Gazzetta ufficiale dell'Unione europea C 135

Edizione in lingua italiana

Comunicazioni e informazioni

64° anno

16 aprile 2021

Sommario

IT

([1]) Testo rilevante ai fini del SEE.

III

(Atti preparatori)

CONSIGLIO

POSIZIONE (UE) n. 6/2021 DEL CONSIGLIO IN PRIMA LETTURA

in vista dell'adozione del regolamento del Parlamento europeo e del Consiglio relativo al contrasto della diffusione di contenuti terroristici online

Adottata dal Consiglio il 16 marzo 2021

(Testo rilevante ai fini del SEE)

(2021/C 135/01)

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 ([1]),

deliberando secondo la procedura legislativa ordinaria ([2]),

considerando quanto segue:

(1) Il presente regolamento mira a garantire il buon funzionamento del mercato unico digitale in una società aperta e democratica contrastando l'uso improprio dei servizi di hosting a fini terroristici e contribuendo alla sicurezza pubblica in tutta l'Unione. Dovrebbe essere migliorato il funzionamento del mercato unico digitale rafforzando la certezza del diritto per i prestatori di servizi di hosting e la fiducia degli utilizzatori nell'ambiente online, nonché potenziando le salvaguardie per la libertà di espressione, compresa la libertà di ricevere e comunicare informazioni e idee in una società aperta e democratica, e per la libertà e il pluralismo dei media.

(2) Le misure normative volte a contrastare la diffusione di contenuti terroristici online dovrebbero essere integrate da strategie degli Stati membri intese a contrastare il terrorismo, tra cui il rafforzamento dell'alfabetizzazione mediatica e del pensiero critico, lo sviluppo di narrazioni alternative e controargomentazioni, e altre iniziative volte a ridurre l'impatto dei contenuti terroristici online e la vulnerabilità a essi, nonché investimenti in attività sociali, iniziative di deradicalizzazione e dialogo con le comunità interessate, al fine di raggiungere una prevenzione costante della radicalizzazione nella società.

(3) Contrastare i contenuti terroristici online, che fanno parte del problema più ampio dei contenuti illegali online, richiede una combinazione di misure legislative, non legislative e volontarie basate sulla collaborazione tra le autorità e i prestatori di servizi di hosting, nel pieno rispetto dei diritti fondamentali.

([1]) GU C 110 del 22.3.2019, pag. 67.

([2]) Posizione del Parlamento europeo del 17 aprile 2019 (non ancora pubblicata nella Gazzetta ufficiale) e posizione del Consiglio in prima lettura del 16 marzo 2021. Posizione del Parlamento europeo del … (non ancora pubblicata nella Gazzetta ufficiale).

(4) 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, contribuendo in modo significativo all'innovazione, alla crescita economica, e alla creazione di posti di lavoro nell'Unione. In alcuni casi, tuttavia, i servizi di prestatori di servizi di hosting sono utilizzati impropriamente da terzi al fine di perpetrare attività illegali online. Particolarmente preoccupante è l'uso improprio di tali servizi da parte di gruppi terroristici e dei loro sostenitori per diffondere contenuti terroristici online allo scopo di propagare il loro messaggio, radicalizzare e reclutare adepti, nonché facilitare e dirigere attività terroristiche.

(5) Pur non essendo l'unico fattore, la presenza di contenuti terroristici online si è rivelata un catalizzatore della radicalizzazione degli individui che può portare a atti terroristici e, pertanto, 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 di hosting 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 al contrasto della diffusione di contenuti terroristici attraverso i loro servizi online, tenendo conto al contempo dell'importanza fondamentale della libertà di espressione, compresa la libertà di ricevere e comunicare informazioni e idee in una società aperta e democratica.

(6) 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. Tali sforzi devono essere integrati da un quadro legislativo chiaro al fine di ridurre ulteriormente l'accessibilità dei contenuti terroristici online e affrontare in modo adeguato un problema in rapida evoluzione. Il quadro legislativo fa leva su iniziative volontarie, che sono state rafforzate dalla raccomandazione (UE) 2018/334 della Commissione ([3]), e risponde alla richiesta del Parlamento europeo di rafforzare le misure volte a contrastare i contenuti online illegali e nocivi, in linea con il quadro orizzontale stabilito dalla direttiva 2000/31/CE del Parlamento europeo e del Consiglio ([4]), e a quella del Consiglio europeo di migliorare l'individuazione e la rimozione dei contenuti online che incitano a compiere atti terroristici.

(7) Il presente regolamento non dovrebbe pregiudicare l'applicazione della direttiva 2000/31/CE. In particolare, tutte le misure adottate da un prestatore di servizi di hosting conformemente al presente regolamento, comprese eventuali misure specifiche, non dovrebbero comportare automaticamente la perdita, per il prestatore di servizi di hosting, del beneficio dell'esenzione di responsabilità prevista in tale direttiva. Inoltre, il presente regolamento lascia impregiudicata la competenza delle autorità e degli organi giurisdizionali nazionali a stabilire la responsabilità dei prestatori di servizi di hosting se non sono soddisfatte le condizioni stabilite in tale direttiva per beneficiare dell'esenzione di responsabilità.

(8) In caso di conflitto tra il presente regolamento e la direttiva 2010/13/UE ([5]) per quanto riguarda le disposizioni che disciplinano i servizi di media audiovisivi definiti all'articolo 1, paragrafo 1, lettera a), di tale direttiva. La direttiva 2010/13/UE dovrebbe prevalere. Ciò lascia impregiudicati gli obblighi di cui al presente regolamento, in particolare per quanto riguarda i fornitori di servizi di piattaforma per la condivisione di video.

(9) Il presente regolamento dovrebbe definire norme intese a contrastare l'uso improprio dei servizi di hosting per la diffusione di contenuti terroristici online, al fine di garantire il buon funzionamento del mercato interno. Tali norme dovrebbero rispettare pienamente i diritti fondamentali tutelati nell'ordinamento giuridico dell'Unione e, in particolare, quelli garantiti dalla Carta dei diritti fondamentali dell'Unione europea («Carta»).

([3]) Raccomandazione (UE) 2018/334 della Commissione, del 1º marzo 2018, sulle misure per contrastare efficacemente i contenuti illegali online (GU L 63 del 6.3.2018, pag. 50).

([4]) 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).

([5]) Direttiva 2010/13/UE del Parlamento europeo e del Consiglio, del 10 marzo 2010, relativa al coordinamento di determinate disposizioni legislative, regolamentari e amministrative degli Stati membri concernenti la fornitura di servizi di media audiovisivi (direttiva sui servizi di media audiovisivi) (GU L 95 del 15.4.2010, pag. 1).

(10) Il presente regolamento intende contribuire alla protezione della pubblica sicurezza, attuando nel contempo adeguate e solide salvaguardie per garantire la tutela dei diritti fondamentali, inclusi il diritto al rispetto della vita privata, alla protezione dei dati personali, alla libertà di espressione, compresa la libertà di ricevere e comunicare informazioni, la libertà d'impresa e il diritto a una tutela giurisdizionale effettiva. Inoltre, è proibita ogni discriminazione. Le autorità competenti e i prestatori di servizi di hosting dovrebbero adottare solo le misure che sono necessarie, adeguate e proporzionate in una società democratica, tenendo conto della particolare importanza rivestita dalla libertà di espressione e di informazione, e la libertà e il pluralismo dei media, che costituiscono i fondamenti essenziali di una società pluralista e democratica, nonché valori su cui si fonda l'Unione. Le misure che incidono sulla libertà di espressione e di informazione dovrebbero essere rigorosamente mirate a contrastare la diffusione di contenuti terroristici online, nel rispetto del diritto di ricevere e comunicare 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. L'adozione di misure online efficaci per contrastare i contenuti terroristici online e la protezione della libertà di espressione e informazione non sono elementi contrastanti, bensì obiettivi complementari che si rafforzano a vicenda.

(11) Onde chiarire le azioni che i prestatori di servizi di hosting e le autorità competenti dovrebbero intraprendere per contrastare la diffusione di contenuti terroristici online, è opportuno che il presente regolamento stabilisca una definizione di «contenuti terroristici» per fini di prevenzione coerente con la definizione dei pertinenti reati ai sensi della direttiva (UE) 2017/541 del Parlamento europeo e del Consiglio ([6]). Data la necessità di contrastare la propaganda terroristica online più perniciosa, tale definizione dovrebbe ricomprendere il materiale che istiga o sollecita a commettere o a contribuire alla commissione di reati di terrorismo, o sollecita a partecipare alle attività di un gruppo terroristico o fa l'apologia di attività terroristiche, incluse raffigurazioni di un attentato terroristico. Nella definizione dovrebbe rientrare anche il materiale che fornisce indicazioni per la fabbricazione e l'uso di esplosivi, armi da fuoco o altre armi o sostanze nocive o pericolose, nonché sostanze chimiche, biologiche, radiologiche e nucleari (CBRN), ovvero altri specifici metodi o tecniche, compresa la selezione degli obiettivi, al fine di commettere o contribuire alla commissione di reati di terrorismo. Tali materiali comprendono testi, immagini, registrazioni audio e video, nonché trasmissioni in diretta di reati di terrorismo, che generano il rischio che possano essere commessi ulteriori reati di questo tipo. Nel valutare se del materiale integra contenuti terroristici ai sensi del presente regolamento, le autorità competenti e i prestatori di servizi di hosting, dovrebbero tenere conto di fattori quali la natura e la formulazione del materiale, 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, sia attribuibile, o sia diffuso per conto di una persona, gruppo o entità inclusi nell'elenco di persone, gruppi o entità coinvolte in atti terroristici e soggetto a misure restrittive dovrebbe costituire un elemento importante della valutazione.

(12) Il materiale diffuso per scopi educativi, giornalistici, artistici o di ricerca o a fini di sensibilizzazione contro l'attività terroristica non dovrebbe essere considerato come integrante contenuti terroristici. Nel determinare se il materiale fornito da un fornitore di contenuti integri «contenuti terroristici» in conformità alla definizione fornita dal presente regolamento, si dovrebbe tener conto, in particolare, del diritto alla libertà di espressione e di informazione, compresa la libertà e il pluralismo dei media, e la libertà delle arti e delle scienze. In particolare nei casi in cui il fornitore di contenuti detenga una responsabilità editoriale, qualsiasi decisione relativa alla rimozione del materiale diffuso dovrebbe tener conto delle norme giornalistiche previste dalla regolamentazione della stampa o dei media in conformità del diritto dell'Unione, compresa la Carta. Inoltre, le opinioni radicali, polemiche o controverse espresse nell'ambito di dibattiti politici sensibili non dovrebbero essere considerate contenuti terroristici.

(13) Al fine di contrastare efficacemente la diffusione di contenuti terroristici online, garantendo nel contempo il rispetto della vita privata degli individui, il presente regolamento si dovrebbe applicare ai fornitori di servizi della società dell'informazione che memorizzano e diffondono al pubblico informazioni e materiali forniti da un utilizzatore del servizio su sua richiesta, indipendentemente dal fatto che l'archiviazione e la diffusione al pubblico di tali informazioni e tali materiali siano di natura meramente tecnica, automatica e passiva. Il concetto di «memorizzazione» dovrebbe

([6]) 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).

essere inteso come la detenzione dei dati nella memoria di un server fisico o virtuale. I fornitori di servizi di semplice trasporto (*mere conduit*) o di memorizzazione temporanea (*caching*) nonché di altri servizi forniti in altri strati dell'infrastruttura di internet, che non comportano la memorizzazione, quali registri e autorità di registrazione, come anche fornitori di sistemi dei nomi di dominio (DNS), servizi di pagamento o di protezione contro gli attacchi distribuiti di negazione del servizio (DDoS), pertanto non dovrebbero rientrare nell'ambito di applicazione del presente regolamento.

(14) Il concetto di «diffusione al pubblico» dovrebbe implicare la messa a disposizione delle informazioni a un numero potenzialmente illimitato di persone, ossia il fatto di rendere le informazioni facilmente accessibili agli utilizzatori in generale senza che sia necessario un ulteriore intervento da parte del fornitore di contenuti, indipendentemente dall'accesso effettivo alle informazioni in questione da parte di tali persone. Di conseguenza, qualora l'accesso alle informazioni richieda la registrazione o l'ammissione a un gruppo di utilizzatori, tali informazioni dovrebbero essere considerate diffuse al pubblico solo se gli utilizzatori che intendono accedervi sono automaticamente registrati o ammessi senza una decisione o una selezione umana che stabilisca a chi concedere l'accesso. I servizi di comunicazione interpersonale, definiti all'articolo 2, punto 5, della direttiva (UE) 2018/1972 del Parlamento europeo e del Consiglio ([7]), quali i messaggi di posta elettronica o i servizi di messaggistica privata, non dovrebbero rientrare nell'ambito di applicazione del presente regolamento. Le informazioni dovrebbero essere considerate memorizzate e diffuse al pubblico ai sensi del presente regolamento solo se tali attività sono svolte su richiesta diretta del fornitore di contenuti. Di conseguenza, i fornitori di servizi, quali i servizi di infrastrutture cloud, forniti su richiesta di parti diverse dai fornitori di contenuti e a vantaggio solo indiretto di questi ultimi, non dovrebbero essere contemplati dal presente regolamento. A titolo di esempio, il presente regolamento dovrebbe contemplare i fornitori di servizi di social media, di servizi di condivisione di video, audio e immagini, nonché di servizi di condivisione di file e altri servizi cloud, nella misura in cui tali servizi sono utilizzati per mettere le informazioni memorizzate a disposizione del pubblico su richiesta diretta del fornitore di contenuti. Qualora un prestatore di servizi di hosting offra più servizi, il presente regolamento dovrebbe applicarsi solo ai servizi che rientrano nel suo ambito di applicazione.

(15) I contenuti terroristici sono spesso diffusi al pubblico attraverso servizi forniti da prestatori di servizi di hosting stabiliti in paesi terzi. Al fine di proteggere gli utilizzatori nell'Unione e garantire che tutti i prestatori di servizi di hosting che operano nel mercato unico digitale siano soggetti agli stessi obblighi, il presente regolamento dovrebbe applicarsi a tutti i prestatori di servizi pertinenti offerti nell'Unione, indipendentemente dal paese in cui hanno lo stabilimento principale. Per determinare se un prestatore di servizi offre servizi nell'Unione è necessario verificare se consente alle persone fisiche o giuridiche di uno o più Stati membri di usufruire dei suoi servizi e presenta un collegamento sostanziale con tale Stato membro o con tali Stati membri.

(16) Un collegamento sostanziale con l'Unione dovrebbe considerarsi presente quando il prestatore di servizi di hosting è stabilito nell'Unione, i suoi servizi sono utilizzati da un numero considerevole di utilizzatori in uno o più Stati membri, o le sue attività sono orientate verso uno o più Stati membri. L'orientamento delle attività verso uno o più Stati membri dovrebbe 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 da tale Stato membro. Tale orientamento potrebbe anche desumersi dalla disponibilità di un'applicazione nell'apposito negozio online (*app store*) nazionale, dalla diffusione di pubblicità a livello locale in una lingua generalmente utilizzata nello Stato membro in questione, o dalla gestione dei rapporti con la clientela, ad esempio la fornitura di assistenza alla clientela in una lingua generalmente utilizzata in tale Stato membro. Un collegamento sostanziale dovrebbe essere presunto anche quando le attività di un prestatore di servizi di hosting 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 ([8]). La semplice accessibilità del sito internet di un prestatore di servizi di hosting di un indirizzo di posta elettronica e di altri dati di contatto in uno o più Stati membri, non dovrebbe, in quanto tale, essere sufficiente a costituire un collegamento sostanziale. Inoltre, 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 ([9]) costituisca, di per sé, un collegamento sostanziale.

([7]) Direttiva (UE) 2018/1972 del Parlamento europeo e del Consiglio, dell'11 dicembre 2018, che istituisce il codice europeo delle comunicazioni elettroniche (rifusione) (GU L 321 del 17.12.2018, pag. 36).

([8]) 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).

([9]) 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 60I del 2.3.2018, pag. 1).

(17) È opportuno armonizzare la procedura e gli obblighi che discendono dagli ordini di rimozione che impongono ai prestatori di servizi di hosting di rimuovere o di disabilitare l'accesso a contenuti terroristici, in esito a una valutazione delle autorità competenti. In considerazione della velocità alla quale i contenuti terroristici sono diffusi attraverso i servizi online, dovrebbe essere imposto ai prestatori di servizi di hosting l'obbligo di provvedere a che i contenuti terroristici identificati in un ordine di rimozione siano rimossi o che l'accesso ad essi sia disabilitato in tutti gli Stati membri entro un'ora dal ricevimento dell'ordine di rimozione. Eccetto casi di emergenza debitamente giustificati, l'autorità competente dovrebbe fornire a un prestatore di servizi di hosting informazioni sulle procedure e sui termini applicabili almeno 12 ore prima di emettere il primo ordine di rimozione nei confronti di tale prestatore di servizi di hosting. Si verificano casi debitamente giustificati di emergenza quando una rimozione o una disabilitazione dell'accesso ai contenuti che avvenisse oltre un'ora dopo la ricezione dell'ordine di rimozione provocherebbe un danno grave, ad esempio in situazioni di minaccia imminente per la vita o l'integrità fisica di una persona, o qualora tali contenuti presentino eventi in corso che provocherebbero un danno alla vita o all'integrità fisica di una persona. L'autorità competente dovrebbe determinare se costituiscano casi di emergenza e fornire la debita giustificazione della propria decisione nell'ordine di rimozione. Qualora il prestatore di servizi di hosting non sia in grado di conformarsi all'ordine di rimozione entro un'ora dal suo ricevimento per cause di forza maggiore o di impossibilità di fatto, anche per ragioni tecniche o operative oggettivamente giustificabili, dovrebbe informare l'autorità competente di emissione non appena possibile e conformarsi all'ordine di rimozione non appena la situazione sia risolta.

(18) L'ordine di rimozione dovrebbe contenere una motivazione sulla qualifica del materiale da rimuovere, o il cui accesso debba essere disabilitato, in quanto integrante contenuti terroristici e fornire informazioni sufficienti per la localizzazione di tali contenuti, indicando l'URL esatto e, se necessario, ogni altra informazione aggiuntiva quale ad esempio una copia della schermata (*screenshot*) dei contenuti in questione. Tali motivazioni dovrebbero tuttavia consentire al prestatore di servizi di hosting e, in ultima istanza, al fornitore di contenuti di esercitare effettivamente il loro diritto al ricorso giurisdizionale. Non è necessario che le motivazioni fornite contengano informazioni sensibili che potrebbero compromettere indagini in corso.

(19) L'autorità competente dovrebbe inviare l'ordine di rimozione direttamente al punto di contatto designato o stabilito dal prestatore di servizi di hosting ai fini del presente regolamento con ogni mezzo elettronico che consenta di conservare una traccia scritta in condizioni che permettano al prestatore di servizi di hosting di stabilire l'autenticità di tale ordine, compresa l'esattezza della data e dell'ora di invio e ricevimento dello stesso, quali posta elettronica protetta o piattaforme o altri canali protetti, compresi quelli messi a disposizione dal prestatore di servizi di hosting, in conformità del diritto dell'Unione in materia di protezione dei dati personali. Tale obbligo dovrebbe poter essere assolto tramite l'uso, tra l'altro, di servizi elettronici di recapito certificato qualificati ai sensi del regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio ([10]). Se il prestatore di servizi di hosting ha lo stabilimento principale o il suo rappresentante legale risiede o è stabilito in uno Stato membro diverso da quello dell'autorità competente di emissione, una copia dell'ordine di rimozione dovrebbe essere inviata contemporaneamente all'autorità competente di tale Stato membro.

(20) Dovrebbe essere possibile per l'autorità competente dello Stato membro in cui il prestatore di servizi di hosting ha lo stabilimento principale o in cui il suo rappresentante legale risiede o è stabilito esaminare l'ordine di rimozione emesso dalle autorità competenti di un altro Stato membro per stabilire se esso violi il regolamento in modo grave o manifesto il presente regolamento, o i diritti fondamentali sanciti dalla Carta. Sia il fornitore di contenuti che il prestatore di servizi di hosting dovrebbero avere il diritto di chiedere tale esame da parte dell'autorità competente dello Stato membro in cui il prestatore di servizi di hosting ha lo stabilimento principale o in cui il suo rappresentante legale risiede o è stabilito. Qualora una tale richiesta sia formulata l'autorità competente di emissione dovrebbe adottare una decisione sull'inclusione di tale violazione nell'ordine di rimozione. Se tale decisione riscontra tali violazioni, l'ordine di rimozione dovrebbe cessare di avere effetti giuridici. L'esame dovrebbe essere effettuato rapidamente in modo da assicurare che i contenuti erroneamente rimossi o disabilitati siano ripristinati non appena possibile.

([10]) 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).

(21) I prestatori di servizi di hosting che sono esposti a contenuti terroristici dovrebbero includere nelle loro condizioni contrattuali, ove esistano, disposizioni volte a contrastare l'uso improprio dei loro servizi per la diffusione al pubblico di contenuti terroristici. Essi dovrebbero applicare tali disposizioni in maniera diligente, trasparente, proporzionata e non discriminatoria.

(22) In considerazione della portata del problema e della rapidità necessaria per individuare e rimuovere efficacemente i contenuti terroristici, l'adozione di misure specifiche efficaci e proporzionate costituisce un elemento essenziale di contrasto ai contenuti terroristici online. Al fine di ridurre l'accessibilità ai contenuti terroristici nei loro servizi, i prestatori di servizi di hosting esposti a contenuti terroristici dovrebbero adottare misure specifiche tenendo conto dei rischi e del livello di esposizione a contenuti terroristici nonché delle conseguenze sui diritti dei terzi alle informazioni e dell'interesse pubblico. I prestatori di servizi di hosting dovrebbero determinare le misure specifiche appropriate, efficaci e proporzionate da attuare per individuare e rimuovere contenuti terroristici. Le misure specifiche potrebbero includere adeguate misure o capacità tecniche o operative, quali personale o mezzi tecnici per individuare e rimuovere prontamente contenuti terroristici o disabilitare l'accesso ad essi, meccanismi che consentano agli utilizzatori di segnalare o indicare presunti contenuti terroristici, o qualsiasi altra misura che il prestatore di servizi di hosting ritenga appropriata ed efficace per contrastare la disponibilità di contenuti terroristici nei suoi servizi.

(23) Quando attuano misure specifiche, i prestatori di servizi di hosting dovrebbero assicurare che siano preservati il diritto degli utilizzatori alla libertà di espressione e di informazione, nonché la libertà dei media e il loro pluralismo come tutelati dalla Carta. 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, se del caso, misure di salvaguardia, comprese la sorveglianza e le verifiche umane, al fine di evitare decisioni indesiderate o erronee di rimozione o disabilitazione all'accesso di contenuti che non hanno natura terroristica.

(24) Il prestatore di servizi di hosting dovrebbe riferire all'autorità competente in merito alle misure specifiche attuate al fine di consentire a tale autorità di determinare se siano efficaci e proporzionate e se, qualora siano utilizzati strumenti automatizzati, il prestatore di servizi di hosting disponga delle necessarie capacità in materia di sorveglianza e verifiche umane. Nel valutare l'efficacia e la proporzionalità delle misure, le autorità competenti dovrebbero tenere conto dei parametri pertinenti, compresi il numero di ordini di rimozione emessi verso il prestatore di servizi di hosting, le dimensioni e la capacità economica del prestatore di servizi di hosting nonché l'impatto dei suoi servizi sulla diffusione di contenuti terroristici, ad esempio, sulla base del numero di utilizzatori nell'Unione, come pure delle misure di salvaguardia attuate per contrastare l'uso improprio dei suoi servizi ai fini della diffusione di contenuti terroristici online.

(25) Qualora ritenga che le misure specifiche adottate siano insufficienti per far fronte ai rischi, l'autorità competente dovrebbe poter esigere l'adozione di ulteriori misure specifiche appropriate, efficaci e proporzionate. L'obbligo di attuare tali ulteriori misure specifiche non dovrebbe comportare un obbligo generale di sorveglianza o di ricercare attivamente fatti e circostanze, ai sensi dell'articolo 15, paragrafo 1, della direttiva 2000/31/CE, né l'obbligo di utilizzare strumenti automatizzati. I prestatori di servizi di hosting, tuttavia, dovrebbero poter decidere di utilizzare strumenti automatizzati se lo ritengono opportuno e necessario per contrastare efficacemente l'uso improprio dei loro servizi ai fini della diffusione di contenuti terroristici.

(26) 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 periodo 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 dei contenuti terroristici in questione. I relativi dati possono includere dati quali i dati relativi agli abbonati, in particolare i dati relativi all'identità del fornitore di contenuti, nonché i dati relativi agli accessi, tra cui i dati relativi alla data e all'ora di utilizzo da parte del fornitore di contenuti, e 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.

(27) L'obbligo di conservare i contenuti ai fini di un procedimento di controllo amministrativo o giurisdizionale è necessario e giustificato vista la necessità di garantire ricorsi efficaci al fornitore di contenuti il cui contenuto online è stato rimosso o l' accesso al quale è stato disabilitato, e di garantire il ripristino di tali contenuti, in funzione dell'esito di tali procedimenti di controllo. L'obbligo di conservare il materiale a fini di indagine e azione penale è giustificato e necessario in considerazione della potenziale utilità che potrebbe avere il materiale per scardinare o prevenire attività terroristiche. Pertanto, si dovrebbe considerare giustificata anche la conservazione dei contenuti terroristici a fini di prevenzione, accertamento, indagine e perseguimento di reati di terrorismo. I contenuti

terroristici e i relativi dati dovrebbero essere conservati solo per il periodo necessario a consentire alle autorità di contrasto di controllare tali contenuti terroristici e decidere se siano necessari a tali fini. A fini di prevenzione, accertamento, indagine e perseguimento di reati di terrorismo, l'obbligo di conservazione dovrebbe essere limitato ai dati che possono essere correlati a reati di terrorismo e potrebbe pertanto contribuire a perseguire i reati di terrorismo o a prevenire gravi rischi per la sicurezza pubblica. Se i fornitori di servizi di hosting rimuovono o disabilitano l'accesso al materiale, segnatamente a seguito dell'adozione di proprie misure specifiche, dovrebbero informare tempestivamente le autorità competenti in merito ai contenuti in cui sono presenti informazioni che comportano una minaccia imminente per la vita o un presunto reato di terrorismo.

(28) 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 i procedimenti di controllo amministrativo o giurisdizionale 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 competente o dell'organo giurisdizionale, tuttavia tale termine dovrebbe poter essere prorogato del tempo necessario qualora tali procedimenti siano avviati ma non completati entro tale periodo di sei mesi. La durata del periodo di conservazione dovrebbe essere sufficiente per consentire alle autorità di contrasto di conservare il materiale necessario in relazione alle indagini e alle azioni penali, assicurando nel contempo un equilibrio con i diritti fondamentali.

(29) Il presente regolamento non dovrebbe pregiudicare le garanzie procedurali o 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 dal diritto dell'Unione o dal diritto nazionale.

(30) 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 che, a norma del presente regolamento, hanno adottato misure in un determinato anno civile o sono stati tenuti a farlo dovrebbero rendere disponibili al pubblico relazioni annuali sulla trasparenza contenenti informazioni sulle misure adottate per individuare e rimuovere contenuti terroristici.

(31) Le autorità competenti dovrebbero pubblicare relazioni annuali sulla trasparenza contenenti informazioni sul numero di ordini di rimozione, sul numero di casi in cui un ordine non sia stato eseguito, sul numero di decisioni riguardanti misure specifiche, sul numero di casi soggetti a procedimenti di controllo amministrativo o giurisdizionale e sul numero di decisioni che impongono sanzioni.

(32) Il diritto a un ricorso effettivo è sancito dall'articolo 19 del trattato sull'Unione europea (TUE) e dall'articolo 47 della Carta. Ogni persona fisica o giuridica ha diritto a un ricorso effettivo dinanzi ai competenti organi giurisdizionali nazionali contro una qualsiasi delle misure adottate in base al presente regolamento che possa ledere i diritti di tale persona. Tale diritto dovrebbe comprendere, in particolare, la possibilità per i prestatori di servizi di hosting e i fornitori di contenuti di impugnare effettivamente un ordine di rimozione o le decisioni risultanti dall'esame degli ordini di rimozione ai sensi del presente regolamento dinanzi a un organo giurisdizionale dello Stato membro la cui autorità competente ha emesso l'ordine di rimozione o adottato la decisione, nonché per i prestatori di servizi di hosting di impugnare effettivamente una decisione relativa a misure specifiche o sanzioni dinanzi a un organo giurisdizionale dello Stato membro la cui autorità competente ha adottato tale decisione.

(33) Le procedure di reclamo costituiscono una tutela necessaria contro l'erronea rimozione o disabilitazione dell'accesso a contenuti online ove tali contenuti siano 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, e assicurare che siano trattati tempestivamente e in piena trasparenza nei confronti del fornitore di contenuti. L'obbligo del prestatore di servizi di hosting di ripristinare dei contenuti che siano stati erroneamente rimossi o il cui accesso sia stato disabilitato, non dovrebbe pregiudicare la possibilità che il prestatore di servizi di hosting applichi le proprie condizioni contrattuali.

(34) La tutela giurisdizionale effettiva in conformità dell'articolo 19 TUE e dell'articolo 47 della Carta esige che i fornitori di contenuti siano in grado di conoscere il motivo per cui i contenuti che essi forniscono è stato rimosso o il cui accesso è stato disabilitato. A tal fine, il prestatore di servizi di hosting dovrebbe mettere a disposizione del fornitore di contenuti informazioni che gli consentano di impugnare la rimozione o la disabilitazione. A seconda delle circostanze, i prestatori di servizi di hosting potrebbero sostituire i contenuti rimossi o disabilitati con un messaggio indicante che tali contenuti sono stati rimossi o disabilitati in conformità del presente regolamento. Su sua richiesta, il fornitore di contenuti dovrebbe ricevere maggiori informazioni sui motivi della rimozione e della disabilitazione e sui mezzi di ricorso contro la rimozione e la disabilitazione. Le autorità competenti dovrebbero informare il prestatore di servizi di hosting se, per motivi di pubblica sicurezza, in particolare nel contesto di un'indagine, sia inappropriato o controproducente notificare direttamente al fornitore di contenuti la rimozione o la disabilitazione dell'accesso ai contenuti.

(35) Ai fini dell'applicazione del presente regolamento, gli Stati membri dovrebbero designare autorità competenti. Ciò non dovrebbe necessariamente comportare l'istituzione di una nuova autorità e i compiti stabiliti dal presente regolamento dovrebbero poter essere assegnati a un organismo esistente. Il presente regolamento dovrebbe richiedere la designazione delle autorità competenti a emettere ordini di rimozione, esaminare gli ordini di rimozione, vigilare sulle misure specifiche e irrogare sanzioni, mentre ogni Stato membro dovrebbe poter decidere il numero di autorità competenti da designare e la loro natura amministrativa, esecutiva o giurisdizionale. Gli Stati membri dovrebbero garantire che le autorità competenti svolgano i loro compiti in modo obiettivo e non discriminatorio e non sollecitino né accettino istruzioni da alcun altro organismo in merito allo svolgimento dei compiti ai sensi del presente regolamento. Ciò non dovrebbe impedire la supervisione a norma del diritto costituzionale nazionale. Gli Stati membri dovrebbero comunicare l'autorità competente designata a norma del presente regolamento alla Commissione, che dovrebbe pubblicare online un registro elencante le autorità competenti di ciascuno Stato membro. Tale registro online dovrebbe essere facilmente accessibile per agevolare la rapida verifica dell'autenticità degli ordini di rimozione da parte dei prestatori di servizi di hosting.

(36) Al fine di evitare una duplicazione di sforzi ed eventuali interferenze con le indagini e di ridurre al minimo gli oneri a carico dei prestatori di servizi interessati, le autorità competenti dovrebbero scambiarsi informazioni coordinarsi e cooperare reciprocamente e, se del caso, con Europol, prima di emettere ordini di rimozione. Nel decidere sull'emissione di un ordine di rimozione, l'autorità competente dovrebbe prendere in debita considerazione qualsiasi notifica di interferenza con gli interessi di un'indagine (prevenzione di conflittualità). Qualora un'autorità competente sia informata, da parte di un'autorità competente di un altro Stato membro, dell'esistenza di un ordine di rimozione, non dovrebbe essere emesso ordine di rimozione riguardante la stessa materia. Europol potrebbe sostenere l'attuazione delle disposizioni del presente regolamento, nel rispetto del suo attuale mandato e del quadro giuridico esistente.

(37) Per garantire un'attuazione efficace e sufficientemente coerente delle misure specifiche adottate dai prestatori di servizi di hosting, le autorità competenti dovrebbero coordinarsi e cooperare in merito agli scambi che conducono con i prestatori di servizi di hosting per quanto riguarda gli ordini di rimozione e l'individuazione, l'attuazione e la valutazione di misure specifiche. Il coordinamento e la cooperazione sono necessarie anche per quanto riguarda altre misure per attuare il presente regolamento, anche in relazione all'adozione di norme in materia di sanzioni e all'imposizione di sanzioni. La Commissione dovrebbe facilitare tale coordinamento e cooperazione.

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

(39) Per facilitare il rapido scambio tra le autorità competenti nonché con i prestatori di servizi di hosting, e per evitare una duplicazione di sforzi, gli Stati membri dovrebbero essere incoraggiati ad avvalersi degli appositi strumenti sviluppati da Europol, ad esempio l'applicazione di gestione delle segnalazioni su internet attuale o suoi sostituti.

(40) Le segnalazioni da parte degli Stati membri e di Europol si sono dimostrate uno strumento efficace e rapido per sensibilizzare i prestatori di servizi di hosting in merito a contenuti specifici disponibili attraverso i loro servizi e per consentire loro di intervenire rapidamente. Tali segnalazioni, che sono un meccanismo inteso ad allertare i prestatori di servizi di hosting in merito alle informazioni che potrebbero essere considerate essere contenuti terroristici, affinché possano su base volontaria esaminare la compatibilità di tali contenuti con le proprie condizioni contrattuali, dovrebbe rimanere disponibile in aggiunta agli ordini di rimozione. La decisione finale in merito all'opportunità di rimuovere l'informazione, in quanto incompatibile con le proprie condizioni contrattuali, spetta al prestatore di servizi di hosting. Il presente regolamento non dovrebbe incidere sul mandato di Europol, come definito nel regolamento (UE) 2016/794 del Parlamento europeo e del Consiglio ([11]). Pertanto, nessuna disposizione del presente regolamento dovrebbe essere interpretata nel senso che impedisce agli Stati membri e a Europol di utilizzare le segnalazioni come strumento per contrastare i contenuti terroristici online.

(41) Considerata la particolare gravità delle conseguenze di determinati contenuti terroristici online, i prestatori di servizi di hosting dovrebbero informare tempestivamente le pertinenti autorità dello Stato membro interessato, o le autorità competenti dello Stato membro in cui sono stabiliti o hanno un rappresentante legale, in merito ai contenuti terroristici che comportano una minaccia imminente per la vita o un presunto reato di terrorismo. Al fine di garantire la proporzionalità, tale obbligo dovrebbe essere limitato ai reati di terrorismo quali definiti all'articolo 3, paragrafo 1, della direttiva (UE) 2017/541. Tale obbligo di informare non dovrebbe imporre ai prestatori di servizi di hosting l'obbligo di cercare attivamente prove di una tale minaccia imminente per la vita o un presunto reato di terrorismo. Lo Stato membro interessato dovrebbe essere lo Stato membro che ha la competenza giurisdizionale sulle indagini e sull'azione penale nei confronti di tali reati di terrorismo in base alla cittadinanza dell'autore o della vittima potenziale del reato o al luogo interessato dall'atto terroristico. In caso di dubbio, i prestatori di servizi di hosting dovrebbero inviare le informazioni a Europol, che è tenuta a darvi seguito in conformità del suo mandato, anche inoltrando tali informazioni alle autorità nazionali interessate. Le autorità competenti degli Stati membri dovrebbero essere autorizzate a utilizzare tali informazioni per adottare le misure investigative previste dal diritto dell'Unione o nazionale.

(42) I prestatori di servizi di hosting dovrebbero designare o istituire punti di contatto per facilitare il rapido trattamento degli ordini di rimozione. Il punto di contatto dovrebbe assolvere solamente compiti di natura operativa. Il punto di contatto dovrebbe disporre degli strumenti specifici, interni o esternalizzati, che permettono di trasmettere per via elettronica gli ordini di rimozione e delle risorse tecniche o personali che consentono di trattarli rapidamente. Il punto di contatto del prestatore di servizi di hosting non deve necessariamente essere situato nell'Unione. Il prestatore di servizi di hosting dovrebbe essere libero di utilizzare un punto di contatto già esistente ai fini del presente regolamento, a condizione che il punto di contatto sia in grado di svolgere le funzioni previste dal presente regolamento. Al fine di garantire che i contenuti terroristici siano rimossi o che l'accesso sia disattivato entro un'ora dal ricevimento di un ordine di rimozione, è necessario che il punto di contatto dei prestatori di servizi di hosting esposti a contenuti terroristici sia accessibile in qualsiasi momento. 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 delle istituzioni dell'Unione nella quale sono disponibili le loro condizioni contrattuali.

(43) In assenza di un obbligo generale per i prestatori di servizi di hosting 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 il suo rappresentante legale risiede o è stabilito. Ciò dovrebbe lasciare impregiudicate le norme in materia di competenza stabilite ai fini degli ordini di rimozione e delle decisioni risultanti dall'esame degli ordini di rimozione ai sensi del presente regolamento. Anche se un prestatore di servizi di hosting non ha uno stabilimento nell'Unione e non vi ha designato un rappresentante legale, qualsiasi Stato membro dovrebbe comunque avere la giurisdizione e, dunque, poter irrogare sanzioni, a condizione che sia rispettato il principio del *ne bis in idem*.

([11]) 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).

(44) 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. I prestatori di servizi di hosting dovrebbero poter designare, ai fini del presente regolamento, un rappresentante legale già designato per tali fini, a condizione che tale rappresentante legale sia in grado di svolgere le funzioni previste dal presente regolamento. Il rappresentante legale dovrebbe essere autorizzato ad agire per conto del prestatore di servizi di hosting.

(45) Le sanzioni sono necessarie per garantire che i prestatori di servizi di hosting diano effettiva attuazione al presente regolamento. Occorre che gli Stati membri adottino norme relative alle sanzioni, che possono essere di natura amministrativa o penale, nonché, eventualmente, linee guida per il calcolo delle stesse. La mancata conformità in casi individuali potrebbe essere soggetta a sanzioni nel rispetto del principio del *ne bis in idem* e del principio di proporzionalità, assicurando che tali sanzioni tengano conto dell'inosservanza sistematica. Le sanzioni potrebbero assumere forme diverse, tra cui avvertimenti formali in caso di violazioni minori o sanzioni pecuniarie in relazione a violazioni più gravi o sistematiche. Sanzioni particolarmente severe dovrebbero essere inflitte nel caso in cui il prestatore di servizi di hosting ometta in modo sistematico o persistente di rimuovere contenuti terroristici o di disabilitare l'accesso agli stessi entro un'ora dal ricevimento di un ordine di rimozione. Al fine di garantire la certezza del diritto, il presente regolamento dovrebbe stabilire quali violazioni sono soggette a sanzioni e quali circostanze sono pertinenti per valutare la tipologia e il livello di tali sanzioni. Nel determinare se debbano essere inflitte sanzioni pecuniarie si dovrebbe tenere debito conto delle risorse finanziarie del prestatore di servizi di hosting. L'autorità competente dovrebbe altresì considerare se il prestatore di servizi di hosting è una start-up, una microimpresa, o una piccola o media impresa come definita nella raccomandazione 2003/361/CE della Commissione ([12]). Si dovrebbero inoltre considerare ulteriori circostanze, ad esempio se il comportamento del prestatore di servizi di hosting è stato oggettivamente imprudente o riprovevole o se la violazione è stata commessa per negligenza o intenzionalmente. Gli Stati membri dovrebbero assicurare che le sanzioni inflitte per la violazione del presente regolamento non incoraggino la rimozione di materiale che non ha natura terroristica.

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

(47) 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 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 ([13]). 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.

(48) Gli Stati membri dovrebbero raccogliere informazioni sull'attuazione del presente regolamento. Gli Stati membri dovrebbero poter utilizzare le relazioni sulla trasparenza dei prestatori di servizi di hosting integrandole, ove necessario, con informazioni più dettagliate, come ad esempio le proprie relazioni sulla trasparenza ai sensi del presente regolamento. 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 dell'attuazione del presente regolamento.

([12]) Raccomandazione 2003/361/CE della Commissione, del 6 maggio 2003, relativa alla definizione delle microimprese, piccole e medie imprese (GU L 124 del 20.5.2003, pag. 36).

([13]) GU L 123 del 12.5.2016, pag. 1.

(49) 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 entro tre anni dalla data della sua entrata in vigore. La valutazione dovrebbe essere basata sui criteri di efficienza, necessità, efficacia, proporzionalità, pertinenza, coerenza e valore aggiunto dell'Unione. Dovrebbe valutare il funzionamento delle diverse misure operative e tecniche previste dal presente regolamento, in particolare l'efficacia delle misure volte a migliorare l'accertamento, l'individuazione e la rimozione di contenuti terroristici online, l'efficacia dei meccanismi di salvaguardia nonché le potenziali conseguenze per i diritti fondamentali, quali la libertà di espressione e informazione, inclusi la libertà e il pluralismo dei media, la libertà d'impresa e il diritto alla vita privata e alla protezione dei dati personali. La Commissione dovrebbe altresì valutare le potenziali conseguenze per gli interessi di terzi.

(50) Poiché l'obiettivo del presente regolamento, ossia garantire il buon funzionamento del mercato unico digitale mediante il contrasto 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 contrastare l'uso improprio dei servizi di hosting ai fini della diffusione al pubblico di contenuti terroristici online, in particolare su:

a) obblighi di diligenza ragionevoli e proporzionati che i prestatori di servizi di hosting sono tenuti ad applicare per contrastare la diffusione al pubblico di contenuti terroristici tramite i loro servizi e garantirne, ove necessario, la rapida rimozione o la disabilitazione dell'accesso a tali contenuti;

b) misure che gli Stati membri sono tenuti ad attuare, nel rispetto del diritto dell'Unione e fatte salve adeguate salvaguardie a tutela dei diritti fondamentali, in particolare la libertà di espressione e di informazione in una società aperta e democratica, in modo da:

   i) individuare e assicurare la rapida rimozione dei contenuti terroristici da parte dei prestatori di servizi di hosting; e

   ii) facilitare la cooperazione tra le autorità competenti degli Stati membri, i prestatori di servizi di hosting e, se del caso, Europol.

2. Il presente regolamento si applica ai prestatori di servizi di hosting che offrono servizi nell'Unione, indipendentemente dal luogo del loro stabilimento principale, nella misura in cui diffondono informazioni al pubblico.

3. Il materiale diffuso al pubblico per scopi educativi, giornalistici, artistici o di ricerca o a fini di prevenzione o di lotta al terrorismo, compresi i materiali che rappresentano l'espressione di opinioni polemiche o controverse nell'ambito di dibattiti pubblici, non è considerato come integrante contenuti terroristici. Una valutazione accerta il reale scopo di tale diffusione e se il materiale è diffuso al pubblico per tali finalità.

4. Il presente regolamento non ha l'effetto di modificare l'obbligo di rispettare i diritti, le libertà e i principi di cui all'articolo 6 TUE e si applica fatti salvi i principi fondamentali relativi alla libertà di espressione e informazione, compresa la libertà e il pluralismo dei media.

5. Il presente regolamento non pregiudica l'applicazione delle direttive 2000/31/CE e 2010/13/UE. Per quanto riguarda i servizi di media audiovisivi definiti all'articolo 1, paragrafo 1, lettera a), della direttiva 2010/13/UE, prevale la direttiva 2010/13/UE.

Articolo 2

Definizioni

Ai fini del presente regolamento si applicano le definizioni seguenti:

1) «prestatore di servizi di hosting»: un prestatore di servizi di cui all'articolo 1, lettera b), della direttiva 2015/1535 del Parlamento europeo e del Consiglio ([14]) che consistono nel memorizzare le informazioni fornite dal fornitore di contenuti su richiesta di quest'ultimo;

2) «fornitore di contenuti»: un utilizzatore che ha fornito informazioni che sono, o sono state, memorizzate e diffuse al pubblico da un prestatore di servizi di hosting;

3) «diffusione al pubblico »: messa a disposizione di informazioni, su richiesta di un fornitore di contenuti, per un numero potenzialmente illimitato di persone;

4) «offerta di servizi nell'Unione»: consentire a persone fisiche o giuridiche in uno o più Stati membri di utilizzare i servizi di un prestatore di servizi di hosting che presenta un collegamento sostanziale con tale Stato membro o con tali Stati membri;

5) «collegamento sostanziale»: collegamento del prestatore di servizi con uno o più Stati membri che risulti dal suo stabilimento nell'Unione o da specifici criteri di fatto, quali:

   a) avere un numero considerevole di utilizzatori dei suoi servizi in uno o più Stati membri; oppure

   b) l'orientamento delle sue attività verso uno o più Stati membri;

6) «reati di terrorismo»: i reati ai sensi dell'articolo 3 della direttiva (UE) 2017/541;

7) «contenuti terroristici»: uno o più delle seguenti tipologie di materiale, vale a dire materiali che:

   a) istigano alla commissione di uno dei reati di cui all'articolo 3, paragrafo 1, lettere da a) a i), della direttiva (UE) 2017/541, se tali materiali, direttamente o indirettamente, ad esempio mediante l'apologia di atti terroristici, incitano a compiere reati di terrorismo, generando in tal modo il pericolo che uno o più di tali reati siano commessi;

   b) sollecita una persona o un gruppo di persone a commettere o a contribuire a commettere uno dei reati di cui all'articolo 3, paragrafo 1, lettere da a) a i), della direttiva (UE) 2017/541;

   c) sollecita una persona o un gruppo di persone a partecipare alle attività di un gruppo terroristico, ai sensi dell'articolo 4, lettera b);

   d) impartisca istruzioni per la fabbricazione o l'uso di esplosivi, armi da fuoco o altre armi o sostanze nocive o pericolose, ovvero altri metodi o tecniche specifici allo scopo di commettere o contribuire alla commissione di uno dei reati di terrorismo di cui all'articolo 3, paragrafo 1, lettere da a) a i), della direttiva (UE) 2017/541;

   e) costituisca una minaccia di commissione di uno dei reati di cui all'articolo 3, paragrafo 1, lettere da a) a i), della direttiva (UE) 2017/541;

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

8) «condizioni contrattuali»: tutti i termini, 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 dei suoi servizi;

9) «stabilimento principale»: la sede centrale o la sede legale del prestatore di servizi di hosting nella quale sono esercitate le principali funzioni finanziarie ed eseguiti i controlli operativi.

Sezione II

Misure volte a contrastare la diffusione di contenuti terroristici online

Articolo 3

Ordini di rimozione

1. L'autorità competente di ogni Stato membro ha facoltà di emettere un ordine di rimozione imponendo ai prestatori di servizi di rimuovere contenuti terroristici o di disabilitare l'accesso a contenuti terroristici in tutti gli Stati membri.

2. Se l'autorità competente interessata non ha emesso in precedenza un ordine di rimozione nei confronti di un prestatore di servizi di hosting, essa fornisce a tale prestatore di servizi di hosting informazioni sulle procedure e sui termini applicabili almeno 12 ore prima dell'emissione dell'ordine di rimozione.

Il primo comma non si applica tranne in casi di emergenza debitamente giustificati.

3. I prestatori di servizi di hosting rimuovono i contenuti terroristici o disabilitano l'accesso ai contenuti terroristici in tutti gli Stati membri il prima possibile e in ogni caso entro un'ora dal ricevimento dell'ordine di rimozione.

4. Le autorità competenti emettono gli ordini di rimozione utilizzando i modelli di cui all'allegato I. Gli ordini di rimozione recano gli elementi seguenti:

a) dati identificativi dell'autorità competente che emette l'ordine di rimozione e l'autenticazione dell'ordine di rimozione da parte di tale autorità competente;

b) la motivazione, sufficientemente dettagliata, per cui i contenuti sono considerati contenuti terroristici e un riferimento alle pertinenti tipologie di materiale di cui all'articolo 2, punto 7;

c) un indirizzo URL (Uniform Resource Locator) esatto e, se necessario, ulteriori informazioni che consentano di individuare i contenuti terroristici;

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

e) la data, l'ora e la firma elettronica dell'autorità competente che emette l'ordine di rimozione;

f) informazioni facilmente comprensibili sui mezzi di ricorso a disposizione del prestatore di servizi di hosting e del fornitore di contenuti, ivi comprese informazioni sul ricorso all'autorità competente, il ricorso a un organo giurisdizionale nonché sui termini per il ricorso;

g) ove necessario e proporzionato, la decisione di non divulgare informazioni sulla rimozione o sulla disabilitazione dell'accesso ai contenuti terroristici conformemente all'articolo 11, paragrafo 3.

5. L'autorità competente indirizza l'ordine di rimozione allo stabilimento principale del prestatore di servizi di hosting o al suo rappresentante legale in conformità dell'articolo 17.

Tale autorità competente trasmette l'ordine di rimozione al punto di contatto di cui all'articolo 15, paragrafo 1, con mezzi elettronici in grado di produrre 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 ricevimento dell'ordine.

6. Il prestatore di servizi di hosting informa, senza indebito ritardo, l'autorità competente, utilizzando il modello di cui all'allegato II, della rimozione dei contenuti terroristici o della disabilitazione dell'accesso ai contenuti terroristici in tutti gli Stati membri, indicando, in particolare, la data e l'ora della rimozione o disabilitazione.

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, compreso per motivi tecnici o operativi obiettivamente giustificabili, il prestatore di servizi di hosting ne informa, senza indebito ritardo, l'autorità competente che ha emesso l'ordine di rimozione spiegando i motivi, utilizzando il modello di cui all'allegato III.

Il termine di cui al paragrafo 3 decorre dal momento in cui i motivi di cui al primo comma del presente paragrafo vengono meno.

8. Se non è in grado di conformarsi all'ordine di rimozione, in quanto quest'ultimo è viziato da errori manifesti o non contiene informazioni sufficienti per la sua esecuzione, il prestatore di servizi di hosting ne informa, senza indebito ritardo, l'autorità competente che ha emesso l'ordine di rimozione e chiede i chiarimenti necessari, utilizzando il modello di cui all'allegato III.

La scadenza di cui al paragrafo 3 si applica non appena il prestatore di servizi di hosting abbia ricevuto i chiarimenti necessari.

9. Un ordine di rimozione diventa definitivo alla scadenza del termine per il ricorso o quando non è stato presentato alcun ricorso ai sensi del diritto nazionale o se è stato confermato in esito al ricorso.

Quando l'ordine di rimozione diviene definitivo, l'autorità competente che ha emesso l'ordine di rimozione ne informa l'autorità competente di cui all'articolo 12, paragrafo 1, lettera c), dello Stato membro in cui il prestatore di servizi di hosting ha il suo stabilimento principale, o in cui il suo rappresentante legale risiede o è stabilito.

Articolo 4

Procedura per gli ordini di rimozione transfrontalieri

1. Fatto salvo l'articolo 3, se il prestatore di servizi di hosting non ha lo stabilimento principale o il rappresentante legale nello Stato membro dell'autorità competente che emette l'ordine di rimozione, tale autorità trasmette contemporaneamente una copia dell'ordine di rimozione all'autorità competente dello Stato membro in cui il prestatore di servizi di hosting ha lo stabilimento principale o in cui il suo rappresentante legale risiede o è stabilito.

2. Se il prestatore di servizi di hosting riceve un ordine di rimozione di cui al presente articolo, adotta le misure previste dall'articolo 3 e adotta le misure necessarie per poter ripristinare i contenuti o riabilitare l'accesso agli stessi, in conformità del paragrafo 7 del presente articolo.

3. L'autorità competente dello Stato membro in cui il prestatore di servizi di hosting ha lo stabilimento principale o in cui il suo rappresentante legale risiede o è stabilito può, di propria iniziativa, entro 72 ore dal ricevimento della copia dell'ordine di rimozione in conformità del paragrafo 1, esaminare l'ordine di rimozione per stabilire se esso violi in modo grave o manifesto il presente regolamento o i diritti e delle libertà fondamentali garantiti dalla Carta.

Qualora riscontri una violazione, adotta una decisione motivata a tale scopo entro lo stesso termine.

4. Un prestatore di servizi di hosting e un fornitore di contenuti hanno il diritto di presentare, entro 48 ore dal ricevimento dell'ordine di rimozione o delle informazioni a norma dell'articolo 11, paragrafo 2, una richiesta motivata all' autorità competente dello Stato membro in cui il prestatore di servizi di hosting ha lo stabilimento principale o in cui il suo rappresentante legale risiede o è stabilito per esaminare l'ordine di rimozione di cui al primo comma del paragrafo 3 del presente articolo.

Entro 72 ore dal ricevimento della richiesta, l'autorità competente adotta una decisione motivata a seguito dell'esame dell'ordine di rimozione, in cui espone le proprie conclusioni sull'esistenza di una violazione.

5. Prima di adottare una decisione a norma del paragrafo 3, secondo comma, o una decisione che riconosce una violazione a norma del paragrafo 4, secondo comma, l'autorità competente informa l'autorità competente che ha emesso l'ordine di rimozione della sua intenzione di adottare la decisione e delle relative motivazioni.

6. Qualora l'autorità competente dello Stato membro in cui il prestatore di servizi di hosting ha lo stabilimento principale o in cui il suo rappresentante legale risiede o è stabilito adotti una decisione motivata in conformità del paragrafo 3 o 4 del presente articolo, comunica senza indugio tale decisione all'autorità competente che ha emesso l'ordine di rimozione, al prestatore di servizi di hosting, al fornitore di contenuti che ha richiesto l'esame ai sensi del paragrafo 4 del presente articolo e, conformemente all'articolo 14, a Europol. Se la decisione accerta violazioni ai sensi del paragrafo 3 o 4 del presente articolo, l'ordine di rimozione cessa di avere effetti giuridici.

7. Non appena riceve una decisione che rileva una violazione comunicata in conformità del paragrafo 6, il prestatore di servizi di hosting interessato ripristina immediatamente i contenuti o l'accesso agli stessi, fatta salva la possibilità di applicare le proprie condizioni contrattuali conformemente al diritto dell'Unione e nazionale.

Articolo 5

Misure specifiche

1. Un prestatore di servizi di hosting esposto a contenuti terroristici di cui al paragrafo 4, include, ove applicabile, nelle sue condizioni contrattuali e applica disposizioni volte a contrastare l'uso improprio dei suoi servizi per la diffusione al pubblico di contenuti terroristici.

Esso agisce in modo diligente, proporzionato e non discriminatorio, presta debito rispetto, in tutte le circostanze, ai diritti fondamentali degli utilizzatori e tenendo conto, in particolare, della fondamentale importanza che riveste la libertà di espressione e di informazione in una società aperta e democratica, al fine di evitare la rimozione di contenuti che non siano di natura terroristica.

2. Un prestatore di servizi di hosting esposto a contenuti terroristici di cui al paragrafo 4, adotta misure specifiche per proteggere i propri servizi dalla diffusione al pubblico di contenuti terroristici.

La decisione in merito alla scelta delle misure specifiche spetta al prestatore di servizi di hosting. Tali misure possono comprendere una o più delle misure seguenti:

a) adeguate misure o capacità tecniche e operative, quali personale o mezzi tecnici adeguati per individuare e rimuovere rapidamente o disabilitare l'accesso a contenuti terroristici;

b) meccanismi facilmente accessibili e di facile uso per consentire agli utilizzatori di segnalare o indicare al prestatore di servizi di hosting presunti contenuti terroristici;

c) qualsiasi altro meccanismo per sensibilizzare maggiormente in merito ai contenuti terroristici nei suoi servizi, quali i meccanismi di moderazione per l'utilizzatore;

d) qualsiasi altra misura che il prestatore di servizi di hosting ritenga appropriata per contrastare la disponibilità di contenuti terroristici nei suoi servizi.

3. Le misure specifiche devono soddisfare tutti i requisiti seguenti:

a) devono essere efficaci per mitigare il livello di esposizione dei servizi di un prestatore di servizi di hosting a contenuti terroristici;

b) devono essere mirate e proporzionate, tenuto conto, in particolare, della gravità del livello di esposizione di un prestatore di servizi di hosting a contenuti terroristici, nonché delle capacità tecniche e operative, della solidità finanziaria, del numero di utilizzatori del prestatore di servizi di hosting e della quantità di contenuti forniti;

c) devono essere applicate in una maniera che tenga pienamente conto dei diritti e degli interessi legittimi degli utilizzatori, in particolare dei diritti fondamentali degli utilizzatori relativi alla libertà di espressione e di informazione, al rispetto della vita privata e alla protezione dei dati personali;

d) devono essere applicate in maniera diligente e non discriminatoria.

Qualora le misure specifiche comportino l'uso di misure tecniche, sono fornite salvaguardie adeguate ed efficaci, in particolare attraverso la sorveglianza e le verifiche umane, per garantire l'accuratezza ed evitare la rimozione di materiale che non sono contenuti terroristici.

4. Un prestatore di servizi di hosting è esposto a contenuti terroristici se l'autorità competente dello Stato membro in cui ha lo stabilimento principale o in cui il suo rappresentante legale risiede o è stabilito:

a) ha adottato una decisione basata su fattori oggettivi, come il ricevimento da parte del prestatore di servizi di hosting di due o più ordini di rimozione definitivi nei 12 mesi precedenti, che ha stabilito che il prestatore di servizi di hosting è esposto a contenuti terroristici; e

b) ha notificato la decisione di cui alla lettera a) al prestatore di servizi di hosting.

5. Dopo aver ricevuto una decisione di cui al paragrafo 4 o, se del caso, al paragrafo 6, un prestatore di servizi di hosting riferisce all'autorità competente in merito alle misure specifiche che ha adottato e che intende adottare per conformarsi ai paragrafi 2 e 3. Lo fa entro tre mesi dal ricevimento della decisione e successivamente su base annuale. Tale obbligo cessa una volta che l'autorità competente abbia deciso, su richiesta ai sensi del paragrafo 7, che il prestatore di servizi di hosting non è più esposto a contenuti terroristici.

6. Se, sulla base delle relazioni di cui al paragrafo 5 e, se del caso, di altri fattori oggettivi, l'autorità competente ritiene che le misure specifiche adottate non soddisfino le prescrizioni di cui ai paragrafi 2 e 3, tale autorità competente indirizza al prestatore di servizi di hosting una decisione che gli impone di adottare le misure necessarie per garantire il rispetto dei paragrafi 2 e 3.

Il prestatore di servizi di hosting può decidere la tipologia di misure specifiche da adottare.

7. Un prestatore di servizi di hosting può, in qualsiasi momento, chiedere all'autorità competente il riesame e, eventualmente, la modifica o la revoca delle decisioni di cui, rispettivamente, al paragrafo 4 o 6.

Entro tre mesi dal ricevimento della richiesta, l'autorità competente adotta una decisione motivata in merito alla richiesta basata su fattori oggettivi e la notifica al prestatore di servizi di hosting.

8. L'obbligo di adottare misure specifiche lascia impregiudicato l'articolo 15, paragrafo1, della direttiva 2000/31/CE e non comporta l'obbligo generale per i prestatori di servizi di hosting di sorvegliare le informazioni che trasmettono o memorizzano, né l'obbligo generale di ricercare attivamente fatti o circostanze che indichino la presenza di attività illecite.

L'obbligo di adottare misure specifiche non comporta l'obbligo per i prestatori di servizi di hosting di utilizzare strumenti automatizzati.

Articolo 6

Conservazione dei contenuti e dei relativi dati

1. I prestatori di servizi di hosting conservano i contenuti terroristici rimossi o il cui accesso è stato disabilitato a seguito di un ordine di rimozione o di misure specifiche in conformità dell'articolo 3 o 5, come pure i relativi dati rimossi in conseguenza della rimozione di tali contenuti terroristici e che sono necessari per:

a) i procedimenti di ricorso amministrativo o giurisdizionale, la gestione dei reclami ai sensi dell'articolo 10 contro una decisione di rimuovere o di disabilitare l'accesso ai contenuti terroristici e i relativi dati;

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 dalla rimozione o dalla disabilitazione. Su richiesta dell'autorità competente o di un organo giurisdizionale, i contenuti terroristici sono conservati per un periodo ulteriore specificato solo se necessario e per tutto il tempo richiesto per il procedimento di ricorso amministrativo o giurisdizionale 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 del paragrafo 1 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 7

Obblighi di trasparenza per i prestatori di servizi di hosting

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

2. Un prestatore di servizi di hosting che, a norma del presente regolamento, abbia adottato misure contro la diffusione di contenuti terroristici in un determinato anno civile o sia stato tenuto a farlo, rende disponibile al pubblico una relazione sulla trasparenza in merito a tali azioni per tale anno. Pubblica tale relazione prima del 1° marzo dell'anno seguente.

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

a) informazioni sulle misure intraprese dal prestatore di servizi di hosting per quanto concerne l'individuazione e la rimozione o la disabilitazione dell'accesso a contenuti terroristici;

b) informazioni sulle misure intraprese dal prestatore di servizi di hosting per contrastare la ricomparsa online di materiale che in precedenza sia stato rimosso o il cui accesso è stato disabilitato perché era stato considerato come integrante contenuti terroristici, in particolare ove siano stati utilizzati strumenti automatizzati;

c) il numero di elementi integranti contenuti terroristici che sono stati rimossi o il cui accesso è stato disabilitato, a seguito di ordini di rimozione o misure specifiche e il numero di ordini di rimozione i cui contenuti non sono stati rimossi, o il cui accesso non è stato disabilitato, a norma dell'articolo 3, paragrafo 7, primo comma, e dell'articolo 3, paragrafo 8, primo comma, unitamente ai relativi motivi;

d) il numero e l'esito dei reclami trattati dal prestatore di servizi di hosting, in conformità dell'articolo 10;

e) il numero e l'esito dei procedimenti di ricorso giurisdizionale o amministrativo avviati dal prestatore di servizi di hosting;

f) il numero di casi in cui quest'ultimo è stato tenuto a ripristinare i contenuti, o l'accesso agli stessi, a seguito di procedimenti di ricorso giurisdizionale o amministrativo;

g) il numero di casi in cui il prestatore di servizi di hosting ha ripristinato i contenuti, o l'accesso agli stessi, dopo aver esaminato un reclamo da parte del fornitore di contenuti.

Articolo 8

Relazioni sulla trasparenza delle autorità competenti

1. Le autorità competenti pubblicano relazioni annuali sulla trasparenza relative alle loro attività a norma del presente regolamento. Tali relazioni contengono almeno le seguenti informazioni relative all'anno civile considerato:

a) il numero di ordini di rimozione emessi a norma dell'articolo 3, specificando il numero di ordini di rimozione soggetti all'articolo 4, paragrafo 1, il numero di ordini di rimozione esaminati a norma dell'articolo 4, e le informazioni relative all'attuazione di tali ordini di rimozione da parte dei prestatori di servizi di hosting interessati, compreso il numero di casi di rimozione di contenuti terroristici, o di disabilitazione dell'accesso ad essi, e il numero di casi di mancata rimozione di contenuti terroristici, o di mancata disabilitazione dell'accesso ad essi;

b) il numero di decisioni adottate conformemente all'articolo 5, paragrafi 4, 6 o 7, e informazioni sull'attuazione di tali decisioni dai prestatori di servizi di hosting, compresa una descrizione delle misure specifiche;

c) il numero di casi in cui gli ordini di rimozione e le decisioni adottate conformemente all'articolo 5, paragrafi 4 e 6, sono stati oggetto di un procedimento di controllo amministrativo o giurisdizionale e informazioni sull'esito del relativo procedimento;

d) il numero di decisioni che irrogano sanzioni ai sensi dell'articolo 18, e una descrizione del tipo di sanzione inflitta.

2. Le relazioni annuali sulla trasparenza di cui al paragrafo 1 non includono informazioni che possono arrecare pregiudizio alle attività in corso per la prevenzione, l'accertamento, l'indagine o il perseguimento di reati di terrorismo o per interessi di sicurezza nazionale.

Articolo 9

Ricorso effettivo

1. I prestatori di servizi di hosting che hanno ricevuto un ordine di rimozione emesso a norma dell'articolo 3, paragrafo 1 o una decisione a norma dell'articolo 4, paragrafo 4, o dell'articolo 5, paragrafi 4, 6 o 7, hanno diritto a un ricorso effettivo. Tale diritto include il diritto di impugnare tale ordine di rimozione dinanzi agli organi giurisdizionali dello Stato membro dell'autorità competente che ha emesso l'ordine di rimozione, e il diritto di impugnare la decisione a norma dell'articolo 4, paragrafo 4, o dell'articolo 5, paragrafi 4, 6 o 7, dinanzi agli organi giurisdizionali dello Stato membro dell'autorità competente che ha adottato la decisione.

2. I fornitori di contenuti i cui contenuti siano stati rimossi o l'accesso ai quali sia stato disabilitato a seguito di un ordine di rimozione hanno diritto a un ricorso effettivo. Tale diritto include il diritto di impugnare un ordine di rimozione emesso a norma dell'articolo 3, paragrafo 1, dinanzi agli organi giurisdizionali dello Stato membro dell'autorità competente che ha emesso l'ordine di rimozione, e il diritto di impugnare la decisione a norma dell'articolo 4, paragrafo 4, dinanzi agli organi giurisdizionali dello Stato membro dell'autorità competente che ha adottato la decisione.

3. Gli Stati membri mettono in atto procedure efficaci per l'esercizio dei diritti di cui al presente articolo.

Articolo 10

Meccanismi di reclamo

1. Ciascun prestatore di servizi di hosting predispone un meccanismo efficace e accessibile che consente ai fornitori di contenuti i cui contenuti siano stati rimossi o l'accesso ai quali sia stato disabilitato a seguito di misure specifiche a norma dell'articolo 5 di presentare un reclamo nei confronti di tale rimozione o disabilitazione, chiedendo la reintegrazione dei contenuti o del relativo accesso.

2. Ciascun prestatore di servizi di hosting esamina tempestivamente ogni reclamo che riceve il meccanismo di cui al paragrafo 1 e ripristina i contenuti o il relativo accesso senza indebito ritardo se la rimozione o la disabilitazione si rivela ingiustificata. Esso informa l'autore del reclamo delle conclusioni del reclamo entro due settimane dal ricevimento dello stesso.

Qualora il reclamo sia rigettato, il prestatore di servizi di hosting fornisce al reclamante i motivi della propria decisione.

Il ripristino dei contenuti o dell'accesso allo stesso non osta all'avvio di procedimenti di controllo amministrativi o giurisdizionali che impugnino la decisione del prestatore di servizi di hosting o dell'autorità competente.

Articolo 11

Informazioni ai fornitori di contenuti

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

2. Su richiesta del fornitore di contenuti, il prestatore di servizi di hosting comunica i motivi della rimozione o della disabilitazione al fornitore di contenuti e lo informa dei diritti di ricorso contro l'ordine di rimozione o gli fornisce copia dell'ordine di rimozione.

3. L'obbligo previsto ai paragrafi 1 e 2 non si applica se l'autorità competente che emette l'ordine di rimozione decide che è necessario e proporzionato, che la motivazione non sia divulgata per motivi 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 sei settimane dalla suddetta 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.

Tale autorità competente può prorogare tale termine di ulteriori sei settimane, ove tale non divulgazione continui a essere giustificata.

Sezione IV

Autorità competenti e cooperazione

Articolo 12

Designazione delle autorità competenti

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

a) emette ordini di rimozione a norma dell'articolo 3;

b) esaminare ordini di rimozione a norma dell'articolo 4;

c) sorvegliare l'attuazione delle misure specifiche a norma dell'articolo 5;

d) irrogare sanzioni a norma dell'articolo 18.

2. Ciascuno Stato membro si assicura che sia designato o istituito un punto di contatto in seno all'autorità competente di cui al paragrafo 1, lettera a), per trattare le richieste di chiarimenti e di riscontro in relazione agli ordini di rimozione emessi da tale autorità competente.

Gli Stati membri si assicurano che le informazioni relative al punto di contatto siano rese pubbliche.

3. Entro il … [dodici mesi dall'entrata in vigore del presente regolamento] gli Stati membri notificano alla Commissione l'autorità o le autorità competenti di cui al paragrafo 1 e ogni relativa modifica. La Commissione pubblica la notifica e le eventuali relative modifiche nella *Gazzetta ufficiale dell'Unione europea*.

4. Entro il … [dodici mesi dall'entrata in vigore del presente regolamento] la Commissione istituisce un registro online che elenca le autorità competenti di cui al paragrafo 1 e il punto di contatto designato o istituito a norma del paragrafo 2 per ciascuna autorità competente. La Commissione pubblica periodicamente tutte le relative modifiche.

Articolo 13

Autorità competenti

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

2. Gli Stati membri provvedono affinché le rispettive autorità competenti svolgano i loro compiti ai sensi del presente regolamento in modo obiettivo, non discriminatorio e nel pieno rispetto dei diritti fondamentali. Le autorità competenti non sollecitano né accettano istruzioni da alcun altro organismo in merito allo svolgimento dei loro compiti a norma dell'articolo 12, paragrafo 1.

Il primo comma del presente paragrafo non osta alla supervisione a norma del diritto costituzionale nazionale.

Articolo 14

Cooperazione tra i prestatori di servizi di hosting, le autorità competenti e Europol

1. Le autorità competenti scambiano informazioni, si coordinano e cooperano tra loro e, se del caso, con Europol, per quanto riguarda gli ordini di rimozione, in particolare, in modo da evitare una duplicazione di sforzi, 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 le autorità competenti di cui all'articolo 12, paragrafo 1, lettere c) e d), per quanto riguarda le misure specifiche adottate a norma dell'articolo 5, e le sanzioni inflitte a norma dell'articolo 18. Gli Stati membri provvedono a che le autorità competenti di cui all'articolo 12, paragrafo 1, lettere c) e d), siano in possesso di tutte le informazioni pertinenti.

3. Ai fini del paragrafo 1, gli Stati membri predispongono canali e meccanismi di comunicazione adeguati e sicuri per garantire che le informazioni pertinenti siano scambiate tempestivamente.

4. Ai fini dell'efficace attuazione del presente regolamento, nonché per evitare una duplicazione di sforzi, gli Stati membri e i prestatori di servizi di hosting possono avvalersi di appositi strumenti, inclusi […] quelli stabiliti […] da Europol, per facilitare in particolare:

a) il trattamento dei dati e il riscontro relativi agli ordini di rimozione a norma dell'articolo 3; e

b) la cooperazione allo scopo di individuare ed attuare misure specifiche a norma dell'articolo 5.

5. Laddove sia a conoscenza di contenuti terroristici che comportano una minaccia imminente per la vita, il prestatore di servizi di hosting ne informa immediatamente l'autorità competente per l'indagine e il perseguimento di reati negli Stati membri *interessati*. Ove non sia possibile individuare gli Stati membri interessati, il prestatore di servizi di hosting informa il punto di contatto a norma dell'articolo 12, paragrafo 2, dello Stato membro in cui ha lo stabilimento principale o in cui il suo rappresentante legale risiede o è stabilito e trasmette le informazioni relative ai contenuti terroristici a Europol, che vi darà adeguato seguito.

6. Le autorità competenti sono incoraggiate a inviare copie degli ordini di rimozione a Europol, per permettergli così di presentare una relazione annuale comprensiva di un'analisi dei tipi di contenuti terroristici oggetto di ordini di rimozione o di disabilitazione dell'accesso a norma del presente regolamento.

Articolo 15

Punti di contatto dei prestatori di servizi di hosting

1. Ciascun prestatore di servizi di hosting designa o istituisce un punto di contatto per la ricezione degli ordini di rimozione per via elettronica e per il rapido trattamento ai sensi degli articoli 3 e 4. Il prestatore di servizi di hosting provvede affinché le informazioni relative al punto di contatto siano disponibili al pubblico.

2. Le informazioni di cui al paragrafo 1 del presente articolo precisano le lingue ufficiali delle istituzioni dell'Unione, di cui al regolamento 1/58 ([15]), nelle quali è possibile rivolgersi al punto di contatto e nelle quali avvengono gli ulteriori scambi relativi agli ordini di rimozione a norma dell'articolo 3. 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 il suo rappresentante legale risiede o è stabilito.

([15]) Regolamento n. 1 che determina le lingue che devono essere usate dalla Comunità economica europea (GU P 17 del 6.10.1958, pag. 385).

Sezione V

Attuazione ed esecuzione

Articolo 16

Competenza

1. Lo Stato membro nel quale il prestatore di servizi di hosting ha lo stabilimento principale è competente ai fini degli articoli 5, 18 e 21. Il prestatore di servizi di hosting che non ha il proprio stabilimento principale nell'Unione è considerato soggetto alla competenza dello Stato membro in cui il suo rappresentante legale risiede o è stabilito.

2. Laddove il prestatore di servizi di hosting che non ha il suo stabilimento principale nell'Unione ometta di designare un rappresentante legale, tutti gli Stati membri sono competenti.

3. Laddove un'autorità competente di uno Stato membro eserciti la propria competenza a norma del paragrafo 2, ne informa le autorità competenti di tutti gli altri Stati membri.

Articolo 17

Rappresentante legale

1. Il prestatore di servizi di hosting che non ha il proprio stabilimento principale nell'Unione designa, per iscritto, una persona fisica o giuridica quale suo rappresentante legale nell'Unione ai fini del ricevimento, dell'attuazione e dell'esecuzione degli ordini di rimozione, e delle decisioni emesse dalle autorità competenti.

2. Il prestatore di servizi di hosting conferisce al proprio rappresentante legale i poteri e le risorse necessari per ottemperare a tali ordini di rimozione e decisioni e per cooperare con le autorità competenti.

Il rappresentante legale risiede o è stabilito in uno degli Stati membri in cui il prestatore di servizi di hosting offre i propri servizi.

3. Il rappresentante legale può essere ritenuto responsabile per le violazioni del presente regolamento, fatte salve le responsabilità e le azioni legali del prestatore di servizi di hosting.

4. Il prestatore di servizi di hosting informa della designazione l'autorità competente di cui all'articolo 12, paragrafo 1, lettera d), dello Stato membro in cui il suo rappresentante legale risiede o è stabilito.

Il prestatore di servizi di hosting rende pubbliche le informazioni relative al rappresentante legale.

Sezione VI

Disposizioni finali

Articolo 18

Sanzioni

1. Gli Stati membri stabiliscono le norme relative alle sanzioni applicabili alle violazioni del presente regolamento da parte dei prestatori di servizi di hosting e adottano tutte le misure necessarie per assicurarne l'applicazione. Tali sanzioni sono limitate a contrastare le violazioni degli articoli seguenti: articolo 3, paragrafi 3 e 6, articolo 4, paragrafi 2 e 7, articolo 5 paragrafi 1, 2, 3 5 e 6, articoli 6, 7, 10 e 11, articolo 14, paragrafo 5, articolo 15, paragrafo 1 e articolo 17.

Le sanzioni di cui al primo comma sono effettive, proporzionate e dissuasive. Gli Stati membri notificano tali norme e misure alla Commissione, entro il … [12 mesi dall'entrata in vigore del presente regolamento], e provvedono poi a dare immediata notifica delle eventuali modifiche successive.

2. Gli Stati membri provvedono a che, nello stabilire se imporre o meno una sanzione e nel determinare il tipo e il livello della sanzione, le autorità competenti tengano conto di tutte le circostanze pertinenti, tra cui:

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

b) l'eventuale carattere doloso o colposo della violazione;

c) precedenti violazioni da parte del prestatore di servizi di hosting;

d) la solidità finanziaria del prestatore di servizi di hosting;

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

f) la natura e le dimensioni del prestatore di servizi di hosting, in particolare se si tratta di una microimpresa, o di una piccola o media impresa;

g) il grado di colpa del prestatore di servizi di hosting, tenuto conto delle misure tecniche e organizzative adottate dal prestatore di servizi di hosting per conformarsi al presente regolamento.

3. Gli Stati membri provvedono a che la sistematica o persistente inosservanza degli obblighi ai sensi dell'articolo 3, paragrafo 3, sia passibile di sanzioni pecuniarie fino al 4% del fatturato mondiale del prestatore di servizi di hosting del precedente esercizio finanziario.

Articolo 19

Requisiti tecnici e modifiche degli allegati

1. Alla Commissione è conferito il potere di adottare atti delegati conformemente all'articolo 20 al fine di integrare nel presente regolamento i necessari 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 atti delegati conformemente all'articolo 20 per modificare gli allegati al fine di rispondere efficacemente all'eventuale necessità di migliorare il contenuto dei modelli degli ordini di e per fornire informazioni sull'impossibilità di dare esecuzione agli ordini 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 indeterminato a decorrere dal … [un anno dalla data di entrata in vigore 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 nell'anno civile precedente e le trasmettono alla Commissione ogni anno entro il 31 marzo. Tali informazioni riguardano:

a) il numero di ordini di rimozione emessi, il numero di elementi integranti contenuti terroristici che sono stati rimossi o il cui accesso è stato disabilitato, nonché le tempistiche di rimozione e disabilitazione;

b) le misure specifiche adottate a norma dell'articolo 5, compresa la quantità di elementi integranti contenuti terroristici che è stata rimossa o il cui accesso è stato disabilitato, nonché le tempistiche della rimozione e della disabilitazione;

c) il numero di richieste di accesso emesse dalle autorità competenti riguardanti i contenuti conservati dai prestatori di servizi di hosting a norma dell'articolo 6;

d) il numero di procedimenti di reclamo avviati e le azioni intraprese dai prestatori di servizi di hosting a norma dell'articolo 10;

e) il numero di procedimenti di controllo amministrativo o giurisdizionale avviati e le decisioni adottate dalle autorità competenti in conformità del diritto nazionale.

2. Entro il … [due anni dalla data di entrata in vigore 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 il ... [due anni dall'entrata in vigore del presente regolamento], la Commissione presenta al Parlamento europeo e al Consiglio una relazione sull'applicazione del presente regolamento. Tale relazione comprende le 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 redazione della relazione.

Articolo 23

Valutazione

Entro il … [tre anni dopo la data di entrata in vigore del presente regolamento], la Commissione procede a una valutazione del presente regolamento e trasmette al Parlamento europeo e al Consiglio una relazione sulla sua applicazione, compresi:

a) il funzionamento e l'efficacia dei meccanismi di salvaguardia, in particolare di quelli previsti dall'articolo 4, paragrafo 4, dall'articolo 6, paragrafo 3 e dagli articoli da 7 a 11;

b) l'impatto dell'applicazione del presente regolamento sui diritti fondamentali, in particolare la libertà di espressione e di informazione, il rispetto della vita privata e la protezione dei dati personali; e

c) il contributo del presente regolamento alla protezione della sicurezza pubblica.

Se opportuno, la relazione è accompagnata da proposte legislative.

Gli Stati membri trasmettono alla Commissione le informazioni necessarie per la redazione della relazione.

La Commissione valuta inoltre la necessità e la fattibilità dell'istituzione di una piattaforma europea sui contenuti terroristici online per facilitare la comunicazione e la cooperazione a norma del presente regolamento.

Articolo 24

Entrata in vigore e applicazione

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

Esso si applica a decorrere dal … [12 mesi dopo l'entrata in vigore del presente regolamento].

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

Fatto a …, il

Per il Parlamento europeo	*Per il Consiglio*
Il presidente	*Il presidente*
…	…

ALLEGATO I

ORDINE DI RIMOZIONE

(articolo 3 del regolamento (UE) 2021/ … del Parlamento europeo e del Consiglio ([1]) ([*]))

A norma dell'articolo 3 del regolamento (UE) 2021/… ([*])(«regolamento ») il destinatario del presente ordine di rimozione deve rimuovere i contenuti terroristici o disabilitare l'accesso ai contenuti terroristici in tutti gli Stati membri al più presto possibile e, in ogni caso,. entro un'ora dal ricevimento dell'ordine di rimozione.

A norma dell'articolo 6 del regolamento, i destinatari sono tenuti a conservare i contenuti e i relativi dati che sono stati rimossi o resi inaccessibili per un periodo di sei mesi o, su richiesta dell'autorità competente o di un organo giurisdizionale, per un periodo più lungo.

A norma dell'articolo 15, paragrafo 2, del regolamento il presente ordine di rimozione è inviato in una delle lingue indicate dal destinatario.

SEZIONE A:

Stato membro dell'autorità competente di emissione: …

……

NB: i dettagli relativi all'autorità competente di emissione vanno indicati nelle sezioni E ed F

Destinatario e, se del caso, rappresentante legale:

……

Punto di contatto:

……

Stato membro in cui il prestatore di servizi di hosting ha il suo stabilimento principale, o in cui il suo rappresentante legale risiede o è stabilito:

……

Data e ora di emissione dell'ordine di rimozione:

……

Numero di riferimento dell'ordine di rimozione:

……

([1]) Regolamento (UE) 2021/ … ([*]) del Parlamento europeo e del Consiglio relativo al contrasto della diffusione di contenuti terroristici online (GU L…).

([*]) Numero del regolamento contenuto nel documento ST 14308/20 [2018/0331 (COD)].

SEZIONE B: Contenuto terroristico da rimuovere o cui disabilitare l'accesso in tutti gli Stati membri al più presto possibile e in ogni caso entro un'ora dal ricevimento dell'ordine di rimozione:

Indirizzo URL e ulteriori informazioni che consentano di individuare e localizzare con esattezza i contenuti terroristici:

……

Motivi per cui il materiale è considerato come integrante contenuti terroristici ai sensi dell'articolo 2, punto 7, del regolamento.

Il materiale (spuntare le caselle pertinenti):

☐ istiga alla commissione di reati di terrorismo, anche mediante l'apologia del terrorismo, incitando alla commissione di reati di terrorismo (articolo 2, punto 7, lettera a), del presente regolamento)

☐ sollecita altri a commettere o a contribuire alla commissione di reati di terrorismo (articolo 2, punto 7, lettera b) del presente regolamento)

☐ sollecita altri a partecipare alle attività di un gruppo terroristico, (articolo 2, punto 7, lettera c) del presente regolamento)

☐ impartisce istruzioni per la fabbricazione o l'uso di esplosivi, armi da fuoco o altre armi o sostanze nocive o pericolose, ovvero altri metodi o tecniche specifici allo scopo di commettere o contribuire a commettere reati di terrorismo (articolo 2, punto 7, del presente regolamento)

☐ costituisce una minaccia di commissione di reati di terrorismo (articolo 2, punto 7, lettera e), del presente regolamento).

Informazioni supplementari sui motivi per cui il materiale è considerato come integrante contenuti terroristici:

……

……

……

SEZIONE C: Informazioni per il fornitore di contenuti

Si fa presente che (spuntare la casella, se pertinente):

☐ per motivi di pubblica sicurezza, il destinatario deve astenersi dall'informare il fornitore di contenuti della rimozione o della disabilitazione dell'accesso ai contenuti terroristici

Se la casella non è pertinente, cfr. sezione G per le informazioni circa le possibilità di ricorso contro l'ordine di rimozione nello Stato membro dell'autorità competente di emissione in base al diritto nazionale (una copia dell'ordine di rimozione deve essere inoltrato al fornitore di contenuti, su sua richiesta)

SEZIONE D: Informazioni all'autorità competente dello Stato membro in cui il prestatore di servizi di hosting ha il suo stabilimento principale o in cui il suo rappresentante legale risiede o è stabilito

Spuntare le caselle pertinenti:

☐ lo Stato membro in cui il prestatore di servizi di hosting, o in cui il suo rappresentante legale ha il suo stabilimento principale, o in cui il suo rappresentante legale risiede o è stabilito, è diverso dallo Stato membro dell'autorità competente di emissione

☐ una copia dell'ordine di rimozione è inviata all'autorità competente dello Stato membro in cui il prestatore di servizi di hosting ha il suo stabilimento principale o in cui il suo rappresentante legale risiede o è stabilito

SEZIONE E: Dettagli relativi all'autorità competente di emissione

Tipo (spuntare la casella pertinente):

☐ giudice, organo giurisdizionale o magistrato inquirente

☐ autorità di contrasto

☐ altra autorità competente → compilare anche la sezione F

Dettagli relativi all'autorità competente di emissione o al suo rappresentante che certifica che l'ordine di rimozione è accurato e corretto:

Denominazione dell'autorità di emissione competente: …

……

Nome del suo rappresentante e funzione ricoperta (titolo e grado):

……

Numero di fascicolo: ……

Indirizzo e-mail: ……

Tel.: (prefisso internazionale) (prefisso urbano) ……

Fax: (prefisso internazionale) (prefisso urbano) ……

E-mail: ……

Data: ……

Timbro ufficiale (se disponibile) e firma ([2]): ……

([2]) La firma non è necessaria se l'ordine di rimozione è trasmesso tramite canali autenticati che possono garantire l'autenticità dell'ordine di rimozione.

SEZIONE F: Dati di contatto per il follow-up

Dati di contatto dell'autorità competente di emissione per il riscontro sull'ora della rimozione o della disabilitazione dell'accesso, o per la trasmissione di ulteriori chiarimenti:

……

Dati di contatto dell'autorità competente dello Stato membro in cui il fornitore di servizi di hosting ha lo stabilimento principale o in cui risiede o ha lo stabilimento il suo rappresentante legale:

……

SEZIONE G: Informazioni sulle possibilità di ricorso

Informazioni relative all'organismo o all'organo giurisdizionale competente, ai termini e alle procedure per impugnare l'ordine di rimozione:

Organismo o organo giurisdizionale competente innanzi al quale l'ordine di rimozione può essere impugnato:

……

Termine per impugnare l'ordine di rimozione:

[giorni/mesi a decorrere dal]

……

Link alle disposizioni della legislazione nazionale:

……

ALLEGATO II

RISCONTRO A SEGUITO DELLA RIMOZIONE O DELLA DISABILITAZIONE DELL'ACCESSO A CONTENUTI TERRORISTICI

(articolo 3, paragrafo 6, del regolamento (UE) 2021/ … del Parlamento europeo e del Consiglio ([1]) ([*]))

SEZIONE A:

Destinatario dell'ordine di rimozione:

……

Autorità competente che ha emesso l'ordine di rimozione:

……

Riferimento del fascicolo dell'autorità competente che ha emesso l'ordine di rimozione:

……

Riferimento del fascicolo del destinatario:

……

Data e ora di ricevimento dell'ordine di rimozione:

……

SEZIONE B: Misure adottate in esecuzione dell'ordine di rimozione

(spuntare la casella pertinente):

☐ i contenuti terroristici sono stati rimossi

☐ l'accesso ai contenuti terroristici è stato disabilitato in tutti gli Stati membri

Ora e data della misura adottata:

……

([1]) Regolamento (UE) 2021/ … ([*]) del Parlamento europeo e del Consiglio relativo al contrasto della diffusione di contenuti terroristici online (GU L …).

([*]) Numero del regolamento contenuto nel documento ST 14308/20 [2018/0331 (COD)].

SEZIONE C: Dati del destinatario

Nome del prestatore di servizi di hosting:

……

O

Nome del rappresentante legale:

……

Stato membro di stabilimento principale del prestatore di servizi di hosting:

……

O

Stato membro di residenza o di stabilimento del rappresentante legale del prestatore di servizi di hosting:

……

Nome della persona autorizzata:

……

Indirizzo e-mail del punto di contatto:

……

Data:

……

ALLEGATO III

INFORMAZIONI SULL'IMPOSSIBILITÀ DI ESEGUIRE UN ORDINE DI RIMOZIONE

(articolo 3, paragrafi 7 e 8, del regolamento (UE) 2021/ … del Parlamento europeo e del Consiglio ([1]) ([*]))

SEZIONE A:

Destinatario dell'ordine di rimozione:

……

Autorità competente che ha emesso l'ordine di rimozione:

……

Riferimento del fascicolo dell'autorità competente che ha emesso l'ordine di rimozione:

……

Riferimento del fascicolo del destinatario:

……

Data e ora di ricevimento dell'ordine di rimozione:

……

SEZIONE B: Mancata esecuzione

1) l'ordine di rimozione non può essere eseguito entro il termine per le seguenti ragioni (spuntare le caselle pertinenti):

   ☐ cause di forza maggiore o impossibilità di fatto non imputabile al prestatore di servizi di hosting, compreso per motivi tecnici o operativi obiettivamente giustificabili

   ☐ l'ordine di rimozione è viziato da errori manifesti

   ☐ l'ordine di rimozione non contiene informazioni sufficienti

2) fornire ulteriori informazioni sui motivi della mancata esecuzione:

   ……

3) se l'ordine di rimozione è viziato da errori manifesti e/o non contiene informazioni sufficienti, precisare gli errori di cui si tratta e le informazioni o i chiarimenti ulteriori che sono necessari:

   ……

([1]) Regolamento (UE) 2021/ … ([*]) del Parlamento europeo e del Consiglio relativo al contrasto della diffusione di contenuti terroristici online (GU L …).

([*]) Regolamento contenuto nel documento ST 14308/20 [2018/0331 (COD)].

SEZIONE C: Dati del prestatore di servizi di hosting o del suo rappresentante legale

Nome del prestatore di servizi di hosting:

……

O

Nome del rappresentante legale del prestatore di servizi di hosting:

……

Nome della persona autorizzata:

……

Dati di contatto (indirizzo e-mail):

……

Firma:

……

Data e ora:

……

Motivazione del Consiglio: Posizione (UE) n. 6/2021 del Consiglio in prima lettura in vista dell'adozione del regolamento del Parlamento europeo e del Consiglio relativo al contrasto della diffusione di contenuti terroristici online

(2021/C 135/02)

I. INTRODUZIONE

1. Il 12 settembre 2018 la Commissione ha presentato al Consiglio e al Parlamento europeo la proposta di regolamento in oggetto ([1]) relativo alla prevenzione della diffusione di contenuti terroristici online. La proposta è fondata sull'articolo 114 [ravvicinamento delle disposizioni legislative] del trattato sul funzionamento dell'Unione europea ed è soggetta alla procedura legislativa ordinaria.

2. Il Comitato economico e sociale europeo (CESE) è stato consultato dal Consiglio con lettera del 24 ottobre 2018 e ha formulato il suo parere sulla proposta ([2]) il 12 dicembre 2018 nella plenaria di dicembre.

3. Il 6 dicembre 2018 il Consiglio ha concordato un orientamento generale sui contenuti terroristici online ([3]) che ha costituito il mandato per i negoziati con il Parlamento europeo nel contesto della procedura legislativa ordinaria.

4. Il 12 febbraio 2019 il Garante europeo della protezione dei dati ha inviato al Parlamento europeo, alla Commissione e al Consiglio ([4]) «osservazioni formali» sul progetto di regolamento. Lo stesso giorno, l'Agenzia dell'Unione europea per i diritti fondamentali, su richiesta del Parlamento europeo del 6 febbraio 2019, ha formulato un parere sulla proposta ([5]).

5. Il 17 aprile 2019, con 308 voti favorevoli, 204 contrari e 70 astensioni, il Parlamento europeo ha adottato la sua posizione in prima lettura ([6]) sulla proposta della Commissione, con 155 emendamenti a tale proposta.

6. Il Consiglio e il Parlamento europeo hanno avviato i negoziati nell'ottobre 2019 al fine di raggiungere un accordo rapido in seconda lettura. I negoziati si sono conclusi positivamente il 10 dicembre 2020 con il raggiungimento, da parte del Parlamento europeo e del Consiglio, di un accordo provvisorio su un testo di compromesso.

7. Il 16 dicembre 2020 il Coreper (parte seconda) ha esaminato e confermato provvisoriamente il testo di compromesso finale in vista dell'accordo raggiunto con il Parlamento europeo ([7]).

8. L'11 gennaio 2021 il compromesso è stato approvato dalla commissione per le libertà civili, la giustizia e gli affari interni (LIBE) del Parlamento europeo. Il 13 gennaio il presidente della commissione LIBE ha indirizzato una lettera al presidente del Coreper (parte seconda) per informarlo che, se il Consiglio trasmettesse formalmente la sua posizione al Parlamento europeo nella forma che figura nell'allegato della lettera, egli raccomanderebbe alla plenaria di accettare la posizione del Consiglio senza emendamenti, previa messa a punto da parte dei giuristi-linguisti, nella fase di seconda lettura del Parlamento europeo ([8]).

([1]) Doc. 12129/18 + ADD 1-3.
([2]) GU C 110 del 22.3.2019, pag. 67 (15729/19).
([3]) Doc. 15336/18.
([4]) Rif. 2018-0822 D2545 (WK 9232/2019).
([5]) Parere dell'Agenzia dell'Unione europea per i diritti fondamentali - 2/2019 (WK 9235/2019).
([6]) Cfr. doc. 8663/19 (Nota informativa del GIP.2 (Relazioni interistituzionali) al Coreper che presenta i risultati della prima lettura del Parlamento europeo); il mandato del Parlamento è stato confermato dalla plenaria del 10 e 11 ottobre 2019.
([7]) Doc. 12906/20.
([8]) Doc. 5634/21.

II. **OBIETTIVO**

9. Il regolamento fornisce un quadro giuridico chiaro che stabilisce le responsabilità degli Stati membri e dei prestatori di servizi di hosting al fine di contrastare l'uso improprio dei servizi di hosting per la diffusione di contenuti terroristici online, garantire il buon funzionamento del mercato unico digitale e assicurare nel contempo la fiducia e la sicurezza nell'ambiente online. In particolare, mira a fornire chiarimenti in merito alla responsabilità dei prestatori di servizi di hosting nel garantire la sicurezza dei loro servizi, nonché nel contrastare, individuare e rimuovere i contenuti terroristici online o nel disabilitare l'accesso a essi in modo rapido ed efficace. Crea uno strumento operativo nuovo ed efficace per l'eliminazione dei contenuti terroristici consentendo l'emissione di ordini di rimozione aventi effetti transfrontalieri. Si mira inoltre a mantenere salvaguardie per garantire la tutela dei diritti fondamentali, inclusa la libertà di espressione e di informazione in una società aperta e democratica e la libertà d'impresa. Il regolamento dispone che i contenuti terroristici siano rimossi entro al massimo un'ora dal ricevimento dell'ordine di rimozione e stabilisce le responsabilità delle piattaforme online nel garantire la rimozione di tali contenuti. Oltre alle possibilità di ricorso giurisdizionale garantite dal diritto a un ricorso effettivo, il regolamento introduce una serie di salvaguardie e di meccanismi di reclamo.

10. Le autorità competenti di ciascuno Stato membro possono emettere un ordine di rimozione nei confronti di qualunque prestatore di servizi di hosting che offre servizi all'interno dell'UE. Le autorità competenti dello Stato membro in cui il prestatore di servizi ha lo stabilimento principale avranno il diritto — e, su richiesta motivata dei prestatori di servizi di hosting o dei fornitori di contenuti, l'obbligo — di esaminare l'ordine di rimozione qualora si ritenga che esso violi in modo grave o manifesto il regolamento o i diritti fondamentali sanciti dalla Carta dei diritti fondamentali dell'Unione europea. Gli Stati membri dovrebbero adottare norme sulle sanzioni applicabili in caso di violazioni degli obblighi, che tengano conto, tra l'altro, della natura e delle dimensioni dell'impresa in questione.

III. **ANALISI DELLA POSIZIONE DEL CONSIGLIO IN PRIMA LETTURA**

CONSIDERAZIONI GENERALI

11. Il Parlamento europeo e il Consiglio hanno condotto negoziati allo scopo di concludere un accordo in seconda lettura sulla base di una posizione in prima lettura del Consiglio che il Parlamento possa approvare senza modifiche. Il testo della posizione in prima lettura del Consiglio sul regolamento relativo alla prevenzione della diffusione di contenuti terroristici online rispecchia appieno il compromesso raggiunto tra i due colegislatori, assistiti dalla Commissione europea.

SINTESI DELLE PRINCIPALI QUESTIONI

12. Su richiesta del Parlamento europeo, il titolo del regolamento è stato modificato in «regolamento relativo al contrasto [...] della diffusione di contenuti terroristici online».

13. La definizione di «contenuti terroristici» è coerente con le definizioni dei reati pertinenti ai sensi della direttiva sulla lotta contro il terrorismo ([9]). Per quanto riguarda l'ambito di applicazione, la posizione in prima lettura del Consiglio riguarda materiale diffuso al pubblico, ossia a un numero potenzialmente illimitato di persone. Il materiale diffuso per scopi educativi, giornalistici, artistici o di ricerca o a fini di sensibilizzazione per prevenire o contrastare il terrorismo non dovrebbe essere considerato come integrante contenuti terroristici, compresi i contenuti che esprimono opinioni polemiche o controverse nell'ambito di dibattiti politici sensibili. Una valutazione accerta il reale scopo della diffusione. Si è inoltre specificato che il regolamento non ha l'effetto di modificare l'obbligo di rispettare i diritti, le libertà e i principi di cui all'articolo 6 TUE e si applica fatti salvi i principi fondamentali relativi alla libertà di espressione e informazione, compresa la libertà e il pluralismo dei media.

([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).

14. I prestatori di servizi di hosting adottano misure opportune, ragionevoli e proporzionate al fine di contrastare efficacemente l'uso improprio dei loro servizi per la diffusione di contenuti terroristici online. Se sono esposti a contenuti terroristici, i prestatori di servizi di hosting dovranno adottare misure specifiche per proteggere i propri servizi dalla diffusione di tali contenuti. Il testo concordato fonde tre articoli (l'articolo 3, *Obblighi di diligenza*, l'articolo 6, *Misure proattive*, e l'articolo 9, *Salvaguardie specifiche per quanto riguarda l'uso e l'attuazione di misure proattive*) in un unico articolo dal titolo «Misure specifiche». La scelta in merito a tali misure spetta al singolo prestatore di servizi di hosting. La posizione in prima lettura del Consiglio chiarisce che il prestatore di servizi di hosting può adottare misure diverse per contrastare la diffusione di contenuti terroristici, comprese misure automatizzate, che possono essere adattate alle capacità del prestatore di servizi di hosting e alla natura dei servizi offerti. Qualora ritenga che le misure specifiche adottate siano insufficienti per far fronte ai rischi, l'autorità competente dovrà poter esigere l'adozione di ulteriori misure specifiche appropriate, efficaci e proporzionate. Tuttavia, l'obbligo di attuare tali ulteriori misure specifiche non dovrebbe comportare un obbligo generale di sorveglianza o di ricercare attivamente fatti e circostanze, ai sensi dell'articolo 15, paragrafo 1, della direttiva 2000/31/CE ([10]), né l'obbligo di utilizzare strumenti automatizzati. Per garantire la trasparenza, i prestatori di servizi di hosting pubblicheranno relazioni annuali sulla trasparenza in merito alle misure intraprese contro la diffusione di contenuti terroristici.

15. Per quanto concerne gli ordini di rimozione aventi effetti transfrontalieri, il ruolo dello Stato membro ospitante è stato potenziato con l'introduzione di una procedura di esame: l'autorità competente dello Stato membro in cui il prestatore di servizi di hosting ha lo stabilimento principale o il suo rappresentante legale può, di propria iniziativa, esaminare l'ordine di rimozione emesso dalle autorità competenti di un altro Stato membro per stabilire se esso violi o meno in modo grave o manifesto il regolamento o i diritti fondamentali sanciti nella Carta dei diritti fondamentali dell'Unione europea. Su richiesta motivata di un prestatore di servizi di hosting o di un fornitore di contenuti, lo Stato membro ospitante è tenuto a esaminare l'esistenza di una tale violazione.

16. Eccetto casi di emergenza debitamente giustificati, è opportuno trasmettere ai prestatori di servizi di hosting che non hanno ricevuto in precedenza un ordine di rimozione dalla suddetta autorità, almeno 12 ore prima, una notifica contenente, tra l'altro, informazioni sulle procedure e sui termini applicabili, in particolare al fine di ridurre l'onere per le piccole e medie imprese (PMI).

17. È soppresso l'articolo relativo alle segnalazioni (un meccanismo inteso ad allertare i prestatori di servizi di hosting in merito a contenuti terroristici affinché possano su base volontaria esaminarli in base alle proprie condizioni contrattuali), ma un considerando chiarisce che le segnalazioni restano a disposizione degli Stati membri e di Europol.

18. I contenuti terroristici che sono stati rimossi o il cui accesso è stato disabilitato a seguito di ordini di rimozione o di misure specifiche devono essere conservati per un periodo di sei mesi dalla rimozione o dalla disabilitazione; tale periodo può essere prorogato se necessario e per tutto il tempo richiesto in caso di ricorso.

19. Gli Stati membri stabiliscono le norme relative alle sanzioni applicabili alle violazioni del regolamento da parte dei prestatori di servizi di hosting. Le sanzioni potrebbero assumere forme diverse, tra cui avvertimenti formali in caso di violazioni minori o sanzioni pecuniarie in relazione a violazioni più gravi. La posizione in prima lettura del Consiglio definisce quali violazioni sono soggette a sanzioni e quali circostanze sono pertinenti per valutare la tipologia e il livello di tali sanzioni. Ai prestatori di servizi di hosting possono essere comminate sanzioni fino al 4% del loro fatturato globale in caso di sistematica o persistente inosservanza dell'obbligo di rimuovere o disabilitare l'accesso a contenuti terroristici entro un'ora.

IV. **CONCLUSIONE**

20. La posizione del Consiglio rispecchia pienamente il compromesso raggiunto nei negoziati tra il Parlamento europeo e il Consiglio con il contributo della Commissione. Tale compromesso è confermato dalla lettera del presidente della commissione LIBE del Parlamento europeo al presidente del Coreper (parte seconda) datata 13 gennaio 2021.

([10]) 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).

ISSN 1977-0944 (edizione elettronica)
ISSN 1725-2466 (edizione cartacea)

Ufficio delle pubblicazioni
dell'Unione europea
L-2985 Lussemburgo
LUSSEMBURGO

IT