizi e alcune organizzazioni della società civile hanno indicato che occorre garantire la certezza del diritto nella cooperazione con le autorità pubbliche e evitare i conflitti di legge. Per quanto riguarda le preoccupazioni per le ripercussioni della nuova legislazione dell'UE sui diritti, secondo i portatori di interessi condizione necessaria per qualunque strumento transfrontaliero è la predisposizione di garanzie specifiche.

Dai contributi ottenuti dalla valutazione d'impatto iniziale è emerso che i portatori di interessi ritengono che colmando le lacune dell'attuale sistema di assistenza giudiziaria si potrebbe

rendere il sistema più efficace e migliorare la certezza del diritto. Alcune organizzazioni della società civile si sono opposte a una legislazione a livello dell'UE sulla cooperazione diretta, preferendo che l'azione dell'UE si limiti al miglioramento delle procedure di assistenza giudiziaria. Questa posizione sarà portata avanti nel quadro delle misure pratiche approvate dal Consiglio nel giugno 2016.

Da un sondaggio mirato presso le autorità pubbliche degli Stati membri è emersa l'assenza di un approccio comune all'ottenimento dell'accesso transfrontaliero alle prove elettroniche, in quanto ogni Stato membro ha le proprie prassi nazionali. Anche i prestatori di servizi reagiscono in maniera diversa alle richieste delle autorità di contrasto straniere, e i tempi di risposta variano a seconda dello Stato membro richiedente. Ciò crea incertezza giuridica per tutti gli attori coinvolti.

In generale, la consultazione dei portatori di interessi ha messo in luce la frammentarietà e la complessità dell'attuale quadro giuridico, da cui conseguono ritardi durante la fase di esecuzione e l'inefficacia delle indagini e dei procedimenti nei confronti di reati per i quali è necessario l'accesso transfrontaliero alle prove elettroniche.

- **Valutazione d'impatto**

Il comitato per il controllo normativo ha emesso un parere favorevole sulla valutazione d'impatto che accompagna la presente proposta[20] e ha formulato varie proposte di miglioramento[21]. A seguito di tale parere, la valutazione d'impatto è stata modificata per approfondire ulteriormente le questioni relative ai diritti fondamentali correlate allo scambio transfrontaliero di dati, in particolare i collegamenti tra le diverse misure che fanno parte dell'opzione prescelta. La valutazione è stata modificata per rispecchiare meglio le opinioni dei portatori di interessi e degli Stati membri e il modo in cui sono state prese in considerazione. Inoltre, è stato rivisto il contesto politico per includere ulteriori riferimenti a vari aspetti, come le discussioni nei gruppi di esperti che hanno contribuito a dare forma all'iniziativa. La complementarità tra le diverse misure (in particolare la direttiva OEI, i negoziati sul protocollo addizionale alla convenzione di Budapest e il riesame congiunto dell'accordo di assistenza giudiziaria UE-USA) è stata chiarita in termini di ambito di applicazione, tempistica e intensità, e lo scenario di base è stato riveduto per rispecchiare meglio gli sviluppi che potrebbero verificarsi indipendentemente dall'adozione delle misure proposte. Infine, sono stati aggiunti diagrammi di flusso per descrivere meglio le procedure per lo scambio dei dati.

Sono state esaminate quattro principali opzioni strategiche oltre allo scenario di base (opzione O): una serie di misure pratiche per migliorare le procedure di cooperazione giudiziaria e la cooperazione diretta tra le autorità pubbliche e i prestatori di servizi (opzione A: non legislativa); un'opzione che combina le misure pratiche dell'opzione A con soluzioni internazionali a livello bilaterale o multilaterale (opzione B: legislativa); un'opzione che

---

20 Documento di lavoro dei servizi della Commissione — *Impact Assessment accompanying the Proposal for a Regulation on European Production and Preservation Orders for electronic evidence in criminal matters and the Proposal for a Directive laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings*, SWD(2018) 118.

21 Parere del comitato per il controllo normativo della Commissione europea sul documento *Impact Assessment accompanying the Proposal for a Regulation on European Production and Preservation Orders for electronic evidence in criminal matters and the Proposal for a Directive laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings*, SEC(2018) 199.

combina le misure dell'opzione B con un ordine europeo di produzione e una misura per migliorare l'accesso alle banche dati che forniscono informazioni sugli abbonati sulla base di una ricerca, come il sistema WHOIS per i nomi di dominio (opzione C: legislativa); un'opzione che combina le misure dell'opzione C con una legislazione sull'accesso diretto ai dati conservati a distanza (opzione D: legislativa)[22].

Se non viene presa nessuna misura (opzione O), l'aumento del numero di richieste peggiorerà la situazione. Tutte le altre opzioni contribuiscono a realizzare gli obiettivi dell'iniziativa, ma in misura diversa. L'opzione A migliorerebbe l'efficienza dei processi attuali, ad esempio migliorando la qualità delle richieste, ma il margine di miglioramento sarebbe limitato dalle carenze strutturali dell'attuale sistema.

L'opzione B permetterebbe più miglioramenti prevedendo soluzioni accettate a livello internazionale, ma il risultato di queste soluzioni dipenderebbe in larga misura dai paesi terzi. Le soluzioni sono pertanto incerte e meno efficaci di una soluzione dell'Unione e incapaci di offrire le stesse garanzie di quest'ultima.

L'opzione C apporterebbe chiaramente un valore aggiunto rispetto alle precedenti opzioni e inoltre fornirebbe uno strumento intra-UE per la cooperazione diretta con i prestatori di servizi, che risponderebbe alla maggior parte delle problematiche individuate nel caso in cui un prestatore di servizi detenga i dati ricercati.

L'opzione D è la più completa. Oltre alle misure di cui sopra, comporta una misura legislativa sull'accesso diretto nelle situazioni in cui il coinvolgimento del prestatore di servizi non è necessario.

La presente iniziativa legislativa proposta dalla Commissione si basa sui risultati della valutazione d'impatto. Essa sarà integrata dalle misure pratiche descritte nella valutazione d'impatto e dai lavori sul protocollo addizionale alla convenzione di Budapest. Sulla base di tale proposta legislativa, la Commissione discuterà con gli Stati Uniti e altri paesi terzi la possibilità di futuri accordi bilaterali o multilaterali sull'accesso transfrontaliero alle prove elettroniche con le relative garanzie. Per quanto concerne le misure dell'opzione D sull'accesso diretto e sull'accesso alle banche dati, la Commissione attualmente non propone alcuna iniziativa legislativa e rifletterà sul modo più appropriato di procedere al riguardo.

L'iniziativa dovrebbe aumentare l'efficacia e l'efficienza delle indagini e delle azioni penali nonché la trasparenza e la responsabilità, e assicurare il rispetto dei diritti fondamentali. Dovrebbe inoltre promuovere la fiducia nel mercato unico digitale, migliorando la sicurezza e riducendo la percezione di impunità per i reati commessi su dispositivi connessi in rete o tramite tali dispositivi.

Per le autorità pubbliche, l'iniziativa dovrebbe generare costi iniziali di attuazione che, a lungo termine, dovrebbero essere compensati dai risparmi in costi correnti. Le autorità nazionali dovrebbero inizialmente adeguarsi alle nuove procedure e procedere ad attività di formazione. Dopo però trarrebbero vantaggio dalla semplificazione e dalla centralizzazione e

[22] Per maggiori dettagli si rinvia al documento di lavoro dei servizi della Commissione — *Impact Assessment accompanying the Proposal for a Regulation on European Production and Preservation Orders for electronic evidence in criminal matters and the Proposal for a Directive laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings*, SWD(2018) 118.

dalla chiarezza del quadro giuridico che disciplina le richieste di accesso ai dati, poiché ne dovrebbero conseguire guadagni di efficienza. Analogamente, poiché l'opzione prescelta dovrebbe eliminare la pressione sui canali di cooperazione giudiziaria, i paesi che ricevono le richieste dovrebbero vedere una riduzione del numero di richieste da trattare.

I prestatori di servizi dovrebbero adattarsi al nuovo quadro legislativo mettendo a punto (nuove) procedure e provvedendo alla formazione del personale. D'altro canto, un quadro armonizzato potrebbe ridurre l'onere per tali prestatori che attualmente rispondono alle richieste di dati non relativi al contenuto, dovendole valutare nel quadro delle diverse legislazioni di tutti gli Stati membri. La certezza giuridica e l'armonizzazione delle procedure dovrebbero avere un impatto positivo anche sulle piccole e medie imprese, in quanto allevierebbero l'onere amministrativo e favorirebbero la competitività. Nel complesso, l'iniziativa dovrebbe generare risparmi anche per loro.

- **Diritti fondamentali**

La proposta potrebbe potenzialmente incidere su una serie di diritti fondamentali:

- i diritti delle persone fisiche ai cui dati è previsto l'accesso: il diritto alla protezione dei dati personali; il diritto al rispetto della vita privata e familiare; il diritto alla libertà di espressione; il diritto alla difesa; il diritto a un ricorso effettivo e a un giudice imparziale;
- i diritti del prestatore di servizi: il diritto alla libertà d'impresa; il diritto a un ricorso effettivo;
- i diritti di tutti i cittadini: il diritto alla libertà e alla sicurezza.

Tenuto conto delle pertinenti disposizioni dell'*acquis* in materia di protezione dei dati, nel regolamento proposto sono incluse garanzie sufficienti e importanti per garantire che i diritti di tali soggetti siano tutelati.

Poiché gli ordini possono essere emessi solo nell'ambito di un procedimento penale, sia durante la fase preprocessuale che durante quella processuale, e se vi sono situazioni nazionali comparabili, tutte le garanzie procedurali di diritto penale sono applicabili, tra cui, in particolare, il diritto a un equo processo sancito dall'articolo 6 della convenzione europea dei diritti dell'uomo ("CEDUA") e dagli articoli 47 e 48 della Carta dei diritti fondamentali dell'Unione europea ("Carta") e la legislazione pertinente dell'UE in materia di diritti procedurali nei procedimenti penali, vale a dire la direttiva 2010/64/UE sul diritto all'interpretazione e alla traduzione nei procedimenti penali, la direttiva 2012/13/UE sul diritto a ricevere informazioni relative ai diritti e all'accusa e ad accedere al fascicolo, la direttiva 2013/48/UE relativa al diritto di avvalersi di un difensore e di comunicare con familiari al momento dell'arresto e della detenzione, la direttiva 2016/343 sul rafforzamento di alcuni aspetti della presunzione di innocenza e del diritto di presenziare al processo, la direttiva 2016/800 sulle garanzie procedurali per i minori e la direttiva 2016/1919 sull'ammissione al patrocinio a spese dello Stato per indagati e imputati nell'ambito di procedimenti penali e per le persone ricercate nell'ambito di procedimenti di esecuzione del mandato d'arresto europeo.

Più specificamente, il previo intervento di un'autorità giudiziaria ai fini dell'emissione dell'ordine garantisce che siano verificate la legittimità della misura e la sua necessità e proporzionalità nel caso di specie. Garantisce inoltre che l'ordine non abbia effetti indebiti sui diritti fondamentali, ivi compreso su principi giuridici come il segreto professionale dell'avvocato. L'autorità di emissione è tenuta ad assicurarsi che nel caso di specie la misura

sia necessaria e proporzionata, anche in considerazione della gravità del reato oggetto dell'indagine. La proposta prevede inoltre delle soglie per i dati relativi alle operazioni e al contenuto, garantendo che, per tali dati, l'ordine europeo di produzione sia usato solo per i reati più gravi.

La proposta prevede esplicitamente anche il diritto a un ricorso effettivo per le persone i cui dati sono richiesti. Le immunità e i privilegi di talune professioni, come quella di avvocato, nonché gli interessi fondamentali connessi alla sicurezza o alla difesa nazionali nello Stato del destinatario devono parimenti essere presi in considerazione nel corso del processo nello Stato di emissione. Il riesame da parte di un'autorità giudiziaria costituisce un'ulteriore garanzia.

Essendo una misura vincolante, l'ordine incide anche sui diritti dei prestatori di servizi, in particolare sulla libertà d'impresa. La proposta comprende il diritto del prestatore di servizi di sollevare obiezioni nello Stato membro di emissione, ad esempio se l'ordine non è stato emesso o convalidato da un'autorità giudiziaria. Se l'ordine è trasmesso allo Stato di esecuzione per esecuzione, l'autorità di esecuzione può decidere, previa consultazione dell'autorità di emissione, di non riconoscere o non eseguire l'ordine qualora i motivi di opposizione sollevati siano evidenti. Inoltre, in caso di avvio della procedura di esecuzione, il destinatario può opporsi all'ordine dinanzi all'autorità di esecuzione sulla base di uno di tali motivi limitati, tra cui, ad esempio, se è evidente che l'ordine non è stato emesso o convalidato da un'autorità competente, se ottemperare all'ordine significa violare manifestamente la Carta o se l'ordine è manifestamente arbitrario. Ciò non esclude il diritto del destinatario a un ricorso giurisdizionale effettivo contro l'eventuale decisione che infligge una sanzione.

Un potenziale problema connesso alle misure dell'UE in questo settore è la possibilità che esse spingano paesi terzi a imporre ai prestatori di servizi dell'UE obblighi di reciprocità incompatibili con le condizioni dei diritti fondamentali dell'Unione, tra cui l'alto livello di protezione dei dati garantito dall'*acquis* dell'UE. La proposta affronta tale situazione in due modi: in primo luogo, prevedendo una misura che contiene solide garanzie e riferimenti espliciti alle condizioni e garanzie già previste dall'*acquis* dell'UE e che funge così da modello per la legislazione straniera; in secondo luogo, prevedendo una specifica clausola di "contrasto di obblighi" che consente ai prestatori di servizi di identificare e segnalare eventuali obblighi contrastanti e far scattare un controllo giurisdizionale. Tale clausola serve per garantire il rispetto sia di disposizioni di legge generali di divieto, quali l'*Electronic Communications Privacy Acta* (EPA) degli Stati Uniti che vieta la divulgazione di dati relativi al contenuto che rientrano nel suo ambito di applicazione geografico ad eccezione di casi limitati, sia di leggi che non vietano in generale la divulgazione ma possono farlo in singoli casi. Per i casi rientranti nell'ambito di applicazione dell'EPA, attualmente l'accesso ai dati relativi al contenuto può essere impedito in determinate situazioni, pertanto gli accordi di assistenza giudiziaria dovrebbero restare lo strumento principale per accedere a tali dati. Tuttavia, a seguito delle modifiche introdotte dal *CLOU Acta*[23], le disposizioni generali di divieto potrebbero essere abolite qualora l'UE concluda un accordo con gli Stati Uniti. Ulteriori accordi internazionali con altri partner chiave possono ridurre ulteriormente le situazioni di conflitto di leggi.

[23] Il 23 marzo 2018 gli Stati Uniti hanno adottato il *Clarifying Lawful Overseas Use of Data (CLOUD) Act*. Tale legge è consultabile qui.

Alla luce di quanto precede, le misure della presente proposta sono compatibili con i diritti fondamentali.

4. INCIDENZA SUL BILANCIO

Nessuna.

5. ALTRI ELEMENTI

- **Piani attuativi e modalità di monitoraggio, valutazione e informazione**

Il regolamento è direttamente applicabile nell'Unione. Esso sarà applicato direttamente dagli operatori del settore, senza la necessità di modificare i sistemi giuridici nazionali.

Il regolamento formerà oggetto di valutazione e la Commissione presenterà una relazione al Parlamento europeo e al Consiglio al più tardi 5 anni dopo la sua entrata in vigore. Sulla base dei risultati della relazione, in particolare del fatto che il regolamento lasci o meno lacune rilevanti nella pratica, e tenuto conto degli sviluppi tecnologici, la Commissione valuterà l'opportunità di estendere il campo di applicazione del regolamento. Se necessario, la Commissione presenterà proposte di modifica del regolamento. Gli Stati membri trasmetteranno alla Commissione le informazioni necessarie per la preparazione della relazione. Essi raccoglieranno i dati necessari per il monitoraggio annuale del regolamento.

Se necessario, la Commissione elaborerà orientamenti per i prestatori di servizi per agevolare l'ottemperanza agli obblighi imposti dal regolamento.

- **Illustrazione dettagliata delle singole disposizioni della proposta**

	REGOLAMENTO	
	Articolo	**Considerando**
I. Oggetto, definizioni e ambito di applicazione	1. Oggetto	1-15
	2. Definizioni	16-23
	3. Ambito di applicazione	24-27
II. Ordine europeo di produzione, ordine europeo di conservazione e certificati, rappresentante legale	4. Autorità di emissione	30
	5. Condizioni di emissione dell'ordine europeo di produzione	28-29, 31-35
	6. Condizioni di emissione dell'ordine europeo di conservazione	36
	7. Destinatario dell'ordine europeo di produzione e dell'ordine europeo di conservazione	37
	8. Certificato di ordine europeo di produzione e certificato di ordine europeo di conservazione	38-39

	9. Esecuzione dell'EPOC	40-41
	10. Esecuzione dell'EPOC-PR	42
	11. Riservatezza e informazioni all'utente	43
	12. Rimborso delle spese	Nessuno
III. Sanzioni ed esecuzione	13. Sanzioni	Nessuno
	14. Procedura di esecuzione	44-45, 55
IV. Mezzi di ricorso	15. e 16. Procedura di riesame in caso di obblighi contrastanti derivanti dal diritto di un paese terzo	47-53
	17. Ricorso effettivo	54
	18. Privilegi e immunità ai sensi del diritto dello Stato di esecuzione	35
V. Disposizioni finali	19. Monitoraggio e relazioni	58
	20. Modifiche dei certificati e dei moduli	59-60
	21. Esercizio della delega	60
	22. Notifiche	Nessuno
	23. Relazione con l'ordine europeo di indagine	61
	24. Valutazione	62
	25. Entrata in vigore	Nessuno

Capo 1: Oggetto, definizioni e ambito di applicazione

Articolo 1: Oggetto

Questo articolo fissa l'ambito di applicazione generale e l'obiettivo della proposta, che è quello di stabilire le norme in base alle quali un'autorità giudiziaria competente dell'Unione europea può, mediante un ordine europeo di produzione o di conservazione, ingiungere a un prestatore di servizi che offre servizi nell'Unione di produrre o conservare prove elettroniche. Questi strumenti possono essere usati solo in situazioni transfrontaliere, ossia nei casi in cui il prestatore di servizi è stabilito o rappresentato in un altro Stato membro.

Il regolamento offre strumenti supplementari alle autorità inquirenti per ottenere prove elettroniche, senza limitare i poteri già conferiti loro dal diritto nazionale per obbligare i prestatori di servizi stabiliti o rappresentati nel loro territorio. Pertanto se il prestatore di servizi è stabilito o rappresentato nello stesso Stato membro le autorità di tale Stato membro devono avvalersi delle misure nazionali.

I dati richiesti tramite l'ordine europeo di produzione dovrebbero essere forniti direttamente alle autorità senza che sia necessario l'intervento delle autorità dello Stato membro in cui il prestatore di servizi è stabilito o rappresentato. Il regolamento inoltre abbandona il criterio di collegamento rappresentato dall'ubicazione dei dati, poiché generalmente la conservazione dei dati non comporta alcun controllo da parte dello Stato nel cui territorio i dati sono conservati. Nella maggior parte dei casi il luogo di conservazione è determinato dal prestatore di servizi sulla base di considerazioni commerciali[24].

Inoltre, il regolamento si applica anche se il prestatore di servizi non è stabilito o rappresentato nell'Unione ma offre servizi nell'Unione. Questa disposizione si rispecchia nell'articolo 3, paragrafo 1.

Quando il regolamento fa riferimento a un prestatore di servizi stabilito o rappresentato in uno Stato membro tramite un rappresentante legale, la sola designazione di un rappresentante legale non crea di per sé uno stabilimento del prestatore di servizi ai fini del regolamento.

L'articolo 1, paragrafo 2, ricorda che il regolamento non ha l'effetto di modificare l'obbligo di rispettare i diritti fondamentali e i principi giuridici sanciti all'articolo 6 del trattato sull'Unione europea.

Articolo 2: Definizioni

Questo articolo stabilisce le definizioni che si applicano in tutto lo strumento.

Rientrano nell'ambito di applicazione del regolamento i seguenti tipi di prestatori di servizi: i prestatori di servizi di comunicazione elettronica, i prestatori di servizi della società dell'informazione per i quali la conservazione dei dati è una componente propria del servizio fornito all'utente, compresi i social network nella misura in cui non possono essere considerati servizi di comunicazione elettronica, i mercati online che agevolano le operazioni tra utenti (come consumatori o imprese) e altri prestatori di servizi di hosting, e i prestatori di servizi di nomi di dominio internet e di numerazione.

L'ambito di applicazione del regolamento comprende i prestatori di servizi di comunicazione elettronica come definiti [nella direttiva che istituisce il codice europeo delle comunicazioni elettroniche]. I servizi di telecomunicazione tradizionali, i consumatori e le imprese si affidano sempre più ai nuovi servizi basati su internet intesi a consentire le comunicazioni interpersonali, quali il voice-over-IP, la messaggistica istantanea e i servizi di posta elettronica, anziché fruire dei servizi di comunicazione tradizionali. Tali servizi, insieme alle reti sociali quali Twitter e Facebook che consentono agli utenti di condividere contenuti, dovrebbero pertanto essere coperti dalla presente proposta.

In molti casi i dati non sono più conservati nel dispositivo dell'utente ma sono messi a disposizione su un'infrastruttura cloud che consente in linea di massima l'accesso da qualsiasi luogo. I prestatori di servizi non hanno bisogno di essere stabiliti o avere server in ogni giurisdizione ma ricorrono piuttosto a un'amministrazione centralizzata e a sistemi decentrati per conservare i dati e fornire i servizi. In tal modo ottimizzano il bilanciamento del carico e riducono i tempi di risposta alle richieste di dati degli utenti. Le reti di diffusione di contenuti (CDN) sono generalmente usate per accelerare la fornitura di contenuti copiando i contenuti in più server sparpagliati in tutto il mondo. Le imprese possono così fornire i contenuti dal

[24] Per ulteriori spiegazioni si veda la valutazione d'impatto.

server più vicino all'utente o in grado di inoltrare la comunicazione attraverso una rete meno congestionata. Per tenere conto di questo sviluppo, la definizione comprende i 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 strumento si applica anche ai mercati digitali che consentono ai consumatori e/o alle imprese di concludere operazioni tramite contratti di vendita o di servizi online. Tali operazioni sono effettuate o sul sito web del mercato online o sul sito web di un professionista che utilizza i servizi informatici forniti dal mercato online. È pertanto questo mercato che generalmente detiene prove elettroniche che possono essere necessarie nel corso di procedimenti penali.

I servizi per i quali la conservazione di dati non è una componente propria non sono contemplati dalla proposta. Sebbene la maggior parte dei servizi forniti dai prestatori comprenda qualche tipo di conservazione dei dati, specialmente quando sono forniti online a distanza, è possibile distinguere servizi per i quali la conservazione dei dati non è una caratteristica principale bensì un elemento puramente accessorio, quali servizi giuridici, architettonici, ingegneristici e contabili forniti online a distanza.

I dati detenuti dai prestatori di servizi di infrastruttura internet, quali i registrar di nomi di dominio e i registri e prestatori di servizi per la privacy o proxy, o i registri regionali di internet per gli indirizzi del protocollo internet, possono essere rilevanti per i procedimenti penali in quanto possono fornire indizi che permettono di identificare persone o entità coinvolti in attività criminali.

Le categorie di dati che le autorità competenti possono ottenere con un ordine europeo di produzione sono i dati relativi agli abbonati, i dati relativi agli accessi, i dati relativi alle operazioni (categorie congiuntamente denominate "dati non relativi al contenuto") e i dati relativi al contenuto conservati. Questa distinzione, a parte i dati relativi agli accessi, esiste negli ordinamenti giuridici di molti Stati membri e di paesi terzi.

Tutte le categorie contengono dati personali e rientrano pertanto nel campo di applicazione delle garanzie previste dall'*acquis* dell'UE sulla protezione dei dati. Il loro impatto sui diritti fondamentali varia, in particolare per quanto riguarda i dati relativi agli abbonati, da un lato, e i dati relativi alle operazioni e al contenuto, dall'altro. È essenziale che tutte queste categorie rientrino nell'ambito di applicazione dello strumento: i dati relativi agli abbonati e i dati relativi agli accessi sono spesso il punto di partenza per ottenere indizi in un'indagine sull'identità dell'indagato, mentre i dati relativi alle operazioni e al contenuto possono essere più pertinenti come materiale probatorio. Considerati i diversi livelli di impatto sui diritti fondamentali, è giustificato fissare condizioni diverse per i dati relativi agli abbonati, da un lato, e i dati relativi alle operazioni e al contenuto, dall'altro, come fanno varie disposizioni del regolamento.

È opportuno considerare i dati relativi agli accessi come una categoria specifica di dati ai fini del presente regolamento. I dati relativi agli accessi sono richiesti allo stesso scopo dei dati relativi agli abbonati, ossia per individuare l'utente, e il livello di impatto sui diritti fondamentali è simile. Essi dovrebbero pertanto essere soggetti alle stesse condizioni dei dati relativi agli abbonati. La proposta pertanto introduce una nuova categoria di dati, che devono essere trattati come i dati relativi agli abbonati se l'obiettivo perseguito dal loro ottenimento è analogo.

L'articolo 2 definisce gli Stati membri e le autorità che potrebbero essere coinvolti nella procedura. La definizione di autorità di emissione è inclusa nell'articolo 4.

I casi di emergenza sono situazioni eccezionali che richiedono regolarmente una reazione tempestiva da parte dei prestatori di servizi e per i quali saranno applicabili condizioni speciali. Sono pertanto definiti separatamente in questo articolo.

Articolo 3: Ambito di applicazione

Questo articolo definisce l'ambito di applicazione del regolamento. Quest'ultimo si applica a tutti i prestatori di servizi che offrono servizi nell'Unione, compresi i prestatori di servizi che non sono stabiliti nell'Unione. L'offerta attiva di servizi nell'Unione, con tutti i vantaggi che ne derivano, giustifica che anche tali prestatori di servizi siano soggetti al regolamento e assicura la parità di trattamento tra partecipanti agli stessi mercati. Inoltre, non includere tali prestatori di servizi creerebbe una lacuna e renderebbe più facile per i criminali eludere l'ambito di applicazione del regolamento.

Per determinare se un prestatore di servizi offre servizi nell'Unione le autorità devono verificare se il prestatore consente alle persone fisiche o giuridiche di uno o più Stati membri di usufruire dei suoi servizi. Tuttavia, la semplice accessibilità del servizio (che potrebbe derivare anche dall'accessibilità del sito web del prestatore di servizi o di un intermediario o di un indirizzo di posta elettronica e di altri dati di contatto) non dovrebbe di per sé costituire una condizione sufficiente per l'applicazione del regolamento. Pertanto, per determinare un nesso sufficiente tra il prestatore di servizi e il territorio in cui i servizi sono offerti occorre un collegamento sostanziale con tali Stati membri. Tale collegamento sostanziale sussiste qualora il prestatore di servizi abbia uno stabilimento in uno o più Stati membri. In mancanza di stabilimento nell'Unione, il criterio del collegamento sostanziale con l'Unione dovrebbe essere valutato sulla base dell'esistenza di un numero significativo di utenti in uno o più Stati membri, o dell'orientamento delle attività verso uno o più Stati membri. L'orientamento delle attività verso uno o più Stati membri può essere determinato sulla base di tutte le circostanze pertinenti, tra cui l'uso di una lingua o di una moneta generalmente usata in uno Stato membro. Potrebbe anche desumersi dalla disponibilità di un'app nell'apposito negozio online ("app store") nazionale, dalla fornitura di pubblicità a livello locale o nella lingua usata in uno Stato membro, dal fatto che siano usate informazioni provenienti da persone presenti negli Stati membri nel corso delle attività o dalla gestione dei rapporti con la clientela, ad esempio la fornitura dell'assistenza alla clientela nella lingua generalmente usata in uno Stato membro. Il criterio del collegamento sostanziale dovrebbe inoltre considerarsi soddisfatto qualora il prestatore di servizi diriga le sue attività verso uno o più Stati membri, come previsto all'articolo 17, paragrafo 1, lettera c), del regolamento (UE) n. 1215/2012 concernente la competenza giurisdizionale, il riconoscimento e l'esecuzione delle decisioni in materia civile e commerciale.

L'ordine europeo di produzione e l'ordine europeo di conservazione sono atti di indagine che possono essere emessi solo nell'ambito di un'indagine penale o di un procedimento penale per un reato concreto. Il nesso con un'indagine concreta distingue tali ordini dalle misure preventive e dagli obblighi di conservazione dei dati stabiliti dalla legge e garantisce l'applicazione dei diritti procedurali applicabili nei procedimenti penali. La competenza ad avviare indagini in relazione a uno specifico reato è pertanto un prerequisito per l'uso del regolamento.

Ulteriore requisito è che i dati richiesti siano correlati a servizi offerti dal prestatore di servizi all'interno dell'Unione.

Capo 2: Ordine europeo di produzione, ordine europeo di conservazione e certificati

Articolo 4: Autorità di emissione

All'emissione di un ordine europeo di produzione o di conservazione deve sempre partecipare un'autorità giudiziaria in veste di autorità di emissione o di autorità di convalida. Per gli ordini di produzione riguardanti dati relativi alle operazioni o al contenuto tale autorità deve essere un giudice o un organo giurisdizionale, mentre per quelli riguardanti dati relativi agli abbonati o agli accessi può essere anche un pubblico ministero.

Articolo 5: Condizioni di emissione dell'ordine europeo di produzione

L'articolo 5 stabilisce le condizioni per l'emissione di un ordine europeo di produzione, che devono essere valutate dall'autorità giudiziaria di emissione.

L'ordine europeo di produzione può essere emesso solo se è necessario e proporzionato nel caso di specie. Inoltre, dovrebbe essere emesso solo se una misura dello stesso tipo è disponibile in una situazione nazionale comparabile nello Stato di emissione.

L'ordine di produrre dati relativi agli abbonati o dati relativi agli accessi può essere emesso per qualsiasi reato. Per i dati relativi alle operazioni o al contenuto dovrebbero essere soddisfatti requisiti più rigorosi onde tener conto della natura più sensibile di tali dati e del corrispondente maggiore impatto dell'ordine rispetto ai dati relativi agli abbonati o agli accessi. Pertanto per i dati relativi alle operazioni o al contenuto l'ordine può essere emesso solo in relazione a reati che comportano una pena detentiva della durata massima di almeno 3 anni. La fissazione di una soglia basata sulla durata massima della pena detentiva consente 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.

La soglia non dovrebbe però compromettere l'efficacia dello strumento e il suo uso da parte degli operatori. La durata massima delle pene detentive varia tra gli Stati membri e dipende dal sistema giuridico nazionale. I codici penali nazionali differiscono l'uno dall'altro e non sono armonizzati. Anche i reati e le sanzioni applicabili sono diversi. Parimenti i codici di procedura nazionali differiscono per quanto riguarda le soglie per ottenere dati relativi alle operazioni o al contenuto: alcuni Stati membri non fissano nessuna soglia specifica; altri invece prevedono un elenco di reati. Una soglia di tre anni circoscrive l'ambito di applicazione dello strumento ai reati più gravi senza limitare eccessivamente la possibilità di uso dello strumento da parte degli operatori del settore. Tale soglia esclude dall'ambito di applicazione un'ampia serie di reati che dipende da ogni singolo codice penale nazionale (ad esempio in alcuni Stati membri l'uso di un ordine di produzione transnazionale riguardante dati più sensibili può essere considerato sproporzionato per reati quali non solo la partecipazione ad attività di un gruppo criminale organizzato e la sottrazione di minori, ma anche il furto, la frode e la minaccia di violenza fisica). D'altro canto, una soglia di tre anni abbraccia i reati che richiedono un approccio più efficace, come l'appartenenza a un'organizzazione criminale, il finanziamento di gruppi terroristici, il sostegno o la pubblicità a un'organizzazione criminale, la formazione per la commissione di reati terroristici, determinati reati commessi con finalità di terrorismo, la preparazione di reati da commettere con finalità di terrorismo e la preparazione di presa di ostaggi, che sarebbero altrimenti esclusi se fosse applicata una soglia più elevata, a seconda dello Stato membro. Tale soglia è stata

scelta per garantire in tutti gli Stati membri un equilibrio tra l'efficienza delle indagini penali e la protezione dei diritti e della proporzionalità. Una soglia offre inoltre il vantaggio di essere facilmente applicabile nella pratica.

Inoltre, l'ordine di produrre dati relativi alle operazioni o al contenuto può essere emesso anche per specifici reati armonizzati elencati in determinati strumenti, per i quali le prove sono tipicamente disponibili per lo più solo in formato elettronico. Ciò giustifica l'applicazione del regolamento anche nei casi in cui la pena detentiva massima è inferiore alla suddetta soglia, altrimenti le indagini non potrebbero essere adeguate, il che potrebbe determinare l'impunità. Gli strumenti in cui sono elencati tali reati sono: i) la decisione quadro 2001/413/GAI del Consiglio relativa alla lotta contro le frodi e le falsificazioni di mezzi di pagamento diversi dai contanti, ii) la direttiva 2011/92/UE relativa alla lotta contro l'abuso e lo sfruttamento sessuale dei minori e la pornografia minorile, e che sostituisce la decisione quadro 2004/68/GAI del Consiglio e iii) la direttiva 2013/40/UE relativa agli attacchi contro i sistemi di informazione e che sostituisce la decisione quadro 2005/222/GAI del Consiglio. L'ordine può essere emesso anche per i reati elencati nella direttiva (UE) 2017/541 sulla lotta contro il terrorismo e che sostituisce la decisione quadro 2002/475/GAI del Consiglio e che modifica la decisione 2005/671/GAI del Consiglio. Per alcuni di questi reati la soglia massima è di almeno 1 anno, per altri di 2 anni, ma per nessuno è inferiore a 1 anno.

Questo articolo inoltre stabilisce le informazioni obbligatorie che devono figurare nell'ordine europeo di produzione per permettere al prestatore di servizi di identificare i dati richiesti e di produrli. Anche i motivi della necessità e della proporzionalità della misura fanno parte integrante dell'ordine.

L'ordine europeo di produzione è attuato mediante l'emissione di un certificato di ordine europeo di produzione (European Production Order Certificate, EPOC) (si veda l'articolo 8), che è tradotto e trasmesso al prestatore di servizi. L'EPOC contiene le stesse informazioni obbligatorie figuranti nell'ordine, tranne i motivi della necessità e della proporzionalità della misura o altri dettagli sul caso.

Qualora i dati ricercati siano conservati o trattati nell'ambito di un'infrastruttura fornita dal prestatore di servizi a una società, tipicamente nel caso dei servizi di hosting o di software, il principale destinatario della richiesta delle autorità inquirenti dovrebbe essere la società. Se questa non è un prestatore di servizi ai sensi del regolamento è necessario ricorrere a un OEI o a un accordo di assistenza giudiziaria. L'ordine europeo di produzione può essere rivolto al prestatore di servizi solo se non risulta appropriato rivolgere la richiesta alla società, soprattutto per il rischio di compromettere l'indagine, ad esempio quando l'impresa stessa è oggetto di indagine.

Prima di emettere un ordine europeo di produzione, l'autorità di emissione deve tener conto anche dei potenziali privilegi e immunità previsti dal diritto dello Stato membro del prestatore di servizi e di qualsiasi impatto sugli interessi fondamentali di tale Stato membro, come la sicurezza e la difesa nazionali. Lo scopo di questa disposizione è garantire che i privilegi e le immunità che proteggono i dati richiesti nello Stato membro del prestatore di servizi siano presi in considerazione nello Stato di emissione, in particolare qualora riconoscano una protezione maggiore rispetto a quella accordata dal diritto dello Stato di emissione.

Articolo 6: Condizioni di emissione dell'ordine europeo di conservazione

L'ordine europeo di conservazione è soggetto a condizioni simili a quelle cui è soggetto l'ordine europeo di produzione. Può essere emesso per qualsiasi reato in linea con le altre condizioni di cui all'articolo 6. Il suo scopo è impedire la rimozione, la cancellazione o la modifica di dati pertinenti in situazioni in cui potrebbe occorrere più tempo per ottenere la produzione di tali dati, ad esempio quando saranno usati i canali della cooperazione giudiziaria. Dato che, ad esempio, l'OEI può essere emesso per qualsiasi reato senza limiti di soglia, anche l'ordine europeo di conservazione non deve essere sottoposto a limiti, altrimenti non sarebbe efficace. Per consentire alle autorità inquirenti di agire rapidamente e considerato che la richiesta pertinente di produrre i dati sarà emessa successivamente, dopo che tutte le condizioni saranno nuovamente esaminate, l'ordine europeo di conservazione può essere emesso o convalidato anche da un pubblico ministero.

Articolo 7: Destinatario dell'ordine europeo di produzione o dell'ordine europeo di conservazione

L'ordine europeo di produzione e l'ordine europeo di conservazione dovrebbero essere rivolti al rappresentante legale designato dal prestatore di servizi ai fini dell'acquisizione di prove nei procedimenti penali conformemente alla direttiva che stabilisce norme armonizzate sulla nomina dei rappresentanti legali ai fini dell'acquisizione di prove nei procedimenti penali. La trasmissione sarà effettuata sotto forma di un certificato di ordine europeo di produzione (European Production Order Certificate, EPOC) o un certificato di ordine europeo di conservazione (European Preservation Order Certificate, EPOC-PR) di cui all'articolo 8. Il rappresentante legale sarà responsabile della loro ricezione e della loro esecuzione tempestiva e completa. In questo modo i prestatori di servizi sono liberi di scegliere come organizzarsi per produrre i dati richiesti dalle autorità degli Stati membri.

In assenza di designazione del rappresentante legale, l'ordine europeo di produzione e l'ordine europeo di conservazione possono essere rivolti a qualsiasi stabilimento del prestatore di servizi nell'Unione. Questa possibilità di riserva consente di garantire l'efficacia del sistema qualora il prestatore di servizi non abbia (ancora) nominato un apposito rappresentante, ad esempio quando non sussiste l'obbligo di designare un rappresentante legale ai sensi della direttiva dal momento che il prestatore è stabilito e opera in un solo Stato membro o quando l'obbligo di designare un rappresentante legale non è ancora in vigore, ossia prima del termine ultimo per il recepimento della direttiva.

Qualora il rappresentante legale non ottemperi all'ordine, vi sono due situazioni in cui l'autorità di emissione può rivolgersi a qualsiasi stabilimento del prestatore di servizi nell'Unione: nei casi di emergenza definiti all'articolo 9, paragrafo 2, e nei casi in cui il rappresentante legale non ottempera agli obblighi di cui all'articolo 9 e 10, e quando l'autorità di emissione ritiene che sussista un chiaro rischio di perdita dei dati.

Articolo 8: Certificato di ordine europeo di produzione e certificato di ordine europeo di conservazione

L'EPOC e l'EPOC-PR servono a trasmettere gli ordini al destinatario di cui all'articolo 7. I modelli di entrambi i certificati figurano negli allegati I e II del regolamento; essi devono essere tradotti in una delle lingue ufficiali dello Stato membro in cui il destinatario è situato. Il prestatore di servizi può dichiarare che gli ordini saranno accettati anche in altre lingue ufficiali dell'Unione. Lo scopo dei certificati è fornire tutte le informazioni necessarie da

trasmettere al destinatario in un formato standardizzato, riducendo al minimo le fonti di errore, consentendo di identificare facilmente i dati ed evitando, per quanto possibile, testi liberi, riducendo così i costi di traduzione. I motivi della necessità e della proporzionalità e ulteriori dettagli sul caso non sono inclusi nel certificato per non compromettere le indagini. Essi sono pertanto necessari come parte integrante dell'ordine solo successivamente per consentire all'indagato di contestare l'ordine durante il procedimento penale.

Alcuni prestatori di servizi hanno già creato piattaforme per la presentazione delle richieste da parte delle autorità di contrasto. Il regolamento non impedisce l'uso di queste piattaforme, che offrono numerosi vantaggi, tra cui la possibilità di un'autenticazione rapida e una trasmissione sicura dei dati. Tuttavia, le piattaforme devono consentire la presentazione dell'EPOC e dell'EPOC-PR nel formato di cui agli allegati I e II, senza chiedere dati aggiuntivi sull'ordine.

Anche le piattaforme istituite dagli Stati membri o dagli organi dell'Unione possono fornire mezzi sicuri di trasmissione e agevolare l'autenticazione degli ordini e la raccolta di statistiche. È opportuno prendere in considerazione la possibilità di espandere le piattaforme eCodex e SIRIUS per includere una connessione sicura ai prestatori di servizi ai fini della trasmissione dell'EPOC e dell'EPOC-PR e, se del caso, delle risposte dei prestatori di servizi.

Articolo 9: Esecuzione dell'EPOC

L'articolo 9 obbliga i destinatari a rispondere all'EPOC e introduce termini obbligatori. Il termine normale è di 10 giorni, anche se le autorità possono stabilire un termine più breve ove giustificato. In caso di emergenza, definito come una situazione in cui vi è una minaccia imminente per la vita o l'integrità fisica di una persona o per un'infrastruttura critica, il termine è di 6 ore.

La disposizione garantisce inoltre la possibilità di un dialogo tra il destinatario e l'autorità di emissione. Se l'EPOC è incompleto, manifestamente inesatto o non contiene informazioni sufficienti affinché il prestatore di servizi possa ottemperarvi il destinatario deve contattare l'autorità di emissione e chiedere chiarimenti usando il modulo di cui all'allegato III. Il destinatario deve informare l'autorità di emissione anche qualora non possa fornire i dati a causa di forza maggiore o per impossibilità materiale, ad esempio quando la persona i cui dati sono richiesti non era cliente del servizio o quando i dati sono stati legittimamente cancellati dal prestatore di servizi, ad esempio nell'ambito di altri obblighi di tutela della vita privata, prima che il prestatore o il suo rappresentante legale ricevesse l'ordine. L'autorità di emissione deve conoscere tali circostanze per reagire velocemente, ad esempio per acquisire le prove elettroniche da un altro prestatore o evitare di avviare una procedura di esecuzione laddove ciò non abbia senso.

Se per motivi diversi da quelli indicati non fornisce le informazioni o non le fornisce in modo esaustivo o tempestivo, il destinatario deve comunicare all'autorità di emissione i motivi usando il modulo di cui all'allegato III. Il destinatario può quindi sollevare qualsiasi questione connessa all'esecuzione dell'EPOC con l'autorità di emissione. Questo permette all'autorità di emissione di rettificare o riesaminare l'EPOC in una fase precoce, prima di attivarsi per far rispettare l'ordine.

Se i dati non sono prodotti immediatamente, in particolare quando è avviato un dialogo tra il destinatario e l'autorità di emissione, con conseguente inosservanza dei termini di cui all'articolo 9, paragrafo 1, il prestatore di servizi deve conservare i dati per evitare che questi vengano persi, sempre che i dati possano essere individuati. La conservazione può servire per

un successivo EPOC chiarito o una successiva richiesta di assistenza giudiziaria o un OEI che verrà inviato in luogo dell'iniziale EPOC.

Articolo 10: Esecuzione dell'EPOC-PR

L'esecuzione dell'EPOC-PR richiede la conservazione dei dati disponibili al momento della ricezione dell'ordine. Il prestatore di servizi dovrebbe conservare i dati per il tempo necessario alla loro produzione su richiesta, a condizione che l'autorità di emissione confermi entro 60 giorni dalla data di emissione di aver avviato la successiva richiesta di produzione. A tal fine è necessario che siano espletate almeno alcune formalità, ad esempio l'invio di una richiesta di assistenza giudiziaria ai fini della traduzione.

D'altro canto, la richiesta di conservazione dovrebbe essere presentata o mantenuta solo per il tempo necessario per consentire la presentazione della successiva richiesta di produzione dei dati. Se decide di non emettere o ritirare l'ordine di produzione o la richiesta di cooperazione giudiziaria, l'autorità di emissione ne informa immediatamente il destinatario per evitare che i dati siano conservati inutilmente o per troppo tempo.

Questa disposizione inoltre garantisce la possibilità di un dialogo tra il destinatario e l'autorità di emissione, analogamente alla disposizione dell'articolo 9. Se l'EPOC-PR è incompleto, manifestamente inesatto o non contiene informazioni sufficienti affinché il prestatore di servizi possa ottemperarvi il destinatario deve contattare l'autorità di emissione e chiedere chiarimenti usando il modulo di cui all'allegato III. Il destinatario deve informare l'autorità di emissione anche qualora non possa fornire i dati a causa di forza maggiore, per impossibilità materiale o per altri motivi.

Articolo 11: Riservatezza e informazioni all'utente

La riservatezza delle indagini in corso, tra cui il fatto che è stato emesso un ordine per ottenere i dati pertinenti, deve essere protetta. Questo articolo si ispira all'articolo 19 della direttiva OEI. Prevede l'obbligo per il destinatario e, se diverso, il prestatore di servizi di garantire la riservatezza dell'EPOC o dell'EPOC-PR, in particolare astenendosi dall'informare la persona i cui dati sono ricercati, se richiesto dall'autorità di emissione, al fine di proteggere le indagini sui reati, in conformità all'articolo 23 del regolamento generale sulla protezione dei dati.

D'altro canto è importante, in particolare per l'esercizio dei mezzi di ricorso, che la persona i cui dati sono ricercati venga informata. Se non lo fa il prestatore di servizi su richiesta dell'autorità di emissione, quest'ultima vi provvede ai sensi dell'articolo 13 della direttiva sulla protezione dei dati nelle attività di polizia e giustizia, quando non c'è più il rischio di compromettere le indagini, e include informazioni sui mezzi di ricorso disponibili. A causa del minore impatto sui diritti coinvolti, tali informazioni sono fornite solo per l'ordine europeo di produzione, non per l'ordine europeo di conservazione.

Articolo 12: Rimborso delle spese

Laddove ciò sia previsto dal diritto nazionale dello Stato di emissione per gli ordini nazionali in situazioni analoghe, il prestatore di servizi può chiedere allo Stato di emissione il rimborso delle spese conformemente al diritto nazionale di tale Stato. Ciò garantisce parità di trattamento tra i prestatori di servizi cui è stato rivolto un ordine nazionale e quelli cui è stato rivolto un EPOC da parte dello stesso Stato membro, qualora quest'ultimo abbia scelto di

rimborsare determinati prestatori di servizi. D'altra parte, il regolamento non armonizza il rimborso delle spese, in quanto gli Stati membri hanno compiuto scelte diverse al riguardo.

Il rimborso può essere chiesto direttamente dal prestatore di servizi o tramite il suo rappresentante legale. Le spese possono essere rimborsate solo una volta.

Capo 3: Sanzioni ed esecuzione

Articolo 13: Sanzioni

Gli Stati membri assicurano che siano disponibili sanzioni effettive, proporzionate e dissuasive per il caso in cui il prestatore di servizi non ottemperi agli obblighi di cui all'articolo 9, 10 o 11. Ciò non pregiudica i diritti nazionali che prevedono l'irrogazione di sanzioni penali per tali situazioni.

Articolo 14: Procedura di esecuzione

L'articolo 14 stabilisce la procedura da seguire in caso di inottemperanza per far eseguire gli ordini con l'aiuto dello Stato membro in cui è situato il destinatario del certificato trasmesso. A seconda del destinatario iniziale, tale Stato è lo Stato membro del prestatore di servizi o del rappresentante legale. L'autorità di emissione trasferisce l'intero ordine, compresi i motivi della necessità e della proporzionalità, insieme al certificato, all'autorità competente dello Stato di esecuzione, che lo fa eseguire conformemente al proprio diritto nazionale, se necessario irrogando le sanzioni di cui all'articolo 13. Se l'ordine è trasmesso per esecuzione allo Stato di esecuzione, l'autorità di esecuzione può decidere, previa consultazione dell'autorità di emissione, di non riconoscere o non eseguire l'ordine qualora si applichino i motivi di opposizione. Inoltre, in caso di avvio della procedura di esecuzione, il destinatario potrà opporsi all'ordine dinanzi all'autorità di esecuzione sulla base di uno di tali motivi, esclusi i privilegi e le immunità ma compresi i casi in cui è evidente che l'ordine non è stato emesso o convalidato da un'autorità competente, che ottemperare all'ordine significa violare manifestamente la Carta o che l'ordine è manifestamente arbitrario. Ad esempio, un ordine che chieda la produzione di dati relativi al contenuto riguardanti una categoria indeterminata di persone in un'area geografica o che non ha alcun collegamento concreto con un procedimento penale ignorerebbe in modo manifesto le condizioni per l'emissione dell'ordine europeo di produzione previste dal regolamento e ciò sarebbe evidente già dal contenuto del certificato. Altri motivi possono essere invocati dalla persona i cui dati sono richiesti, nell'ambito dei mezzi di ricorso dello Stato di emissione (si veda l'articolo 17). Inoltre, il prestatore di servizi deve disporre di un rimedio giurisdizionale contro la decisione dell'autorità di esecuzione che gli irroga una sanzione.

La procedura di esecuzione contiene vari termini per l'autorità di esecuzione e di emissione al fine di evitare ritardi nel corso di tale procedura.

Capo 4: Mezzi di ricorso

Articoli 15 e 16: Procedura di riesame in caso di obblighi contrastanti derivanti dal diritto di un paese terzo

Gli articoli 15 e 16 prevedono una procedura di riesame nel caso in cui i prestatori di servizi aventi sede in un paese terzo debbano far fronte a obblighi contrastanti. Tali disposizioni sono di grande importanza per garantire la tutela dei diritti dei singoli e la cortesia internazionale. Fissando un livello elevato, mirano a incoraggiare i paesi terzi a prevedere un livello di tutela

analogo. In caso contrario, qualora le autorità di un paese terzo cerchino di ottenere i dati di un cittadino dell'UE da un prestatore di servizi dell'UE, il diritto dell'Unione o degli Stati membri che tutela i diritti fondamentali, come l'*acquis* in materia di protezione dei dati, può allo stesso modo impedire la divulgazione. L'Unione europea si attende che i paesi terzi rispettino tali divieti come lo fa il regolamento proposto.

Il destinatario può attivare la procedura di cui all'articolo 15 qualora ottemperare all'ordine europeo di produzione significhi violare il diritto di un paese terzo che vieta la divulgazione dei dati per la necessità di tutelare i diritti fondamentali delle persone interessate o interessi fondamentali del paese terzo connessi alla sicurezza o alla difesa nazionali. Il destinatario deve informare l'autorità di emissione, con obiezione motivata, dei motivi per i quali ritiene che sussistano obblighi contrastanti. Tale obiezione motivata non può fondarsi sul mero fatto che il diritto del paese terzo non prevede disposizioni analoghe né sulla sola circostanza che i dati sono conservati in un paese terzo. L'obiezione motivata è presentata secondo la procedura di cui all'articolo 9, paragrafo 5, per notificare l'intenzione di non ottemperare, usando il modulo di cui all'allegato III.

Sulla base dell'obiezione motivata l'autorità di emissione rivede il proprio ordine. Se decide di ritirarlo la procedura si conclude. Se invece intende confermarlo trasferisce il caso all'organo giurisdizionale competente del proprio Stato membro. L'organo giurisdizionale valuta quindi, sulla base dell'obiezione motivata e tenuto conto di tutti i fatti pertinenti del caso, se il diritto del paese terzo si applica al caso di specie e, in caso affermativo, se sussistono effettivamente obblighi contrastanti. Nell'effettuare tale valutazione l'organo giurisdizionale dovrebbe esaminare se il diritto del paese terzo, anziché tutelare i diritti fondamentali o interessi fondamentali del paese terzo connessi alla sicurezza o alla difesa nazionali, intenda manifestamente tutelare altri interessi o proteggere attività illecite dalle richieste delle autorità di contrasto nell'ambito delle indagini penali.

Se conclude che nella fattispecie esiste un contrasto con gli obblighi derivanti dalla legislazione a tutela dei diritti fondamentali delle persone o degli interessi fondamentali del paese terzo connessi alla sicurezza o alla difesa nazionali, l'organo giurisdizionale deve chiedere il parere del paese terzo interessato tramite le autorità centrali nazionali di quest'ultimo. Se il paese terzo consultato conferma l'esistenza del contrasto e si oppone all'esecuzione dell'ordine, l'organo giurisdizionale deve ritirare l'ordine.

Se il contrasto deriva da una legislazione del paese terzo che non mira a tutelare i diritti fondamentali delle persone o gli interessi fondamentali del paese terzo connessi alla sicurezza o alla difesa nazionali, l'organo giurisdizionale adotta la sua decisione bilanciando gli interessi a favore e quelli contro la conferma dell'ordine.

Le condizioni di cui all'articolo 9, soprattutto gli obblighi di conservazione di cui al paragrafo 6, si applicano anche in caso di obblighi contrastanti derivanti dal diritto di un paese terzo. Qualora concluda che l'ordine va confermato, l'organo giurisdizionale ne informa l'autorità di emissione e il prestatore di servizi ai fini della sua esecuzione. Qualora l'ordine sia revocato, può essere emesso un ordine europeo di conservazione per garantire la disponibilità dei dati nel caso in cui questi possano essere ottenuti mediante una richiesta di assistenza giudiziaria.

Poiché l'ordine europeo di conservazione non comporta di per sé la divulgazione dei dati e pertanto non dà luogo a preoccupazioni analoghe, la procedura di riesame è limitata all'ordine europeo di produzione.

Articolo 17: Ricorso effettivo

Questa disposizione garantisce che le persone colpite dall'ordine europeo di produzione dispongano di un ricorso effettivo. Il ricorso dovrebbe essere esercitato nello Stato di emissione conformemente al diritto nazionale. Per quanto riguarda gli indagati e gli imputati, il ricorso dovrebbe essere esercitato nel corso del procedimento penale. Il diritto a un ricorso effettivo non è disponibile per l'ordine europeo di conservazione, giacché tale ordine di per sé non consente la divulgazione dei dati; tuttavia qualora esso sia seguito da un ordine europeo di produzione o da un altro strumento che comporta la divulgazione dei dati il ricorso è possibile in virtù di questi strumenti.

Le persone i cui dati sono richiesti pur non essendo tali persone indagati o imputati in un procedimento penale hanno diritto a un ricorso nello Stato di emissione. Tutti questi diritti non pregiudicano i mezzi di ricorso disponibili ai sensi della direttiva sulla protezione dei dati nelle attività di polizia e giustizia e del regolamento generale sulla protezione dei dati.

A differenza di quanto previsto per i prestatori di servizi, il regolamento non limita i possibili motivi adducibili da tutte queste persone per contestare la legittimità dell'ordine. Tali motivi includono la necessità e la proporzionalità dell'ordine.

L'esercizio del ricorso nello Stato di emissione non deve imporre un onere sproporzionato alle persone colpite. Come per gli ordini che sono eseguiti attraverso altre forme di cooperazione giudiziaria, gli organi giurisdizionali dello Stato di emissione sono nella posizione migliore per controllare la legittimità degli ordini europei di produzione emessi dalle proprie autorità e valutare la compatibilità con il proprio diritto nazionale. Inoltre, durante la fase di esecuzione il destinatario può opporsi all'esecuzione dell'EPOC o dell'EPOC-PR nel proprio Stato membro ospitante sulla base di un elenco di motivi enumerati nel regolamento stesso (si veda l'articolo 14).

Articolo 18: Privilegi e immunità ai sensi del diritto dello Stato di esecuzione

Questa disposizione persegue lo stesso obiettivo dell'articolo 5, paragrafo 7, ossia garantire che i privilegi e le immunità che proteggono i dati ricercati nello Stato membro del prestatore di servizi siano presi in considerazione nello Stato di emissione, in particolare qualora sussistano disparità tra tali Stati membri, così come gli interessi fondamentali di tale Stato membro, quali la sicurezza e la difesa nazionali. L'articolo 18 impone all'organo giurisdizionale dello Stato di emissione di tenerne conto come se fossero previsti dal suo diritto nazionale. A causa delle differenze esistenti tra gli Stati membri nel valutare la pertinenza e l'ammissibilità delle prove, la disposizione lascia una certa libertà agli organi giurisdizionali su come tenerne conto.

Capo 5: Disposizioni finali

Articolo 19: Monitoraggio e relazioni

Questo articolo fa obbligo agli Stati membri di fornire informazioni specifiche concernenti l'applicazione del regolamento al fine di assistere la Commissione nell'esercizio dei suoi obblighi di cui all'articolo 24. La Commissione stabilisce un programma dettagliato di monitoraggio per controllare gli esiti, i risultati e gli effetti del regolamento.

Articolo 20: Modifiche dei certificati e dei moduli

I certificati e i moduli che figurano negli allegati I, II, e III del regolamento agevoleranno l'esecuzione dell'EPOC e dell'EPOC-PR. Per tale motivo è necessario che in futuro sia possibile migliorarne il contenuto il più rapidamente possibile. Considerato che modificare i tre allegati attraverso la procedura legislativa ordinaria non risponde a tale esigenza e che i tre allegati costituiscono elementi non essenziali dell'atto legislativo giacché i principali elementi sono definiti all'articolo 8, l'articolo 20 prevede una procedura più rapida e più flessibile per le modifiche tramite atti delegati.

Articolo 21: Esercizio della delega

Questo articolo fissa le condizioni alle quali la Commissione ha il potere di adottare atti delegati per apportare le modifiche necessarie ai certificati e ai moduli di cui agli allegati. Stabilisce una procedura standard per l'adozione di tali atti delegati.

Articolo 22: Notifiche

Gli Stati membri sono tenuti a notificare alla Commissione le autorità di emissione e di esecuzione competenti e gli organi giurisdizionali competenti a trattare le obiezioni motivate dei prestatori di servizi in caso di conflitto di legge.

Articolo 23: Relazione con l'ordine europeo di indagine

Questa disposizione chiarisce che il regolamento non impedisce alle autorità degli Stati membri di emettere ordini europei di indagine ai sensi della direttiva 2014/41/UE per ottenere prove elettroniche.

Articolo 24: Valutazione

Questa disposizione obbliga la Commissione ad effettuare una valutazione del regolamento in linea con i suoi orientamenti per legiferare meglio e con il punto 22 dell'accordo interistituzionale del 13 aprile 2016[25]. Cinque anni dopo l'entrata in vigore del regolamento la Commissione presenterà al Parlamento europeo e al Consiglio una relazione sui risultati della valutazione, compresa una valutazione della necessità di estendere l'ambito di applicazione a servizi non ancora coperti ma che potrebbero diventare pertinenti per le indagini.

Articolo 25: Entrata in vigore

Il regolamento entrerà in vigore il ventesimo giorno successivo alla pubblicazione nella Gazzetta ufficiale dell'Unione europea. Esso si applicherà 6 mesi dopo la data di entrata in vigore.

[25] Accordo interistituzionale tra il Parlamento europeo, il Consiglio dell'Unione europea e la Commissione europea "Legiferare meglio", del 13 aprile 2016 (GU L 123 del 12.5.2016, pag. 1).

2018/0108 (COD)

Proposta di

REGOLAMENTO DEL PARLAMENTO EUROPEO E DEL CONSIGLIO

relativo agli ordini europei di produzione e di conservazione di prove elettroniche in materia penale

IL PARLAMENTO EUROPEO E IL CONSIGLIO DELL'UNIONE EUROPEA,

visto il trattato sul funzionamento dell'Unione europea, in particolare l'articolo 82, paragrafo 1,

vista la proposta della Commissione europea,

previa trasmissione del progetto di atto legislativo ai parlamenti nazionali,

visto il parere del Comitato economico e sociale europeo[26],

deliberando secondo la procedura legislativa ordinaria,

considerando quanto segue:

(1) L'Unione si è prefissa l'obiettivo di mantenere e sviluppare uno spazio di libertà, sicurezza e giustizia. Per realizzare gradualmente tale spazio, l'Unione adotta misure nel settore della cooperazione giudiziaria in materia penale basate sul principio del reciproco riconoscimento delle sentenze e decisioni giudiziarie, il quale, a partire dal Consiglio europeo di Tampere del 15 e 16 ottobre 1999, è comunemente considerato una pietra angolare della cooperazione giudiziaria in materia penale nell'Unione.

(2) Le misure per ottenere e conservare prove elettroniche sono sempre più importanti per consentire lo svolgimento delle indagini e dei procedimenti penali all'interno dell'Unione. Per combattere la criminalità sono essenziali meccanismi efficaci per l'ottenimento di prove elettroniche, che garantiscano nel contempo il pieno rispetto dei diritti fondamentali e dei principi riconosciuti dalla Carta dei diritti fondamentali dell'Unione europea e sanciti nei trattati, in particolare i principi di necessità e proporzionalità e i diritti al giusto processo, alla protezione dei dati, alla segretezza della corrispondenza e al rispetto della vita privata.

(3) La dichiarazione congiunta dei ministri della Giustizia e degli Affari interni e dei rappresentanti delle istituzioni dell'UE del 22 marzo 2016 sugli attentati terroristici di Bruxelles ha sottolineato la necessità, in via prioritaria, di trovare modalità per assicurare ed ottenere più rapidamente ed efficacemente prove elettroniche e di individuare misure concrete per far fronte al problema.

(4) Le conclusioni del Consiglio del 9 giugno 2016 hanno sottolineato il rilievo crescente delle prove elettroniche nei procedimenti penali e l'importanza di proteggere il ciberspazio da abusi e attività criminali nell'interesse delle economie e società e, di conseguenza, la necessità per le autorità di contrasto e giudiziarie di disporre di strumenti efficaci per indagare e perseguire atti criminali connessi al ciberspazio.

[26] GU C […] del […], pag. […].

(5) Nella comunicazione congiunta del 13 settembre 2017 sulla resilienza, deterrenza e difesa[27] la Commissione ha sottolineato che indagare e perseguire efficacemente i reati favoriti dalla cibernetica costituisce un deterrente essenziale dei ciberattacchi, e che il quadro procedurale attuale deve essere adattato meglio all'era di internet. Talvolta le attuali procedure non sono risultate adeguate alla velocità dei ciberattacchi, che richiedono una rapida cooperazione transfrontaliera.

(6) Nella risoluzione del 3 ottobre 2017 sulla lotta contro la criminalità informatica[28] il Parlamento europeo ha ribadito tali preoccupazioni, evidenziando le difficoltà che l'attuale quadro giuridico frammentato può creare per i prestatori di servizi che intendono soddisfare le richieste dei servizi di contrasto, e ha invitato la Commissione a proporre un quadro giuridico europeo in materia di prove elettroniche che comprenda garanzie sufficienti per i diritti e le libertà di tutti gli interessati.

(7) I servizi su rete possono essere forniti da qualsiasi luogo e non necessitano di un'infrastruttura fisica, di locali o personale nel paese di destinazione. Di conseguenza, le prove pertinenti sono spesso conservate al di fuori dello Stato che effettua le indagini o da un prestatore di servizi stabilito al di fuori di tale Stato. Sovente non esiste alcun altro collegamento tra il caso oggetto di indagine nello Stato interessato e lo Stato in cui si trova il luogo di conservazione o lo stabilimento principale del prestatore di servizi.

(8) A causa di questa mancanza di collegamento, le richieste di cooperazione giudiziaria sono spesso rivolte a paesi che ospitano un gran numero di prestatori di servizi ma che non hanno nessun'altra relazione con il caso di specie. Per giunta il numero di richieste è fortemente aumentato a seguito dell'uso sempre maggiore dei servizi su rete, per natura privi di frontiere. Di conseguenza, per ottenere prove elettroniche attraverso i canali della cooperazione giudiziaria occorre spesso molto tempo, più di quello per cui gli eventuali indizi rimangono a disposizione. Inoltre, non esiste un quadro chiaro per la cooperazione con i prestatori di servizi, sebbene alcuni prestatori di paesi terzi accettino le richieste dirette di dati non relativi al contenuto quando consentito dal diritto nazionale applicabile. Di conseguenza, tutti gli Stati membri si basano sul canale della cooperazione con i prestatori di servizi, ove disponibile, ricorrendo a strumenti, condizioni e procedure nazionali diversi. Inoltre, per quanto riguarda i dati relativi al contenuto, alcuni Stati membri hanno preso iniziative unilaterali, mentre altri continuano a basarsi sulla cooperazione giudiziaria.

(9) La frammentarietà del quadro giuridico crea difficoltà per i prestatori di servizi che cercano di ottemperare alle richieste dei servizi di contrasto. Occorre pertanto presentare un quadro giuridico europeo in materia di prove elettroniche che imponga ai prestatori di servizi che rientrano nell'ambito di applicazione dello strumento di rispondere direttamente alle autorità, senza che sia necessario l'intervento di un'autorità giudiziaria nello Stato membro del prestatore di servizio.

(10) Gli ordini di cui al presente regolamento dovrebbero essere rivolti a rappresentanti legali dei prestatori di servizi appositamente designati. Se un prestatore di servizi stabilito nell'Unione non ha designato un rappresentante legale, gli ordini possono essere indirizzati a un qualsiasi stabilimento del prestatore all'interno dell'Unione. Questa possibilità di riserva consente di garantire l'efficacia del sistema qualora il prestatore di servizi non abbia (ancora) nominato un apposito rappresentante.

---

27 JOIN(2017) 450 final.

28 2017/2068(INI).

(11) Il meccanismo dell'ordine europeo di produzione e dell'ordine europeo di conservazione per le prove elettroniche in materia penale può operare solo sulla base di un livello elevato di fiducia reciproca tra gli Stati membri, che è un prerequisito essenziale per il buon funzionamento del presente strumento.

(12) Il presente regolamento rispetta i diritti fondamentali ed osserva i principi riconosciuti in particolare dalla Carta dei diritti fondamentali dell'Unione europea, tra cui il diritto alla libertà e alla sicurezza, il rispetto della vita privata e familiare, la protezione dei dati personali, la libertà di impresa, il diritto di proprietà, il diritto a un ricorso effettivo e a un giudice imparziale, la presunzione di innocenza e i diritti della difesa, i principi della legalità e della proporzionalità e il diritto di non essere giudicato o punito due volte per lo stesso reato. Qualora abbia elementi per ritenere che in un altro Stato membro possa essere in corso un procedimento penale parallelo, lo Stato membro di emissione deve consultare le autorità di tale Stato membro in conformità della decisione quadro 2009/948/GAI del Consiglio[29].

(13) Al fine di garantire il pieno rispetto dei diritti fondamentali, il presente regolamento fa espresso riferimento alle norme necessarie per l'ottenimento dei dati personali, il trattamento di tali dati, il controllo giurisdizionale dell'uso dell'atto d'indagine previsto dal presente strumento e i mezzi di ricorso disponibili.

(14) Il presente regolamento dovrebbe essere applicato senza pregiudizio per i diritti procedurali nei procedimenti penali riconosciuti dalle direttive 2010/64/UE[30], 2012/13/UE[31], 2013/48/UE[32], 2016/343[33], 2016/800[34] e 2016/1919[35] del Parlamento europeo e del Consiglio.

(15) Il presente strumento stabilisce le norme in base alle quali un'autorità giudiziaria competente dell'Unione europea può, mediante un ordine europeo di produzione o di conservazione, ingiungere a un prestatore di servizi che offre servizi nell'Unione di produrre o conservare prove elettroniche. Esso è applicabile in tutti i casi in cui il prestatore di servizi è stabilito o rappresentato in un altro Stato membro. Nelle situazioni nazionali in cui non è possibile usare gli strumenti disposti dal presente

---

29 Decisione quadro 2009/948/GAI del Consiglio, del 30 novembre 2009, sulla prevenzione e la risoluzione dei conflitti relativi all'esercizio della giurisdizione nei procedimenti penali (GU L 328 del 15.12.2009, pag. 42).

30 Direttiva 2010/64/UE del Parlamento europeo e del Consiglio, del 20 ottobre 2010, sul diritto all'interpretazione e alla traduzione nei procedimenti penali (GU L 280 del 26.10.2010, pag. 1).

31 Direttiva 2012/13/UE del Parlamento europeo e del Consiglio, del 22 maggio 2012, sul diritto all'informazione nei procedimenti penali (GU L 142 dell'1.6.2012, pag. 1).

32 Direttiva 2013/48/UE del Parlamento europeo e del Consiglio, del 22 ottobre 2013, relativa al diritto di avvalersi di un difensore nel procedimento penale e nel procedimento di esecuzione del mandato d'arresto europeo, al diritto di informare un terzo al momento della privazione della libertà personale e al diritto delle persone private della libertà personale di comunicare con terzi e con le autorità consolari (GU L 294 del 6.11.2013, pag. 1).

33 Direttiva (UE) 2016/343 del Parlamento europeo e del Consiglio, del 9 marzo 2016, sul rafforzamento di alcuni aspetti della presunzione di innocenza e del diritto di presenziare al processo nei procedimenti penali (GU L 65 dell'11.3.2016, pag. 1).

34 Direttiva (UE) 2016/800 del Parlamento europeo e del Consiglio, dell'11 maggio 2016, sulle garanzie procedurali per i minori indagati o imputati nei procedimenti penali (GU L 132 del 21.5.2016, pag. 1).

35 Direttiva (UE) 2016/1919 del Parlamento europeo e del Consiglio, del 26 ottobre 2016, sull'ammissione al patrocinio a spese dello Stato per indagati e imputati nell'ambito di procedimenti penali e per le persone ricercate nell'ambito di procedimenti di esecuzione del mandato d'arresto europeo (GU L 297 del 4.11.2016, pag. 1).

regolamento, quest'ultimo non dovrebbe limitare i poteri già conferiti dal diritto nazionale alle autorità nazionali competenti per obbligare i prestatori di servizi stabiliti o rappresentati nel loro territorio.

(16) I prestatori di servizi più pertinenti per i 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 proposta di direttiva che istituisce il codice europeo delle comunicazioni elettroniche. Essi comprendono le comunicazioni interpersonali, quali Voice over IP (VoIP), la messaggistica istantanea e i servizi di posta elettronica. Le categorie di servizi della società dell'informazione che rientrano nel presente strumento sono quelle per le quali la conservazione dei dati è una componente propria del servizio fornito all'utente, e riguardano, in particolare, i social network nella misura in cui non possono essere considerati servizi di comunicazione elettronica, i mercati online che agevolano le operazioni tra utenti (come consumatori o imprese) e altri servizi di hosting, anche quando il servizio è fornito attraverso cloud computing. I servizi della società dell'informazione per i quali la conservazione dei dati non è una componente propria del servizio fornito all'utente bensì un elemento puramente accessorio, quali i servizi giuridici, architettonici, ingegneristici e contabili forniti online a distanza, dovrebbero essere esclusi dall'ambito di applicazione del presente regolamento, anche quando possono rientrare nella definizione di servizi della società dell'informazione di cui alla direttiva (UE) 2015/1535.

(17) In molti casi i dati non sono più conservati o trattati nel dispositivo dell'utente ma sono messi a disposizione su un'infrastruttura cloud accessibile da qualsiasi luogo. Per fornire tali servizi i prestatori non hanno bisogno di essere stabiliti o avere server in una data giurisdizione. Pertanto l'applicazione del presente regolamento non dovrebbe dipendere dal luogo effettivo in cui si trova lo stabilimento del prestatore o la struttura per il trattamento o la conservazione dei dati.

(18) I prestatori di servizi di infrastruttura internet relativi all'assegnazione di nomi e numeri, quali i registrar di nomi di dominio e i registri e i prestatori di servizi per la privacy o proxy, o i registri regionali di internet (Regional Internet Registry, RIR) per gli indirizzi del protocollo internet (IP), sono particolarmente rilevanti quando occorre identificare soggetti dietro siti web dannosi o compromessi. I dati in possesso di tali prestatori di servizi sono di particolare rilevanza per i procedimenti penali, in quanto permettono di identificare persone o entità dietro un sito web usato in attività criminali o le vittime dell'attività criminale qualora un sito web compromesso sia stato piratato da criminali.

(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.

(20) Le categorie di dati rientranti nell'ambito di applicazione del presente regolamento comprendono i dati relativi agli abbonati, i dati relativi agli accessi, i dati relativi alle operazioni (categorie congiuntamente denominate "dati non relativi al contenuto") e i dati relativi al contenuto. Questa distinzione, tranne per quanto riguarda i dati relativi

agli accessi, esiste negli ordinamenti giuridici di molti Stati membri e nell'attuale quadro giuridico statunitense, che consente ai prestatori di servizi di condividere su base volontaria i dati non relativi al contenuto con le autorità di contrasto straniere.

(21) È opportuno considerare i dati relativi agli accessi come una categoria specifica di dati ai fini del presente regolamento. I dati relativi agli accessi sono richiesti allo stesso scopo dei dati relativi agli abbonati, ossia per individuare l'utente sottostante, e il livello di impatto sui diritti fondamentali è simile a quello dei dati relativi agli abbonati. I dati relativi agli accessi tipicamente sono registrati nell'ambito di una registrazione di eventi (in altre parole un log server) per indicare l'inizio e la fine di una sessione di accesso utente a un servizio. Il più delle volte si tratta di un indirizzo IP (statico o dinamico) o altro identificatore che individua l'interfaccia di rete usata durante la sessione di accesso. Se l'utente è ignoto, spesso occorre ottenere tali dati prima di poter richiedere al prestatore di servizi i dati relativi agli abbonati correlati a quell'identificatore.

(22) I dati relativi alle operazioni, invece, sono generalmente richiesti per ottenere informazioni sui contatti dell'utente e sul luogo in cui questo si trova e possono servire per definire il profilo di una persona. Ciò detto, i dati relativi agli accessi non possono, di per sé, servire a un siffatto scopo, ad esempio non rivelano nessuna informazione sugli interlocutori dell'utente. La presente proposta pertanto introduce una nuova categoria di dati, che devono essere trattati come i dati relativi agli abbonati se l'obiettivo perseguito dal loro ottenimento è analogo.

(23) Tutte le categorie di dati contengono dati personali e rientrano pertanto nell'ambito di applicazione delle garanzie previste dall'*acquis* dell'Unione in materia di protezione dei dati, ma l'intensità dell'impatto sui diritti fondamentali varia, in particolare tra i dati relativi agli abbonati e i dati relativi agli accessi, da un lato, e i dati relativi alle operazioni e i dati relativi al contenuto, dall'altro. Mentre i dati relativi agli abbonati e i dati relativi agli accessi sono utili per ottenere i primi indizi in un'indagine sull'identità dell'indagato, i dati relativi alle operazioni e i dati relativi al contenuto sono i più pertinenti come materiale probatorio. È pertanto essenziale che tutte queste categorie di dati rientrino nell'ambito di applicazione dello strumento. Considerato il diverso livello di impatto sui diritti fondamentali, sono previste condizioni diverse per l'ottenimento dei dati relativi agli abbonati e dei dati relativi agli accessi, da un lato, e dei dati relativi alle operazioni e dei dati relativi al contenuto, dall'altro.

(24) L'ordine europeo di produzione e l'ordine europeo di conservazione sono atti d'indagine che dovrebbero essere emessi solo nell'ambito di specifici procedimenti penali nei confronti di specifici autori, noti o ancora ignoti, di un reato concreto che è già stato commesso, previa valutazione individuale della proporzionalità e della necessità in ogni singolo caso.

(25) Il presente regolamento non pregiudica i poteri d'indagine delle autorità nei procedimenti civili o amministrativi, anche qualora tali procedimenti possano comportare sanzioni.

(26) Il presente regolamento dovrebbe applicarsi ai prestatori di servizi che offrono servizi nell'Unione, e gli ordini di cui al presente regolamento dovrebbero essere emessi solo in relazione ai dati riguardanti servizi offerti nell'Unione. I servizi offerti esclusivamente al di fuori dell'Unione non rientrano nell'ambito di applicazione del presente regolamento, anche se il prestatore di servizi è stabilito nell'Unione.

(27) Per determinare se un prestatore di servizi offre servizi nell'Unione occorre verificare se il prestatore di servizi consente alle persone fisiche o giuridiche di uno o più Stati membri di usufruire dei suoi servizi. Tuttavia, la semplice accessibilità di un'interfaccia online, ad esempio l'accessibilità del sito web del prestatore di servizi o di un intermediario o di un indirizzo di posta elettronica e di altri dati di contatto in uno o più Stati membri, non dovrebbe di per sé costituire una condizione sufficiente per l'applicazione del presente regolamento.

(28) Per determinare l'ambito di applicazione del presente regolamento dovrebbe sussistere anche un collegamento sostanziale con l'Unione. Tale collegamento dovrebbe considerarsi presente quando il prestatore di servizi ha uno stabilimento nell'Unione. In mancanza di stabilimento nell'Unione, il criterio del collegamento sostanziale dovrebbe essere valutato sulla base dell'esistenza di un numero significativo di utenti in uno o più Stati membri, o dell'orientamento delle attività verso uno o più Stati membri. L'orientamento delle attività verso uno o più Stati membri può essere determinato sulla base di tutte le circostanze pertinenti, tra cui l'uso di una lingua o di una moneta generalmente usata nello Stato membro in questione o la possibilità di ordinare prodotti o servizi. L'orientamento delle attività verso uno o più Stati membri potrebbe anche desumersi dalla disponibilità di un'applicazione ("app") nell'apposito negozio online ("app store") nazionale, dalla fornitura di pubblicità a livello locale o nella lingua usata nello Stato membro in questione, o dalla gestione dei rapporti con la clientela, ad esempio la fornitura dell'assistenza alla clientela nella lingua generalmente usata in tale Stato membro. Il criterio del collegamento sostanziale dovrebbe inoltre considerarsi soddisfatto qualora il prestatore di servizi diriga le sue attività verso uno o più Stati membri, come previsto all'articolo 17, paragrafo 1, lettera c), del regolamento (UE) n. 1215/2012 concernente la competenza giurisdizionale, il riconoscimento e l'esecuzione delle decisioni in materia civile e commerciale[36]. Al contrario, la fornitura del servizio al fine del mero rispetto del divieto di discriminazione imposto dal regolamento (UE) 2018/302[37] non può di per sé considerarsi direzione o orientamento delle attività verso un dato territorio all'interno dell'Unione.

(29) L'ordine europeo di produzione dovrebbe essere emesso solo se è necessario e proporzionato. La valutazione dovrebbe considerare se l'ordine è limitato a quanto necessario per raggiungere il legittimo obiettivo di ottenere i dati pertinenti e necessari che dovranno servire da prova solo nella singola fattispecie.

(30) È opportuno che nel processo di emissione o di convalida di un ordine europeo di produzione o di conservazione intervenga sempre un'autorità giudiziaria. Considerato il carattere più sensibile dei dati relativi alle operazioni e dei dati relativi al contenuto, l'emissione o la convalida di un ordine europeo di produzione per la produzione di queste categorie di dati richiede il riesame da parte di un giudice. Poiché i dati relativi agli abbonati e i dati relativi agli accessi sono meno sensibili, l'ordine europeo di

---

36 Regolamento (UE) n. 1215/2012 del Parlamento europeo e del Consiglio, del 12 dicembre 2012, concernente la competenza giurisdizionale, il riconoscimento e l'esecuzione delle decisioni in materia civile e commerciale (GU L 351 del 20.12.2012, pag. 1).

37 Regolamento (UE) 2018/302 del Parlamento europeo e del Consiglio, del 28 febbraio 2018, recante misure volte a impedire i blocchi geografici ingiustificati e altre forme di discriminazione basate sulla nazionalità, sul luogo di residenza o sul luogo di stabilimento dei clienti nell'ambito del mercato interno e che modifica i regolamenti (CE) n. 2006/2004 e (UE) 2017/2394 e la direttiva 2009/22/CE (GU L 601 del 2.3.2018, pag. 1).

produzione per la loro divulgazione può essere emesso o convalidato anche dai pubblici ministeri competenti.

(31) Per lo stesso motivo occorre effettuare una distinzione per quanto riguarda l'ambito di applicazione materiale del presente regolamento: l'ordine di produrre dati relativi agli abbonati o dati relativi agli accessi può essere emesso per qualsiasi reato, mentre l'accesso ai dati relativi alle operazioni e ai dati relativi al contenuto dovrebbe essere soggetto a requisiti più severi, a causa del carattere più sensibile di questi dati. La fissazione di una soglia consentirebbe un approccio più proporzionato, insieme a una serie di altre condizioni e garanzie ex ante ed ex post previste dal presente regolamento per assicurare il rispetto della proporzionalità e dei diritti degli interessati. La soglia non dovrebbe però limitare l'efficacia dello strumento e il suo uso da parte degli operatori. Autorizzare l'emissione di ordini relativi a indagini per reati punibili con una pena detentiva della durata massima di almeno 3 anni limita l'ambito di applicazione dello strumento ai reati più gravi senza compromettere eccessivamente le possibilità di uso dello strumento da parte degli operatori. Escluderebbe dall'ambito di applicazione un numero significativo di reati che gli Stati membri considerano meno gravi e puniscono con una pena massima inferiore. Offrirebbe inoltre il vantaggio di essere facilmente applicabile nella pratica.

(32) 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 possono causare un danno esteso o considerevole, in particolare nei casi 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 prevalentemente l'impunità. Questa considerazione giustifica l'applicazione del regolamento anche per tali reati qualora la sanzione comminata dalla legge sia inferiore a 3 anni di reclusione. Anche i reati connessi al terrorismo di cui alla direttiva (UE) 2017/541 non richiedono la soglia massima di almeno 3 anni.

(33) È inoltre necessario prevedere che l'ordine europeo di produzione possa essere emesso solo se un ordine dello stesso tipo è disponibile per lo stesso reato in una situazione nazionale comparabile nello Stato di emissione.

(34) Qualora i dati ricercati siano conservati o trattati nell'ambito di un'infrastruttura fornita dal prestatore di servizi a una società o altra entità diversa da una persona fisica, tipicamente nel caso dei servizi di hosting, l'ordine europeo di produzione dovrebbe essere usato solo quando altri atti d'indagine nei confronti della società o dell'entità risultano inappropriati, soprattutto se rischiano di compromettere l'indagine. Questa considerazione è di particolare rilevanza per le entità di grandi dimensioni, come le società per azioni o gli enti pubblici, che si avvalgono dei servizi di prestatori di servizi per la propria infrastruttura informatica aziendale o i propri servizi informatici aziendali o per entrambi. In tali situazioni il primo destinatario dell'ordine europeo di produzione dovrebbe essere la società o altra entità. Tale società o altra entità potrebbe non essere un prestatore di servizi rientrante nell'ambito di applicazione del presente regolamento. Tuttavia, qualora non sia opportuno rivolgersi a tale soggetto, ad esempio perché è sospettato di coinvolgimento nel caso di specie o vi sono indizi di collusione con il soggetto sottoposto all'indagine, le autorità competenti dovrebbero potersi rivolgere al prestatore di servizi che fornisce l'infrastruttura in questione affinché produca i dati richiesti. Questa disposizione non pregiudica il diritto di ingiungere al prestatore di servizi di conservare i dati.

(35) Le immunità e i privilegi, che possono riguardare categorie di persone (ad esempio i diplomatici) o rapporti specificamente protetti (ad esempio i rapporti tra avvocato e cliente), sono trattati in altri strumenti di riconoscimento reciproco quale l'ordine europeo di indagine penale. La loro gamma e il loro impatto variano a seconda del diritto nazionale applicabile di cui occorre tener conto al momento dell'emissione dell'ordine, giacché l'autorità di emissione può emettere un ordine solo se un ordine dello stesso tipo è disponibile in una situazione nazionale comparabile. In aggiunta a questo principio di base, i privilegi e le immunità che proteggono i dati relativi agli accessi, alle operazioni o al contenuto nello Stato membro del prestatore di servizi dovrebbero essere presi in considerazione, per quanto possibile, nello Stato di emissione come se fossero previsti dal diritto nazionale di tale Stato. Questa disposizione è particolarmente rilevante qualora il diritto dello Stato membro in cui ci si rivolge al prestatore di servizi o al suo rappresentante legale offra una protezione maggiore rispetto al diritto dello Stato di emissione. Essa inoltre garantisce il rispetto nei casi in cui la divulgazione dei dati potrebbe incidere su un interesse fondamentale di tale Stato membro, come la sicurezza e la difesa nazionali. Ad ulteriore garanzia, tali aspetti dovrebbero essere presi in considerazione non solo nell'emettere l'ordine, ma anche successivamente nel valutare la pertinenza e l'ammissibilità dei dati in questione nella fase appropriata del procedimento penale e, in caso di procedura di esecuzione, dall'autorità di esecuzione.

(36) L'ordine europeo di conservazione può essere emesso per qualsiasi reato. Il suo scopo è impedire la rimozione, la cancellazione o la modifica di dati pertinenti in situazioni in cui potrebbe occorrere più tempo per ottenere la loro produzione, ad esempio quando sono usati i canali della cooperazione giudiziaria.

(37) Gli ordini europei di produzione e di conservazione dovrebbero essere rivolti al rappresentante legale designato dal prestatore di servizi. In mancanza di rappresentante legale designato, possono essere indirizzati a uno stabilimento del prestatore di servizi all'interno dell'Unione. È il caso di quando non sussiste alcun obbligo giuridico per il prestatore di servizi di nominare un rappresentante legale. Qualora il rappresentante legale non ottemperi all'ordine in situazioni di emergenza, l'ordine europeo di produzione o di conservazione può essere rivolto anche al prestatore di servizi, parallelamente o in alternativa alla procedura per far eseguire l'ordine originale a norma dell'articolo 14. Qualora il rappresentante legale non ottemperi all'ordine in situazioni che non sono di emergenza ma in cui sussiste un chiaro rischio di perdita dei dati, l'ordine europeo di produzione o di conservazione può essere rivolto anche a qualsiasi stabilimento del prestatore di servizi nell'Unione. In considerazione di questi diversi scenari possibili, nelle disposizioni è usato il termine generico "destinatario". Qualora il destinatario non sia il prestatore di servizi e un obbligo, ad esempio di riservatezza, valga non solo per il destinatario ma anche per il prestatore di servizi, la rispettiva disposizione lo specifica.

(38) L'ordine europeo di produzione o di conservazione dovrebbe essere trasmesso al prestatore di servizi mediante un certificato di ordine europeo di produzione (European Production Order Certificate, EPOC) o un certificato di ordine europeo di conservazione (European Preservation Order Certificate, EPOC-PR), che dovrebbe essere tradotto. Il certificato dovrebbe contenere le stesse informazioni obbligatorie figuranti nell'ordine, tranne i motivi della necessità e della proporzionalità della misura o altri dettagli sul caso per non compromettere le indagini. Tuttavia, poiché fanno parte integrante dell'ordine, tali motivi e dettagli consentono all'indagato di contestare successivamente l'ordine durante il procedimento penale. Se necessario, il

certificato deve essere tradotto in una lingua ufficiale dello Stato membro del destinatario o in un'altra lingua ufficiale che il prestatore di servizi abbia dichiarato di accettare.

(39) L'autorità di emissione competente dovrebbe trasmettere l'EPOC o l'EPOC-PR direttamente al destinatario con ogni mezzo che consenta di conservare una traccia scritta in condizioni che permettano al prestatore di servizi di stabilirne l'autenticità, come posta raccomandata, posta elettronica protetta e piattaforme o altri canali protetti, compresi quelli messi a disposizione dal prestatore di servizi, in linea con le norme in materia di protezione dei dati personali.

(40) I dati richiesti dovrebbero essere trasmessi alle autorità entro 10 giorni dalla ricezione dell'EPOC. È opportuno che il prestatore di servizi sia tenuto a rispettare termini più brevi in caso di emergenza o se l'autorità di emissione ha indicato altri motivi per discostarsi dal termine di 10 giorni. Oltre al pericolo imminente di cancellazione dei dati richiesti, detti motivi possono riguardare circostanze connesse all'indagine in corso, ad esempio quando i dati richiesti sono associati ad altri atti d'indagine urgenti che non possono essere condotti senza i dati mancanti o ne dipendono in altro modo.

(41) Per consentire al prestatore di servizi di risolvere eventuali problemi formali è necessario stabilire una procedura di comunicazione tra il prestatore di servizi e l'autorità giudiziaria di emissione nei casi in cui l'EPOC sia incompleto o contenga errori manifesti o informazioni insufficienti per eseguire l'ordine. Inoltre, se il prestatore di servizi non fornisce le informazioni in modo esaustivo o tempestivo per qualsiasi altro motivo, ad esempio perché ritiene che vi sia un contrasto con un obbligo previsto dal diritto di un paese terzo o che l'ordine europeo di produzione non sia stato emesso nel rispetto delle condizioni stabilite dal presente regolamento, il prestatore di servizi dovrebbe contattare l'autorità di emissione e fornire le opportune giustificazioni. Pertanto la procedura di comunicazione dovrebbe consentire in generale all'autorità di emissione di rettificare o riesaminare l'EPOC in una fase precoce. Al fine di garantire la disponibilità dei dati, il prestatore di servizi dovrebbe conservare i dati, sempre che sia possibile identificare i dati richiesti.

(42) Quando riceve un EPOC-PR il prestatore di servizi dovrebbe conservare i dati richiesti per un periodo massimo di 60 giorni, a meno che l'autorità di emissione lo informi di aver avviato la procedura per l'emissione di una successiva richiesta di produzione, nel qual caso la conservazione dovrebbe proseguire. Il periodo di 60 giorni è calcolato per consentire l'avvio di una richiesta ufficiale. A tal fine è necessario che siano espletate almeno alcune formalità, ad esempio l'invio di una richiesta di assistenza giudiziaria ai fini della traduzione. Quando riceve l'informazione di cui sopra, il prestatore di servizi dovrebbe conservare i dati per il tempo necessario alla loro produzione nel quadro di una successiva richiesta di produzione.

(43) I prestatori di servizi e i loro rappresentanti legali dovrebbero assicurare la riservatezza e, se richiesto dall'autorità di emissione, astenersi dall'informare la persona i cui dati sono ricercati, al fine di salvaguardare le indagini sui reati, conformemente all'articolo 23 del regolamento (UE) 2016/679[38]. Tuttavia l'informazione dell'utente è essenziale per consentire il riesame e il ricorso giurisdizionale; pertanto, qualora al

[38] Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati) (GU L 119 del 4.5.2016, pag. 1).

prestatore di servizi sia stato chiesto di non informare l'utente e purché non sussista il rischio di compromettere le indagini in corso, dovrebbe provvedervi l'autorità, conformemente alle misure nazionali di attuazione dell'articolo 13 della direttiva (UE) 2016/680[39].

(44) In caso di inottemperanza da parte del destinatario, l'autorità di emissione può trasmettere l'intero ordine, compresi i motivi della necessità e della proporzionalità, corredato del certificato, all'autorità competente dello Stato membro in cui il destinatario del certificato risiede o è stabilito. Tale Stato membro dovrebbe procedere all'esecuzione dell'ordine conformemente al proprio diritto nazionale. Gli Stati membri dovrebbero prevedere l'irrogazione di sanzioni pecuniarie effettive, proporzionate e dissuasive in caso di violazione degli obblighi previsti dal presente regolamento.

(45) La procedura di esecuzione è una procedura in cui il destinatario può opporsi all'esecuzione sulla base di determinati motivi limitati. L'autorità di esecuzione può rifiutare il riconoscimento e l'esecuzione dell'ordine in base agli stessi motivi, o se si applicano privilegi e immunità a norma del suo diritto nazionale, o se la divulgazione può incidere su interessi fondamentali del proprio Stato, come la sicurezza e la difesa nazionali. Prima di rifiutare di riconoscere o eseguire l'ordine sulla base di tali motivi l'autorità di esecuzione dovrebbe consultare l'autorità di emissione. In caso di inottemperanza, le autorità possono irrogare sanzioni. Tali sanzioni dovrebbero essere proporzionate, anche alla luce di circostanze specifiche come l'inottemperanza reiterata o sistematica.

(46) Fatti salvi gli obblighi in materia di protezione dei dati, i prestatori di servizi non dovrebbero essere ritenuti responsabili negli Stati membri per i pregiudizi agli utenti o a terzi derivanti esclusivamente dall'ottemperanza in buona fede all'EPOC o all'EPOC-PR.

(47) Oltre alle persone i cui dati sono richiesti, anche il prestatore di servizi e paesi terzi possono essere interessati dall'atto d'indagine. Per rispettare il principio di cortesia internazionale rispetto agli interessi sovrani dei paesi terzi, proteggere la persona interessata e far fronte a eventuali obblighi contrastanti in capo al prestatore di servizi, il presente strumento prevede un meccanismo specifico di riesame giurisdizionale nel caso in cui ottemperare a un ordine europeo di produzione costringa il prestatore di servizi a violare un obbligo giuridico derivante dal diritto di un paese terzo.

(48) A tal fine, se il destinatario ritiene che nella fattispecie l'ordine europeo di produzione comporti la violazione di un obbligo giuridico derivante dal diritto di un paese terzo, ne dovrebbe informare l'autorità di emissione a mezzo di un'obiezione motivata, usando l'apposito modulo. L'autorità di emissione dovrebbe quindi riesaminare l'ordine europeo di produzione alla luce dell'obiezione motivata, tenendo conto degli stessi criteri che l'organo giurisdizionale competente dovrebbe seguire. Se l'autorità decide di confermare l'ordine, la procedura dovrebbe essere deferita all'organo giurisdizionale competente, quale notificato dallo Stato membro pertinente, che procederà al riesame dell'ordine.

---

[39] Direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio (GU L 119 del 4.5.2016, pag. 89).

(49) Al fine di stabilire l'esistenza di un obbligo contrastante nel caso di specie, l'organo giurisdizionale competente dovrebbe basarsi, se necessario, su appropriate competenze esterne, ad esempio qualora il riesame sollevi problemi di interpretazione del diritto del paese terzo in questione. In tal caso potrebbero essere consultate le autorità centrali di detto paese.

(50) Le competenze in materia di interpretazione potrebbero essere ottenute anche tramite pareri di esperti, ove disponibili. È opportuno che le informazioni e la giurisprudenza relative all'interpretazione del diritto dei paesi terzi e alle procedure di conflitto degli Stati membri siano rese disponibili su una piattaforma centrale quale il progetto SIRIUS e/o la Rete giudiziaria europea. Gli organi giurisdizionali potrebbero così beneficiare delle esperienze e competenze acquisite da altri organi giurisdizionali sulla stessa questione o su questioni simili. Tutto ciò non dovrebbe impedire una nuova consultazione del paese terzo, se del caso.

(51) Qualora sussistano obblighi contrastanti, l'organo giurisdizionale dovrebbe stabilire se le disposizioni contrastanti del paese terzo vietano la divulgazione dei dati in questione per la necessità di tutelare i diritti fondamentali delle persone interessate o interessi fondamentali del paese terzo connessi alla sicurezza o alla difesa nazionali. Nell'effettuare tale valutazione l'organo giurisdizionale dovrebbe esaminare se il diritto del paese terzo, anziché tutelare i diritti fondamentali o interessi fondamentali del paese terzo connessi alla sicurezza o alla difesa nazionali, intenda manifestamente tutelare altri interessi o proteggere attività illecite dalle richieste delle autorità di contrasto nell'ambito delle indagini penali. Qualora giunga alla conclusione che le disposizioni contrastanti del paese terzo vietano la divulgazione dei dati per la necessità di tutelare i diritti fondamentali delle persone interessate o interessi fondamentali del paese terzo connessi alla sicurezza o alla difesa nazionali, l'organo giurisdizionale dovrebbe consultare il paese terzo tramite le sue autorità centrali, già presenti nella maggior parte del mondo ai fini dell'assistenza giudiziaria. Dovrebbe fissare un termine affinché il paese terzo possa opporsi all'esecuzione dell'ordine europeo di produzione; qualora le autorità del paese terzo non rispondano entro il termine (prorogato) nonostante un sollecito che le informa delle conseguenze della mancata risposta, l'organo giurisdizionale conferma l'ordine. Se le autorità del paese terzo si oppongono alla divulgazione, l'organo giurisdizionale dovrebbe revocare l'ordine.

(52) In tutti gli altri casi di obblighi contrastanti, non correlati ai diritti fondamentali delle persone interessate o a interessi fondamentali del paese terzo connessi alla sicurezza o alla difesa nazionali, l'organo giurisdizionale dovrebbe decidere l'eventuale conferma dell'ordine europeo di produzione ponderando una serie di elementi intesi a verificare la solidità del collegamento con una delle due giurisdizioni coinvolte, i rispettivi interessi ad ottenere o impedire la divulgazione dei dati e le possibili conseguenze per il prestatore di servizi derivanti dall'obbligo di ottemperare all'ordine. Aspetto di rilievo per i reati connessi all'informatica, il luogo di commissione del reato comprende sia il luogo o i luoghi in cui è avvenuta l'azione, sia il luogo o i luoghi in cui si sono prodotti gli effetti del reato.

(53) Le condizioni di cui all'articolo 9 si applicano anche in caso di obblighi contrastanti derivanti dal diritto di un paese terzo. Nel corso di tale procedura i dati dovrebbero essere conservati. Qualora l'ordine sia revocato, è possibile emettere un nuovo ordine di conservazione per consentire all'autorità di emissione di chiedere la produzione dei dati attraverso altri canali, ad esempio l'assistenza giudiziaria.

(54) È essenziale che tutte le persone i cui dati sono richiesti nel corso di indagini o procedimenti penali abbiano accesso a un ricorso giurisdizionale effettivo, in linea con l'articolo 47 della Carta dei diritti fondamentali dell'Unione europea ("Carta"). Per quanto riguarda gli indagati e gli imputati, il diritto a un ricorso effettivo dovrebbe essere esercitato nel corso del procedimento penale. Ciò può incidere sull'ammissibilità delle prove ottenute con detti mezzi o, a seconda del caso, sul peso di tali prove nell'ambito del procedimento. Inoltre, gli indagati e gli imputati beneficiano di tutte le garanzie procedurali loro applicabili, come il diritto all'informazione. Anche le persone diverse dagli indagati o imputati dovrebbero avere il diritto a un ricorso effettivo. È pertanto opportuno prevedere, come minimo, la possibilità di contestare la legittimità di un ordine europeo di produzione, comprese la sua necessità e la sua proporzionalità. Il presente regolamento non dovrebbe limitare i motivi per contestare la legittimità dell'ordine. Questi rimedi dovrebbero essere esercitati nello Stato di emissione, conformemente al diritto nazionale. Le norme in materia di provvedimenti provvisori dovrebbero essere disciplinate dal diritto nazionale.

(55) Durante la procedura di esecuzione e la successiva impugnazione il destinatario può opporsi all'esecuzione dell'ordine europeo di produzione o di conservazione per un numero limitato di motivi, tra cui il fatto che l'ordine non è stato emesso o convalidato da un'autorità competente, o che esso viola manifestamente la Carta o è manifestamente arbitrario. Ad esempio, un ordine che chieda la produzione di dati relativi al contenuto riguardanti una categoria indeterminata di persone in un'area geografica, o che non ha alcun collegamento concreto con un procedimento penale, ignorerebbe in modo manifesto le condizioni per l'emissione dell'ordine europeo di produzione.

(56) La protezione delle persone fisiche in relazione al trattamento dei dati personali è un diritto fondamentale. A norma dell'articolo 8, paragrafo 1, della Carta e dell'articolo 16, paragrafo 1, TFUE ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano. Nell'attuare il presente regolamento gli Stati membri dovrebbero assicurare che i dati personali siano protetti e possano essere trattati solo in conformità del regolamento (UE) 2016/679 e della direttiva (UE) 2016/680.

(57) I dati personali acquisiti ai sensi del presente regolamento dovrebbero essere trattati solamente laddove necessario e proporzionato ai fini della prevenzione, dell'indagine, dell'accertamento e del perseguimento di reati o dell'esecuzione di sanzioni penali e dell'esercizio dei diritti della difesa. In particolare gli Stati membri dovrebbero garantire che alla trasmissione di dati personali da parte delle autorità competenti ai prestatori di servizi ai fini del presente regolamento si applichino politiche e misure adeguate in materia di protezione dei dati, comprese misure per garantire la sicurezza dei dati. I prestatori di servizi dovrebbero garantire altrettanto per la trasmissione di dati personali alle autorità competenti. Soltanto le persone autorizzate dovrebbero avere accesso alle informazioni contenenti dati personali che possono essere acquisiti tramite processi di autenticazione. È opportuno che sia preso in considerazione il ricorso a meccanismi per garantire l'autenticità dei dati, come i regimi nazionali di identificazione elettronica notificati o i servizi fiduciari di cui al regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio, del 23 luglio 2014, in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE.

(58) La Commissione dovrebbe effettuare una valutazione del presente regolamento basata sui cinque criteri di efficienza, efficacia, pertinenza, coerenza e valore aggiunto dell'UE, che dovrebbe servire da fondamento per le valutazioni d'impatto di altre possibili misure. È opportuno che siano raccolte periodicamente informazioni al fine di contribuire alla valutazione del presente regolamento.

(59) L'uso di moduli standard pretradotti facilita la cooperazione e lo scambio di informazioni tra autorità giudiziarie e prestatori di servizi, consentendo loro di ottenere e trasmettere prove elettroniche in modo più rapido ed efficace e soddisfacendo al contempo i necessari requisiti di sicurezza in modo più semplice. Tali moduli riducono i costi di traduzione e contribuiscono a un livello elevato di qualità. Analogamente, i moduli di risposta dovrebbero consentire uno scambio standardizzato di informazioni, in particolare quando i prestatori di servizi non sono in grado di adempiere a quanto richiesto perché l'account non esiste o i dati non sono disponibili. I moduli dovrebbero inoltre facilitare la raccolta di statistiche.

(60) Al fine di rispondere efficacemente all'eventuale necessità di migliorare il contenuto dell'EPOC, dell'EPOC-PR e del modulo per fornire informazioni sull'impossibilità di eseguire l'EPOC o l'EPOC-PR, è opportuno delegare alla Commissione il potere di adottare atti conformemente all'articolo 290 del trattato sul funzionamento dell'Unione europea riguardo alla modifica degli allegati I, II e III del presente regolamento. È di particolare importanza che durante i lavori preparatori la Commissione svolga adeguate consultazioni, anche a livello di esperti, nel rispetto dei principi stabiliti nell'accordo interistituzionale "Legiferare meglio" del 13 aprile 2016[40]. In particolare, al fine di garantire la parità di partecipazione alla preparazione degli atti delegati, il Parlamento europeo e il Consiglio ricevono tutti i documenti contemporaneamente agli esperti degli Stati membri, e i loro esperti hanno sistematicamente accesso alle riunioni dei gruppi di esperti della Commissione incaricati della preparazione di tali atti delegati.

(61) Le misure basate sul presente regolamento non dovrebbero sostituire l'ordine europeo di indagine di cui alla direttiva 2014/41/UE del Parlamento europeo e del Consiglio[41] ai fini dell'ottenimento di prove elettroniche. Le autorità degli Stati membri dovrebbero scegliere lo strumento più adatto alla situazione; se preferiscono possono usare l'ordine europeo di indagine per richiedere una serie di tipi diversi di atti di indagine, tra cui, ma non solo, la produzione di prove elettroniche da un altro Stato membro.

(62) A causa dell'evoluzione tecnologica, tra qualche anno potrebbero predominare nuove forme di strumenti di comunicazione o emergere lacune nell'applicazione del presente regolamento. È pertanto importante prevedere un riesame della sua applicazione.

(63) Poiché l'obiettivo del presente regolamento, vale a dire migliorare la protezione e l'ottenimento di prove elettroniche a livello transfrontaliero, non può essere conseguito in misura sufficiente dagli Stati membri data la sua natura transfrontaliera, ma può essere conseguito meglio a livello di Unione, quest'ultima può intervenire in base al principio di sussidiarietà sancito dall'articolo 5 del trattato sull'Unione europea. Il presente regolamento si limita a quanto è necessario per conseguire tale

---

40 GU L 123 del 12.5.2016, pag. 1.

41 Direttiva 2014/41/UE del Parlamento europeo e del Consiglio, del 3 aprile 2014, relativa all'ordine europeo di indagine penale (GU L 130 dell'1.5.2014, pag. 1).

obiettivo in ottemperanza al principio di proporzionalità enunciato nello stesso articolo.

(64) A norma dell'articolo 3 del protocollo sulla posizione del Regno Unito e dell'Irlanda rispetto allo spazio di libertà, sicurezza e giustizia, allegato al trattato sull'Unione europea e al trattato sul funzionamento dell'Unione europea, *[il Regno Unito/l'Irlanda ha notificato che desidera partecipare all'adozione e all'applicazione del presente regolamento] oppure [e fatto salvo l'articolo 4 di tale protocollo, il Regno Unito/l'Irlanda non partecipa all'adozione del presente regolamento, non è da esso vincolato/a né è soggetto/a alla sua applicazione]*.

(65) A norma degli articoli 1 e 2 del protocollo n. 22 sulla posizione della Danimarca, allegato al trattato sull'Unione europea e al trattato sul funzionamento dell'Unione europea, la Danimarca non partecipa all'adozione del presente regolamento, non è da esso vincolata né è soggetta alla sua applicazione.

(66) Il garante europeo della protezione dei dati è stato consultato a norma dell'articolo 28, paragrafo 2, del regolamento (CE) n. 45/2001 del Parlamento europeo e del Consiglio[42] e ha espresso un parere il [...][43],

HANNO ADOTTATO IL PRESENTE REGOLAMENTO:

Capo 1: Oggetto, definizioni e ambito di applicazione

Articolo 1
Oggetto

1. Il presente regolamento stabilisce le norme in base alle quali un'autorità di uno Stato membro può ingiungere a un prestatore di servizi che offre servizi nell'Unione di produrre o conservare prove elettroniche, indipendentemente dall'ubicazione dei dati. Il presente regolamento non pregiudica la facoltà delle autorità nazionali di ingiungere ai prestatori di servizi stabiliti o rappresentati nel loro territorio di ottemperare a misure nazionali dello stesso tipo.

2. Il presente regolamento non ha l'effetto di modificare l'obbligo di rispettare i diritti fondamentali e i principi giuridici sanciti dall'articolo 6 TUE, compresi i diritti di difesa delle persone sottoposte a procedimento penale, e lascia impregiudicati gli obblighi spettanti a tale riguardo alle autorità di contrasto o giudiziarie.

Articolo 2
Definizioni

Ai fini del presente regolamento si applicano le seguenti definizioni:

---

42 Regolamento (CE) n. 45/2001 del Parlamento europeo e del Consiglio, del 18 dicembre 2000, concernente la tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni e degli organismi comunitari, nonché la libera circolazione di tali dati (GU L 8 del 12.1.2001, pag. 1).

43 GU C […] del […], pag. […].

(1) "ordine europeo di produzione": la decisione vincolante di un'autorità di emissione di uno Stato membro che ingiunge a un prestatore di servizi che offre servizi nell'Unione ed è stabilito o rappresentato in un altro Stato membro di produrre prove elettroniche;

(2) "ordine europeo di conservazione": la decisione vincolante di un'autorità di emissione di uno Stato membro che ingiunge a un prestatore di servizi che offre servizi nell'Unione ed è stabilito o rappresentato in un altro Stato membro di conservare prove elettroniche in vista di una successiva richiesta di produzione;

(3) "prestatore di servizi": la persona fisica o giuridica che fornisce una o più delle seguenti categorie di servizi:

(a) servizi di comunicazione elettronica come definiti all'articolo 2, punto 4, della [direttiva che istituisce il codice europeo delle comunicazioni elettroniche];

(b) servizi della società dell'informazione come definiti all'articolo 1, paragrafo 1, lettera b), della direttiva (UE) 2015/1535 del Parlamento europeo e del Consiglio[44], per i quali la conservazione dei dati è una componente propria del servizio fornito all'utente, tra cui i social network, i mercati online che agevolano le operazioni tra utenti e altri prestatori di servizi di hosting;

(c) servizi di nomi di dominio internet e di numerazione IP, quali i prestatori di indirizzi IP, i registri di nomi di dominio, i registrar di nomi di dominio e i connessi servizi per la privacy o proxy;

(4) "che offre servizi nell'Unione":

(a) che consente alle persone fisiche o giuridiche in uno o più Stati membri di usare i servizi elencati al punto 3, e

(b) che ha un collegamento sostanziale con lo Stato membro o gli Stati membri di cui alla lettera a);

(5) "stabilimento": l'esercizio effettivo di un'attività economica a tempo indeterminato con un'infrastruttura stabile a partire dalla quale viene svolta l'attività di prestazione di servizi, o l'infrastruttura stabile a partire dalla quale l'attività è gestita;

(6) "prove elettroniche": le prove conservate in formato elettronico dal prestatore di servizi o per suo conto al momento della ricezione del certificato di ordine europeo di produzione o di conservazione, consistenti nei dati conservati relativi agli abbonati, agli accessi, alle operazioni o al contenuto;

(7) "dati relativi agli abbonati": i dati 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 e i dati connessi alla convalida dell'uso del servizio, ad

[44] Direttiva (UE) 2015/1535 del Parlamento europeo e del Consiglio, del 9 settembre 2015, che prevede una procedura d'informazione nel settore delle regolamentazioni tecniche delle regole relative ai servizi della società dell'informazione (GU L 241 del 17.9.2015, pag. 1).

esclusione di password o altri mezzi di autenticazione usati al posto di una password, forniti dall'utente o creati a sua richiesta;

(8) "dati relativi agli accessi": i dati riguardanti l'inizio e la fine di una sessione di accesso utente a un servizio strettamente necessari al solo fine di identificare l'utente del servizio, come la data e l'ora d'uso, o la connessione al servizio (log-in) e la disconnessione (log-off) dal medesimo, unitamente all'indirizzo IP assegnato all'utente dal prestatore di servizi di accesso a internet, ai dati che identificano le interfacce usate e all'identificativo utente. Rientrano in questa categoria i metadati delle comunicazioni elettroniche come definiti all'articolo 4, paragrafo 3, lettera c), del [regolamento relativo al rispetto della vita privata e alla tutela dei dati personali nelle comunicazioni elettroniche];

(9) "dati relativi alle operazioni": 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, i dati sull'ubicazione del dispositivo, la data, l'ora, la durata, le dimensioni, il percorso, il formato, il protocollo usato e il tipo di compressione, a meno che tali dati costituiscano dati relativi agli accessi. Rientrano in questa categoria i metadati delle comunicazioni elettroniche come definiti all'articolo 4, paragrafo 3, lettera c), del [regolamento relativo al rispetto della vita privata e alla tutela dei dati personali nelle comunicazioni elettroniche];

(10) "dati relativi al contenuto": qualsiasi dato conservato in formato digitale, come testo, voce, video, immagine o suono, diverso dai dati relativi agli abbonati, agli accessi e alle operazioni;

(11) "sistema di informazione": il sistema di informazione come definito all'articolo 2, lettera a), della direttiva 2013/40/UE del Parlamento europeo e del Consiglio[45];

(12) "Stato di emissione": lo Stato membro nel quale è emesso l'ordine europeo di produzione o l'ordine europeo di conservazione;

(13) "Stato di esecuzione": lo Stato membro nel quale il destinatario dell'ordine europeo di produzione o dell'ordine europeo di conservazione risiede o è stabilito e a cui l'ordine europeo di produzione e il certificato di ordine europeo di produzione o l'ordine europeo di conservazione e il certificato di ordine europeo di conservazione sono trasmessi ai fini dell'esecuzione;

(14) "autorità di esecuzione": l'autorità competente dello Stato di esecuzione alla quale l'ordine europeo di produzione e il certificato di ordine europeo di produzione o l'ordine europeo di conservazione e il certificato di ordine europeo di conservazione sono trasmessi dall'autorità di emissione ai fini dell'esecuzione;

(15) "casi di emergenza": le situazioni in cui sussiste una minaccia imminente per la vita o l'integrità fisica di una persona o per un'infrastruttura critica come definita all'articolo 2, lettera a), della direttiva 2008/114/CE del Consiglio[46].

---

45 Direttiva 2013/40/UE del Parlamento europeo e del Consiglio, del 12 agosto 2013, relativa agli attacchi contro i sistemi di informazione e che sostituisce la decisione quadro 2005/222/GAI del Consiglio (GU L 218 del 14.8.2013, pag. 8).

46 Direttiva 2008/114/CE del Consiglio, dell'8 dicembre 2008, relativa all'individuazione e alla designazione delle infrastrutture critiche europee e alla valutazione della necessità di migliorarne la protezione (GU L 345 del 23.12.2008, pag. 75).

Articolo 3
Ambito di applicazione

1. Il presente regolamento si applica ai prestatori di servizi che offrono servizi nell'Unione.

2. L'ordine europeo di produzione e l'ordine europeo di conservazione possono essere emessi solo per procedimenti penali, in fase sia preprocessuale che processuale. Gli ordini possono essere emessi anche per procedimenti relativi a reati per i quali una persona giuridica può essere considerata responsabile o punibile nello Stato di emissione.

3. Gli ordini di cui al presente regolamento possono essere emessi solo per i dati riguardanti i servizi definiti all'articolo 2, punto 3, offerti nell'Unione.

Capo 2: Ordine europeo di produzione, ordine europeo di conservazione e certificati

Articolo 4
Autorità di emissione

1. L'ordine europeo di produzione riguardante dati relativi agli abbonati o dati relativi agli accessi può essere emesso 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. L'ordine europeo di produzione è convalidato, previo esame della sua conformità alle condizioni di emissione di un ordine europeo di produzione ai sensi del presente regolamento, da un giudice, un organo giurisdizionale, un magistrato inquirente o un pubblico ministero nello Stato di emissione.

2. L'ordine europeo di produzione riguardante dati relativi alle operazioni o dati relativi al contenuto può essere emesso solo da:

   (a) un giudice, un organo giurisdizionale o un magistrato inquirente 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. L'ordine europeo di produzione è convalidato, previo esame della sua conformità alle condizioni di emissione di un ordine europeo di produzione ai sensi del presente regolamento, da un giudice, un organo giurisdizionale o un magistrato inquirente nello Stato di emissione.

3. L'ordine europeo di conservazione può essere emesso 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. 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.

4. Laddove l'ordine sia stato convalidato da un'autorità giudiziaria a norma del paragrafo 1, lettera b), del paragrafo 2, lettera b) o del paragrafo 3, lettera b), tale autorità può anche essere considerata l'autorità di emissione ai fini della trasmissione del certificato di ordine europeo di produzione e del certificato di ordine europeo di conservazione.

Articolo 5
Condizioni di emissione dell'ordine europeo di produzione

1. L'autorità di emissione può emettere un ordine europeo di produzione se sono 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 3, paragrafo 2, e può essere emesso solo se una misura dello stesso tipo è disponibile per lo stesso reato in una situazione nazionale comparabile nello Stato di emissione.

3. L'ordine europeo di produzione per la produzione di dati relativi agli abbonati o dati relativi agli accessi può essere emesso per qualsiasi reato.

4. L'ordine europeo di produzione per la produzione di dati relativi alle operazioni o dati relativi al contenuto può essere emesso solo

(a) per i reati punibili nello Stato di emissione con una pena detentiva della durata massima di almeno 3 anni, oppure

(b) per i seguenti reati, se commessi in tutto o in parte a mezzo di un sistema di informazione:

– i reati di cui agli articoli 3, 4 e 5 della decisione quadro 2001/413/GAI del Consiglio[47];

– i reati di cui agli articoli da 3 a 7 della direttiva 2011/92/UE del Parlamento europeo e del Consiglio[48];

– i reati di cui agli articoli da 3 a 8 della direttiva 2013/40/UE del Parlamento europeo e del Consiglio;

(c) per i reati di cui agli articoli da 3 a 12 e all'articolo 14 della direttiva (UE) 2017/541 del Parlamento europeo e del Consiglio[49].

---

47 Decisione quadro 2001/413/GAI del Consiglio, del 28 maggio 2001, relativa alla lotta contro le frodi e le falsificazioni di mezzi di pagamento diversi dai contanti (GU L 149 del 2.6.2001, pag. 1).

48 Direttiva 2011/92/UE del Parlamento europeo e del Consiglio, del 13 dicembre 2011, relativa alla lotta contro l'abuso e lo sfruttamento sessuale dei minori e la pornografia minorile, e che sostituisce la decisione quadro 2004/68/GAI del Consiglio (GU L 335 del 17.12.2011, pag. 1).

5. L'ordine europeo di produzione contiene le seguenti informazioni:

(a) i dati relativi all'autorità di emissione e, laddove applicabile, all'autorità di convalida;

(b) il destinatario dell'ordine europeo di produzione, di cui all'articolo 7;

(c) le persone i cui dati sono richiesti, tranne quando l'unico fine dell'ordine è identificare una persona;

(d) la categoria di dati richiesti (dati relativi agli abbonati, dati relativi agli accessi, dati relativi alle operazioni o dati relativi al contenuto);

(e) se del caso, l'intervallo di tempo per il quale è richiesta la produzione;

(f) le disposizioni di diritto penale applicabili dello Stato di emissione;

(g) in caso di emergenza o richiesta di divulgazione anticipata, i relativi motivi;

(h) se i dati ricercati sono conservati o trattati nell'ambito di un'infrastruttura fornita dal prestatore di servizi a una società o altra entità diversa da una persona fisica, la conferma che l'ordine è effettuato in conformità al paragrafo 6;

(i) i motivi della necessità e della proporzionalità della misura.

6. Se i dati ricercati sono conservati o trattati nell'ambito di un'infrastruttura fornita dal prestatore di servizi a una società o altra entità diversa da una persona fisica, e se risulta inappropriato rivolgere atti d'indagine a detta società o entità, soprattutto perché si rischierebbe di compromettere l'indagine, l'ordine europeo di produzione è rivolto solo al prestatore di servizi.

7. Se l'autorità di emissione ha motivo di ritenere che i dati richiesti relativi alle operazioni o al contenuto siano protetti con immunità e privilegi riconosciuti dal diritto dello Stato membro nel quale il destinatario risiede o è stabilito o che la loro divulgazione possa incidere su interessi fondamentali di tale Stato membro, come la sicurezza e la difesa nazionali, essa chiede chiarimenti prima di emettere l'ordine europeo di produzione, anche consultando le autorità competenti di detto Stato membro direttamente o tramite Eurojust o la Rete giudiziaria europea. Se ritiene che i dati richiesti relativi all'accesso, alle operazioni o al contenuto siano protetti con immunità e privilegi o che la loro divulgazione incida su interessi fondamentali dell'altro Stato membro, l'autorità di emissione non emette l'ordine europeo di produzione.

Articolo 6
Condizioni di emissione dell'ordine europeo di conservazione

1. L'autorità di emissione può emettere un ordine europeo di conservazione se sono soddisfatte le condizioni stabilite dal presente articolo.

2. L'ordine europeo di conservazione può essere emesso se è necessario e proporzionato per impedire la rimozione, la cancellazione o la modifica di dati in vista di una successiva richiesta di produzione dei medesimi tramite l'assistenza giudiziaria, un ordine europeo d'indagine o un ordine europeo di produzione.

---

[49] Direttiva (UE) 2017/541 del Parlamento europeo e del Consiglio, del 15 marzo 2017, sulla lotta contro il terrorismo e che sostituisce la decisione quadro 2002/475/GAI del Consiglio e che modifica la decisione 2005/671/GAI del Consiglio (GU L 88 del 31.3.2017, pag. 6).

L'ordine europeo di conservazione per la conservazione di dati può essere emesso per qualsiasi reato.

3. L'ordine europeo di conservazione contiene le seguenti informazioni:

   (a) i dati relativi all'autorità di emissione e, laddove applicabile, all'autorità di convalida;

   (b) il destinatario dell'ordine europeo di conservazione, di cui all'articolo 7;

   (c) le persone i cui dati devono essere conservati, tranne quando l'unico fine dell'ordine è identificare una persona;

   (d) la categoria di dati da conservare (dati relativi agli abbonati, dati relativi agli accessi, dati relativi alle operazioni o dati relativi al contenuto);

   (e) se del caso, l'intervallo di tempo per il quale è richiesta la conservazione;

   (f) le disposizioni di diritto penale applicabili dello Stato di emissione;

   (g) i motivi della necessità e della proporzionalità della misura.

Articolo 7

Destinatario dell'ordine europeo di produzione e dell'ordine europeo di conservazione

1. L'ordine europeo di produzione e l'ordine europeo di conservazione sono rivolti direttamente al rappresentante legale designato dal prestatore di servizi ai fini dell'acquisizione delle prove nei procedimenti penali.

2. In assenza di designazione del rappresentante legale, l'ordine europeo di produzione e l'ordine europeo di conservazione possono essere rivolti a qualsiasi stabilimento del prestatore di servizi nell'Unione.

3. Se il rappresentante legale non ottempera all'EPOC in un caso di emergenza conformemente all'articolo 9, paragrafo 2, l'EPOC può essere rivolto a qualsiasi stabilimento del prestatore di servizi nell'Unione.

4. Se il rappresentante legale non ottempera agli obblighi di cui all'articolo 9 o 10 e l'autorità di emissione ritiene che sussista un grave rischio di perdita dei dati, l'ordine europeo di produzione o l'ordine europeo di conservazione può essere rivolto a qualsiasi stabilimento del prestatore di servizi nell'Unione.

Articolo 8

Certificato di ordine europeo di produzione e certificato di ordine europeo di conservazione

1. L'ordine europeo di produzione o l'ordine europeo di conservazione è trasmesso al prestatore di servizi mediante un certificato di ordine europeo di produzione (European Production Order Certificate, EPOC) o un certificato di ordine europeo di conservazione (European Preservation Order Certificate, EPOC-PR), rispettivamente.

   L'autorità di emissione o di convalida completa l'EPOC di cui all'allegato I o l'EPOC-PR di cui all'allegato II, lo firma e certifica che le informazioni in esso contenute sono accurate e corrette.

2. L'EPOC o l'EPOC-PR è trasmesso direttamente con ogni mezzo che consenta di conservare una traccia scritta in condizioni che permettano al destinatario di stabilirne l'autenticità.

   Qualora i prestatori di servizi, gli Stati membri o gli organi dell'Unione abbiano istituito piattaforme dedicate o altri canali sicuri per il trattamento delle richieste di dati da parte delle autorità giudiziarie e di contrasto, l'autorità di emissione può scegliere di trasmettere il certificato tramite questi canali.

3. L'EPOC contiene le informazioni di cui all'articolo 5, paragrafo 5, lettere da a) a h), comprese informazioni sufficienti a permettere al destinatario di identificare e contattare l'autorità di emissione. I motivi della necessità e della proporzionalità della misura o ulteriori dettagli sulle indagini non sono inclusi.

4. L'EPOC-PR contiene le informazioni di cui all'articolo 6, paragrafo 3, lettere da a) a f), comprese informazioni sufficienti a permettere al destinatario di identificare e contattare l'autorità di emissione. I motivi della necessità e della proporzionalità della misura o ulteriori dettagli sulle indagini non sono inclusi.

5. Se necessario, l'EPOC o l'EPOC-PR è tradotto in una lingua ufficiale dell'Unione accettata dal destinatario. Qualora non sia stata specificata nessuna lingua, l'EPOC o l'EPOC-PR è tradotto in una delle lingue ufficiali dello Stato membro in cui il rappresentante legale risiede o è stabilito.

Articolo 9
Esecuzione dell'EPOC

1. Quando riceve l'EPOC il destinatario provvede affinché i dati richiesti siano trasmessi direttamente all'autorità di emissione o alle autorità di contrasto, come indicato nell'EPOC, entro 10 giorni dalla sua ricezione, a meno che l'autorità di emissione indichi motivi per una divulgazione anticipata.

2. In caso di emergenza il destinatario trasmette i dati richiesti senza indebito ritardo, al più tardi entro 6 ore dalla ricezione dell'EPOC.

3. Se non può ottemperare ai suoi obblighi perché l'EPOC è incompleto o contiene errori manifesti o informazioni insufficienti per eseguirlo, il destinatario ne informa l'autorità di emissione specificata nell'EPOC senza indebito ritardo e chiede chiarimenti, usando il modulo di cui all'allegato III. Esso comunica all'autorità di emissione se è stato o meno possibile procedere all'identificazione e alla conservazione conformemente al paragrafo 6. L'autorità di emissione reagisce tempestivamente, al più tardi entro 5 giorni. I termini di cui ai paragrafi 1 e 2 non si applicano fino a quando sono forniti i chiarimenti.

4. Se non può ottemperare ai suoi obblighi a causa di forza maggiore o per impossibilità materiale non imputabile al destinatario o, se diverso, al prestatore di servizi, in particolare perché la persona i cui dati sono ricercati non è sua cliente o i dati sono stati cancellati prima della ricezione dell'EPOC, il destinatario ne informa l'autorità di emissione specificata nell'EPOC senza indebito ritardo e spiega i motivi, usando il modulo di cui all'allegato III. Se le condizioni pertinenti sono soddisfatte, l'autorità di emissione ritira l'EPOC.

5. In tutti i casi in cui per altri motivi non fornisce le informazioni richieste o non le fornisce in maniera esaustiva o entro i termini, il destinatario ne comunica i motivi all'autorità di emissione senza indebito ritardo, al più tardi entro i termini di cui ai

paragrafi 1 e 2, usando il modulo di cui all'allegato III. L'autorità di emissione riesamina l'ordine alla luce delle informazioni fornite dal prestatore di servizi e, se necessario, fissa a quest'ultimo un nuovo termine per la produzione dei dati.

Qualora ritenga di non poter ottemperare all'EPOC perché dalle sole informazioni ivi contenute risulta che esso viola manifestamente la Carta dei diritti fondamentali dell'Unione europea o che è manifestamente arbitrario, il destinatario invia il modulo di cui all'allegato III anche all'autorità di esecuzione competente del proprio Stato membro. In tali casi l'autorità di esecuzione competente può chiedere all'autorità di emissione chiarimenti sull'ordine europeo di produzione, direttamente o tramite Eurojust o la Rete giudiziaria europea.

6. Se non produce immediatamente i dati richiesti, il destinatario li conserva, tranne se le informazioni contenute nell'EPOC non consentono di indentificarli, nel qual caso il destinatario chiede chiarimenti conformemente al paragrafo 3. I dati sono conservati fino alla loro produzione sulla base dell'ordine europeo di produzione chiarito e il relativo certificato o attraverso altri canali, quali l'assistenza giudiziaria. Se la produzione e la conservazione dei dati non sono più necessarie, l'autorità di emissione e, ove applicabile ai sensi dell'articolo 14, paragrafo 8, l'autorità di esecuzione, ne informa il destinatario senza indebito ritardo.

Articolo 10
Esecuzione dell'EPOC-PR

1. Quando riceve l'EPOC-PR il destinatario provvede, senza indebito ritardo, a conservare i dati richiesti. La conservazione cessa dopo 60 giorni, a meno che l'autorità di emissione confermi che è stata avviata la successiva richiesta di produzione.

2. Se l'autorità di emissione conferma entro il termine di cui al paragrafo 1 l'avvio della successiva richiesta di produzione, il destinatario conserva i dati per tutto il tempo necessario per la loro produzione una volta che la successiva richiesta di produzione è stata notificata.

3. Se la conservazione non è più necessaria, l'autorità di emissione ne informa il destinatario senza indebito ritardo.

4. Se non può ottemperare ai suoi obblighi perché il certificato è incompleto o contiene errori manifesti o informazioni insufficienti per eseguirlo, il destinatario ne informa l'autorità di emissione specificata nell'EPOC-PR senza indebito ritardo e chiede chiarimenti, usando il modulo di cui all'allegato III. L'autorità di emissione reagisce tempestivamente, al più tardi entro 5 giorni. Il destinatario, da parte sua, provvede affinché possano essere ricevuti i chiarimenti necessari per ottemperare all'obbligo di cui al paragrafo 1.

5. Se non può ottemperare ai suoi obblighi a causa di forza maggiore o per impossibilità materiale non imputabile al destinatario o, se diverso, al prestatore di servizi, in particolare perché la persona i cui dati sono ricercati non è sua cliente o i dati sono stati cancellati prima della ricezione dell'ordine, il destinatario ne informa l'autorità di emissione specificata nell'EPOC-PR senza indebito ritardo e spiega i motivi, usando il modulo di cui all'allegato III. Se le condizioni pertinenti sono soddisfatte, l'autorità di emissione ritira l'EPOC-PR.

6. In tutti i casi in cui, per altri motivi indicati nel modulo di cui all'allegato III, non conserva le informazioni richieste, il destinatario ne comunica i motivi all'autorità di

emissione senza indebito ritardo, usando il modulo di cui all'allegato III. L'autorità di emissione riesamina l'ordine alla luce della giustificazione fornita dal prestatore di servizi.

Articolo 11
Riservatezza e informazioni all'utente

1. Il destinatario e, se diverso, il prestatore di servizi prende le misure necessarie per garantire la riservatezza dell'EPOC o dell'EPOC-PR e dei dati prodotti o conservati e, se richiesto dall'autorità di emissione, si astiene dall'informare la persona i cui dati sono ricercati, per non ostacolare il pertinente procedimento penale.
2. Se ha chiesto al destinatario di astenersi dall'informare la persona i cui dati sono ricercati dall'EPOC, l'autorità di emissione informa senza indebito ritardo tale persona in merito alla produzione dei dati. Detta informazione può essere posticipata per il tempo necessario e proporzionato per non ostacolare il pertinente procedimento penale.
3. Nell'informare la persona, l'autorità di emissione fornisce anche informazioni su qualsiasi mezzo di ricorso disponibile a norma dell'articolo 17.

Articolo 12
Rimborso delle spese

Laddove ciò sia previsto dal diritto nazionale dello Stato di emissione per gli ordini nazionali in situazioni analoghe, il prestatore di servizi può chiedere allo Stato di emissione il rimborso delle spese conformemente alle disposizioni nazionali.

Capo 3: Sanzioni ed esecuzione

Articolo 13
Sanzioni

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 obblighi di cui agli articoli 9, 10 e 11 del presente regolamento e adottano tutti i provvedimenti necessari per assicurarne l'applicazione. Le sanzioni pecuniarie previste devono essere effettive, proporzionate e dissuasive. Gli Stati membri notificano senza indugio alla Commissione tali norme e provvedimenti nonché loro eventuali modifiche.

Articolo 14
Procedura di esecuzione

1. Se il destinatario non ottempera all'EPOC entro il termine stabilito o all'EPOC-PR, senza fornire motivi che siano accettati dall'autorità di emissione, questa può trasferire all'autorità competente dello Stato di esecuzione l'ordine europeo di produzione e l'EPOC, o l'ordine europeo di conservazione e l'EPOC-PR, unitamente al modulo di cui all'allegato III compilato dal destinatario e a qualsiasi altro documento pertinente, ai fini dell'esecuzione dell'ordine, con ogni mezzo che

consenta di conservare una traccia scritta in condizioni che permettano all'autorità di esecuzione di stabilirne l'autenticità. A tal fine l'autorità di emissione traduce l'ordine, il modulo e qualsiasi altro documento di accompagnamento in una delle lingue ufficiali di tale Stato membro e informa il destinatario del trasferimento.

2. Una volta ricevuta la documentazione, l'autorità di esecuzione riconosce senza ulteriori formalità l'ordine europeo di produzione o l'ordine europeo di conservazione trasmesso conformemente al paragrafo 1 e adotta le misure necessarie alla sua esecuzione, a meno che ritenga che si applichi uno dei motivi di cui al paragrafo 4 o 5 o che i dati in questione siano protetti con un'immunità o un privilegio ai sensi del proprio diritto nazionale o che la loro divulgazione possa incidere su interessi fondamentali del proprio Stato, come la sicurezza e la difesa nazionali. La decisione sul riconoscimento è adottata senza indebito ritardo e comunque entro 5 giorni lavorativi dalla ricezione dell'ordine da parte dell'autorità di esecuzione.

3. Se riconosce l'ordine, l'autorità di esecuzione ingiunge formalmente al destinatario di ottemperare all'obbligo pertinente, informandolo della possibilità di opporsi all'esecuzione invocando uno dei motivi elencati al paragrafo 4 o 5, nonché delle sanzioni applicabili in caso di inottemperanza, e fissa un termine per l'ottemperanza o l'opposizione.

4. Il destinatario può opporsi all'esecuzione dell'ordine europeo di produzione solo per uno dei seguenti motivi:

   (a) l'ordine europeo di produzione non è stato emesso o convalidato da un'autorità di emissione conformemente all'articolo 4;

   (b) l'ordine europeo di produzione non è stato emesso in relazione a un reato di cui all'articolo 5, paragrafo 4;

   (c) il destinatario non ha potuto ottemperare all'EPOC per impossibilità materiale o forza maggiore o perché l'EPOC contiene errori manifesti;

   (d) l'ordine europeo di produzione non riguarda dati conservati dal prestatore di servizi o per suo conto al momento della ricezione dell'EPOC;

   (e) il servizio esula dall'ambito di applicazione del presente regolamento;

   (f) dalle sole informazioni contenute nell'EPOC risulta che esso viola manifestamente la Carta dei diritti fondamentali dell'Unione europea o che è manifestamente arbitrario.

5. Il destinatario può opporsi all'esecuzione dell'ordine europeo di conservazione solo per i seguenti motivi:

   (a) l'ordine europeo di conservazione non è stato emesso o convalidato da un'autorità di emissione conformemente all'articolo 4;

   (b) il prestatore di servizi non ha potuto ottemperare all'EPOC-PR per impossibilità materiale o forza maggiore o perché l'EPOC-PR contiene errori manifesti;

   (c) l'ordine europeo di conservazione non riguarda dati conservati dal prestatore di servizi o per suo conto al momento della ricezione dell'EPOC-PR;

   (d) il servizio esula dall'ambito di applicazione del presente regolamento;

(e) dalle sole informazioni contenute nell'EPOC-PR risulta che esso viola manifestamente la Carta dei diritti fondamentali dell'Unione europea o che è manifestamente arbitrario.

6. In caso di opposizione del destinatario, l'autorità di esecuzione decide se eseguire l'ordine sulla base delle informazioni fornite dal destinatario e, se necessario, delle informazioni supplementari ottenute dall'autorità di emissione in conformità al paragrafo 7.

7. Prima di decidere di non riconoscere o non eseguire l'ordine conformemente ai paragrafi 2 e 6, l'autorità di esecuzione consulta l'autorità di emissione con qualsiasi mezzo appropriato. Se del caso, chiede ulteriori informazioni all'autorità di emissione. L'autorità di emissione risponde alla richiesta entro 5 giorni lavorativi.

8. Tutte le decisioni sono comunicate immediatamente all'autorità di emissione e al destinatario con ogni mezzo che consenta di conservare una traccia scritta.

9. Se ottiene i dati dal destinatario, l'autorità di esecuzione li trasmette all'autorità di emissione entro 2 giorni lavorativi, a meno che tali dati siano protetti con un'immunità o un privilegio ai sensi del proprio diritto nazionale o incidano su interessi fondamentali del proprio Stato, come la sicurezza e la difesa nazionali. In tali casi informa l'autorità di emissione dei motivi della mancata trasmissione dei dati.

10. Se il destinatario non ottempera agli obblighi derivanti da un ordine che è stato riconosciuto e la cui esecutività è stata confermata dall'autorità di esecuzione, quest'ultima irroga una sanzione pecuniaria conformemente al proprio diritto nazionale. Contro la decisione che irroga la sanzione è disponibile un ricorso giurisdizionale effettivo.

Capo 4: Mezzi di ricorso

Articolo 15
Procedura di riesame in caso di obblighi contrastanti basati su diritti fondamentali o interessi fondamentali di un paese terzo

1. Se ritiene che l'ottemperanza all'ordine europeo di produzione sia in contrasto con il diritto applicabile di un paese terzo che vieta la divulgazione dei dati in questione per la necessità di tutelare i diritti fondamentali delle persone interessate o interessi fondamentali del paese terzo connessi alla sicurezza o alla difesa nazionali, il destinatario informa l'autorità di emissione dei motivi per non eseguire l'ordine conformemente alla procedura di cui all'articolo 9, paragrafo 5.

2. L'opposizione motivata contiene tutte le informazioni pertinenti sul diritto del paese terzo, sulla sua applicabilità al caso di specie e sulla natura dell'obbligo contrastante. Essa non può fondarsi sull'assenza, nel diritto applicabile del paese terzo, di disposizioni analoghe riguardo alle condizioni, alle formalità e alle procedure di emissione di un ordine di produzione, né sulla sola circostanza che i dati sono conservati in un paese terzo.

3. L'autorità di emissione riesamina l'ordine europeo di produzione sulla base dell'obiezione motivata. Se intende confermarlo, ne chiede il riesame da parte dell'organo giurisdizionale competente del proprio Stato membro. L'esecuzione dell'ordine è sospesa in attesa del completamento della procedura di riesame.

L'organo giurisdizionale competente valuta innanzitutto se esista un contrasto, esaminando

(a) se, in base alle circostanze specifiche del caso di specie, si applica il diritto del paese terzo e, in caso affermativo,

(b) se il diritto del paese terzo, ove applicato alle circostanze specifiche del caso, vieta la divulgazione dei dati in questione.

4. Nell'effettuare tale valutazione l'organo giurisdizionale dovrebbe esaminare se il diritto del paese terzo, anziché tutelare i diritti fondamentali o interessi fondamentali del paese terzo connessi alla sicurezza o alla difesa nazionali, intenda manifestamente tutelare altri interessi o proteggere attività illecite dalle richieste delle autorità di contrasto nell'ambito delle indagini penali.

5. Se ritiene che non esista alcun contrasto pertinente ai sensi dei paragrafi 1 e 4, l'organo giurisdizionale competente conferma l'ordine. Se accerta l'esistenza di un contrasto pertinente ai sensi dei paragrafi 1 e 4, l'organo giurisdizionale competente trasmette alle autorità centrali del paese terzo in questione, tramite la sua autorità centrale nazionale, tutte le pertinenti informazioni fattuali e giuridiche relative al caso, compresa la propria valutazione, fissando un termine di 15 giorni per rispondere. Su richiesta motivata dell'autorità centrale del paese terzo, il termine può essere prorogato di 30 giorni.

6. Se entro il termine stabilito l'autorità centrale del paese terzo comunica all'organo giurisdizionale competente che essa si oppone all'esecuzione dell'ordine europeo di produzione nel caso di specie, l'organo giurisdizionale competente revoca l'ordine e ne informa l'autorità di emissione e il destinatario. Se entro il termine (prorogato) non riceve alcuna opposizione, l'organo giurisdizionale competente invia un sollecito all'autorità centrale del paese terzo concedendole altri 5 giorni per rispondere e informandola delle conseguenze della mancata risposta. Qualora non riceva alcuna opposizione entro tale ulteriore termine, l'organo giurisdizionale competente conferma l'ordine.

7. Se stabilisce che l'ordine deve essere confermato, l'organo giurisdizionale competente ne informa l'autorità di emissione e il destinatario, che deve procedere nell'esecuzione dell'ordine.

Articolo 16

Procedura di riesame in caso di obblighi contrastanti basati su altri motivi

1. Se ritiene che l'ottemperanza all'ordine europeo di produzione sia in contrasto con il diritto applicabile di un paese terzo che vieta la divulgazione dei dati in questione per motivi diversi da quelli di cui all'articolo 15, il destinatario informa l'autorità di emissione dei motivi per non eseguire l'ordine conformemente alla procedura di cui all'articolo 9, paragrafo 5.

2. L'opposizione motivata contiene tutte le informazioni pertinenti sul diritto del paese terzo, sulla sua applicabilità al caso di specie e sulla natura dell'obbligo contrastante. Essa non può fondarsi sull'assenza, nel diritto applicabile del paese terzo, di disposizioni analoghe riguardo alle condizioni, alle formalità e alle procedure di emissione di un ordine di produzione, né sulla sola circostanza che i dati sono conservati in un paese terzo.

3. L'autorità di emissione riesamina l'ordine europeo di produzione sulla base dell'obiezione motivata. Se intende confermarlo, ne chiede il riesame da parte dell'organo giurisdizionale competente del proprio Stato membro. L'esecuzione dell'ordine è sospesa in attesa del completamento della procedura di riesame.

4. L'organo giurisdizionale competente valuta innanzitutto se esista un contrasto, esaminando

   (a) se, in base alle circostanze specifiche del caso di specie, si applica il diritto del paese terzo e, in caso affermativo,

   (b) se il diritto del paese terzo, ove applicato alle circostanze specifiche del caso, vieta la divulgazione dei dati in questione.

5. Se ritiene che non esista alcun contrasto pertinente ai sensi dei paragrafi 1 e 4, l'organo giurisdizionale competente conferma l'ordine. Se accerta che il diritto del paese terzo, ove applicato alle circostanze specifiche del caso, vieta la divulgazione dei dati in questione, l'organo giurisdizionale competente decide se confermare o ritirare l'ordine basandosi, in particolare, sui seguenti elementi:

   (a) l'interesse tutelato dal diritto del paese terzo, compreso l'interesse del paese terzo a impedire la divulgazione dei dati;

   (b) il grado di collegamento del procedimento penale per il quale l'ordine è stato emesso con una delle due giurisdizioni, risultante, tra l'altro:

   dall'ubicazione, dalla cittadinanza e dalla residenza della persona i cui dati sono richiesti e/o della vittima,

   dal luogo in cui il reato in questione è stato commesso;

   (c) il grado di collegamento tra il prestatore di servizi e il paese terzo in questione; in tale contesto, il luogo di conservazione dei dati non è di per sé sufficiente per stabilire un grado di collegamento significativo;

   (d) l'interesse dello Stato dell'indagine a ottenere le prove in questione, sulla base della gravità del reato e dell'importanza di acquisire le prove rapidamente;

   (e) le possibili conseguenze per il destinatario o il prestatore di servizi in caso di ottemperanza all'ordine europeo di produzione, comprese le sanzioni in cui può incorrere.

6. Se decide di revocare l'ordine, l'organo giurisdizionale competente ne informa l'autorità di emissione e il destinatario. Se stabilisce che l'ordine deve essere confermato, l'organo giurisdizionale competente ne informa l'autorità di emissione e il destinatario, che deve procedere ad eseguire l'ordine.

Articolo 17
Ricorso effettivo

1. Gli indagati e gli imputati i cui dati sono stati ottenuti tramite un ordine europeo di produzione hanno il diritto a un ricorso effettivo contro tale ordine durante il procedimento penale per il quale l'ordine è stato emesso, fatti salvi i mezzi di ricorso disponibili ai sensi della direttiva (UE) 2016/680 e del regolamento (UE) 2016/679.

2. Le persone i cui dati sono stati ottenuti, diverse dagli indagati e imputati nel procedimento penale per il quale l'ordine europeo di produzione è stato emesso,

hanno il diritto a un ricorso effettivo contro tale ordine nello Stato di emissione, fatti salvi i mezzi di ricorso disponibili ai sensi della direttiva (UE) 2016/680 e del regolamento (UE) 2016/679.

3. Il diritto a un ricorso effettivo è esercitato dinanzi a un organo giurisdizionale dello Stato di emissione in conformità al diritto nazionale di tale Stato e include la possibilità di contestare la legittimità della misura, comprese la sua necessità e la sua proporzionalità.

4. Fatto salvo l'articolo 11, l'autorità di emissione adotta le misure appropriate per garantire che siano fornite informazioni sulle possibilità di ricorso ai sensi del diritto nazionale e per garantirne l'esercizio effettivo.

5. I termini o altre condizioni per la proposizione del ricorso sono uguali a quelli previsti in casi interni analoghi e sono applicati in modo da garantire alle persone interessate l'esercizio effettivo del ricorso.

6. Fatte salve le norme procedurali nazionali, gli Stati membri assicurano che nei procedimenti penali nello Stato di emissione siano rispettati i diritti della difesa e sia garantito un giusto processo nel valutare le prove acquisite tramite l'ordine europeo di produzione.

Articolo 18
Privilegi e immunità ai sensi del diritto dello Stato di esecuzione

Se i dati relativi alle operazioni o al contenuto ottenuti tramite l'ordine europeo di produzione sono protetti con immunità o privilegi ai sensi del diritto dello Stato membro del destinatario, o incidono su interessi fondamentali di tale Stato membro come la sicurezza e la difesa nazionali, l'organo giurisdizionale dello Stato di emissione garantisce, durante il procedimento penale per il quale l'ordine è stato emesso, che nel valutare la pertinenza e l'ammissibilità delle prove in questione tali motivi siano presi in considerazione come se fossero previsti dal suo diritto nazionale. L'organo giurisdizionale può consultare le autorità dello Stato membro pertinente, la Rete giudiziaria europea in materia penale o Eurojust.

Capo 5: Disposizioni finali

Articolo 19
Monitoraggio e relazioni

1. Entro il *[data di applicazione del presente regolamento]*, la Commissione istituisce un programma dettagliato per monitorare gli esiti, i risultati e gli effetti del presente regolamento. Il programma di monitoraggio definisce i mezzi da utilizzare per raccogliere i dati e le altre evidenze necessarie, nonché la periodicità di tali acquisizioni. Esso specifica le misure che la Commissione e gli Stati membri devono adottare nella raccolta e nell'analisi dei dati e altre evidenze.

2. In ogni caso, gli Stati membri raccolgono e conservano dati statistici esaurienti provenienti dalle autorità pertinenti. I dati raccolti sono inviati alla Commissione ogni anno entro il 31 marzo per l'anno civile precedente e includono:

   (a) il numero di EPOC e EPOC-PR emessi, per tipo di dati richiesti, prestatori di servizi destinatari e situazione (di emergenza o meno);

(b) il numero di EPOC e EPOC-PR adempiuti e non adempiuti, per tipo di dati richiesti, prestatori di servizi destinatari e situazione (di emergenza o meno);

(c) per gli EPOC adempiuti, la durata media per l'ottenimento dei dati richiesti dal momento dell'emissione dell'EPOC all'ottenimento dei dati, per tipo di dati richiesti, prestatori di servizi destinatari e situazione (di emergenza o meno);

(d) il numero di ordini europei di produzione trasmessi a uno Stato di esecuzione e da questo ricevuti ai fini dell'esecuzione, per tipo di dati richiesti, prestatori di servizi destinatari e situazione (di emergenza o meno), e il numero di tali ordini adempiuti;

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

Articolo 20
Modifiche dei certificati e dei moduli

La Commissione adotta atti delegati conformemente all'articolo 21 per modificare gli allegati I, II e III al fine di rispondere efficacemente all'eventuale necessità di migliorare il contenuto dei moduli EPOC e EPOC-PR e del modulo per fornire informazioni sull'impossibilità di eseguire l'EPOC o l'EPOC-PR.

Articolo 21
Esercizio della delega

1. Il potere di adottare atti delegati è conferito alla Commissione alle condizioni stabilite nel presente articolo.

2. La delega di potere di cui all'articolo 20 è conferita per un periodo indeterminato a decorrere dal *[data di applicazione del presente regolamento]*.

3. La delega di potere di cui all'articolo 20 può essere revocata in qualsiasi momento dal Parlamento europeo o dal Consiglio. La decisione di revoca pone fine alla delega di potere ivi specificata. Gli effetti della decisione decorrono dal giorno successivo alla pubblicazione della decisione nella *Gazzetta ufficiale dell'Unione europea* o da una data successiva ivi specificata. Essa non pregiudica la validità degli atti delegati già in vigore.

4. Prima dell'adozione dell'atto delegato la Commissione consulta gli esperti designati da ciascuno Stato membro nel rispetto dei principi stabiliti nell'accordo interistituzionale "Legiferare meglio" del 13 aprile 2016[50].

5. Non appena adotta un atto delegato, la Commissione ne dà contestualmente notifica al Parlamento europeo e al Consiglio.

6. L'atto delegato adottato ai sensi dell'articolo 20 entra in vigore solo se né il Parlamento europeo né il Consiglio hanno sollevato obiezioni entro il termine di due mesi dalla data in cui esso è stato loro notificato o se, prima della scadenza di tale termine, sia il Parlamento europeo che il Consiglio hanno informato la Commissione che non intendono sollevare obiezioni. Tale termine è prorogato di due mesi su iniziativa del Parlamento europeo o del Consiglio.

[50] GU L 123 del 12.5.2016, pag. 13.

Articolo 22
Notifiche

1. Entro il *[data di applicazione del presente regolamento]* ogni Stato membro notifica alla Commissione:

   (a) le autorità che, conformemente al proprio diritto nazionale, sono competenti ai sensi dell'articolo 4 per l'emissione e/o la convalida degli ordini europei di produzione e degli ordini europei di conservazione;

   (b) l'autorità o le autorità di esecuzione che sono competenti per l'esecuzione degli ordini europei di produzione e degli ordini europei di conservazione per conto di un altro Stato membro;

   (c) gli organi giurisdizionali competenti a trattare le obiezioni motivate dei destinatari conformemente agli articoli 15 e 16.

2. La Commissione rende disponibili le informazioni ricevute ai sensi del presente articolo pubblicandole su un apposito sito web o sul sito web della Rete giudiziaria europea di cui all'articolo 9 della decisione 2008/976/GAI del Consiglio[51].

Articolo 23
Relazione con l'ordine europeo di indagine

Le autorità degli Stati membri possono continuare a emettere ordini europei di indagine conformemente alla direttiva 2014/41/UE per l'acquisizione di prove che rientrano anche nell'ambito di applicazione del presente regolamento.

Articolo 24
Valutazione

Entro il *[5 anni dopo la data di applicazione del presente regolamento]*, la Commissione effettua una valutazione del presente regolamento e presenta al Parlamento europeo e al Consiglio una relazione sul suo funzionamento, che include una valutazione della necessità di ampliarne l'ambito di applicazione. Se necessario, la relazione è corredata di proposte legislative. La valutazione è svolta secondo gli orientamenti della Commissione per legiferare meglio. Gli Stati membri trasmettono alla Commissione le informazioni necessarie per la preparazione della relazione.

Articolo 25
Entrata in vigore

Il presente regolamento entra in vigore il ventesimo giorno successivo alla pubblicazione nella *Gazzetta ufficiale dell'Unione europea*.

Esso si applica a decorrere dal *[6 mesi dopo l'entrata in vigore]*.

[51] Decisione 2008/976/GAI del Consiglio, del 16 dicembre 2008, relativa alla Rete giudiziaria europea (GU L 348 del 24.12.2008, pag.130).

Il presente regolamento è obbligatorio in tutti i suoi elementi e direttamente applicabile negli Stati membri conformemente ai trattati.

Fatto a Bruxelles, il

Per il Parlamento europeo
Il presidente

Per il Consiglio
Il presidente