Consiglio dell'Unione europea

Bruxelles, 14 settembre 2018
(OR. en)

12129/18

Fascicolo interistituzionale: 2018/0331 (COD)

CT 144
ENFOPOL 450
COTER 114
JAI 881
CYBER 193
TELECOM 288
FREMP 142
AUDIO 64
DROIPEN 127
COHOM 107
CODEC 1468

PROPOSTA

Origine:	Jordi AYET PUIGARNAU, Direttore, per conto del Segretario Generale della Commissione europea
Data:	12 settembre 2018
Destinatario:	Jeppe TRANHOLM-MIKKELSEN, Segretario Generale del Consiglio dell'Unione europea
n. doc. Comm.:	COM(2018) 640 final
Oggetto:	Proposta di REGOLAMENTO DEL PARLAMENTO EUROPEO E DEL CONSIGLIO relativo alla prevenzione della diffusione di contenuti terroristici online *Contributo della Commissione europea alla riunione dei leader, riunitisi a Salisburgo il 19-20 settembre 2018*

Si trasmette in allegato, per le delegazioni, il documento COM(2018) 640 final.

All.: COM(2018) 640 final

COMMISSIONE
EUROPEA

Bruxelles, 12.9.2018
COM(2018) 640 final

2018/0331 (COD)

Proposta di

REGOLAMENTO DEL PARLAMENTO EUROPEO E DEL CONSIGLIO

relativo alla prevenzione della diffusione di contenuti terroristici online

Contributo della Commissione europea alla riunione dei leader, riunitisi a Salisburgo il 19-20 settembre 2018

{SEC(2018) 397 final} - {SWD(2018) 408 final} - {SWD(2018) 409 final}

RELAZIONE

1. CONTESTO DELLA PROPOSTA

1.1. Motivi e obiettivi della proposta

L'onnipresenza di Internet consente ai suoi utilizzatori di comunicare, lavorare, socializzare, creare, raccogliere e condividere informazioni e contenuti con centinaia di milioni di persone in tutto il mondo. Le piattaforme di Internet contribuiscono notevolmente al benessere economico e sociale degli utilizzatori in tutta l'Unione e al di fuori di essa. Tuttavia, la capacità di raggiungere un pubblico così vasto a costi minimi attira anche criminali intenzionati a usare Internet a fini illeciti. Gli attentati terroristici commessi di recente sul territorio dell'UE hanno dimostrato che i terroristi usano Internet per adescare e reclutare sostenitori, preparare e agevolare le attività terroristiche, celebrare le loro atrocità e istigare altri a seguire il loro esempio, infondendo paura nella popolazione.

I contenuti terroristici condivisi online a tal fine, che vengono diffusi attraverso prestatori di servizi di hosting che permettono il caricamento di contenuti di terzi, si sono rivelati determinanti nella radicalizzazione dei cosiddetti "lupi solitari" i quali, ispirati da tali contenuti, hanno compiuto diversi attentati terroristici di recente in Europa. Tali contenuti non hanno solo un considerevole impatto negativo sui singoli e sulla società in generale, ma minano anche la fiducia degli utilizzatori in Internet e pregiudicano i modelli commerciali e la reputazione delle imprese interessate. Oltre alle grandi piattaforme di social media, i terroristi si rivolgono sempre più a piccoli prestatori che offrono diversi tipi di servizi di hosting su scala mondiale. L'uso improprio di Internet solleva la questione della particolare responsabilità sociale che devono assumersi le piattaforme Internet per proteggere i loro utilizzatori dall'esposizione a contenuti terroristici e dai gravi rischi per la sicurezza che questi contenuti comportano per la società in generale.

Dando seguito alla richiesta delle autorità pubbliche, i prestatori di servizi di hosting hanno messo in atto diverse misure per contrastare la diffusione di contenuti terroristici attraverso i loro servizi. Sono stati compiuti progressi nell'ambito di iniziative volontarie e di partenariati, tra cui il Forum dell'UE su Internet avviato nel dicembre 2015 nel quadro dell'agenda europea sulla sicurezza. Il Forum dell'UE su Internet ha incoraggiato gli Stati membri e i prestatori di servizi di hosting a cooperare e ad adottare iniziative volontarie al fine di ridurre l'accessibilità dei contenuti terroristici online e dare alla società civile gli strumenti per moltiplicare i messaggi efficaci di segno opposto online. Queste iniziative hanno contribuito a rafforzare la cooperazione, migliorando le risposte da parte delle imprese alle segnalazioni effettuate dalle autorità nazionali e dall'unità addetta alle segnalazioni su Internet di Europol, ad attuare misure proattive volontarie volte a migliorare l'individuazione automatizzata di contenuti terroristici, a intensificare la cooperazione tra gli operatori del settore - compreso nel quadro dello sviluppo della "banca dati di hash" per evitare che contenuti terroristici noti siano caricati su piattaforme connesse - nonché ad accrescere la trasparenza delle iniziative. Anche se è auspicabile che la cooperazione nell'ambito del Forum dell'UE su Internet sia portata avanti in futuro, gli accordi volontari hanno anche mostrato i loro limiti. In primo luogo, non tutti i prestatori di servizi di hosting hanno aderito al Forum e, in secondo luogo, globalmente i progressi compiuti dai prestatori di servizi di hosting non sono sufficientemente estesi e rapidi per risolvere il problema in modo adeguato.

Alla luce di tali limiti, è chiaramente necessario che l'Unione europea adotti un'azione più incisiva per lottare contro i contenuti terroristici online. Il 1º marzo 2018 la Commissione ha adottato una raccomandazione sulle misure per contrastare i contenuti illegali online, prendendo spunto dalla comunicazione della Commissione di settembre[1] nonché dagli sforzi compiuti nell'ambito del Forum dell'UE su Internet. La raccomandazione conteneva un capitolo specifico che individuava una serie di misure atte ad arrestare efficacemente la pubblicazione e la diffusione di propaganda terroristica online, tra cui il miglioramento del processo di segnalazione, un termine di un'ora per rispondere alle segnalazioni, misure più proattive per individuare tali contenuti, la rimozione efficace e salvaguardie sufficienti per valutare accuratamente i contenuti terroristici[2].

La necessità di potenziare l'azione in materia di contenuti terroristici online è stata ribadita anche dagli Stati membri dell'UE, alcuni dei quali hanno già legiferato in materia o prevedono di farlo. A seguito di una serie di attentati terroristici commessi nell'UE e tenuto conto del fatto che i contenuti terroristici online continuano ad essere facilmente accessibili, il Consiglio europeo del 22-23 giugno 2017 ha esortato le imprese a sviluppare "nuove tecnologie e nuovi strumenti al fine di migliorare l'individuazione automatica e la rimozione dei contenuti che incitano a compiere atti terroristici", sostenendo che "[s]e necessario si dovrebbero completare tali iniziative con le pertinenti misure legislative a livello dell'UE". Il 28 giugno 2018 il Consiglio europeo ha accolto con favore "l'intenzione della Commissione di presentare una proposta legislativa che migliori l'individuazione e la rimozione di contenuti che incitano all'odio e a compiere atti terroristici". Inoltre il Parlamento europeo, nella sua risoluzione sulle piattaforme online e il mercato unico digitale del 15 giugno 2017, ha esortato tali piattaforme a "rafforzare le misure per affrontare i contenuti illegali e nocivi", invitando nel contempo la Commissione a presentare proposte per risolvere questi problemi.

Per far fronte a tali sfide e per rispondere alle esortazioni degli Stati membri e del Parlamento europeo, la presente proposta della Commissione mira a stabilire un quadro giuridico chiaro e armonizzato per prevenire l'uso improprio dei servizi di hosting per la diffusione di contenuti terroristici online, al fine di garantire il corretto funzionamento del mercato unico digitale e di tutelare la fiducia e la sicurezza. Il presente regolamento intende fare chiarezza riguardo alla responsabilità che incombe ai prestatori di servizi di hosting di adottare tutte le opportune misure necessarie, ragionevoli e proporzionate al fine di garantire la sicurezza dei loro servizi e l'individuazione e la rimozione efficaci dei contenuti terroristici online, tenendo in considerazione l'importanza fondamentale della libertà di espressione e di informazione in una società aperta e democratica. Il regolamento introduce inoltre una serie di misure di salvaguardia necessarie intese a garantire il pieno rispetto dei diritti fondamentali quali la libertà di espressione e di informazione in una società democratica, oltre alle possibilità di ricorso giudiziario garantite dal diritto a un ricorso effettivo sancito dall'articolo 19 del TUE e dall'articolo 47 della Carta dei diritti fondamentali dell'UE.

Fissando un insieme minimo di obblighi di diligenza per i prestatori di servizi di hosting, tra cui una serie di disposizioni e obblighi specifici, nonché obblighi per gli Stati membri, la proposta intende aumentare l'efficacia delle attuali misure per rilevare, individuare e rimuovere i contenuti terroristici online senza intaccare i diritti fondamentali come la libertà di espressione e di informazione. Tale quadro giuridico armonizzato agevolerà la fornitura di

---

1 Comunicazione sulla lotta ai contenuti illeciti online (COM (2017) 555 final).

2 Raccomandazione del 1° marzo 2018 sulle misure per contrastare efficacemente i contenuti illegali online (C(2018)1177 final).

servizi online in tutto il mercato unico digitale, garantirà condizioni di parità per tutti i prestatori di servizi di hosting che offrono i loro servizi nell'Unione europea e fornirà un solido quadro giuridico per l'individuazione e la rimozione di contenuti terroristici, accompagnato da adeguate salvaguardie a tutela dei diritti fondamentali. In particolare, gli obblighi di trasparenza rafforzeranno la fiducia dei cittadini, in particolare degli utilizzatori di Internet, e miglioreranno la responsabilità e la trasparenza delle azioni delle imprese, anche rispetto alle autorità pubbliche. La proposta stabilisce inoltre l'obbligo di predisporre meccanismi di reclamo e ricorso per assicurare che gli utilizzatori possano impugnare un ordine di rimozione dei loro contenuti. Gli obblighi previsti per gli Stati membri contribuiranno al raggiungimento di tali obiettivi e miglioreranno la capacità delle autorità competenti di adottare le opportune misure nei confronti di contenuti terroristici online e di combattere la criminalità. Se i prestatori di servizi di hosting non rispettano il regolamento, gli Stati membri possono imporre sanzioni.

1.2. Coerenza con le disposizioni vigenti nel settore normativo interessato

La presente proposta è coerente con l'acquis relativo al mercato unico digitale, in particolare la direttiva sul commercio elettronico. In particolare, tutte le misure adottate dal prestatore di servizi di hosting conformemente al presente regolamento, comprese le eventuali misure proattive, non dovrebbero di per sé implicare che il prestatore di servizi di hosting perde il beneficio dell'esenzione di responsabilità che è previsto, a determinate condizioni, all'articolo 14 della direttiva sul commercio elettronico. La decisione delle autorità nazionali di imporre specifiche misure proattive e proporzionate non dovrebbe, in linea di principio, comportare l'imposizione di un obbligo generale di sorveglianza, come stabilito all'articolo 15, paragrafo 1, della direttiva 2000/31/CE, per gli Stati membri. Tuttavia, in considerazione dei rischi particolarmente gravi associati alla diffusione dei contenuti terroristici, le decisioni prese a norma del presente regolamento possono, in via eccezionale, derogare a tale principio nell'ambito di un quadro dell'UE. Prima di adottare tali decisioni, l'autorità competente dovrebbe garantire un giusto equilibrio tra le esigenze di sicurezza pubblica e gli interessi e i diritti fondamentali lesi, tra cui, in particolare, la libertà di espressione e di informazione, la libertà d'impresa, la protezione dei dati personali e della vita privata. Gli obblighi di diligenza per i prestatori di servizi di hosting dovrebbero riflettere e rispettare l'equilibrio menzionato nella direttiva sul commercio elettronico.

La proposta è inoltre coerente e del tutto in linea con la direttiva (UE) 2017/541 sulla lotta contro il terrorismo, che mira ad armonizzare le normative degli Stati membri in materia di reati di terrorismo. L'articolo 21 della direttiva prevede che gli Stati membri adottino misure per assicurare la tempestiva rimozione dei contenuti online che costituiscono una pubblica provocazione lasciando agli Stati membri la scelta delle misure. Il presente regolamento, dato il suo carattere preventivo, riguarda non solo i materiali che incitano al terrorismo ma anche quelli finalizzati al reclutamento o all'addestramento, che corrispondono ad altri reati connessi ad attività terroristiche, anch'essi disciplinati dalla direttiva (UE) 2017/541. Il presente regolamento dispone direttamente obblighi di diligenza per i prestatori di servizi di hosting volti alla rimozione dei contenuti terroristici e armonizza l'iter degli ordini di rimozione al fine di ridurre l'accessibilità dei contenuti terroristici online.

Il regolamento integra le norme stabilite nella futura direttiva sui servizi di media audiovisivi, nella misura in cui il suo ambito di applicazione personale e materiale è più ampio. Il regolamento non comprende solo le piattaforme di condivisione di video ma tutti i diversi tipi di prestatori di servizi di hosting. Inoltre, non riguarda solo video, ma anche immagini e testo.

Inoltre, armonizzando le disposizioni sostanziali relative alle richieste di rimozione dei contenuti terroristici e alle misure proattive, il presente regolamento va oltre la direttiva.

Il regolamento proposto si basa sulla raccomandazione della Commissione[3] sui contenuti illegali del marzo 2018. La raccomandazione rimane in vigore e tutti i soggetti che svolgono un ruolo nel ridurre l'accessibilità dei contenuti illegali - compreso dei contenuti terroristici - dovrebbero continuare ad allineare i loro sforzi alle misure elencate nella raccomandazione.

1.3. Sintesi del regolamento proposto

L'ambito di applicazione personale della proposta comprende i prestatori di servizi di hosting che offrono i loro servizi all'interno dell'Unione, a prescindere dal loro luogo di stabilimento o alla loro dimensione. La normativa proposta introduce una serie di misure volte a prevenire l'uso improprio dei servizi di hosting per la diffusione di contenuti terroristici online al fine di garantire il corretto funzionamento del mercato unico digitale, garantendo nel contempo la fiducia e la sicurezza. La definizione di contenuti terroristici illegali è in linea con quella di reati di terrorismo di cui alla direttiva (UE) 2017/541: si tratta di messaggi utilizzati per istigare, mediante apologia del terrorismo, alla commissione di reati terroristici e che incitano a contribuire a tali reati, forniscono istruzioni finalizzate alla commissione di tali reati e promuovono la partecipazione a gruppi terroristici.

Al fine di garantire la rimozione di contenuti terroristici illegali, il regolamento introduce un ordine di rimozione, che può essere emesso come decisione amministrativa o giudiziaria da un'autorità competente di uno Stato membro. In questi casi, il prestatore di servizi di hosting è tenuto a rimuovere i contenuti o disabilitarne l'accesso entro un'ora. Inoltre, il regolamento armonizza i requisiti minimi per le segnalazioni inviate dalle autorità competenti degli Stati membri e dagli organismi dell'Unione (come Europol) ai prestatori di servizi di hosting, le quali saranno valutate sulla base delle rispettive condizioni contrattuali. Infine, il regolamento prevede l'obbligo per i prestatori di servizi di hosting, se del caso, di adottare misure proattive proporzionate al livello di rischio e di rimuovere il materiale terroristico dai loro servizi, anche ricorrendo a strumenti di individuazione automatizzata.

Le misure intese a ridurre i contenuti terroristici online sono accompagnate da una serie di importanti misure di salvaguardia per garantire la piena protezione dei diritti fondamentali. Nel quadro delle misure intese a proteggere dalla rimozione erronea i contenuti non terroristici, la proposta stabilisce l'obbligo di predisporre meccanismi di ricorso per assicurare che gli utilizzatori possano impugnare la rimozione dei loro contenuti. Inoltre, il regolamento introduce obblighi di trasparenza per le misure prese contro i contenuti terroristici dai prestatori di servizi di hosting, in modo che questi si assumano le loro responsabilità nei confronti degli utilizzatori, dei cittadini e delle autorità pubbliche.

Il regolamento obbliga inoltre gli Stati membri a provvedere a che le loro autorità competenti dispongano della capacità necessaria per intervenire contro i contenuti terroristici online. In aggiunta, gli Stati membri sono tenuti a comunicare e a cooperare tra loro e possono avvalersi dei canali istituiti da Europol per garantire un coordinamento per quanto riguarda gli ordini di rimozione e le segnalazioni. Il regolamento prevede anche l'obbligo per i prestatori di servizi di hosting di comunicare nel dettaglio le misure adottate e di informare le autorità di contrasto quando individuano contenuti che costituiscono una minaccia per la vita o la sicurezza. Infine,

[3] Raccomandazione (C(2018)1177 final) del 1° marzo 2018 sulle misure per contrastare efficacemente i contenuti illegali online.

è previsto l'obbligo per i prestatori di servizi di hosting di conservare i contenuti rimossi, che serve funge da tutela contro la rimozione erronea ed evita che vadano persi eventuali elementi di prova a fini di prevenzione, accertamento, indagine e perseguimento dei reati di terrorismo.

2. BASE GIURIDICA, SUSSIDIARIETÀ E PROPORZIONALITÀ

2.1. Base giuridica

La base giuridica è l'articolo 114 del trattato sul funzionamento dell'Unione europea, che prevede l'adozione di misure volte a garantire il funzionamento del mercato interno.

L'articolo 114 è la base giuridica adeguata per armonizzare le condizioni alle quali i prestatori di servizi di hosting forniscono servizi transfrontalieri nel mercato unico digitale e per affrontare le divergenze tra le disposizioni degli Stati membri che potrebbero altrimenti ostacolare il funzionamento del mercato interno. Questa disposizione permette inoltre di evitare che emergano ostacoli futuri all'attività economica che potrebbero derivare da differenze nell'evoluzione delle legislazioni nazionali.

L'articolo 114 del TFUE può anche essere utilizzato per imporre obblighi ai prestatori di servizi stabiliti al di fuori del territorio dell'UE quando la loro offerta di servizi riguarda il mercato interno, nella misura in cui ciò è necessario per conseguire l'obiettivo perseguito sul mercato interno.

2.2. Scelta dell'atto giuridico

L'articolo 114 del TFUE offre al legislatore dell'Unione la possibilità di adottare regolamenti e direttive.

Poiché la proposta riguarda gli obblighi per i prestatori di servizi che solitamente prestano i loro servizi in più di uno Stato membro, le divergenze nell'applicazione di tali norme ostacolerebbero la prestazione di servizi da parte di prestatori che operano in più Stati membri. Un regolamento permette di applicare lo stesso obbligo in modo uniforme in tutta l'Unione, è direttamente applicabile, offre chiarezza e una maggiore certezza giuridica e consente di evitare divergenze nel recepimento da parte degli Stati membri. Per questi motivi, si ritiene che il regolamento sia la forma più appropriata per questo strumento.

2.3. Sussidiarietà

Tenuto conto della dimensione transfrontaliera dei problemi da affrontare, le misure contenute nella proposta devono essere adottate a livello di Unione per conseguire gli obiettivi. Poiché Internet è per sua natura transfrontaliera, i contenuti ospitati in uno Stato membro possono di norma essere consultati da qualsiasi altro Stato membro.

Sta emergendo e rischia di diffondersi sempre più un quadro frammentario di norme nazionali per la lotta ai contenuti terroristici online, il quale potrebbe costituire un onere per le imprese, costrette a conformarsi a regolamentazioni divergenti, comportando una disparità di condizioni e lacune sul piano della sicurezza.

Pertanto, l'azione dell'UE promuove la certezza del diritto e aumenta l'efficacia delle azioni adottate dai prestatori di servizi di hosting contro i contenuti terroristici online. Un numero

maggiore di imprese, comprese quelle stabilite al di fuori dell'UE, sarebbe quindi in grado di adottare provvedimenti e l'integrità del mercato unico digitale ne sarebbe rafforzata.

Pertanto l'azione dell'UE è necessaria, come ribadito dalle conclusioni del Consiglio europeo del giugno 2018 che invitano la Commissione a presentare una proposta legislativa in questo ambito.

2.4. Proporzionalità

La proposta stabilisce le norme in base alle quali i prestatori di servizi di hosting applicano misure volte a rimuovere rapidamente i contenuti terroristici dai loro servizi. Le caratteristiche principali della proposta fanno sì che essa si limiti solo a quanto necessario per conseguire gli obiettivi strategici.

La proposta tiene conto dell'onere che ricade sui prestatori di servizi di hosting e prevede delle misure di salvaguardia, compresa la tutela della libertà di espressione e di informazione e di altri diritti fondamentali. Il termine di un'ora per la rimozione si applica solo agli ordini di rimozione, ovvero decisioni soggette a riesame giurisdizionale con le quali le autorità competenti hanno stabilito l'illiceità dei contenuti esaminati. Quanto alle segnalazioni, è previsto l'obbligo di predisporre misure intese a facilitare la valutazione tempestiva dei contenuti terroristici, senza tuttavia imporre obblighi di rimozione, né una scadenza tassativa. La decisione definitiva resta una decisione volontaria del prestatore di servizi di hosting. L'onere che incombe alle imprese riguardo alla valutazione del contenuto è attenuato dal fatto che le autorità competenti degli Stati membri e gli organismi dell'Unione forniscono ulteriori chiarimenti sui motivi per i quali il contenuto può essere considerato terroristico. Se necessario, i prestatori di servizi di hosting adottano misure proattive per proteggere i loro servizi contro la diffusione di contenuti terroristici. Gli obblighi specifici relativi alle misure proattive sono limitati ai prestatori di servizi di hosting esposti a contenuti terroristici che hanno ricevuto un ordine di rimozione divenuto definitivo e dovrebbero essere proporzionati al livello di rischio e alle risorse dell'impresa. La conservazione del contenuto rimosso e dei relativi dati è limitata a un periodo di tempo proporzionato inteso a consentire un procedimento di riesame amministrativo o giurisdizionale e a fini di prevenzione, accertamento, indagine o perseguimento di reati di terrorismo.

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

3.1. Consultazioni dei portatori di interessi

Ai fini dell'elaborazione della presente proposta legislativa, la Commissione ha consultato tutti i portatori di interessi per conoscere le loro posizioni e trovare una possibile soluzione. La Commissione ha svolto una consultazione pubblica aperta sulle misure per migliorare l'efficacia della lotta ai contenuti illegali, ricevendo 8 961 risposte, di cui 8 749 da singoli cittadini, 172 da organizzazioni, 10 da pubbliche amministrazioni e 30 da altre categorie di partecipanti. È stata svolta, in parallelo, un'indagine Eurobarometro su un campione casuale di 33 500 residenti nell'UE sui contenuti illegali online. La Commissione ha anche consultato le autorità degli Stati membri e i prestatori di servizi di hosting a maggio e giugno 2018 per quanto riguarda le misure specifiche volte a contrastare i contenuti terroristici online.

In generale, la maggior parte dei portatori di interessi hanno affermato che i contenuti terroristici online costituiscono un grave problema per la società, che nuoce agli utilizzatori di

Internet e ai modelli commerciali dei prestatori di servizi di hosting. Più in generale, il 65 % dei partecipanti al sondaggio Eurobarometro[4] ritiene che Internet non sia sicura per i suoi utilizzatori e il 90 % ritiene importante limitare la diffusione di contenuti illeciti online. Dalle consultazioni con gli Stati membri è emerso che, anche se gli accordi volontari stanno dando risultati, molti sentono la necessità di introdurre obblighi vincolanti in materia di contenuti terroristici, una posizione che è stata ribadita nelle conclusioni del Consiglio europeo del giugno 2018. Mentre, nel complesso, si sono espressi a favore del mantenimento di misure volontarie, i prestatori di servizi di hosting hanno anche messo in evidenza i potenziali effetti negativi dell'emergente frammentazione del quadro giuridico nell'Unione.

Diversi portatori di interessi hanno altresì rilevato la necessità che le misure di regolamentazione per la rimozione dei contenuti, tra cui le misure proattive e le scadenze rigorose, siano accompagnate da salvaguardie per la tutela dei diritti fondamentali, in particolare la libertà di espressione. I portatori di interessi hanno evidenziato una serie di misure necessarie in materia di trasparenza e responsabilità, oltre all'esigenza di sottoporre l'uso degli strumenti automatici a una sorveglianza umana.

3.2. Valutazione d'impatto

Il comitato per il controllo normativo ha espresso un parere positivo, corredato di riserve, sulla valutazione d'impatto e ha formulato varie proposte di miglioramento[5]. A seguito di tale parere, la relazione sulla valutazione d'impatto è stata modificata per tener conto delle principali osservazioni del comitato, ponendo l'accento specificamente sui contenuti terroristici, sottolineando le implicazioni sul funzionamento del mercato unico digitale e fornendo un'analisi più approfondita dell'impatto sui diritti fondamentali e sul funzionamento delle misure di salvaguardia proposte nelle opzioni.

Se non sono state adottate misure supplementari, verranno portate avanti le azioni volontarie previste nello scenario di base, con effetti sulla riduzione dei contenuti terroristici online. Tuttavia, è improbabile che tutti i prestatori di servizi di hosting esposti a tali contenuti adottino misure volontarie e potrebbe conseguirne un'ulteriore frammentazione giuridica, che frapporrebbe ulteriori barriere alla fornitura di servizi transfrontalieri. Oltre allo scenario di base sono state esaminate tre opzioni strategiche principali con crescenti livelli di efficacia nel soddisfare gli obiettivi fissati nella valutazione d'impatto e l'obiettivo politico generale di ridurre i contenuti terroristici online.

Per tutte e tre le opzioni, l'ambito di applicazione di tali obblighi comprende tutti i prestatori di servizi di hosting (ambito di applicazione personale) stabiliti nell'UE e nei paesi terzi - nella misura in cui offrono i loro servizi nell'Unione (ambito geografico). Data la natura del problema e la necessità di evitare l'uso improprio di piattaforme di minori dimensioni, nessuna delle opzioni prevede esenzioni per le PMI. Tutte le opzioni impongono ai prestatori di servizi di hosting di designare un rappresentante legale nell'UE - compreso per le imprese stabilite al di fuori dell'UE - al fine di garantire l'applicabilità delle norme dell'UE. In tutte le opzioni gli Stati membri sono tenuti a sviluppare meccanismi sanzionatori.

Tutte le opzioni prevedono la creazione di un nuovo sistema armonizzato di ordini giuridici di rimozione per i contenuti terroristici online, che sono emessi dalle autorità nazionali nei confronti dei prestatori di servizi di hosting, e l'obbligo di rimuovere tale contenuto entro

[4] Eurobarometro 469, Contenuti illegali online, giugno 2018.

[5] Link al parere del comitato per il controllo normativo su RegDoc.

un'ora. Tali ordini non implicano necessariamente una valutazione da parte dei prestatori di servizi di hosting e prevedono la possibilità di ricorrere per via giudiziaria.

Tra le caratteristiche comuni alle tre opzioni vi sono le misure di salvaguardia, in particolare i procedimenti di reclamo e i mezzi di ricorso effettivi, compreso il ricorso giudiziario, e altre disposizioni intese ad evitare la rimozione erronea dei contenuti che non hanno natura terroristica, garantendo al contempo il rispetto dei diritti fondamentali. Inoltre, tutte le opzioni prevedono obblighi di comunicazione sotto forma di relazioni sulla trasparenza e comunicazioni agli Stati membri e alla Commissione, nonché alle autorità competenti per l'accertamento delle ipotesi di reato. Sono previsti inoltre obblighi di cooperazione tra le autorità nazionali, i prestatori di servizi di hosting, e, se del caso, Europol.

Le principali differenze tra le tre opzioni riguardano l'ambito di applicazione della definizione dei contenuti terroristici, il livello di armonizzazione delle segnalazioni, la portata delle misure proattive, gli obblighi di coordinamento per gli Stati membri e i requisiti di conservazione dei dati. L'opzione 1 limiterebbe l'ambito di applicazione materiale ai contenuti diffusi al fine di istigare direttamente a commettere un atto terroristico, secondo una definizione ristretta, mentre le opzioni 2 e 3 adottano un approccio più globale, che comprende anche il materiale relativo al reclutamento e all'addestramento. In materia di misure proattive, nell'ambito dell'opzione 1, i prestatori di servizi di hosting esposti a contenuti terroristici dovrebbero effettuare una valutazione dei rischi ma le misure proattive destinate a farvi fronte rimarrebbero di carattere volontario. L'opzione 2 prevede che i prestatori di servizi di hosting predispongano un piano d'azione che può comprendere l'uso di strumenti automatizzati per evitare che contenuti già rimossi siano nuovamente caricati. L'opzione 3 prevede misure proattive più complete che prevedono anche l'obbligo per i prestatori di servizi esposti a contenuti terroristici di individuare nuovi materiali. In tutte le opzioni, le condizioni relative alle misure proattive dovrebbero essere proporzionate al livello di esposizione al materiale terroristico nonché alla capacità economica del prestatore di servizi. Per quanto riguarda le segnalazioni, l'opzione 1 non prevede un approccio armonizzato, mentre l'opzione 2 lo farebbe per Europol e l'opzione 3 includerebbe anche le segnalazioni degli Stati membri. Secondo le opzioni 2 e 3, gli Stati membri sarebbero tenuti a comunicare, cooperare e a coordinarsi tra loro, mentre secondo l'opzione 3 dovrebbero altresì assicurare che le loro autorità competenti siano in grado di individuare e segnalare i contenuti terroristici. Infine, l'opzione 3 prevede anche un obbligo di conservare i dati come misura di salvaguardia in caso di rimozione erronea e al fine di agevolare le indagini penali.

In aggiunta alle disposizioni giuridiche, si prevede che tutte le opzioni legislative siano accompagnate da una serie di misure di sostegno (in particolare per favorire la cooperazione tra le autorità nazionali e Europol) e prevedano la collaborazione con i prestatori di servizi di hosting e il sostegno della ricerca, sviluppo e innovazione per lo sviluppo e l'adozione di soluzioni tecnologiche. A seguito dell'adozione dello strumento giuridico, si potrebbero prevedere ulteriori strumenti di sensibilizzazione e di sostegno per le PMI.

La valutazione d'impatto ha concluso che è necessaria una serie di misure per raggiungere l'obiettivo politico. La definizione più ampia di contenuti terroristici che includa i materiali più nocivi sarebbe preferibile rispetto a una definizione ristretta (opzione 1). L'introduzione di obblighi proattivi limitati al ricaricamento dei contenuti terroristici (opzione 2) avrebbe effetti meno incisivi rispetto agli obblighi relativi all'individuazione di nuovi contenuti terroristici (opzione 3). Le disposizioni in materia di segnalazioni dovrebbero includere le segnalazioni sia di Europol che degli Stati membri (opzione 3) e non limitarsi alla sola Europol (opzione 2), in quanto le segnalazioni degli Stati membri sono un contributo importante all'impegno globale volto a ridurre l'accessibilità dei contenuti terroristici online. Tali misure dovrebbero

essere attuate in aggiunta alle misure comuni a tutte le opzioni, ivi comprese solide misure di salvaguardia contro la rimozione erronea di contenuti.

3.3. Diritti fondamentali

La propaganda dei terroristi online mira a istigare altre persone a commettere attentati terroristici, tra l'altro dando loro istruzioni dettagliate sulle modalità con le quali provocare il massimo danno. Inoltre, dopo che sono state commesse tali atrocità vengono solitamente rilasciate dichiarazioni propagandistiche in cui i terroristi si gloriano di tali atti terroristici, istigando altri a seguire il loro esempio. Il presente regolamento contribuisce alla tutela della sicurezza pubblica, riducendo l'accessibilità dei contenuti terroristici che promuovono e incoraggiano la violazione dei diritti fondamentali.

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

(a) i diritti del fornitore di contenuti; il diritto alla libertà di espressione; il diritto alla protezione dei dati personali; il diritto al rispetto della vita privata e familiare, il principio di non discriminazione e il diritto a un ricorso effettivo;

(b) i diritti del prestatore di servizi: il diritto alla libertà d'impresa; il diritto a un ricorso effettivo;

(c) i diritti di tutti i cittadini: e il diritto alla libertà di espressione e di informazione.

Tenuto conto dell'acquis in materia, la proposta di regolamento include opportune e solide misure di salvaguardia per garantire che i diritti di tali soggetti siano tutelati.

Un primo elemento in questo contesto è che il regolamento stabilisce una definizione di contenuti terroristici online in conformità della definizione di reati di terrorismo di cui alla direttiva (UE) 2017/541. Questa definizione si applica agli ordini di rimozione e alle segnalazioni, nonché alle misure proattive. La definizione garantisce che siano rimossi solo i contenuti illegali che corrispondono a una definizione di reati connessi valida a livello dell'Unione. Inoltre, il regolamento prevede l'obbligo generale per i prestatori di servizi di hosting di agire in modo diligente, proporzionato e non discriminatorio riguardo ai contenuti che memorizzano, in particolare nell'attuazione delle loro condizioni contrattuali, al fine di evitare la rimozione di contenuti non terroristici.

Più specificamente, il regolamento è stato concepito in modo da garantire la proporzionalità delle misure adottate rispetto alla tutela dei diritti fondamentali. Per quanto riguarda gli ordini di rimozione, la valutazione del contenuto (comprese le verifiche legali, ove necessario) da parte di un'autorità competente giustifica la rimozione entro il termine di un'ora per questa misura. Inoltre, le disposizioni del presente regolamento relative alle segnalazioni sono circoscritte alle segnalazioni effettuate dalle autorità competenti e dagli organismi dell'Unione che spiegano i motivi per cui il contenuto può essere considerato terroristico. Anche se la responsabilità per la rimozione dei contenuti identificati in una segnalazione ricade sul prestatore di servizi di hosting, tale decisione è agevolata dalla valutazione sopra descritta.

Per quanto riguarda le misure proattive, la responsabilità di individuare, valutare e rimuovere i contenuti ricade sui prestatori di servizi di hosting, i quali sono tenuti a predisporre misure di salvaguardia per garantire che il contenuto non sia rimosso erroneamente, anche attraverso una sorveglianza umana, soprattutto qualora si renda necessaria un'ulteriore valutazione del contesto. Inoltre, a differenza dello scenario di base in cui le imprese più colpite

predispongono strumenti automatizzati senza controllo pubblico, la concezione delle misure e la loro attuazione dovrebbero essere comunicate agli organismi competenti negli Stati membri. Questo obbligo riduce il rischio di rimozione erronea sia per le imprese che introducono nuovi strumenti, sia per quelle che li utilizzano già. Inoltre, i prestatori di servizi di hosting sono tenuti a prevedere meccanismi di reclamo di facile uso per i prestatori di contenuti (per impugnare la decisione di rimuovere i loro contenuti) nonché a pubblicare relazioni sulla trasparenza per il pubblico.

Infine, qualora i contenuti e i relativi dati fossero rimossi erroneamente malgrado le salvaguardie in atto, i prestatori di servizi di hosting sono tenuti a conservarli per un periodo di sei mesi al fine di ripristinarli, garantendo l'efficacia dei procedimenti di reclamo e di ricorso al fine di proteggere la libertà di espressione e di informazione. Al tempo stesso, la conservazione contribuisce anche agli obiettivi delle autorità di contrasto. I prestatori di servizi di hosting devono inoltre attuare misure di salvaguardia tecniche e organizzative per assicurare che i dati non siano utilizzati per altri scopi.

Le misure proposte, in particolare quelle relative agli ordini di rimozione, alle segnalazioni, alle misure proattive e alla conservazione dei dati non dovrebbero solo proteggere gli utilizzatori di Internet dai contenuti terroristici ma anche contribuire a tutelare il diritto dei cittadini alla vita, riducendo l'accessibilità dei contenuti terroristici online.

4. INCIDENZA SUL BILANCIO

Nessuna.

5. ALTRI ELEMENTI

5.1. Piani attuativi e modalità di monitoraggio, valutazione e informazione

La Commissione elabora entro [un anno dalla data di applicazione del presente regolamento] un programma dettagliato per monitorare gli esiti, i risultati e gli effetti del regolamento. Il programma di monitoraggio definisce gli indicatori e i mezzi da utilizzare per raccogliere i dati e gli altri elementi di prova necessari, nonché la periodicità di tali acquisizioni. Esso specifica le misure che la Commissione e gli Stati membri devono adottare per la raccolta e l'analisi dei dati e di altri elementi di prova per monitorare i progressi e valutare il presente regolamento.

Sulla base del programma di monitoraggio stabilito, entro due anni dall'entrata in vigore del presente regolamento, la Commissione presenta una relazione sulla sua attuazione, sulla base delle relazioni sulla trasparenza pubblicate dalle imprese e delle informazioni fornite dagli Stati membri. La Commissione effettuerà una valutazione non prima di quattro anni dall'entrata in vigore del regolamento.

Sulla base delle conclusioni della valutazione, in particolare se permangono eventuali lacune o vulnerabilità, e tenendo conto degli sviluppi tecnologici, la Commissione valuterà la necessità di estendere l'ambito di applicazione del regolamento. Se necessario, la Commissione presenterà proposte di modifica del regolamento.

La Commissione intende sostenere l'attuazione, il monitoraggio e la valutazione del regolamento attraverso un suo gruppo di esperti. Il gruppo avrà anche il compito di facilitare

la cooperazione tra i prestatori di servizi di hosting, le autorità di contrasto e Europol; di facilitare gli scambi e le pratiche per individuare e rimuovere i contenuti terroristici, fornire la sua consulenza sull'evoluzione del modus operandi dei terroristi online; nonché, se del caso, fornire consulenza e orientamenti per l'attuazione delle disposizioni.

L'attuazione del regolamento proposto potrebbe essere agevolata attraverso una serie di misure di sostegno, tra cui l'eventuale sviluppo di una piattaforma in seno a Europol per assistere nel coordinamento delle segnalazioni e degli ordini di rimozione. La ricerca finanziata dall'UE sull'evoluzione del modus operandi dei terroristi ha accresciuto la comprensione e la sensibilizzazione di tutti i portatori di interessi. Inoltre, Orizzonte 2020 sostiene la ricerca al fine di sviluppare nuove tecnologie, tra cui la prevenzione automatica del caricamento di contenuti terroristici. La Commissione continuerà inoltre a esaminare il modo in cui i prestatori di servizi di hosting e le autorità competenti attuano il presente regolamento attraverso gli strumenti finanziari dell'UE.

5.2. Illustrazione dettagliata delle singole disposizioni della proposta

L'articolo 1 definisce l'oggetto, precisando che il regolamento stabilisce regole uniformi per impedire l'uso improprio dei servizi di hosting ai fini della diffusione di contenuti terroristici online, tra cui obblighi di diligenza per i prestatori di servizi di hosting e misure che gli Stati membri sono tenuti ad attuare. Esso stabilisce inoltre l'ambito di applicazione geografico, che comprende i prestatori di servizi di hosting che offrono servizi nell'Unione, indipendentemente dal luogo del loro stabilimento.

L'articolo 2 contiene le definizioni dei termini utilizzati nella proposta. Esso stabilisce inoltre una definizione di contenuto terroristico a fini di prevenzione che trae spunto dalla direttiva sulla lotta al terrorismo e ricomprende il materiale e i messaggi che istigano, anche mediante l'apologia del terrorismo, alla commissione di reati di terrorismo, incitano a contribuire a reati di terrorismo, impartiscono istruzioni finalizzate alla commissione di tali reati o incoraggiano la partecipazione alle attività di un gruppo terroristico.

L'articolo 3 prevede gli obblighi di diligenza ai quali i prestatori di servizi di hosting devono attenersi quando agiscono in conformità del presente regolamento e, in particolare, nel rispetto dei diritti fondamentali interessati. L'articolo prevede opportune disposizioni che i prestatori di servizi di hosting devono includere nelle loro condizioni contrattuali e far sì che siano applicate.

L'articolo 4 impone agli Stati membri di dare facoltà alle autorità competenti di emettere ordini di rimozione e prevede l'obbligo per i prestatori di servizi di hosting di rimuovere i contenuti entro un'ora dal ricevimento dell'ordine di rimozione. Esso definisce inoltre gli elementi minimi che gli ordini di rimozione dovrebbero contenere e le procedure alle quali i prestatori di servizi di hosting informano l'autorità che emette gli ordini e le comunicano se non sono in grado di conformarsi all'ordine o se occorrono ulteriori chiarimenti. L'articolo fa obbligo all'autorità che emette gli ordini di informare l'autorità che vigila sull'attuazione delle misure proattive dello Stato di competenza del prestatore di servizi di hosting.

L'articolo 5 stabilisce l'obbligo per i prestatori di servizi di hosting di predisporre rapidamente misure per valutare i contenuti segnalati attraverso una segnalazione di un'autorità competente di uno Stato membro o un organismo dell'Unione, ma non impone l'obbligo di rimuovere il contenuto segnalato né fissa termini specifici per l'intervento. Esso definisce inoltre gli elementi minimi che le segnalazioni devono contenere e le procedure in base alle quali i

prestatori di servizi di hosting informano l'autorità che emette gli ordini e chiedono chiarimenti all'autorità che ha segnalato il contenuto.

L'articolo 6 dispone che i prestatori di servizi di hosting adottino, se del caso, misure proattive efficaci e proporzionate. Esso prevede una procedura volta a garantire che alcuni prestatori di servizi di hosting (ossia quelli che hanno ricevuto un ordine di rimozione divenuto definitivo) adottino misure proattive supplementari, se del caso, al fine di attenuare i rischi e in funzione dell'esposizione dei loro servizi a contenuti terroristici. Il prestatore di servizi di hosting dovrebbe cooperare con l'autorità competente per quanto riguarda la misure necessarie, e, qualora non sia possibile raggiungere un accordo, l'autorità può imporre misure al prestatore di servizi. L'articolo stabilisce inoltre un procedimento di riesame della decisione dell'autorità.

L'articolo 7 dispone che i prestatori di servizi di hosting conservino i contenuti rimossi e i relativi dati per sei mesi ai fini dei procedimenti di riesame e di indagine. Tale periodo può essere prorogato per consentire il completamento del riesame. L'articolo impone inoltre ai prestatori di servizi di mettere in atto salvaguardie per assicurare che il contenuto e i relativi dati non siano consultati o trattati per altre finalità.

L'articolo 8 stabilisce l'obbligo per i prestatori di servizi di hosting di spiegare le politiche da essi attuate contro i contenuti terroristici e di pubblicare relazioni annuali sulla trasparenza in merito alle azioni intraprese a tale riguardo.

L'articolo 9 prevede salvaguardie specifiche per quanto riguarda l'uso e l'attuazione di misure proattive nel caso siano utilizzati strumenti automatizzati per garantire l'accuratezza e la fondatezza delle decisioni.

L'articolo 10 dispone che i prestatori di servizi di hosting attuino meccanismi di reclamo per le rimozioni, le segnalazioni e le misure proattive ed esaminino tempestivamente ogni reclamo.

L'articolo 11 stabilisce l'obbligo per i prestatori di servizi di hosting di mettere a disposizione del fornitore di contenuti informazioni concernenti la rimozione, a meno che l'autorità competente non richieda la riservatezza per ragioni di pubblica sicurezza.

L'articolo 12 impone agli Stati membri di garantire che le autorità competenti dispongano di capacità e risorse sufficienti per adempiere agli obblighi loro incombenti a norma del presente regolamento.

L'articolo 13 fa obbligo agli Stati membri di cooperare tra loro e, se del caso, con Europol, al fine di evitare duplicazioni e interferenze con le indagini. L'articolo prevede anche la possibilità per gli Stati membri e i prestatori di servizi di hosting di avvalersi di appositi strumenti, compresi quelli di Europol, per il trattamento degli ordini di rimozione e delle segnalazioni e il relativo feedback, e di collaborare per quanto riguarda le misure proattive. L'articolo fa obbligo agli Stati membri di predisporre adeguati canali di comunicazione per garantire il tempestivo scambio di informazioni nell'attuazione e applicazione delle disposizioni del presente regolamento. L'articolo obbliga inoltre i prestatori di servizi di hosting a informare le autorità competenti qualora vengano a conoscenza di eventuali prove di reati di terrorismo ai sensi dell'articolo 3 della direttiva (UE) 2017/541 sulla lotta contro il terrorismo.

L'articolo 14 prevede l'istituzione di punti di contatto sia da parte dei prestatori di servizi di hosting che degli Stati membri al fine di agevolare la comunicazione tra di loro, in particolare per quanto riguarda le segnalazioni e gli ordini di rimozione.

L'articolo 15 stabilisce la giurisdizione dello Stato membro ai fini del controllo delle misure proattive, dell'imposizione di sanzioni e delle azioni di monitoraggio.

L'articolo 16 prevede l'obbligo per i prestatori di servizi di hosting che non sono stabiliti in uno Stato membro ma prestano servizi all'interno dell'Unione di designare un rappresentante legale nell'Unione.

L'articolo 17 impone agli Stati membri di designare autorità incaricate dell'emissione di ordini di rimozione, della segnalazione di contenuti terroristici, del controllo dell'attuazione delle misure proattive e dell'applicazione del regolamento.

L'articolo 18 dispone che gli Stati membri stabiliscano norme relative alle sanzioni applicabili in caso di violazione del regolamento e definisce i criteri che gli Stati membri devono prendere in considerazione nel determinare il tipo e il livello di sanzioni. Data la particolare importanza della tempestiva rimozione di contenuti terroristici individuati in un ordine di rimozione, bisognerebbe attuare norme specifiche in materia di sanzioni pecuniarie in caso di sistematica inosservanza di tale obbligo.

L'articolo 19 prevede una procedura più rapida e più flessibile per modificare, tramite atti delegati, i modelli previsti per gli ordini di rimozione, nonché canali di trasmissione autenticati.

L'articolo 20 fissa le condizioni alle quali la Commissione può adottare atti delegati per introdurre le modifiche necessarie ai modelli e ai requisiti tecnici per gli ordini di rimozione.

L'articolo 21 fa obbligo agli Stati membri di raccogliere e trasmettere informazioni specifiche concernenti l'applicazione del regolamento al fine di assistere la Commissione nell'esercizio dei suoi obblighi di cui all'articolo 23. La Commissione stabilisce un programma dettagliato per monitorare gli esiti, i risultati e gli effetti del regolamento.

L'articolo 22 stabilisce che la Commissione presenta una relazione sull'applicazione del presente regolamento due anni dopo la sua entrata in vigore.

L'articolo 23 stabilisce che la Commissione presenta una relazione sulla valutazione del presente regolamento non prima di tre anni dalla sua entrata in vigore.

L'articolo 24 stabilisce che il regolamento proposto entra in vigore il ventesimo giorno successivo alla sua pubblicazione nella Gazzetta ufficiale e si applica sei mesi dopo l'entrata in vigore. Tale termine è dettato dalla necessità di attuare misure di esecuzione, ma viene anche riconosciuta l'urgenza di applicare pienamente le norme del regolamento proposto. Il termine di sei mesi è stato stabilito con il presupposto che i negoziati saranno condotti rapidamente.

2018/0331 (COD)

Proposta di

REGOLAMENTO DEL PARLAMENTO EUROPEO E DEL CONSIGLIO

relativo alla prevenzione della diffusione di contenuti terroristici online

Contributo della Commissione europea alla riunione dei leader, riunitisi a Salisburgo il 19-20 settembre 2018

IL PARLAMENTO EUROPEO E IL CONSIGLIO DELL'UNIONE EUROPEA,

visto il trattato sul funzionamento dell'Unione europea, in particolare l'articolo 114,

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[6],

deliberando secondo la procedura legislativa ordinaria,

considerando quanto segue:

(1) Il presente regolamento mira a garantire il buon funzionamento del mercato unico digitale in una società aperta e democratica prevenendo l'uso improprio dei servizi di hosting a fini terroristici. Occorre migliorare il funzionamento del mercato unico digitale rafforzando la certezza del diritto per i prestatori di servizi di hosting, il che aumenterà la fiducia degli utilizzatori nell'ambiente online, e potenziando le salvaguardie per la libertà di espressione e di informazione.

(2) I prestatori di servizi di hosting che operano in Internet svolgono un ruolo essenziale nell'economia digitale mettendo in relazione le imprese e i cittadini e facilitando il dibattito pubblico così come la diffusione e la ricezione di informazioni, opinioni e idee, e contribuiscono in modo significativo alla crescita economica, all'innovazione e alla creazione di posti di lavoro nell'Unione. In alcuni casi, tuttavia, i loro servizi sono utilizzati impropriamente da terzi per perpetrare attività illegali online. Particolarmente preoccupante è l'uso improprio dei servizi di hosting da parte di gruppi terroristici e dei loro sostenitori per pubblicare contenuti terroristici online allo scopo di propagare il loro messaggio, radicalizzare e attirare nuove reclute, nonché facilitare e dirigere attività terroristiche.

[6] GU C [...] del [...], pag. [...].

(3) La presenza di contenuti terroristici online ha gravi conseguenze negative per gli utilizzatori, i cittadini e la società in generale così come per i prestatori di servizi online che ospitano tali contenuti, poiché mina la fiducia dei loro utilizzatori e nuoce ai loro modelli commerciali. In considerazione dell'importanza del ruolo che svolgono nonché delle capacità e dei mezzi tecnologici associati ai servizi che forniscono, i prestatori di servizi online hanno particolari responsabilità nei confronti della società sotto il profilo della protezione dei loro servizi dall'uso improprio che potrebbero farne i terroristi e del contributo che possono apportare al contrasto della diffusione di contenuti terroristici attraverso i loro servizi.

(4) Gli sforzi volti a contrastare i contenuti terroristici online sono stati avviati a livello dell'Unione nel 2015 nel quadro della cooperazione volontaria tra gli Stati membri e i prestatori di servizi di hosting; essi dovrebbero essere integrati da un quadro legislativo chiaro al fine di ridurre l'accessibilità dei contenuti terroristici online e affrontare in modo adeguato un fenomeno in rapida evoluzione. Tale quadro legislativo poggerebbe su iniziative volontarie, che sono state rafforzate dalla raccomandazione (UE) 2018/334[7], e risponde alla richiesta del Parlamento europeo di rafforzare le misure volte ad affrontare i contenuti illegali e nocivi e a quella del Consiglio europeo di migliorare l'individuazione automatizzata e la rimozione dei contenuti che incitano a compiere atti terroristici.

(5) L'applicazione del presente regolamento non dovrebbe pregiudicare l'applicazione dell'articolo 14 della direttiva 2000/31/CE[8]. In particolare, tutte le misure adottate dal prestatore di servizi di hosting conformemente al presente regolamento, comprese le eventuali misure proattive, non dovrebbero comportare automaticamente la perdita, per il prestatore di servizi, del beneficio dell'esenzione di responsabilità prevista in tale disposizione. Il presente regolamento lascia impregiudicata la competenza delle autorità e degli organi giurisdizionali nazionali a stabilire la responsabilità dei prestatori di servizi di hosting in determinati casi se non sono soddisfatte le condizioni di cui all'articolo 14 della direttiva 2000/31/CE per beneficiare dell'esenzione di responsabilità.

(6) Il presente regolamento definisce, nel pieno rispetto dei diritti fondamentali tutelati nell'ordinamento giuridico dell'Unione e, in particolare, quelli garantiti dalla Carta dei diritti fondamentali dell'Unione europea, norme intese a prevenire l'uso improprio dei servizi di hosting per la diffusione di contenuti terroristici online, al fine di garantire il buon funzionamento del mercato interno.

(7) Il presente regolamento contribuisce alla protezione della pubblica sicurezza, attuando nel contempo adeguate e solide salvaguardie per garantire la tutela dei diritti fondamentali in gioco. Ciò include i diritti al rispetto della vita privata e alla protezione dei dati personali, il diritto ad una tutela giurisdizionale effettiva, il diritto alla libertà di espressione, compresa la libertà di ricevere e trasmettere informazioni, la libertà d'impresa e il principio di non discriminazione. Le autorità competenti e i prestatori di servizi di hosting dovrebbero adottare solo le misure che sono necessarie,

---

7 Raccomandazione (UE) 2018/334 della Commissione, dell'1 marzo 2018, sulle misure per contrastare efficacemente i contenuti illegali online (GU L 63 del 6.2.2018, pag. 50).

8 Direttiva 2000/31/CE del Parlamento europeo e del Consiglio, dell'8 giugno 2000, relativa a taluni aspetti giuridici dei servizi della società dell'informazione, in particolare il commercio elettronico, nel mercato interno (direttiva sul commercio elettronico) (GU L 178 del 17.7.2000, pag. 1).

adeguate e proporzionate in una società democratica, tenendo conto della particolare importanza rivestita dalla libertà di espressione e di informazione, che costituisce uno dei fondamenti essenziali di una società democratica e pluralista e uno dei valori su cui si fonda l'Unione. Le misure che costituiscano un'ingerenza nella libertà di espressione e d'informazione dovrebbero essere rigorosamente mirate, nel senso che devono servire a prevenire la diffusione di contenuti terroristici, ma senza pregiudicare il diritto di ricevere e diffondere informazioni in modo lecito, tenuto conto del ruolo centrale dei prestatori di servizi di hosting nel facilitare il dibattito pubblico e la diffusione e la ricezione di informazioni, pareri e idee nel rispetto della legge.

(8) Il diritto a un ricorso effettivo è sancito dall'articolo 19 del TUE e dall'articolo 47 della Carta dei diritti fondamentali dell'Unione europea. Ogni persona fisica o giuridica ha diritto a un ricorso giurisdizionale effettivo dinanzi alle competenti autorità giurisdizionali nazionali contro una qualsiasi delle misure adottate in base al presente regolamento che possa ledere i diritti di tale persona. Il diritto comprende in particolare la possibilità per i prestatori di servizi di hosting e i fornitori di contenuti di impugnare effettivamente un ordine di rimozione dinanzi all'autorità giurisdizionale dello Stato membro la cui autorità l'ha emanato.

(9) Onde chiarire le misure che i prestatori di servizi di hosting e le autorità competenti dovrebbero adottare per prevenire la diffusione di contenuti terroristici online, è opportuno che il presente regolamento stabilisca una definizione dei contenuti terroristici per fini di prevenzione sulla base della definizione dei reati di terrorismo ai sensi della direttiva (UE) 2017/541 del Parlamento europeo e del Consiglio[9]. Data la necessità di contrastare la propaganda terroristica online più perniciosa, la definizione dovrebbe ricomprendere il materiale e i messaggi che incitano, incoraggiano o appoggiano la commissione di reati di terrorismo e la partecipazione agli stessi, impartiscono istruzioni finalizzate alla commissione di tali reati o promuovono la partecipazione nelle attività di un gruppo terroristico. Tali materiali comprendono, in particolare, testi, immagini, registrazioni audio e video. Nel valutare se il contenuto pubblicato online costituisce contenuto terroristico ai sensi del presente regolamento, le autorità competenti, così come i prestatori di servizi di hosting, dovrebbero tenere conto di fattori quali la natura e la formulazione dei messaggi, il contesto in cui sono emessi e il loro potenziale di portare a conseguenze dannose, compromettendo la sicurezza e l'incolumità delle persone. Il fatto che il materiale sia prodotto o diffuso da un'organizzazione terroristica o da una persona che figura negli elenchi dell'Unione costituisce un elemento importante della valutazione. Occorre proteggere adeguatamente la diffusione di contenuti per scopi giornalistici, educativi o di ricerca. Inoltre, le opinioni radicali, polemiche o controverse espresse nell'ambito di dibattiti politici sensibili non dovrebbero essere considerate contenuti terroristici.

(10) Al fine di ricomprendere i servizi di hosting attraverso i quali sono diffusi i contenuti terroristici online, il presente regolamento si dovrebbe applicare ai servizi della società dell'informazione che memorizzano informazioni fornite da un destinatario del servizio su sua richiesta e che rendono disponibili a terzi tali informazioni memorizzate, indipendentemente dalla natura meramente tecnica, automatica o passiva

[9] 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).

di tale attività. Ad esempio, i prestatori di servizi della società dell'informazione includono le piattaforme dei social media, i servizi di streaming video, i servizi di condivisione di video, audio e immagini, servizi di condivisione di file e altri servizi *cloud*, nella misura in cui mettono queste informazioni a disposizione di terzi e di siti web in cui gli utilizzatori possono esprimere commenti o postare recensioni. Il regolamento dovrebbe inoltre applicarsi ai prestatori di servizi di hosting che offrono servizi nell'Unione, ma che sono stabiliti al di fuori di essa, dal momento che una quota significativa dei prestatori di servizi di hosting esposti a contenuti terroristici che possono essere diffusi tramite i loro servizi sono stabiliti in paesi terzi. Ciò dovrebbe garantire che tutte le imprese operanti nel mercato unico digitale si conformino agli stessi obblighi a prescindere dal paese di stabilimento. Per determinare se offre servizi nell'Unione, è necessario 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 del sito Internet di un prestatore di servizi 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.

(11) L'esistenza di un collegamento sostanziale con l'Unione dovrebbe essere presa in considerazione al fine di determinare l'ambito di applicazione del presente regolamento. Tale collegamento sostanziale con l'Unione dovrebbe considerarsi presente quando il prestatore di servizi è stabilito nell'Unione o, in caso contrario, sulla base dell'esistenza di un numero considerevole di utilizzatori in uno o più Stati membri o dell'orientamento delle sue 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 Stato membro potrebbe anche desumersi dalla disponibilità di un'applicazione nell'apposito negozio online ("app store") nazionale, dalla diffusione 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 di assistenza alla clientela nella lingua generalmente parlata in tale Stato membro. Un collegamento sostanziale dovrebbe essere presunto anche quando le attività di un prestatore di servizi sono dirette verso uno o più Stati membri come previsto all'articolo 17, paragrafo 1, lettera c), del regolamento (UE) n. 1215/2012 del Parlamento europeo e del Consiglio[10]. Al contrario, non si può considerare che la prestazione del servizio al solo scopo di conformarsi al divieto di discriminazione imposto dal regolamento (UE) 2018/302 del Parlamento europeo e del Consiglio[11] comprovi, di per sé, che le sue attività sono dirette o orientate verso un dato territorio all'interno dell'Unione.

---

10 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).

11 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).

(12) I prestatori di servizi di hosting dovrebbero rispettare determinati obblighi di diligenza al fine di prevenire la diffusione di contenuti terroristici tramite i loro servizi. Tali obblighi di diligenza non dovrebbero costituire un obbligo generale di sorveglianza. Gli obblighi di diligenza dovrebbero tra l'altro significare che, quando applicano il presente regolamento, i prestatori di servizi di hosting agiscono in maniera diligente, proporzionata e non discriminatoria nei confronti dei contenuti che memorizzano, in particolare quando applicano le proprie condizioni contrattuali, al fine di evitare la rimozione di contenuti che non hanno natura terroristica. La rimozione di contenuti o la disabilitazione dell'accesso agli stessi devono essere effettuate nel rispetto della libertà di espressione e di informazione.

(13) Occorre armonizzare la procedura e gli obblighi che discendono dagli ordini giuridici che ingiungono ai prestatori di servizi di hosting di rimuovere contenuti terroristici o di disabilitarne l'accesso, in esito a una valutazione delle autorità competenti. Gli Stati membri dovrebbero designare le autorità competenti, assegnando tale compito alle autorità amministrative, esecutive o giudiziarie di loro scelta. In considerazione della velocità alla quale i contenuti terroristici sono diffusi attraverso i servizi online, la presente disposizione impone ai prestatori di servizi di hosting l'obbligo di provvedere a che i contenuti terroristici oggetto di un ordine di rimozione siano rimossi o che l'accesso sia disattivato entro un'ora dal ricevimento del provvedimento. Spetta ai prestatori di servizi di hosting decidere se rimuovere il contenuto in questione o disabilitarne l'accesso per gli utilizzatori nell'Unione.

(14) L'autorità competente dovrebbe trasmettere l'ordine di rimozione direttamente al destinatario e al punto di contatto con ogni mezzo elettronico che consenta di conservare una traccia scritta in condizioni che permettano al prestatore di stabilirne l'autenticità, compresa l'esattezza della data e dell'ora di invio e ricevimento dell'ordine, quali posta elettronica protetta e piattaforme o altri canali protetti, compresi quelli messi a disposizione dal prestatore di servizi, in conformità delle norme in materia di protezione dei dati personali. Segnatamente, tale obbligo può essere assolto usando servizi elettronici di recapito certificato qualificati ai sensi del regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio[12].

(15) Le segnalazioni emesse dalle autorità competenti o da Europol costituiscono un modo efficace e rapido di sensibilizzare i prestatori di servizi di hosting alla presenza di contenuti specifici nei loro servizi. Questo meccanismo inteso ad allertare i prestatori di servizi di hosting nei confronti delle informazioni che possono essere considerate contenuti terroristici, che permette loro su base volontaria di esaminare la compatibilità delle proprie clausole contrattuali, dovrebbe rimanere disponibile in aggiunta agli ordini di rimozione. È importante che i prestatori di servizi di hosting valutino tali segnalazioni in via prioritaria e forniscano rapidamente un feedback in merito alle azioni intraprese. La decisione finale in merito all'opportunità di rimuovere il contenuto, in quanto non compatibile con le proprie condizioni contrattuali spetta al prestatore di servizi di hosting. Nell'attuazione del presente regolamento con

[12] 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 (GU L 257 del 28.8.2014, pag. 73).

riferimento alle segnalazioni, il mandato di Europol, definito nel regolamento (UE) 2016/794[13], resta invariato.

(16) In considerazione della portata e della rapidità necessarie per individuare e rimuovere efficacemente i contenuti terroristici, l'adozione proattiva di misure proporzionate, compreso il ricorso in alcuni casi a strumenti automatizzati, costituisce un elemento essenziale di lotta ai contenuti terroristici online. Al fine di ridurre l'accessibilità ai contenuti terroristici nei loro servizi, i prestatori di servizi di hosting dovrebbero valutare se sia opportuno adottare misure proattive in funzione dei rischi e dell'esposizione a contenuti terroristici nonché delle conseguenze sui diritti dei terzi alle informazioni e dell'interesse pubblico. Di conseguenza, i prestatori di servizi di hosting dovrebbero determinare le misure proattive appropriate, efficaci e proporzionate da attuare. Tale obbligo non dovrebbe implicare un obbligo generale di sorveglianza. Nel contesto di tale valutazione, l'assenza di ordini di rimozione e di segnalazioni inviate a un prestatore di servizi di hosting è un'indicazione di un basso livello di esposizione a contenuti terroristici.

(17) Quando attuano misure proattive, i prestatori di servizi di hosting dovrebbero assicurare che sia preservato il diritto degli utilizzatori alla libertà di espressione e di informazione, compresa la libertà di ricevere e diffondere informazioni. Oltre ai requisiti stabiliti nella legislazione, anche in materia di protezione dei dati personali, i prestatori di servizi di hosting dovrebbero agire con la debita diligenza e attuare misure di salvaguardia, comprese in particolare la sorveglianza e le verifiche umane, se del caso, al fine di evitare decisioni indesiderate ed erronee di rimozione di contenuti che non hanno natura terroristica. Ciò vale in particolare quando i prestatori di servizi di hosting utilizzano strumenti automatizzati per individuare i contenuti terroristici. Qualsiasi decisione di ricorrere a strumenti automatizzati, adottata dal prestatore di servizi di hosting stesso o su richiesta dell'autorità competente, dovrebbe essere valutata sotto il profilo dell'affidabilità della tecnologia utilizzata e delle conseguenze per i diritti fondamentali.

(18) Al fine di garantire che i prestatori di servizi di hosting esposti a contenuti terroristici adottino misure adeguate per prevenire l'uso improprio dei loro servizi, le autorità competenti dovrebbero imporre ai prestatori di servizi di hosting che hanno ricevuto un ordine di rimozione, divenuto definitivo, di riferire in merito alle misure proattive adottate. Si potrebbe trattare di misure volte a prevenire che il contenuto terroristico rimosso o il cui accesso è stato disabilitato sia nuovamente caricato online a seguito di un ordine di rimozione o di una segnalazione ricevuta, utilizzando strumenti pubblici o privati che permettano di confrontarlo con contenuti terroristici noti. Tali misure possono inoltre fare uso di strumenti tecnici affidabili per individuare nuovi contenuti terroristici, avvalendosi di quelli disponibili sul mercato o quelli sviluppati dal prestatore di servizi di hosting. Il prestatore di servizi dovrebbe riferire in merito alle specifiche misure proattive attuate al fine di consentire all'autorità competente di valutare se siano efficaci e proporzionate e se, qualora siano utilizzati strumenti automatizzati, il prestatore di servizi di hosting dispone delle necessarie competenze in materia di sorveglianza e verifiche umane. Nel valutare l'efficacia e la proporzionalità

[13] 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 (GU L 135 del 24.5.2016, pag. 53).

delle misure, le autorità competenti dovrebbero tenere conto dei parametri pertinenti, compresi il numero di ordini di rimozione e segnalazioni trasmessi al prestatore, la sua capacità economica e l'impatto dei suoi servizi sulla diffusione di contenuti terroristici (ad esempio, in considerazione del numero di utilizzatori nell'Unione).

(19) A seguito della richiesta, l'autorità competente dovrebbe avviare un dialogo con il prestatore di servizi di hosting sulle misure proattive necessarie da attuare. Se necessario, l'autorità competente dovrebbe esigere l'adozione di misure proattive appropriate, efficaci e proporzionate qualora ritenga che le misure adottate siano insufficienti per far fronte ai rischi. La decisione di imporre tali misure proattive non dovrebbe, in linea di principio, comportare l'imposizione di un obbligo generale di sorveglianza, conformemente all'articolo 15, paragrafo 1, della direttiva 2000/31/CE. Considerando i rischi particolarmente gravi connessi alla diffusione di contenuti terroristici, le decisioni adottate dalle autorità competenti sulla base del presente regolamento possono derogare all'approccio di cui all'articolo 15, paragrafo 1, della direttiva 2000/31/CE per talune misure specifiche e mirate la cui adozione sia necessaria per motivi imperativi di sicurezza pubblica. Prima di adottare tale decisione, l'autorità competente dovrebbe garantire un giusto equilibrio tra obiettivi di interesse generale e i diritti fondamentali in questione, in particolare la libertà di espressione e d'informazione e la libertà d'impresa, e addurre un'adeguata giustificazione.

(20) L'obbligo per i prestatori di servizi di hosting di conservare i contenuti rimossi e i relativi dati dovrebbe essere previsto per finalità specifiche e limitato al tempo necessario. Tale obbligo di conservazione dei dati dovrebbe essere esteso ai relativi dati, nella misura in cui tali dati andrebbero altrimenti perduti a seguito della rimozione del contenuto in questione. I relativi dati possono ad esempio includere dati relativi agli abbonati, compresi in particolare i dati relativi all'identità del fornitore di contenuti, nonché i «dati relativi agli accessi», tra cui ad esempio i dati relativi alla data e all'ora di utilizzo da parte del fornitore di contenuti, o la connessione al servizio (*log-in*) e la disconnessione (*log-off*) dal medesimo, unitamente all'indirizzo IP assegnato al fornitore di contenuti dal prestatore di servizi di accesso a Internet.

(21) L'obbligo di conservare il contenuto ai fini di un procedimento di riesame amministrativo o giurisdizionale è necessario e giustificato per garantire misure di tutela efficaci al fornitore di contenuti il cui contenuto è stato rimosso o l'accesso disabilitato o per garantire il ripristino di tale contenuto allo stato precedente alla sua rimozione, in funzione dell'esito del procedimento di riesame. L'obbligo di conservare il contenuto a fini di indagine e azione penale è giustificato e necessario in considerazione della potenziale utilità di tale materiale per scardinare o prevenire attività terroristiche. Se le imprese rimuovo i contenuti o ne disabilitano l'accesso, segnatamente a seguito dell'adozione proattiva di proprie misure, e non ne informano le pertinenti autorità ritenendo che non rientrino nell'ambito di applicazione dell'articolo 13, paragrafo 4, del presente regolamento, le autorità di contrasto potrebbero non essere a conoscenza dell'esistenza di tale contenuto. Ciò giustifica anche la conservazione di contenuti a fini di prevenzione, accertamento, indagine e perseguimento di reati di terrorismo. A tal fine, l'obbligo di conservazione è limitato ai dati che possono riguardare reati di terrorismo e può pertanto contribuire a perseguire i reati di terrorismo o la prevenzione di gravi rischi per la sicurezza pubblica.

(22) Per garantire la proporzionalità, il periodo di conservazione dovrebbe essere limitato a sei mesi, in modo da dare ai fornitori di contenuti il tempo sufficiente ad avviare il procedimento di riesame e consentire alle autorità di contrasto di accedere ai dati pertinenti ai fini delle indagini e dell'azione penale nei confronti dei reati di terrorismo. Su richiesta dell'autorità che effettua il riesame, tale termine può tuttavia essere prorogato del tempo necessario qualora il procedimento di riesame sia avviato ma non completato entro il periodo di sei mesi. Tale periodo dovrebbe essere sufficiente per consentire alle autorità di contrasto di conservare gli elementi di prova necessari in relazione alle loro indagini assicurando nel contempo un equilibrio con i diritti fondamentali in questione.

(23) Il presente regolamento non pregiudica le garanzie procedurali e le misure investigative procedurali relative all'accesso ai contenuti e ai relativi dati conservati a fini di indagine e azione penale nei confronti dei reati di terrorismo, stabilite dalla legislazione nazionale degli Stati membri o dal diritto dell'Unione.

(24) La trasparenza della politica applicata dai prestatori di servizi di hosting in relazione ai contenuti terroristici è essenziale ai fini della loro maggiore responsabilità nei confronti dei propri utilizzatori e per rafforzare la fiducia dei cittadini nel mercato unico digitale. I prestatori di servizi di hosting dovrebbero pubblicare relazioni annuali sulla trasparenza contenenti informazioni utili sulle misure adottate per individuare, identificare e rimuovere contenuti terroristici.

(25) Le procedure di reclamo costituiscono una tutela necessaria contro la rimozione erronea di contenuti protetti nell'ambito della libertà di espressione e di informazione. I prestatori di servizi di hosting dovrebbero pertanto predisporre meccanismi di facile uso per i reclami, assicurando che siano trattati tempestivamente e in piena trasparenza nei confronti del fornitore di contenuti. L'obbligo di ripristinare il contenuto rimosso erroneamente non pregiudica la possibilità che il prestatore di servizi di hosting applichi le proprie condizioni contrattuali per altri motivi.

(26) L'articolo 19 del TUE e l'articolo 47 della Carta dei diritti fondamentali dell'Unione europea sanciscono il diritto a una tutela giurisdizionale effettiva, in forza del quale le persone devono essere in grado di conoscere il motivo per cui il contenuto da loro caricato è stato rimosso o il relativo accesso disabilitato. A tal fine, il prestatore di servizi di hosting dovrebbe mettere a disposizione del fornitore di contenuti utili informazioni che gli consentano di impugnare la decisione. Può tuttavia non essere necessario inviare una notifica al fornitore di contenuti. A seconda delle circostanze, i prestatori di servizi di hosting possono sostituire il contenuto considerato terroristico con un messaggio indicante che il contenuto è stato rimosso o disattivato in conformità del presente regolamento. Su sua richiesta, il fornitore di contenuti dovrebbe ricevere maggiori informazioni sui motivi della rimozione e sui mezzi di ricorso. Le autorità competenti dovrebbero informare il prestatore di servizi di hosting se, per motivi di pubblica sicurezza, in particolare nel contesto di un'indagine, ritengono inappropriato o controproducente notificare direttamente la rimozione del contenuto o la disabilitazione dell'accesso al contenuto.

(27) Al fine di evitare duplicazioni ed eventuali interferenze con le indagini, le autorità competenti dovrebbero scambiarsi informazioni, coordinarsi e cooperare reciprocamente e, se del caso, con Europol, quando emettono ordini di rimozione o trasmettono segnalazioni ai prestatori di servizi di hosting. Europol potrebbe sostenere

l'attuazione delle disposizioni del presente regolamento, nel rispetto del suo attuale mandato e del quadro giuridico esistente.

(28) Per garantire un'attuazione efficace e sufficientemente coerente di misure proattive, le autorità competenti degli Stati membri dovrebbero consultarsi in merito alle discussioni che conducono con i prestatori di servizi di hosting sull'identificazione, l'attuazione e la valutazione di misure proattive specifiche. Analogamente, tale cooperazione è necessaria anche per quanto riguarda l'adozione di norme in materia di sanzioni, comprese l'attuazione e l'esecuzione delle stesse.

(29) È essenziale che l'autorità competente dello Stato membro responsabile di infliggere le sanzioni sia pienamente informata degli ordini di rimozione e delle segnalazioni, così come dei successivi scambi tra il prestatore di servizi di hosting e l'autorità competente pertinente. A tal fine, gli Stati membri dovrebbero provvedere affinché siano predisposti canali e meccanismi di comunicazione adeguati per condividere tempestivamente le informazioni pertinenti.

(30) Per facilitare il rapido scambio tra le autorità competenti nonché con i prestatori di servizi di hosting, e per evitare duplicazioni, gli Stati membri possono avvalersi degli strumenti messi a punto dall'unità addetta alle segnalazioni su Internet di Europol, ad esempio l'applicazione IRMA, attualmente in uso, per la gestione di tali segnalazioni o gli strumenti che la sostituiranno.

(31) Considerata la particolare gravità delle conseguenze di determinati contenuti terroristici, i prestatori di servizi di hosting dovrebbero informare tempestivamente l'autorità dello Stato membro interessato o le autorità competenti del paese in cui sono stabiliti o hanno un rappresentante legale, circa l'esistenza di eventuali prove di reati di terrorismo di cui vengano a conoscenza. Ai fini di proporzionalità, tale obbligo è limitato ai reati di terrorismo quali definiti all'articolo 3, paragrafo 1, della direttiva (UE) 2017/541. L'obbligo di informare non impone ai prestatori di servizi di hosting l'obbligo di cercare attivamente tali prove. Lo Stato membro interessato è lo Stato membro che ha giurisdizione sulle indagini e sull'azione penale nei confronti dei reati di terrorismo di cui alla direttiva (UE) 2017/541 in base alla cittadinanza dell'autore o della vittima potenziale del reato o del luogo interessato dall'atto terroristico. In caso di dubbio, i prestatori di servizi di hosting possono trasmettere le informazioni a Europol, che è tenuto a darvi seguito in conformità del suo mandato, o inoltrarle alle autorità nazionali competenti.

(32) Le autorità competenti degli Stati membri dovrebbero essere autorizzate a utilizzare tali informazioni per adottare le misure investigative previste dalla legislazione dello Stato membro o dell'Unione europea, ivi inclusa l'emissione di un ordine europeo di produzione ai sensi del regolamento relativo agli ordini europei di produzione e di conservazione di prove elettroniche in materia penale[14].

(33) Sia i prestatori di servizi di hosting sia gli Stati membri dovrebbero istituire punti di contatto per facilitare il rapido trattamento degli ordini di rimozione e delle segnalazioni. Contrariamente al rappresentante legale, il punto di contatto assolve compiti di natura operativa. Il punto di contatto del prestatore di servizi di hosting

[14] COM(2018) 225 final.

dovrebbe disporre degli strumenti specifici che permettono di trasmettere per via elettronica gli ordini di rimozione e le segnalazioni e delle risorse tecniche e personali che consentono di trattarli rapidamente. Il punto di contatto del prestatore di servizi di hosting non deve necessariamente essere situato nell'Unione e il prestatore di servizi di hosting è libero di designare un punto di contatto già esistente, a condizione che questi sia in grado di svolgere le funzioni previste dal presente regolamento. Al fine di garantire che il contenuto terroristico sia rimosso o l'accesso disattivato entro un'ora dal ricevimento di un ordine di rimozione, i prestatori di servizi di hosting dovrebbero far sì che il punto di contatto sia accessibile 24 ore su 24 e 7 giorni su 7. Le informazioni sul punto di contatto dovrebbero comprendere informazioni sulla lingua in cui il punto di contatto può essere contattato. Per facilitare la comunicazione tra i prestatori di servizi di hosting e le autorità competenti, i prestatori di servizi di hosting sono incoraggiati ad ammettere la comunicazione in una delle lingue ufficiali dell'Unione nella quale sono disponibili le loro condizioni contrattuali.

(34) In assenza di un obbligo generale per i prestatori di servizi di assicurare la presenza fisica all'interno del territorio dell'Unione, è necessario determinare in modo chiaro lo Stato membro nella cui giurisdizione ricade il prestatore di servizi di hosting che offre servizi all'interno dell'Unione. Generalmente, il prestatore di servizi di hosting ricade nella giurisdizione dello Stato membro in cui ha lo stabilimento principale o in cui ha designato un rappresentante legale. Tuttavia, quando un altro Stato membro emette un ordine di rimozione, le sue autorità dovrebbero poter dare esecuzione ai loro ordini adottando misure coercitive di natura non punitiva, ad esempio sanzioni pecuniarie. Anche se un prestatore di servizi di hosting non ha sede nell'Unione e non vi ha designato un rappresentante legale, qualsiasi Stato membro dovrebbe comunque poter infliggere sanzioni, a condizione che sia rispettato il principio del *ne bis in idem*.

(35) I prestatori di servizi di hosting che non sono stabiliti nell'Unione dovrebbero designare, per iscritto, un rappresentante legale al fine di assicurare il rispetto e l'esecuzione degli obblighi ai sensi del presente regolamento.

(36) Il rappresentante legale dovrebbe essere legalmente autorizzato ad agire per conto del prestatore di servizi di hosting.

(37) Ai fini dell'applicazione del presente regolamento, gli Stati membri dovrebbero designare autorità competenti. L'obbligo di designare le autorità competenti non richiede necessariamente l'istituzione di nuove autorità; i compiti stabiliti dal presente regolamento possono essere assegnati ad organismi esistenti. Il presente regolamento fa obbligo di designare autorità competenti a emettere ordini di rimozione e segnalazioni, vigilare sulle misure proattive e infliggere sanzioni. Spetta agli Stati membri decidere quante autorità intendono designare per tali compiti.

(38) Le sanzioni sono necessarie per garantire che i prestatori di servizi di hosting diano effettiva attuazione agli obblighi previsti dal presente regolamento. Occorre che gli Stati membri adottino norme relative alle sanzioni, comprese, eventualmente, linee guida per il calcolo delle stesse. Sanzioni particolarmente severe dovrebbero essere inflitte nel caso in cui il prestatore di servizi di hosting ometta sistematicamente di rimuovere contenuti terroristici o di disabilitarne l'accesso entro un'ora dal ricevimento di un ordine di rimozione. La mancata conformità in casi individuali potrebbe essere sanzionata nel rispetto del principio *ne bis in idem* e del principio di proporzionalità, assicurando che tali sanzioni tengano conto dell'inosservanza sistematica. Al fine di

garantire la certezza del diritto, il regolamento dovrebbe stabilire in che misura gli obblighi pertinenti possano essere soggetti a sanzioni. Sanzioni in caso di mancato rispetto dell'articolo 6 dovrebbero essere adottate solo in relazione agli obblighi derivanti dalla richiesta di riferire a norma dell'articolo 6, paragrafo 2, o da una decisione che impone misure proattive supplementari a norma dell'articolo 6, paragrafo 4. Nel determinare se debbano essere inflitte sanzioni pecuniarie si dovrebbe tenere debito conto delle risorse finanziarie del prestatore. Gli Stati membri assicurano che le sanzioni non incoraggino la rimozione di contenuti che non hanno natura terroristica.

(39) L'utilizzo di modelli standardizzati facilita la cooperazione e lo scambio di informazioni tra le autorità competenti e i prestatori di servizi, consentendo loro di comunicare in modo più rapido ed efficace. È particolarmente importante garantire un intervento rapido dopo la ricezione di un ordine di rimozione. I modelli riducono i costi di traduzione e contribuiscono a un livello elevato di qualità. Analogamente, formulari di risposta dovrebbero consentire uno scambio di informazioni standardizzato, particolarmente importante nel caso in cui i prestatori di servizi non sono in grado di conformarsi a una richiesta. Canali di trasmissione autenticati possono garantire l'autenticità dell'ordine di rimozione, compresa l'esattezza della data e dell'ora di invio e di ricezione dell'ordine.

(40) Per poter modificare rapidamente, se necessario, il contenuto del modello da utilizzare ai fini del presente regolamento, 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. Per tenere conto dello sviluppo tecnologico e del relativo quadro giuridico, alla Commissione dovrebbe essere inoltre conferito il potere di adottare atti delegati al fine di integrare il presente regolamento con requisiti tecnici per gli strumenti elettronici destinati ad essere utilizzati dalle autorità competenti per trasmettere gli ordini di rimozione. 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"[15]. 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.

(41) Gli Stati membri dovrebbero raccogliere informazioni sull'attuazione della legislazione. Occorre elaborare un programma dettagliato volto a monitorare gli esiti, i risultati e gli effetti del presente regolamento, al fine di fornire elementi per la valutazione della normativa.

(42) Sulla base delle constatazioni e conclusioni formulate nella relazione di attuazione e dell'esito dell'esercizio di monitoraggio, la Commissione dovrebbe effettuare una valutazione del presente regolamento non prima di tre anni dalla sua entrata in vigore. La valutazione dovrebbe essere basata sui cinque criteri di efficienza, efficacia, pertinenza, coerenza e valore aggiunto dell'UE. Sarà valutato il funzionamento delle

[15] GU L 123 del 12.5.2016, pag. 1.

diverse misure operative e tecniche previste dal regolamento, in particolare l'efficacia delle misure volte a migliorare l'individuazione, l'identificazione e la rimozione di contenuti terroristici, l'efficacia dei meccanismi di salvaguardia nonché le potenziali conseguenze per i diritti e gli interessi di terzi, compresa una revisione dell'obbligo di informare i fornitori di contenuti.

(43) Poiché l'obiettivo del presente regolamento, ossia garantire il buon funzionamento del mercato unico digitale mediante la prevenzione della diffusione di contenuti terroristici online, non può essere conseguito in misura sufficiente dagli Stati membri e può dunque, a motivo della portata e degli effetti dell'azione in questione, 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 obiettivo in ottemperanza al principio di proporzionalità enunciato nello stesso articolo,

HANNO ADOTTATO IL PRESENTE REGOLAMENTO:

SEZIONE I
DISPOSIZIONI GENERALI

Articolo 1
Oggetto e ambito di applicazione

1. Il presente regolamento stabilisce regole uniformi per impedire l'uso improprio dei servizi di hosting ai fini della diffusione di contenuti terroristici online. Esso prevede in particolare:

   (a) norme relative agli obblighi di diligenza che i prestatori di servizi di hosting sono tenuti ad applicare per impedire la diffusione di contenuti terroristici tramite i loro servizi e garantirne, ove necessario, la rapida rimozione;

   (b) una serie di misure che gli Stati membri sono tenuti ad attuare per individuare i contenuti terroristici, consentirne la rapida rimozione da parte dei prestatori di servizi di hosting e facilitare la cooperazione con le autorità competenti di altri Stati membri, i prestatori di servizi di hosting e, se del caso, gli organismi pertinenti dell'Unione.

2. Il presente regolamento si applica ai prestatori di servizi di hosting che offrono servizi nell'Unione, indipendentemente dal luogo del loro stabilimento principale.

Articolo 2
Definizioni

Ai fini del presente regolamento si applicano le seguenti definizioni:

(1) "prestatore di servizi di hosting": un prestatore di servizi della società dell'informazione che consistono nel memorizzare informazioni fornite dal fornitore di contenuti su richiesta di quest'ultimo e nel rendere le informazioni memorizzate disponibili a terzi;

(2) "fornitore di contenuti": un utilizzatore che ha fornito informazioni che sono (o sono state) memorizzate, su sua richiesta, da un prestatore di servizi di hosting;

(3) "offrire servizi nell'Unione": consentire a persone fisiche o giuridiche in uno o più Stati membri di utilizzare i servizi del prestatore di servizi di hosting che presenta un collegamento sostanziale con tale Stato membro o con tali Stati membri, ad esempio:

(a) lo stabilimento del prestatore di servizi di hosting nell'Unione;

(b) un numero significativo di utenti in uno o più Stati membri;

(c) orientamento delle attività verso uno o più Stati membri;

(4) "reati di terrorismo": i reati ai sensi dell'articolo 3, paragrafo 1, della direttiva (UE) 2017/541;

(5) "contenuto terroristico": uno o più dei seguenti messaggi:

(a) istigazione, anche mediante l'apologia del terrorismo, alla commissione di reati di terrorismo, generando in tal modo il pericolo che tali reati siano effettivamente commessi;

(b) incitamento a contribuire a reati di terrorismo;

(c) promozione delle attività di un gruppo terroristico, in particolare incoraggiando la partecipazione o il sostegno a un gruppo terroristico ai sensi dell'articolo 2, paragrafo 3, della direttiva (UE) 2017/541;

(d) istruzioni su metodi o tecniche allo scopo di commettere reati di terrorismo;

(6) "diffusione di contenuti terroristici": il fatto di rendere accessibili a terzi i contenuti terroristici tramite i servizi dei prestatori di servizi di hosting;

(7) "condizioni contrattuali": tutte le modalità, le condizioni e le clausole che, indipendentemente dalla loro denominazione o forma, disciplinano il rapporto contrattuale tra il prestatore di servizi di hosting e gli utilizzatori di tali servizi;

(8) "segnalazione": un avviso trasmesso da un'autorità competente o, se del caso, da un pertinente organismo dell'Unione a un prestatore di servizi di hosting in merito a contenuti che possono essere considerati contenuti terroristici, affinché il prestatore proceda, su base volontaria, alla verifica della compatibilità con le proprie condizioni contrattuali al fine di prevenire la diffusione di contenuti terroristici;

(9) "stabilimento principale": la sede centrale o la sede legale nella quale sono esercitate le principali funzioni finanziarie ed eseguiti i controlli operativi.

SEZIONE II
Misure volte a prevenire la diffusione di contenuti terroristici online

Articolo 3
Obblighi di diligenza

1. I prestatori di servizi di hosting adottano, in conformità al presente regolamento, misure adeguate, ragionevoli e proporzionate, per prevenire la diffusione di contenuti terroristici e proteggere gli utilizzatori da tali contenuti. In tale contesto, essi agiscono in modo diligente, proporzionato e non discriminatorio, prestano il debito rispetto ai diritti fondamentali degli utilizzatori e tengono conto della fondamentale importanza che riveste la libertà di espressione e di informazione in una società aperta e democratica.

2. I prestatori di servizi di hosting includono nelle loro condizioni contrattuali disposizioni volte a prevenire la diffusione di contenuti terroristici e ne assicurano l'applicazione.

Articolo 4
Ordini di rimozione di contenuti

1. L'autorità competente ha facoltà di adottare una decisione che imponga al prestatore di servizi di hosting di rimuovere contenuti terroristici o di disabilitarne l'accesso.

2. I prestatori di servizi di hosting rimuovono i contenuti terroristici o ne disabilitano l'accesso entro un'ora dal ricevimento dell'ordine di rimozione.

3. Gli ordini di rimozione recano i seguenti elementi in conformità al modello di cui all'allegato I:

   (a) l'identificazione dell'autorità competente che emette l'ordine di rimozione e l'autenticazione dell'ordine di rimozione da parte dell'autorità competente;

   (b) la motivazione per cui il contenuto è considerato contenuto terroristico, almeno con riferimento alle categorie di contenuti terroristici elencati all'articolo 2, paragrafo 5;

   (c) un indirizzo URL (*Uniform Resource Locator*) e, se necessario, ulteriori informazioni che consentano di individuare il contenuto in questione;

   (d) un riferimento al presente regolamento come base giuridica dell'ordine di rimozione;

   (e) la data e l'ora dell'emissione dell'ordine;

   (f) informazioni sui mezzi di ricorso a disposizione del prestatore di servizi di hosting e del fornitore di contenuti;

   (g) se del caso, la decisione di cui all'articolo 11 di non divulgare informazioni sulla rimozione dei contenuti terroristici o sulla disabilitazione dell'accesso a tali contenuti.

4. Su richiesta del prestatore di servizi di hosting o del fornitore di contenuti, l'autorità competente trasmette una motivazione dettagliata, fermo restando l'obbligo del

prestatore di servizi di hosting di conformarsi all'ordine di rimozione entro il termine di cui al paragrafo 2.

5. Le autorità competenti indirizzano l'ordine di rimozione allo stabilimento principale del prestatore di servizi di hosting o al rappresentante legale designato dal prestatore di servizi di hosting ai sensi dell'articolo 16 e lo trasmettono al punto di contatto di cui all'articolo 14, paragrafo 1. Tali ordini sono trasmessi con mezzi elettronici che producano una traccia scritta in condizioni che consentano di stabilire l'autenticazione del mittente, compresa l'esattezza della data e dell'ora di invio e di ricezione dell'ordine.

6. I prestatori di servizi di hosting accusano ricevuta e informano senza indebito ritardo l'autorità competente della rimozione dei contenuti terroristici o della disabilitazione dell'accesso agli stessi, indicando, in particolare, la data e l'ora dell'intervento, utilizzando il modello di cui all'allegato II.

7. Se non è in grado di conformarsi all'ordine di rimozione per cause di forza maggiore o di impossibilità di fatto a lui non imputabile, il prestatore di servizi di hosting ne informa, senza indebito ritardo, l'autorità competente e ne spiega i motivi, utilizzando il modello di cui all'allegato III. La scadenza di cui al paragrafo 2 si applica non appena i motivi addotti vengono meno.

8. Se non è in grado di conformarsi all'ordine di rimozione, in quanto il provvedimento è viziato da errori manifesti o non contiene informazioni sufficienti per l'esecuzione dell'ordine, il prestatore di servizi di hosting ne informa, senza indebito ritardo, l'autorità competente e chiede i chiarimenti necessari, utilizzando il modello di cui all'allegato III. La scadenza di cui al paragrafo 2 si applica non appena sono forniti i chiarimenti.

9. L'autorità competente che ha emesso l'ordine di rimozione informa l'autorità competente che vigila sull'attuazione delle misure proattive di cui all'articolo 17, paragrafo 1, lettera c), quando l'ordine di rimozione diventa definitivo. Un ordine di rimozione diventa definitivo se non è oggetto di ricorso entro il termine stabilito in conformità al diritto nazionale applicabile o se è stato confermato in esito al ricorso.

Articolo 5
Segnalazioni

1. L'autorità competente o l'organismo competente dell'Unione può inviare una segnalazione a un prestatore di servizi di hosting.

2. I prestatori di servizi di hosting mettono in atto misure operative e tecniche per agevolare la rapida valutazione dei contenuti che le autorità competenti e, se del caso, gli organismi pertinenti dell'Unione segnalano loro affinché provvedano, su base volontaria, ad esaminarli.

3. La segnalazione è indirizzata allo stabilimento principale del prestatore di servizi di hosting o al rappresentante legale designato dal prestatore di servizi di hosting ai sensi dell'articolo 16 e trasmessa al punto di contatto di cui all'articolo 14, paragrafo 1. Tali segnalazioni sono trasmesse per via elettronica.

4. La segnalazione contiene informazioni sufficientemente dettagliate, segnatamente i motivi per i quali il contenuto è considerato contenuto terroristico, un URL e, se necessario, ulteriori informazioni che consentano di individuare il contenuto terroristico oggetto della segnalazione.

5. Il prestatore di servizi di hosting procede, in via prioritaria, a valutare il contenuto individuato nella segnalazione rispetto alle proprie condizioni contrattuali e decide se rimuovere tale contenuto o disabilitarne l'accesso.

6. Il prestatore di servizi di hosting informa rapidamente la competente autorità o l'organismo competente dell'Unione dell'esito della valutazione e della tempistica di eventuali misure prese a seguito della segnalazione.

7. Se ritiene che la segnalazione non contenga informazioni sufficienti per valutare il contenuto in oggetto, il prestatore di servizi di hosting ne informa senza indugio l'autorità competente o l'organismo dell'Unione competente, precisando quali ulteriori informazioni o chiarimenti sono necessari.

Articolo 6
Misure proattive

1. I prestatori di servizi di hosting adottano, se del caso, misure proattive per proteggere i loro servizi dalla diffusione di contenuti terroristici. Tali misure sono efficaci e proporzionate, in considerazione del rischio e del livello di esposizione a contenuti terroristici, dei diritti fondamentali degli utilizzatori e dell'importanza fondamentale che riveste la libertà di espressione e di informazione in una società aperta e democratica.

2. Quando è stata informata a norma dell'articolo 4, paragrafo 9, l'autorità competente di cui all'articolo 17, paragrafo 1, lettera c), richiede al prestatore di servizi di hosting di presentare, entro tre mesi dal ricevimento della richiesta e, successivamente, almeno una volta l'anno, una relazione in merito alle specifiche misure proattive adottate, anche facendo ricorso a strumenti automatizzati, al fine di:

   (a) prevenire che siano nuovamente caricati online i contenuti che erano stati rimossi o il cui accesso era stato disattivato perché considerati contenuti terroristici;

   (b) individuare, identificare e rimuovere prontamente i contenuti terroristici o disabilitarne l'accesso.

   La richiesta è indirizzata allo stabilimento principale del prestatore di servizi di hosting o al rappresentante legale designato dal prestatore di servizi di hosting.

   La relazione contiene tutte le informazioni pertinenti che consentano all'autorità competente di cui all'articolo 17, paragrafo 1, lettera c), di valutare se le misure proattive sono efficaci e proporzionate, anche per valutare il funzionamento degli strumenti automatizzati utilizzati nonché la sorveglianza umana e i meccanismi di verifica applicati.

3. Se ritiene che le misure proattive adottate e trasmesse a norma del paragrafo 2 non siano sufficienti per attenuare e gestire il rischio e il livello di esposizione, l'autorità

competente di cui all'articolo 17, paragrafo 1, lettera c), può richiedere al prestatore di servizi di hosting di adottare specifiche misure proattive supplementari. A tal fine, il prestatore di servizi di hosting coopera con l'autorità competente di cui all'articolo 17, paragrafo 1, lettera c), al fine di individuare le misure specifiche che è tenuto ad attuare, definire i principali obiettivi e criteri di riferimento, nonché il calendario dell'attuazione.

4. Se non è possibile raggiungere un accordo entro tre mesi dalla richiesta di cui al paragrafo 3, l'autorità competente di cui all'articolo 17, paragrafo 1, lettera c), può emettere una decisione che impone l'adozione di specifiche misure proattive supplementari necessarie e proporzionate. La decisione tiene conto, in particolare, della capacità economica del prestatore di servizi di hosting, delle ripercussioni di tali misure sui diritti fondamentali degli utilizzatori e dell'importanza fondamentale della libertà di espressione e di informazione. La decisione è indirizzata allo stabilimento principale del prestatore di servizi di hosting o al rappresentante legale designato dal prestatore di servizi di hosting. Il prestatore di servizi di hosting rende periodicamente conto dell'attuazione di tali misure, secondo le indicazioni dell'autorità competente di cui all'articolo 17, paragrafo 1, lettera c).

5. Il prestatore di servizi di hosting può, in qualsiasi momento, chiedere un riesame all'autorità competente di cui all'articolo 17, paragrafo 1, lettera c), e, eventualmente, la revoca della richiesta o della decisione di cui, rispettivamente, ai paragrafi 2, 3 e 4. L'autorità competente adotta una decisione motivata entro un termine ragionevole dopo aver ricevuto la richiesta del prestatore di servizi di hosting.

Articolo 7
Conservazione del contenuto e dei relativi dati

1. Il prestatore di servizi di hosting conserva i contenuti terroristici rimossi o disabilitati a seguito di un ordine di rimozione, di una segnalazione o di misure proattive in conformità degli articoli 4, 5 e 6 e i relativi dati rimossi in conseguenza della rimozione del contenuto terroristico e che sono necessari per:

   (a) i procedimenti di riesame amministrativo o giudiziario;

   (b) la prevenzione, l'accertamento, l'indagine o il perseguimento di reati di terrorismo.

2. I contenuti terroristici e i relativi dati di cui al paragrafo 1 sono conservati per un periodo di sei mesi. Su richiesta dell'autorità competente o di un organo giurisdizionale, i contenuti terroristici sono conservati per un periodo più lungo e per tutto il tempo necessario per il procedimento di riesame amministrativo o giudiziario in corso di cui al paragrafo 1, lettera a).

3. I prestatori di servizi di hosting provvedono a che i contenuti terroristici e i relativi dati conservati a norma dei paragrafi 1 e 2 siano soggetti ad adeguate salvaguardie tecniche e organizzative.

   Tali salvaguardie tecniche e organizzative assicurano che i contenuti terroristici e i relativi dati conservati siano consultati e trattati solo per le finalità di cui al paragrafo 1, e garantiscono un elevato livello di sicurezza dei dati personali in

questione. I prestatori di servizi di hosting riesaminano e aggiornano tali salvaguardie ogniqualvolta sia necessario.

SEZIONE III
SALVAGUARDIE E RENDICONTAZIONE

Articolo 8
Obblighi di trasparenza

1. I prestatori di servizi di hosting definiscono nelle loro condizioni contrattuali la loro politica volta ad impedire la diffusione di contenuti terroristici, che include, se del caso, una valida spiegazione del funzionamento delle misure proattive, compreso l'uso di strumenti automatizzati.

2. I prestatori di servizi di hosting pubblicano relazioni annuali sulla trasparenza in merito alle misure intraprese contro la diffusione di contenuti terroristici.

3. Le relazioni sulla trasparenza contengono almeno le seguenti informazioni:

   (a) informazioni sulle misure intraprese dal prestatore di servizi di hosting per quanto concerne l'individuazione, l'identificazione e la rimozione di contenuti terroristici;

   (b) informazioni sulle misure intraprese dal prestatore di servizi di hosting per prevenire che siano nuovamente caricati online i contenuti che erano stati rimossi o ai quali l'accesso era stato disabilitato perché considerati contenuti terroristici;

   (c) il numero di messaggi con contenuto terroristico che sono stati rimossi o ai quali l'accesso è stato disattivato, a seguito, rispettivamente, di ordini di rimozione, segnalazioni o misure proattive;

   (d) un quadro sintetico e i risultati dei procedimenti di reclamo.

Articolo 9
Salvaguardie specifiche per quanto riguarda l'uso e l'attuazione di misure proattive

1. Laddove utilizzino, in conformità al presente regolamento, strumenti automatizzati in relazione ai contenuti che memorizzano, i prestatori di servizi di hosting predispongono misure di salvaguardia efficaci e appropriate per garantire l'accuratezza e la fondatezza delle decisioni relative a tali contenuti, in particolare delle decisioni di rimuovere i contenuti considerati terroristici o di disabilitarne l'accesso.

2. Tali misure di salvaguardia comprendono, in particolare, la sorveglianza umana e meccanismi di verifica ove opportuno e, in ogni caso, quando sia necessaria una valutazione dettagliata del contesto pertinente al fine di determinare se i contenuti siano da considerare terroristici.

Articolo 10
Meccanismi di reclamo

1. I prestatori di servizi di hosting predispongono meccanismi efficaci e accessibili che consentono ai fornitori di contenuti il cui contenuto è stato rimosso o reso inaccessibile a seguito di una segnalazione a norma dell'articolo 5 o di misure proattive a norma dell'articolo 6, di presentare un reclamo nei confronti della misura adottata dal prestatore di servizi di hosting, chiedendo la reintegrazione del contenuto.

2. I prestatori di servizi di hosting esaminano tempestivamente ogni reclamo che ricevono e ripristinano il contenuto senza indebito ritardo quando la rimozione o la disabilitazione dell'accesso si rivela ingiustificata. Essi informano l'autore del reclamo delle conclusioni del loro esame.

Articolo 11
Informazioni ai fornitori di contenuti

1. Quando rimuove contenuti terroristici o ne disabilita l'accesso, il prestatore di servizi di hosting mette a disposizione del fornitore di contenuti informazioni concernenti la rimozione o la disabilitazione dell'accesso a tali contenuti.

2. Su richiesta del fornitore di contenuti, il prestatore di servizi di hosting gli comunica i motivi della rimozione o della disabilitazione dell'accesso e lo informa delle possibilità di ricorso.

3. L'obbligo previsto ai paragrafi 1 e 2 non si applica se l'autorità competente decide che la motivazione non sia divulgata per ragioni di pubblica sicurezza, quali la prevenzione, l'indagine, l'accertamento e il perseguimento di reati di terrorismo, per il tempo necessario, ma non superiore a [quattro] settimane da tale decisione. In tal caso, il prestatore di servizi di hosting si astiene dal divulgare qualsiasi informazione concernente la rimozione o la disabilitazione dell'accesso a contenuti terroristici.

SEZIONE IV
Cooperazione tra autorità competenti, organismi dell'Unione e prestatori di servizi di hosting

Articolo 12
Capacità delle autorità competenti

Gli Stati membri assicurano che le autorità competenti dispongano della capacità necessaria e di risorse sufficienti per conseguire gli obiettivi e adempiere gli obblighi loro incombenti a norma del presente regolamento.

Articolo 13
Cooperazione tra i prestatori di servizi di hosting, le autorità competenti e, se del caso, gli organismi pertinenti dell'Unione

1. Le autorità competenti degli Stati membri scambiano informazioni, si coordinano e cooperano tra loro e, se del caso, con i pertinenti organismi dell'Unione quali

Europol, per quanto riguarda gli ordini di rimozione e le segnalazioni, in modo da evitare duplicazioni, potenziare il coordinamento ed evitare qualsiasi interferenza con indagini in corso nei diversi Stati membri.

2. Le autorità competenti degli Stati membri scambiano informazioni, si coordinano e cooperano con l'autorità competente di cui all'articolo 17, paragrafo 1, lettere c) e d), per quanto riguarda le misure adottate a norma dell'articolo 6, e i provvedimenti sanzionatori a norma dell'articolo 18. Gli Stati membri provvedono a che l'autorità competente di cui all'articolo 17, paragrafo 1, lettere c) e d), sia in possesso di tutte le informazioni pertinenti. A tal fine, gli Stati membri predispongono canali e meccanismi di comunicazione adeguati per garantire che le informazioni pertinenti siano condivise tempestivamente.

3. Gli Stati membri e i prestatori di servizi di hosting possono scegliere di avvalersi di appositi strumenti, inclusi, se del caso, quelli stabiliti dagli organismi pertinenti dell'Unione quali Europol, per facilitare in particolare:

   (a) il trattamento dei dati e il feedback relativi agli ordini di rimozione a norma dell'articolo 4;

   (b) il trattamento dei dati e il feedback relativi alle segnalazioni a norma dell'articolo 5;

   (c) la cooperazione allo scopo di individuare ed attuare misure proattive a norma dell'articolo 6.

4. Laddove sia a conoscenza di eventuali prove di reati di terrorismo, il prestatore di servizi di hosting ne informa immediatamente l'autorità competente per le indagini e il perseguimento di reati nello Stato membro interessato o il punto di contatto di cui all'articolo 14, paragrafo 2, dello Stato membro in cui ha lo stabilimento principale o un rappresentante legale. In caso di dubbi, il prestatore di servizi di hosting può trasmettere tali informazioni a Europol, che vi darà adeguato seguito.

Articolo 14
Punti di contatto

1. I prestatori di servizi di hosting istituiscono un punto di contatto incaricato di ricevere gli ordini di rimozione e le segnalazioni per via elettronica e di assicurarne il rapido trattamento ai sensi degli articoli 4 e 5. Essi provvedono affinché tali informazioni siano rese pubbliche.

2. Le informazioni di cui al paragrafo 1 precisano la lingua o le lingue ufficiali dell'Unione, elencate al regolamento 1/58, nelle quali è possibile rivolgersi al punto di contatto e nelle quali avvengono gli ulteriori scambi relativi agli ordini di rimozione e alle segnalazioni a norma degli articoli 4 e 5. Tali lingue comprendono almeno una delle lingue ufficiali dello Stato membro in cui il prestatore di servizi di hosting ha lo stabilimento principale o in cui risiede o è stabilito il suo rappresentante legale ai sensi dell'articolo 16.

3. Gli Stati membri istituiscono un punto di contatto per trattare le richieste di chiarimenti e di feedback in relazione agli ordini di rimozione e alle segnalazioni che hanno emesso. Le informazioni relative al punto di contatto sono rese pubbliche.

SEZIONE V
ATTUAZIONE E ESECUZIONE

Articolo 15
Competenza

1. Lo Stato membro nel quale il prestatore di servizi di hosting ha lo stabilimento principale è competente ai fini degli articoli 6, 18 e 21. Il prestatore di servizi di hosting che non ha lo stabilimento principale in uno degli Stati membri è considerato soggetto alla giurisdizione dello Stato membro in cui risiede o è stabilito il rappresentante legale di cui all'articolo 16.

2. Laddove il prestatore di servizi di hosting ometta di designare un rappresentante legale, tutti gli Stati membri sono competenti.

3. Se l'autorità di un altro Stato membro ha emesso un ordine di rimozione a norma dell'articolo 4, paragrafo 1, tale Stato membro è competente ad adottare misure coercitive conformemente alla legislazione nazionale, al fine di dare esecuzione all'ordine di rimozione.

Articolo 16
Rappresentante legale

1. Il prestatore di servizi di hosting che non è stabilito nell'Unione, ma offre servizi nell'Unione, designa, per iscritto, una persona fisica o giuridica quale suo rappresentante legale nell'Unione per la ricezione, l'attuazione e l'esecuzione degli ordini di rimozione, delle segnalazioni, delle richieste e delle decisioni emessi dalle autorità competenti sulla base del presente regolamento. Il rappresentante legale risiede o è stabilito in uno degli Stati membri in cui il prestatore di servizi offre i propri servizi.

2. Il prestatore di servizi di hosting incarica il rappresentante legale di ricevere, attuare ed eseguire, per suo conto, gli ordini di rimozione, le segnalazioni, le richieste e le decisioni di cui al paragrafo 1. Il prestatore di servizi di hosting conferisce al proprio rappresentante legale i poteri e le risorse necessari per cooperare con le autorità competenti e per ottemperare a tali decisioni e ordini.

3. Il rappresentante legale designato può essere ritenuto responsabile per il mancato rispetto degli obblighi derivanti dal presente regolamento, fatte salve le responsabilità del prestatore di servizi di hosting e le azioni legali che possono essere promosse nei confronti di quest'ultimo.

4. Il prestatore di servizi di hosting informa della designazione l'autorità competente di cui all'articolo 17, paragrafo 1, lettera d), dello Stato membro in cui il rappresentante legale risiede o è stabilito. Le informazioni relative al rappresentante legale sono rese pubbliche.

SEZIONE VI
DISPOSIZIONI FINALI

Articolo 17
Designazione delle autorità competenti

1. Ciascuno Stato membro designa la o le autorità competenti per:

   (a) emanare ordini di rimozione a norma dell'articolo 4;

   (b) individuare, identificare e segnalare contenuti terroristici ai prestatori di servizi di hosting a norma dell'articolo 5;

   (c) sorvegliare l'attuazione delle misure proattive a norma dell'articolo 6;

   (d) far rispettare gli obblighi stabiliti dal presente regolamento mediante sanzioni a norma dell'articolo 18.

2. Entro [*sei mesi dopo l'entrata in vigore del presente regolamento*] gli Stati membri notificano alla Commissione le autorità competenti di cui al paragrafo 1. La Commissione pubblica la notifica e le eventuali modifiche della stessa nella *Gazzetta ufficiale dell'Unione europea*.

Articolo 18
Sanzioni

1. Gli Stati membri stabiliscono le norme relative alle sanzioni applicabili in caso di violazione da parte dei prestatori di servizi di hosting degli obblighi derivanti dal presente regolamento e adottano tutte le misure necessarie per assicurarne l'applicazione. Tali sanzioni sono limitate a violazioni degli obblighi sanciti dai seguenti articoli:

   (a) articolo 3, paragrafo 2 (condizioni contrattuali dei prestatori di servizi di hosting);

   (b) articolo 4, paragrafi 2 e 6 (attuazione degli ordini di rimozione e relativo feedback);

   (c) articolo 5, paragrafi 5 e 6 (valutazione delle segnalazioni e relativo feedback);

   (d) articolo 6, paragrafi 2 e 4 (relazioni sulle misure proattive e adozione di misure a seguito di una decisione che impone specifiche misure proattive);

   (e) articolo 7 (conservazione dei dati);

   (f) articolo 8 (trasparenza);

   (g) articolo 9 (salvaguardie in relazione a misure proattive);

   (h) articolo 10 (procedure di reclamo);

   (i) articolo 11 (informazioni ai fornitori di contenuti);

(j) articolo 13, paragrafo 4 (informazioni relative alle prove di reati di terrorismo);

(k) articolo 14, paragrafo 1, (punti di contatto);

(l) articolo 16 (designazione di un rappresentante legale).

2. Le sanzioni previste sono efficaci, proporzionate e dissuasive. Gli Stati membri notificano alla Commissione, entro [*sei mesi dall'entrata in vigore del presente regolamento*], le norme e misure adottate al riguardo nonché ogni modifica ad esse apportata successivamente.

3. Gli Stati membri provvedono a che, nel determinare il tipo e il livello delle sanzioni, le autorità competenti tengano conto di tutte le circostanze pertinenti, tra cui:

(a) la natura, la gravità e la durata della violazione;

(b) il carattere doloso o colposo della violazione;

(c) precedenti violazioni da parte della persona giuridica ritenuta responsabile;

(d) la solidità finanziaria della persona giuridica ritenuta responsabile;

(e) il livello di cooperazione del prestatore di servizi di hosting con le autorità competenti.

4. Gli Stati membri provvedono a che la sistematica inosservanza degli obblighi ai sensi dell'articolo 4, paragrafo 2 sia passibile di sanzioni pecuniarie fino al 4 % del fatturato mondiale del prestatore di servizi di hosting dell'ultimo esercizio finanziario.

Articolo 19

Requisiti tecnici e modifiche ai modelli da utilizzare per gli ordini di rimozione

1. Alla Commissione è conferito il potere di adottare atti delegati conformemente all'articolo 20 al fine di integrare nel presente regolamento i requisiti tecnici relativi agli strumenti elettronici che saranno utilizzati dalle autorità competenti per trasmettere gli ordini di rimozione.

2. Alla Commissione è conferito il potere di adottare tali atti delegati per modificare gli allegati I, II e III al fine di rispondere efficacemente all'eventuale necessità di migliorare il contenuto dei moduli degli ordini di rimozione e dei moduli da utilizzare per fornire informazioni sull'impossibilità di dare esecuzione all'ordine di rimozione.

Articolo 20

Esercizio della delega

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

2. Il potere di adottare gli atti delegati di cui all'articolo 19, è conferito alla Commissione per un periodo di tempo indeterminato a decorrere [*dalla data di applicazione del presente regolamento*].

3. La delega di potere di cui all'articolo 19 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.

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 19 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 periodo è prorogato di due mesi su iniziativa del Parlamento europeo o del Consiglio.

Articolo 21
Monitoraggio

1. Gli Stati membri raccolgono dalle loro autorità competenti e dai prestatori di servizi di hosting soggetti alla loro giurisdizione informazioni concernenti le azioni intraprese a norma del presente regolamento e le trasmettono alla Commissione ogni anno entro il [31 marzo]. Tali informazioni includono:

   (a) informazioni sul numero di ordini di rimozione e segnalazioni, il numero di messaggi con contenuto terroristico che sono stati rimossi o il cui accesso è stato disabilitato, comprese le corrispondenti tempistiche a norma degli articoli 4 e 5;

   (b) informazioni sulle specifiche misure proattive adottate a norma dell'articolo 6, compresa la quantità di contenuti terroristici che è stata rimossa o il cui accesso è stato disabilitato, comprese le corrispondenti tempistiche;

   (c) informazioni sul numero di procedimenti di reclamo avviati e le azioni intraprese dai prestatori di servizi di hosting a norma dell'articolo 10;

   (d) informazioni sul numero di procedimenti di ricorso avviati e le decisioni adottate dalle autorità competenti in conformità al diritto nazionale.

2. Entro [*un anno dalla 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 gli indicatori e i mezzi da utilizzare per raccogliere i dati e gli altri elementi di prova

necessari, nonché la periodicità di tali acquisizioni. Esso specifica le misure che la Commissione e gli Stati membri sono tenuti ad adottare ai fini della raccolta e dell'analisi dei dati e di altri elementi di prova per monitorare i progressi e valutare il presente regolamento, in applicazione dell'articolo 23.

Articolo 22
Relazione sull'applicazione

Entro... [*due anni dopo l'entrata in vigore del presente regolamento*], la Commissione presenta al Parlamento europeo e al Consiglio una relazione sull'applicazione del presente regolamento. La relazione della Commissione tiene conto delle informazioni concernenti il monitoraggio a norma dell'articolo 21 e delle informazioni risultanti dagli obblighi di trasparenza a norma dell'articolo 8. Gli Stati membri trasmettono alla Commissione le informazioni necessarie per la preparazione della relazione.

Articolo 23
Valutazione

Non prima di [*tre anni dalla data di applicazione del presente regolamento*], la Commissione procede a una valutazione del presente regolamento e trasmette una relazione al Parlamento europeo e al Consiglio sull'applicazione del presente regolamento, compreso il funzionamento e l'efficacia dei meccanismi di salvaguardia. Se opportuno, la relazione è accompagnata da proposte legislative. Gli Stati membri trasmettono alla Commissione le informazioni necessarie per la preparazione della relazione.

Articolo 24
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].

Il presente regolamento è obbligatorio in tutti i suoi elementi e direttamente applicabile in ciascuno degli Stati membri.

Fatto a Bruxelles, il

Per il Parlamento europeo
Il presidente

Per il Consiglio
Il presidente