



TESTI APPROVATI

P8_TA(2019)0421

Prevenzione della diffusione di contenuti terroristici online *I**

Risoluzione legislativa del Parlamento europeo del 17 aprile 2019 sulla proposta di regolamento del Parlamento europeo e del Consiglio relativo alla prevenzione della diffusione di contenuti terroristici online (COM(2018)0640 – C8-0405/2018 – 2018/0331(COD))

(Procedura legislativa ordinaria: prima lettura)

Il Parlamento europeo,

- vista la proposta della Commissione al Parlamento europeo e al Consiglio (COM(2018)0640),
 - visti l'articolo 294, paragrafo 2, e l'articolo 114 del trattato sul funzionamento dell'Unione europea, a norma dei quali la proposta gli è stata presentata dalla Commissione (C8-0405/2018),
 - visto l'articolo 294, paragrafo 3, del trattato sul funzionamento dell'Unione europea,
 - visto il parere motivato inviato dalla Camera dei deputati ceca, nel quadro del protocollo n. 2 sull'applicazione dei principi di sussidiarietà e di proporzionalità, in cui si dichiara la mancata conformità del progetto di atto legislativo al principio di sussidiarietà,
 - visto il parere del Comitato economico e sociale europeo del 12 dicembre 2018¹,
 - visto l'articolo 59 del suo regolamento,
 - visti la relazione della commissione per le libertà civili, la giustizia e gli affari interni e i pareri della commissione per la cultura e l'istruzione e della commissione per il mercato interno e la protezione dei consumatori (A8-0193/2019),
1. adotta la posizione in prima lettura figurante in appresso;
 2. chiede alla Commissione di presentargli nuovamente la proposta qualora la sostituisca, la modifichi sostanzialmente o intenda modificarla sostanzialmente;

¹ GU C 110 del 22.3.2019, pag. 67.

3. incarica il suo Presidente di trasmettere la posizione del Parlamento al Consiglio e alla Commissione nonché ai parlamenti nazionali.

P8_TC1-COD(2018)0331

Posizione del Parlamento europeo definita in prima lettura il 17 aprile 2019 in vista dell'adozione del regolamento (UE) .../... del Parlamento europeo e del Consiglio relativo ~~alla prevenzione della~~ *alla lotta alla* diffusione di contenuti terroristici online [Em. 1]

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 europeo¹,

deliberando secondo la procedura legislativa ordinaria²,

¹ GU C [...] del [...], pag. [...].

² Posizione del Parlamento europeo del 17 aprile 2019.

considerando quanto segue:

- (1) Il presente regolamento mira a garantire il buon funzionamento del mercato unico digitale in una società aperta e democratica ~~prevenendo~~ **contrastando** l'uso improprio dei servizi di hosting a fini terroristici **e contribuendo alla sicurezza pubblica nelle società europee**. Occorre migliorare il funzionamento del mercato unico digitale rafforzando la certezza del diritto per i prestatori di servizi di hosting, il che aumenterà la fiducia degli utilizzatori nell'ambiente online, e potenziando le salvaguardie per la libertà di espressione ~~e di informazione~~, **per la libertà di ricevere e diffondere informazioni e idee in una società aperta e democratica e per la libertà e il pluralismo dei media**. [Em. 2]

- (1 bis) La regolamentazione dei prestatori di servizi di hosting può solo integrare le strategie degli Stati membri intese a far fronte al terrorismo, che devono mettere in rilievo misure offline, come gli investimenti in attività sociali, le iniziative di deradicalizzazione e l'impegno nei confronti delle comunità interessate, ai fini di una prevenzione sostenibile della radicalizzazione nella società.* [Em. 3]

(1 ter) I contenuti terroristici fanno parte di un problema più ampio relativo ai contenuti illegali online, che comprende altri tipi di contenuti come lo sfruttamento sessuale dei minori, le pratiche commerciali illecite e le violazioni della proprietà intellettuale. Le organizzazioni terroristiche e altre organizzazioni criminali spesso si dedicano al traffico di contenuti illegali per riciclare denaro e reperire capitale di avviamento per finanziare le loro operazioni. Tale problema richiede una combinazione di misure legislative, non legislative e volontarie basate sulla collaborazione tra le autorità e i prestatori di servizi, nel pieno rispetto dei diritti fondamentali. Sebbene la minaccia rappresentata dai contenuti illegali sia stata attenuata da iniziative di successo come il codice di condotta per contrastare l'illecito incitamento all'odio online, promosso da aziende del settore, e WePROTECT Global Alliance, un progetto che intende porre fine agli abusi sessuali sui minori online, è necessario istituire un quadro legislativo per la cooperazione transfrontaliera tra le autorità nazionali di regolamentazione per la rimozione dei contenuti illegali. [Em. 4]

- (2) I prestatori di servizi di hosting che operano in Internet svolgono un ruolo essenziale nell'economia digitale mettendo in relazione le imprese e i cittadini, *offrendo opportunità di apprendimento* e facilitando il dibattito pubblico così come la diffusione e la ricezione di informazioni, opinioni e idee, e contribuiscono in modo significativo alla crescita economica, all'innovazione e alla creazione di posti di lavoro nell'Unione. In alcuni casi, tuttavia, i loro servizi sono utilizzati impropriamente da terzi per perpetrare attività illegali online. Particolarmente preoccupante è l'uso improprio dei servizi di hosting da parte di gruppi terroristici e dei loro sostenitori per pubblicare contenuti terroristici online allo scopo di propagare il loro messaggio, radicalizzare e attirare nuove reclute, nonché facilitare e dirigere attività terroristiche. **[Em. 5]**

- (3) ***Pur non essendo l'unico fattore***, la presenza di contenuti terroristici online ***si è rivelata essere un catalizzatore della radicalizzazione degli individui che hanno perpetrato 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 ~~elle~~ ***in proporzione alle*** capacità e ~~dei~~ ***ai*** mezzi tecnologici associati ai servizi che forniscono, i prestatori di servizi online hanno particolari responsabilità nei confronti della società sotto il profilo della protezione dei loro servizi dall'uso improprio che potrebbero farne i terroristi e del contributo che possono apportare ~~al contrasto della~~ ***alle autorità competenti per contrastare la*** diffusione di contenuti terroristici attraverso i loro servizi, ***tenendo in considerazione l'importanza fondamentale della libertà di espressione e della libertà di ricevere e diffondere informazioni e idee in una società aperta e democratica.*** [Em. 6]

- (4) Gli sforzi volti a contrastare i contenuti terroristici online sono stati avviati a livello dell'Unione nel 2015 nel quadro della cooperazione volontaria tra gli Stati membri e i prestatori di servizi di hosting; essi dovrebbero essere integrati da un quadro legislativo chiaro al fine di ridurre l'accessibilità dei contenuti terroristici online e affrontare in modo adeguato un fenomeno in rapida evoluzione. Tale quadro legislativo poggerebbe su iniziative volontarie, che sono state rafforzate dalla raccomandazione (UE) 2018/334³, e risponde alla richiesta del Parlamento europeo di rafforzare le misure volte ad affrontare i contenuti illegali e nocivi, ***in linea con il quadro orizzontale stabilito dalla direttiva 2000/31/CE***, e a quella del Consiglio europeo di migliorare l'individuazione automatizzata e la rimozione dei contenuti che incitano a compiere atti terroristici. [Em. 7]

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

- (5) L'applicazione del presente regolamento non dovrebbe pregiudicare l'applicazione dell'articolo 14 della direttiva 2000/31/CE⁴. ~~In particolare, tutte le misure adottate dal prestatore di servizi di hosting conformemente al presente regolamento, comprese le eventuali misure proattive, non dovrebbero comportare automaticamente la perdita, per il prestatore di servizi, del beneficio dell'esenzione di responsabilità prevista in tale disposizione.~~ Il presente regolamento lascia impregiudicata la competenza delle autorità e degli organi giurisdizionali nazionali a stabilire la responsabilità dei prestatori di servizi di hosting in determinati casi se non sono soddisfatte le condizioni di cui all'articolo 14 della *alla* direttiva 2000/31/CE per beneficiare dell'esenzione di responsabilità. [Em. 8]
- (6) Il presente regolamento definisce, ~~nel pieno rispetto dei norme, che dovrebbero~~ *pienamente rispettare i* diritti fondamentali tutelati nell'ordinamento giuridico dell'Unione e, in particolare, quelli garantiti dalla Carta dei diritti fondamentali dell'Unione europea, ~~norme~~ intese a ~~prevenire~~ *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. [Em. 9]

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).

(7) Il presente regolamento ~~contribuisce~~ **intende contribuire** alla protezione della pubblica sicurezza, ~~attuando nel contempo~~ **e dovrebbe attuare** adeguate e solide salvaguardie per garantire la tutela dei diritti fondamentali in gioco. Ciò include i diritti al rispetto della vita privata e alla protezione dei dati personali, il diritto ad una tutela giurisdizionale effettiva, il diritto alla libertà di espressione, compresa la libertà di ricevere e trasmettere informazioni, la libertà d'impresa e il principio di non discriminazione. Le autorità competenti e i prestatori di servizi di hosting dovrebbero adottare solo le misure che sono necessarie, adeguate e proporzionate in una società democratica, tenendo conto della particolare importanza rivestita dalla libertà di espressione ~~e di informazione~~, **dalla libertà di ricevere e diffondere informazioni e idee, dal diritto al rispetto della vita privata e familiare e dal diritto alla protezione dei dati personali**, che ~~costituisce uno dei~~ **costituiscono i** fondamenti essenziali di una società democratica e pluralista ~~e uno dei~~ **i** valori su cui si fonda l'Unione. Le misure ~~che costituiscono un'~~ **dovrebbero evitare qualsiasi** ingerenza nella libertà di espressione e d'informazione **e, nella misura del possibile**, dovrebbero essere ~~rigorosamente mirate, nel senso che devono servire a prevenire~~ **contrastare** la diffusione di contenuti terroristici **attraverso un approccio rigorosamente mirato**, ma senza pregiudicare il diritto di ricevere e diffondere informazioni in modo lecito, tenuto conto del ruolo centrale dei prestatori di servizi di hosting nel facilitare il dibattito pubblico e la diffusione e la ricezione di informazioni, pareri e idee nel rispetto della legge. **L'adozione di misure efficaci per contrastare il terrorismo online e la protezione della libertà di espressione non sono elementi contrastanti, bensì obiettivi complementari e che si rafforzano a vicenda.** [Em. 10]

- (8) Il diritto a un ricorso effettivo è sancito dall'articolo 19 TUE e dall'articolo 47 della Carta dei diritti fondamentali dell'Unione europea. Ogni persona fisica o giuridica ha diritto a un ricorso giurisdizionale effettivo dinanzi alle competenti autorità giurisdizionali nazionali contro una qualsiasi delle misure adottate in base al presente regolamento che possa ledere i diritti di tale persona. Il diritto comprende in particolare la possibilità per i prestatori di servizi di hosting e i fornitori di contenuti di impugnare effettivamente un ordine di rimozione dinanzi all'autorità giurisdizionale dello Stato membro la cui autorità l'ha emanato ***e la possibilità per i fornitori di contenuti di impugnare le misure specifiche adottate dal prestatore di servizi di hosting.*** [Em. 11]

(9) Onde chiarire le misure che i prestatori di servizi di hosting e le autorità competenti dovrebbero adottare per ~~prevenire~~ **contrastare** la diffusione di contenuti terroristici online, è opportuno che il presente regolamento stabilisca una definizione dei contenuti terroristici per fini di prevenzione sulla base della definizione dei reati di terrorismo ai sensi della direttiva (UE) 2017/541 del Parlamento europeo e del Consiglio⁵. Data la necessità di contrastare ~~la propaganda~~ **i contenuti terroristici** online più ~~perniciosa~~ **perniciosi**, la definizione dovrebbe ricomprendere il materiale e i messaggi che ~~incitano, incoraggiano~~ **incita** o ~~appoggiano~~ **sollecita** la commissione di reati di terrorismo e la partecipazione agli stessi, ~~impartiscono istruzioni finalizzate alla commissione di tali reati o promuovono~~ **che promuove** la partecipazione nelle attività di un gruppo terroristico, **generando in tal modo il pericolo che uno o più di tali reati possano essere commessi intenzionalmente. Nella definizione dovrebbero inoltre rientrare i contenuti che forniscono indicazioni per la fabbricazione e l'uso di esplosivi, armi da fuoco o qualsiasi altra arma o sostanza nociva o pericolosa, nonché sostanze chimiche, biologiche, radiologiche e nucleari (CBRN), e qualsiasi istruzione su altri metodi e tecniche, compresa la selezione degli obiettivi, allo scopo di commettere reati di terrorismo.** Tali materiali comprendono, in particolare, testi, immagini, registrazioni audio e video. Nel valutare se il contenuto pubblicato online costituisce contenuto terroristico ai sensi del presente regolamento, le autorità competenti, così come i prestatori di servizi di hosting, dovrebbero tenere conto di fattori quali la natura e la formulazione dei messaggi, il contesto in cui sono emessi e il loro potenziale di portare a conseguenze dannose, compromettendo la sicurezza e l'incolumità delle persone. Il fatto che il materiale sia prodotto o diffuso da un'organizzazione terroristica o da una persona che figura negli elenchi dell'Unione costituisce un elemento importante della valutazione. Occorre proteggere adeguatamente la diffusione di contenuti per scopi giornalistici, educativi o di ricerca **o a fini di sensibilizzazione contro l'attività terroristica. 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 e**

⁵ 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).

della Carta dei diritti fondamentali. Inoltre, le opinioni radicali, polemiche o controverse espresse nell'ambito di dibattiti politici sensibili non dovrebbero essere considerate contenuti terroristici. **[Em. 12]**

(10) Al fine di ricomprendere i servizi di hosting attraverso i quali sono diffusi i contenuti terroristici online, il presente regolamento si dovrebbe applicare ai servizi della società dell'informazione che memorizzano informazioni fornite da un destinatario del servizio su sua richiesta e che rendono disponibili a ~~terzi~~ **al pubblico** informazioni memorizzate, indipendentemente dalla natura meramente tecnica, automatica o passiva di tale attività. Ad esempio, i prestatori di servizi della società dell'informazione includono le piattaforme dei social media, i servizi di streaming video, i servizi di condivisione di video, audio e immagini, servizi di condivisione di file e altri servizi cloud, nella misura in cui mettono queste informazioni a disposizione di ~~terzi~~ **del pubblico** e di siti web in cui gli utilizzatori possono esprimere commenti o postare recensioni. Il regolamento dovrebbe inoltre applicarsi ai prestatori di servizi di hosting che offrono servizi nell'Unione, ma che sono stabiliti al di fuori di essa, dal momento che una quota significativa dei prestatori di servizi di hosting esposti a contenuti terroristici che possono essere diffusi tramite i loro servizi sono stabiliti in paesi terzi. Ciò dovrebbe garantire che tutte le imprese operanti nel mercato unico digitale si conformino agli stessi obblighi a prescindere dal paese di stabilimento. Per determinare se offre servizi nell'Unione, è necessario verificare se il prestatore di servizi consente alle persone fisiche o giuridiche di uno o più Stati membri di usufruire dei suoi servizi. Tuttavia, la semplice accessibilità del sito Internet di un prestatore di servizi o di un indirizzo di posta elettronica e di altri dati di contatto in uno o più Stati membri non dovrebbe di per sé costituire una condizione sufficiente per l'applicazione del presente regolamento. ***Il presente regolamento non dovrebbe applicarsi ai servizi cloud, inclusi i servizi cloud business-to-business, su cui il prestatore di servizi non ha alcun diritto contrattuale in merito alla tipologia di contenuti memorizzati o alla modalità di trattamento o divulgazione al pubblico da parte dei relativi clienti o degli utilizzatori finali di tali clienti, e laddove il prestatore di servizi non abbia la capacità tecnica di rimuovere il contenuto specifico memorizzato dai rispettivi clienti o dagli utilizzatori finali dei rispettivi servizi.*** [Em. 13]

(11) L'esistenza di un collegamento sostanziale con l'Unione dovrebbe essere presa in considerazione al fine di determinare l'ambito di applicazione del presente regolamento. Tale collegamento sostanziale con l'Unione dovrebbe considerarsi presente quando il prestatore di servizi è stabilito nell'Unione o, in caso contrario, sulla base dell'esistenza di un numero considerevole di utilizzatori in uno o più Stati membri o dell'orientamento delle sue attività verso uno o più Stati membri. L'orientamento delle attività verso uno o più Stati membri può essere determinato sulla base di tutte le circostanze pertinenti, tra cui l'uso di una lingua o di una moneta generalmente usata nello Stato membro in questione ~~e la possibilità di ordinare prodotti o servizi~~. L'orientamento delle attività verso uno Stato membro potrebbe anche desumersi dalla disponibilità di un'applicazione nell'apposito negozio online ("app store") nazionale, dalla diffusione di pubblicità a livello locale o nella lingua usata nello Stato membro in questione, o dalla gestione dei rapporti con la clientela, ad esempio la fornitura di assistenza alla clientela nella lingua generalmente parlata in tale Stato membro. Un collegamento sostanziale dovrebbe essere presunto anche quando le attività di un prestatore di servizi sono dirette verso uno o più Stati membri come previsto all'articolo 17, paragrafo 1, lettera c), del regolamento (UE) n. 1215/2012 del Parlamento europeo e del Consiglio⁶. Al contrario, non si può considerare che la prestazione del servizio al solo scopo di conformarsi al divieto di discriminazione imposto dal regolamento (UE) 2018/302 del Parlamento europeo e del Consiglio⁷ compri, di per sé, che le sue attività sono dirette o orientate verso un dato territorio all'interno dell'Unione. **[Em. 14]**

⁶ 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).

⁷ Regolamento (UE) 2018/302 del Parlamento europeo e del Consiglio, del 28 febbraio 2018, recante misure volte a impedire i blocchi geografici ingiustificati e altre forme di discriminazione basate sulla nazionalità, sul luogo di residenza o sul luogo di stabilimento dei clienti nell'ambito del mercato interno e che modifica i regolamenti (CE) n. 2006/2004 e (UE) 2017/2394 e la direttiva 2009/22/CE (GU L 601 del 2.3.2018, pag. 1).

- (12) I prestatori di servizi di hosting dovrebbero rispettare determinati obblighi di diligenza al fine di ~~prevenire~~ **contrastare** la diffusione di contenuti terroristici tramite i loro servizi **al pubblico**. Tali obblighi di diligenza non dovrebbero costituire un obbligo generale di sorveglianza ~~di sorveglianza~~ **per i prestatori di servizi di hosting di sorvegliare le informazioni che memorizzano né un obbligo generale di ricercare attivamente fatti che indichino la presenza di attività illecite**. Gli obblighi di diligenza dovrebbero tra l'altro significare che, quando applicano il presente regolamento, i prestatori di servizi di hosting agiscono in maniera **trasparente**, diligente, proporzionata e non discriminatoria nei confronti dei contenuti che memorizzano, in particolare quando applicano le proprie condizioni contrattuali, al fine di evitare la rimozione di contenuti che non hanno natura terroristica. La rimozione di contenuti o la disabilitazione dell'accesso agli stessi devono essere effettuate nel rispetto della libertà di espressione e di informazione, **della libertà di ricevere e diffondere informazioni e idee in una società aperta e democratica, nonché della libertà e del pluralismo dei media**. [Em. 15]

- (13) Occorre armonizzare la procedura e gli obblighi che discendono dagli ordini ~~giuridici~~ ***di rimozione*** che ingiungono ai prestatori di servizi di hosting di rimuovere contenuti terroristici o di disabilitarne l'accesso, in esito a una valutazione delle autorità competenti. Gli Stati membri dovrebbero designare le autorità competenti, assegnando tale compito ~~alle autorità amministrative, esecutive o giudiziarie~~ ***a un'autorità giudiziaria o a un'autorità amministrativa o esecutiva indipendente dal punto di vista funzionale*** di loro scelta. In considerazione della velocità alla quale i contenuti terroristici sono diffusi attraverso i servizi online, la presente disposizione impone ai prestatori di servizi di hosting l'obbligo di provvedere a che i contenuti terroristici oggetto di un ordine di rimozione siano rimossi o che l'accesso sia disattivato entro un'ora dal ricevimento del provvedimento. ~~Spetta ai prestatori di servizi di hosting decidere se rimuovere il contenuto in questione o disabilitarne l'accesso per gli utilizzatori nell'Unione.~~ **[Em. 16]**

- (14) L'autorità competente dovrebbe trasmettere l'ordine di rimozione direttamente al ~~destinatario~~ e al punto di contatto ***del prestatore di servizi di hosting e, laddove il prestatore di servizi di hosting abbia lo stabilimento principale in un altro Stato membro, all'autorità competente di tale Stato membro*** con ogni mezzo elettronico che consenta di conservare una traccia scritta in condizioni che permettano al prestatore di stabilirne l'autenticità, compresa l'esattezza della data e dell'ora di invio e ricevimento dell'ordine, quali posta elettronica protetta e piattaforme o altri canali protetti, compresi quelli messi a disposizione dal prestatore di servizi, in conformità delle norme in materia di protezione dei dati personali. Segnatamente, tale obbligo può essere assolto usando servizi elettronici di recapito certificato qualificati ai sensi del regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio⁸.

[Em. 17]

⁸ 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).

(15) — Le segnalazioni emesse dalle autorità competenti o da Europol costituiscono un modo efficace e rapido di sensibilizzare i prestatori di servizi di hosting alla presenza di contenuti specifici nei loro servizi. Questo meccanismo inteso ad allertare i prestatori di servizi di hosting nei confronti delle informazioni che possono essere considerate contenuti terroristici, che permette loro su base volontaria di esaminare la compatibilità delle proprie clausole contrattuali, dovrebbe rimanere disponibile in aggiunta agli ordini di rimozione. È importante che i prestatori di servizi di hosting valutino tali segnalazioni in via prioritaria e forniscano rapidamente un feedback in merito alle azioni intraprese. La decisione finale in merito all'opportunità di rimuovere il contenuto, in quanto non compatibile con le proprie condizioni contrattuali spetta al prestatore di servizi di hosting. Nell'attuazione del presente regolamento con riferimento alle segnalazioni, il mandato di Europol, definito nel regolamento (UE) 2016/794⁹, resta invariato. [Em. 18]

⁹ — 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 (G.U.L. 135 del 24.5.2016, pag. 53).

(16) In considerazione della portata e della rapidità necessarie per individuare e rimuovere efficacemente i contenuti terroristici, l'adozione ~~proattiva~~ di misure *specifiche* proporzionate, ~~compreso il ricorso in alcuni casi a strumenti automatizzati,~~ costituisce un elemento essenziale di lotta ai contenuti terroristici online. Al fine di ridurre l'accessibilità ai contenuti terroristici nei loro servizi, i prestatori di servizi di hosting dovrebbero valutare se sia opportuno adottare misure ~~proattive~~ *specifiche* in funzione dei rischi e dell'esposizione a contenuti terroristici nonché delle conseguenze sui diritti dei terzi ~~alle informazioni~~ e dell'interesse pubblico *a ricevere e diffondere informazioni, in particolare in presenza di un livello sostanziale di esposizione a contenuti terroristici e di ordini di rimozione*. Di conseguenza, i prestatori di servizi di hosting dovrebbero determinare le misure ~~proattive~~ *specifiche* appropriate, *mirate*, efficaci e proporzionate da attuare. Tale obbligo non dovrebbe implicare un obbligo generale di sorveglianza. *Tali misure specifiche possono includere l'invio di relazioni periodiche alle autorità competenti, un incremento delle risorse umane che si occupano di misure volte a tutelare i servizi dalla diffusione pubblica di contenuti terroristici, nonché lo scambio delle migliori pratiche*. Nel contesto di tale valutazione, l'assenza di ordini di rimozione e di segnalazioni inviate *indirizzati* a un prestatore di servizi di hosting è un'indicazione di un basso livello di esposizione a contenuti terroristici. [Em. 19]

(17) Quando attuano misure ~~proattive~~ *specifiche*, i prestatori di servizi di hosting dovrebbero assicurare che sia preservato il diritto degli utilizzatori alla libertà di espressione e ~~di informazione, compresa la~~ *alla* libertà di ricevere e diffondere informazioni *e idee in una società aperta e democratica*. Oltre ai requisiti stabiliti nella legislazione, anche in materia di protezione dei dati personali, i prestatori di servizi di hosting dovrebbero agire con la debita diligenza e attuare misure di salvaguardia, comprese in particolare la sorveglianza e le verifiche umane, ~~se del caso,~~ al fine di evitare decisioni indesiderate ed erranee di rimozione di contenuti che non hanno natura terroristica. ~~Ciò vale in particolare quando i prestatori di servizi di hosting utilizzano strumenti automatizzati per individuare i contenuti terroristici. Qualsiasi decisione di ricorrere a strumenti automatizzati, adottata dal prestatore di servizi di hosting stesso o su richiesta dell'autorità competente, dovrebbe essere valutata sotto il profilo dell'affidabilità della tecnologia utilizzata e delle conseguenze per i diritti fondamentali. [Em. 20]~~

(18) Al fine di garantire che i prestatori di servizi di hosting esposti a contenuti terroristici adottino misure adeguate per prevenire l'uso improprio dei loro servizi, ~~le autorità competenti dovrebbero~~ ***l'autorità competente dovrebbe*** imporre ai prestatori di servizi di hosting che hanno ricevuto un ~~ordine~~ ***numero sostanziale di ordini*** di rimozione, ~~divenuto definitivo,~~ ***definitivi*** di riferire in merito alle misure ~~proattive~~ ***specifiche*** adottate. ~~Si potrebbe trattare di misure volte a prevenire che il contenuto terroristico rimosso o il cui accesso è stato disabilitato sia nuovamente caricato online a seguito di un ordine di rimozione o di una segnalazione ricevuta, utilizzando strumenti pubblici o privati che permettano di confrontarlo con contenuti terroristici noti.~~ Tali misure possono inoltre fare uso di strumenti tecnici affidabili per individuare nuovi contenuti terroristici, ~~avvalendosi di quelli disponibili sul mercato o quelli sviluppati dal prestatore di servizi di hosting.~~ Il prestatore di servizi dovrebbe riferire in merito alle specifiche misure ~~proattive~~ attuate al fine di consentire all'autorità competente di valutare se siano ***necessarie***, efficaci e proporzionate e se, qualora siano utilizzati strumenti automatizzati, il prestatore di servizi di hosting dispone delle necessarie competenze in materia di sorveglianza e verifiche umane. Nel valutare l'efficacia, ***la necessità*** e la proporzionalità delle misure, le autorità competenti dovrebbero tenere conto dei parametri pertinenti, compresi il numero di ordini di rimozione e ~~segnalazioni~~ trasmessi al prestatore, ***le sue dimensioni***, la sua capacità economica e l'impatto dei suoi servizi sulla diffusione di contenuti terroristici (ad esempio, in considerazione del numero di utilizzatori nell'Unione), ***nonché le misure di salvaguardia attuate per tutelare la libertà di espressione e di informazione e il numero di casi in cui sono state applicate limitazioni a contenuti legali.*** [Em. 21]

(19) A seguito della richiesta, l'autorità competente dovrebbe avviare un dialogo con il prestatore di servizi di hosting sulle misure ~~proattive~~ **specifiche** necessarie da attuare. Se necessario, l'autorità competente dovrebbe ~~esigere~~ **chiedere al prestatore di servizi di hosting di valutare nuovamente le misure necessarie o dovrebbe chiedere** l'adozione di misure ~~proattive~~ **specifiche** appropriate, efficaci e proporzionate qualora ritenga che le misure adottate **non rispettino i principi di necessità e proporzionalità** o siano insufficienti per far fronte ai rischi. **L'autorità competente dovrebbe richiedere unicamente misure specifiche che il prestatore di servizi di hosting possa ragionevolmente attuare, tenendo conto, tra gli altri fattori, delle risorse finanziarie e di altra natura del prestatore di servizi di hosting.** La ~~decisione~~ **richiesta** di ~~imporre~~ **attuare** tali misure ~~proattive~~ **specifiche** non dovrebbe, ~~in linea di~~ **principio**, comportare l'imposizione di un obbligo generale di sorveglianza, conformemente all'articolo 15, paragrafo 1, della direttiva 2000/31/CE. Considerando i rischi particolarmente gravi connessi alla diffusione di contenuti terroristici, le decisioni adottate dalle autorità competenti sulla base del presente regolamento possono derogare all'approccio di cui all'articolo 15, paragrafo 1, della direttiva 2000/31/CE per talune misure specifiche e mirate la cui adozione sia necessaria per motivi imperativi di sicurezza pubblica. Prima di adottare tale decisione, l'autorità competente dovrebbe garantire un giusto equilibrio tra obiettivi di interesse generale e i diritti fondamentali in questione, in particolare la libertà di espressione e d'informazione e la libertà d'impresa, e addurre un'adeguata giustificazione. [Em. 22]

- (20) L'obbligo per i prestatori di servizi di hosting di conservare i contenuti rimossi e i relativi dati dovrebbe essere previsto per finalità specifiche e limitato al tempo necessario. Tale obbligo di conservazione dei dati dovrebbe essere esteso ai relativi dati, nella misura in cui tali dati andrebbero altrimenti perduti a seguito della rimozione del contenuto in questione. I relativi dati possono ad esempio includere dati relativi agli abbonati, compresi in particolare i dati relativi all'identità del fornitore di contenuti, nonché i «dati relativi agli accessi», tra cui ad esempio i dati relativi alla data e all'ora di utilizzo da parte del fornitore di contenuti, o la connessione al servizio (log-in) e la disconnessione (log-off) dal medesimo, unitamente all'indirizzo IP assegnato al fornitore di contenuti dal prestatore di servizi di accesso a Internet. **[Em. 23]**

(21) L'obbligo di conservare il contenuto ai fini di un procedimento di riesame *o di ricorso* amministrativo o giurisdizionale è necessario e giustificato per garantire misure di tutela efficaci al fornitore di contenuti il cui contenuto è stato rimosso o l'accesso disabilitato o per garantire il ripristino di tale contenuto allo stato precedente alla sua rimozione, in funzione dell'esito del procedimento di riesame. L'obbligo di conservare il contenuto a fini di indagine e azione penale è giustificato e necessario in considerazione della potenziale utilità di tale materiale per scardinare o prevenire attività terroristiche. Se le imprese rimuovono i contenuti o ne disabilitano l'accesso, ~~segnatamente~~ a seguito dell'adozione ~~proattiva~~ di proprie misure *specifiche*, e non ne informano le pertinenti autorità ritenendo che non rientrino nell'ambito di applicazione dell'articolo 13, paragrafo 4, del presente regolamento, le *dovrebbero informarne tempestivamente* le autorità di contrasto ~~potrebbero non essere a conoscenza dell'esistenza di tale contenuto~~ *competenti*. Ciò giustifica anche la conservazione di contenuti a fini di prevenzione, accertamento, indagine e perseguimento di reati di terrorismo. A tal fine, *i contenuti terroristici e i relativi dati dovrebbero essere conservati solo per un periodo di tempo tale da consentire alle autorità di contrasto di controllare i contenuti e decidere se sono necessari ai suddetti fini specifici. Tale periodo ha una durata massima di sei mesi. A fini di prevenzione, accertamento, indagine e perseguimento di reati di terrorismo*, l'obbligo di conservazione è limitato ai dati che possono riguardare reati di terrorismo e può pertanto contribuire a perseguire i reati di terrorismo o la prevenzione di gravi rischi per la sicurezza pubblica. [Em. 24]

- (22) Per garantire la proporzionalità, il periodo di conservazione dovrebbe essere limitato a sei mesi, in modo da dare ai fornitori di contenuti il tempo sufficiente ad avviare il procedimento di riesame e *o* consentire alle autorità di contrasto di accedere ai dati pertinenti ai fini delle indagini e dell'azione penale nei confronti dei reati di terrorismo. Su richiesta dell'autorità che effettua il riesame, tale termine può tuttavia essere prorogato del tempo necessario qualora il procedimento di riesame *o di ricorso* sia avviato ma non completato entro il periodo di sei mesi. Tale periodo dovrebbe *inoltre* essere sufficiente per consentire alle autorità di contrasto di conservare ~~gli elementi di prova necessari~~ *il materiale necessario* in relazione alle loro indagini *e azioni penali* assicurando nel contempo un equilibrio con i diritti fondamentali in questione. [Em. 25]
- (23) Il presente regolamento non pregiudica le garanzie procedurali e le misure investigative procedurali relative all'accesso ai contenuti e ai relativi dati conservati a fini di indagine e azione penale nei confronti dei reati di terrorismo, stabilite dalla legislazione nazionale degli Stati membri o dal diritto dell'Unione.

(24) La trasparenza della politica applicata dai prestatori di servizi di hosting in relazione ai contenuti terroristici è essenziale ai fini della loro maggiore responsabilità nei confronti dei propri utilizzatori e per rafforzare la fiducia dei cittadini nel mercato unico digitale. ***Solo*** i prestatori di servizi di hosting ***che sono soggetti a ordini di rimozione per l'anno di riferimento*** dovrebbero ***essere tenuti a*** pubblicare relazioni annuali sulla trasparenza contenenti informazioni utili sulle misure adottate per individuare, identificare e rimuovere contenuti terroristici. [Em. 26]

(24 bis) Le autorità competenti dell'emissione di ordini di rimozione dovrebbero altresì pubblicare relazioni sulla trasparenza contenenti informazioni sul numero di ordini di rimozione emanati, sul numero di rifiuti opposti, sul numero di contenuti terroristici individuati che hanno condotto a indagini e azioni penali in relazione a reati di terrorismo, nonché sul numero di casi di contenuti erroneamente individuati come terroristici. [Em. 27]

- (25) Le procedure di reclamo costituiscono una tutela necessaria contro la rimozione erronea di contenuti protetti nell'ambito della libertà di espressione e di informazione ~~di informazione~~ *della libertà di ricevere e diffondere informazioni e idee in una società aperta e democratica*. I prestatori di servizi di hosting dovrebbero pertanto predisporre meccanismi di facile uso per i reclami, assicurando che siano trattati tempestivamente e in piena trasparenza nei confronti del fornitore di contenuti. L'obbligo di ripristinare il contenuto rimosso erroneamente non pregiudica la possibilità che il prestatore di servizi di hosting applichi le proprie condizioni contrattuali per altri motivi. **[Em. 28]**

(26) L'articolo 19 del TUE e l'articolo 47 della Carta dei diritti fondamentali dell'Unione europea sanciscono il diritto a una tutela giurisdizionale effettiva, in forza del quale le persone devono essere in grado di conoscere il motivo per cui il contenuto da loro caricato è stato rimosso o il relativo accesso disabilitato. A tal fine, il prestatore di servizi di hosting dovrebbe mettere a disposizione del fornitore di contenuti utili informazioni, *come i motivi della rimozione o della disabilitazione dell'accesso e il fondamento giuridico alla base dell'azione*, che gli consentano di impugnare la decisione. ~~Può tuttavia non essere necessario inviare una notifica al fornitore di contenuti.~~ A seconda delle circostanze, i prestatori di servizi di hosting possono sostituire il contenuto considerato terroristico con un messaggio indicante che il contenuto è stato rimosso o disattivato in conformità del presente regolamento. ~~Su sua richiesta, il fornitore di contenuti dovrebbe ricevere maggiori informazioni sui motivi della rimozione e sui mezzi di ricorso.~~ Le autorità competenti dovrebbero informare il prestatore di servizi di hosting se, per motivi di pubblica sicurezza, in particolare nel contesto di un'indagine, ritengono inappropriato o controproducente notificare direttamente la rimozione del contenuto o la disabilitazione dell'accesso al contenuto. [Em. 29]

(27) Al fine di evitare duplicazioni ed eventuali interferenze con le indagini *e di ridurre al minimo le spese a carico dei prestatori di servizi interessati*, le autorità competenti dovrebbero scambiarsi informazioni, coordinarsi e cooperare reciprocamente e, se del caso, con Europol, quando emettono ordini di rimozione e ~~trasmettono segnalazioni~~ ai prestatori di servizi di hosting. Europol potrebbe sostenere l'attuazione delle disposizioni del presente regolamento, nel rispetto del suo attuale mandato e del quadro giuridico esistente. **[Em. 30]**

(27 bis) Le segnalazioni emesse da Europol costituiscono un modo efficace e rapido di sensibilizzare i prestatori di servizi di hosting alla presenza di contenuti specifici nei loro servizi. Questo meccanismo inteso ad allertare i prestatori di servizi di hosting nei confronti delle informazioni che possono essere considerate contenuti terroristici, che permette loro su base volontaria di esaminare la compatibilità con le proprie clausole contrattuali, dovrebbe rimanere disponibile in aggiunta agli ordini di rimozione. Per tale motivo, è importante che i prestatori di servizi di hosting collaborino con Europol, valutino le segnalazioni di Europol in via prioritaria e forniscano rapidamente un feedback in merito alle azioni intraprese. La decisione finale in merito all'opportunità di rimuovere il contenuto, in quanto non compatibile con le proprie condizioni contrattuali, spetta al prestatore di servizi di hosting. Nell'attuazione del presente regolamento, il mandato di Europol, definito nel regolamento (UE) 2016/794¹⁰, resta invariato. [Em. 31]

¹⁰ *Regolamento (UE) 2016/794 del Parlamento europeo e del Consiglio, dell'11 maggio 2016, che istituisce l'Agenzia dell'Unione europea per la cooperazione nell'attività di contrasto (Europol) e sostituisce e abroga le decisioni del Consiglio 2009/371/GAI, 2009/934/GAI, 2009/935/GAI, 2009/936/GAI e 2009/968/GAI (GU L 135 del 24.5.2016, pag. 53).*

- (28) Per garantire un'attuazione efficace e sufficientemente coerente ~~di~~ *delle* misure ~~proattive~~, *da parte dei prestatori di servizi di hosting*, le autorità competenti degli Stati membri dovrebbero consultarsi in merito alle discussioni che conducono con i prestatori di servizi di hosting *sugli ordini di rimozione* sull'identificazione, l'attuazione e la valutazione di misure ~~proattive~~ specifiche. ~~Analogamente~~. Tale cooperazione è necessaria anche per quanto riguarda l'adozione di norme in materia di sanzioni, comprese l'attuazione e l'esecuzione delle stesse. **[Em. 32]**
- (29) È essenziale che l'autorità competente dello Stato membro responsabile di infliggere le sanzioni sia pienamente informata degli ordini di rimozione ~~e delle segnalazioni~~, così come dei successivi scambi tra il prestatore di servizi di hosting e ~~le~~ *le* autorità ~~competente pertinente~~ *competenti pertinenti di altri Stati membri*. A tal fine, gli Stati membri dovrebbero provvedere affinché siano predisposti canali e meccanismi di comunicazione adeguati per condividere tempestivamente le informazioni pertinenti. **[Em. 33]**

- (30) Per facilitare il rapido scambio tra le autorità competenti nonché con i prestatori di servizi di hosting, e per evitare duplicazioni, gli Stati membri possono avvalersi degli strumenti messi a punto dall'unità addetta alle segnalazioni su Internet di Europol, ad esempio l'applicazione IRMA, attualmente in uso, per la gestione di tali segnalazioni o gli strumenti che la sostituiranno.
- (31) Considerata la particolare gravità delle conseguenze di determinati contenuti terroristici, i prestatori di servizi di hosting dovrebbero informare tempestivamente l'autorità dello Stato membro interessato o le autorità competenti del paese in cui sono stabiliti o hanno un rappresentante legale, circa l'esistenza di eventuali prove di reati di terrorismo di cui vengano a conoscenza. Ai fini di proporzionalità, tale obbligo è limitato ai reati di terrorismo quali definiti all'articolo 3, paragrafo 1, della direttiva (UE) 2017/541. L'obbligo di informare non impone ai prestatori di servizi di hosting l'obbligo di cercare attivamente tali prove. Lo Stato membro interessato è lo Stato membro che ha giurisdizione sulle indagini e sull'azione penale nei confronti dei reati di terrorismo di cui alla direttiva (UE) 2017/541 in base alla cittadinanza dell'autore o della vittima potenziale del reato o del luogo interessato dall'atto terroristico. In caso di dubbio, i prestatori di servizi di hosting possono trasmettere le informazioni a Europol, che è tenuto a darvi seguito in conformità del suo mandato, o inoltrarle alle autorità nazionali competenti.

- (32) Le autorità competenti degli Stati membri dovrebbero essere autorizzate a utilizzare tali informazioni per adottare le misure investigative previste dalla legislazione dello Stato membro o dell'Unione europea, ivi inclusa l'emissione di un ordine europeo di produzione ai sensi del regolamento relativo agli ordini europei di produzione e di conservazione di prove elettroniche in materia penale¹¹.

¹¹ COM(2018)0225.

(33) Sia i prestatori di servizi di hosting sia gli Stati membri dovrebbero istituire punti di contatto per facilitare il rapido trattamento degli ordini di rimozione ~~e delle segnalazioni~~. Contrariamente al rappresentante legale, il punto di contatto assolve compiti di natura operativa. Il punto di contatto del prestatore di servizi di hosting dovrebbe disporre degli strumenti specifici che permettono di trasmettere per via elettronica gli ordini di rimozione ~~e le segnalazioni~~ e delle risorse tecniche e personali che consentono di trattarli rapidamente. Il punto di contatto del prestatore di servizi di hosting non deve necessariamente essere situato nell'Unione e il prestatore di servizi di hosting è libero di designare un punto di contatto già esistente, a condizione che questi sia in grado di svolgere le funzioni previste dal presente regolamento. Al fine di garantire che il contenuto terroristico sia rimosso o l'accesso disattivato entro un'ora dal ricevimento di un ordine di rimozione, i prestatori di servizi di hosting dovrebbero far sì che il punto di contatto sia accessibile 24 ore su 24 e 7 giorni su 7. Le informazioni sul punto di contatto dovrebbero comprendere informazioni sulla lingua in cui il punto di contatto può essere contattato. Per facilitare la comunicazione tra i prestatori di servizi di hosting e le autorità competenti, i prestatori di servizi di hosting sono incoraggiati ad ammettere la comunicazione in una delle lingue ufficiali dell'Unione nella quale sono disponibili le loro condizioni contrattuali. **[Em. 34]**

- (34) In assenza di un obbligo generale per i prestatori di servizi di assicurare la presenza fisica all'interno del territorio dell'Unione, è necessario determinare in modo chiaro lo Stato membro nella cui giurisdizione ricade il prestatore di servizi di hosting che offre servizi all'interno dell'Unione. Generalmente, il prestatore di servizi di hosting ricade nella giurisdizione dello Stato membro in cui ha lo stabilimento principale o in cui ha designato un rappresentante legale. ~~Tuttavia, quando un altro Stato membro emette un ordine di rimozione, le sue autorità dovrebbero poter dare esecuzione ai loro ordini adottando misure coercitive di natura non punitiva, ad esempio sanzioni pecuniarie.~~ Anche se un prestatore di servizi di hosting non ha sede nell'Unione e non vi ha designato un rappresentante legale, qualsiasi Stato membro dovrebbe comunque poter infliggere sanzioni, a condizione che sia rispettato il principio del *ne bis in idem*. [Em. 35]
- (35) I prestatori di servizi di hosting che non sono stabiliti nell'Unione dovrebbero designare, per iscritto, un rappresentante legale al fine di assicurare il rispetto e l'esecuzione degli obblighi ai sensi del presente regolamento. ***I prestatori di servizi di hosting possono avvalersi di un rappresentante legale già esistente, a condizione che questi sia in grado di svolgere le funzioni previste dal presente regolamento.*** [Em. 36]

- (36) Il rappresentante legale dovrebbe essere legalmente autorizzato ad agire per conto del prestatore di servizi di hosting.
- (37) Ai fini dell'applicazione del presente regolamento, gli Stati membri dovrebbero designare **un'unica** autorità ~~competenti~~. **giudiziaria o un'unica autorità amministrativa indipendente dal punto di vista funzionale.** ~~L'~~Tale obbligo di designare le autorità ~~competenti~~ non richiede necessariamente l'istituzione di nuove **una nuova** autorità; i compiti stabiliti dal presente regolamento possono essere assegnati ad organismi esistenti **a un organismo esistente**. Il presente regolamento fa obbligo di designare **un'**autorità ~~competenti~~ **competente** a emettere ordini di rimozione e segnalazioni, vigilare sulle misure proattive **specifiche** e infliggere sanzioni. ~~Spetta agli~~ **Gli** Stati membri ~~decidere quante autorità intendono designare per tali compiti~~ **dovrebbero comunicare l'autorità competente designata a norma del presente regolamento alla Commissione, che dovrebbe pubblicare online un elenco indicante l'autorità competente di ciascuno Stato membro. Il 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.** [Em. 37]

(38) Le sanzioni sono necessarie per garantire che i prestatori di servizi di hosting diano effettiva attuazione agli obblighi previsti dal presente regolamento. Occorre che gli Stati membri adottino norme relative alle sanzioni, comprese, eventualmente, linee guida per il calcolo delle stesse. ~~Sanzioni particolarmente severe~~ Dovrebbero essere inflitte **sanzioni** nel caso in cui il ~~prestatore~~ ***i prestatori*** di servizi di hosting ~~ometta~~ ***omettano*** sistematicamente ~~di rimuovere contenuti terroristici o di disabilitarne l'accesso entro un'ora dal ricevimento di un ordine di rimozione.~~ La mancata conformità in casi individuali potrebbe essere sanzionata nel rispetto del principio *ne bis in idem* e del principio di proporzionalità, assicurando che tali sanzioni tengano conto dell'inosservanza sistematica. Al fine di garantire la certezza del diritto, il regolamento dovrebbe stabilire in che misura gli obblighi pertinenti possano essere soggetti a sanzioni. ***e persistentemente di ottemperare agli obblighi che incombono loro in virtù del presente regolamento.*** Sanzioni in caso di mancato rispetto dell'articolo 6 dovrebbero essere adottate solo in relazione agli obblighi derivanti dalla ***da una*** richiesta di riferire a norma dell'articolo 6, paragrafo 2, o da una decisione che impone ***di attuazione di*** misure proattive ***specifiche*** supplementari a norma dell'articolo 6, paragrafo 4. Nel determinare se debbano essere inflitte sanzioni pecuniarie si dovrebbe tenere debito conto delle risorse finanziarie del prestatore. ***L'autorità competente dovrebbe altresì considerare se il prestatore di servizi di hosting è una start-up o una piccola o media impresa e dovrebbe stabilire, caso per caso, se il prestatore ha la capacità di conformarsi in maniera adeguata all'ordine emesso.*** Gli Stati membri ~~assicurano~~ ***dovrebbero assicurare*** che le sanzioni non incoraggino la rimozione di contenuti che non hanno natura terroristica. [Em. 38]

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

(40) Per poter modificare rapidamente, se necessario, il contenuto del modello da utilizzare ai fini del presente regolamento, è opportuno delegare alla Commissione il potere di adottare atti conformemente all'articolo 290 del trattato sul funzionamento dell'Unione europea riguardo alla modifica degli allegati I, II e III del presente regolamento. Per tenere conto dello sviluppo tecnologico e del relativo quadro giuridico, alla Commissione dovrebbe essere inoltre conferito il potere di adottare atti delegati al fine di integrare il presente regolamento con requisiti tecnici per gli strumenti elettronici destinati ad essere utilizzati dalle autorità competenti per trasmettere gli ordini di rimozione. È di particolare importanza che durante i lavori preparatori la Commissione svolga adeguate consultazioni, anche a livello di esperti, nel rispetto dei principi stabiliti nell'accordo interistituzionale "Legiferare meglio" del 13 aprile 2016¹². In particolare, al fine di garantire la parità di partecipazione alla preparazione degli atti delegati, il Parlamento europeo e il Consiglio ricevono tutti i documenti contemporaneamente agli esperti degli Stati membri, e i loro esperti hanno sistematicamente accesso alle riunioni dei gruppi di esperti della Commissione incaricati della preparazione di tali atti delegati.

- (41) Gli Stati membri dovrebbero raccogliere informazioni sull'attuazione della legislazione, *includere informazioni sul numero di casi in cui l'indagine, l'accertamento e il perseguimento di reati terroristici hanno avuto un esito positivo a seguito 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 della normativa. **[Em. 39]**

(42) Sulla base delle constatazioni e conclusioni formulate nella relazione di attuazione e dell'esito dell'esercizio di monitoraggio, la Commissione dovrebbe effettuare una valutazione del presente regolamento ~~non prima di tre anni~~ **dopo un anno** dalla sua entrata in vigore. La valutazione dovrebbe essere basata sui ~~cinque~~ **sette** criteri di efficienza, **necessità, proporzionalità**, efficacia, pertinenza, coerenza e valore aggiunto dell'UE. ~~Sarà valutato~~ **Dovrebbe esaminare** il funzionamento delle diverse misure operative e tecniche previste dal regolamento, in particolare l'efficacia delle misure volte a migliorare l'individuazione, l'identificazione e la rimozione di contenuti terroristici, l'efficacia dei meccanismi di salvaguardia nonché le potenziali conseguenze per i diritti **fondamentali, inclusi la libertà di espressione e la libertà di ricevere e diffondere informazioni, 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, compresa una revisione dell'obbligo di informare i fornitori di contenuti.

[Em. 40]

(43) Poiché l'obiettivo del presente regolamento, ossia garantire il buon funzionamento del mercato unico digitale mediante la prevenzione della diffusione di contenuti terroristici online, non può essere conseguito in misura sufficiente dagli Stati membri e può dunque, a motivo della portata e degli effetti dell'azione in questione, essere conseguito meglio a livello di Unione, quest'ultima può intervenire in base al principio di sussidiarietà sancito dall'articolo 5 del trattato sull'Unione europea. Il presente regolamento si limita a quanto è necessario per conseguire tale obiettivo in ottemperanza al principio di proporzionalità enunciato nello stesso articolo,

HANNO ADOTTATO IL PRESENTE REGOLAMENTO:

SEZIONE I
DISPOSIZIONI GENERALI

Articolo 1

Oggetto e ambito di applicazione

1. Il presente regolamento stabilisce regole uniformi *mirate* per ~~impedire~~ *contrastare* l'uso improprio dei servizi di hosting ai fini della diffusione *pubblica* di contenuti terroristici online. Esso prevede in particolare: **[Em. 41]**
 - a) norme relative agli obblighi di diligenza *ragionevoli e proporzionati* che i prestatori di servizi di hosting sono tenuti ad applicare per ~~impedire~~ *contrastare* la diffusione *pubblica* di contenuti terroristici tramite i loro servizi e garantirne, ove necessario, la rapida rimozione; **[Em. 42]**
 - b) una serie di misure che gli Stati membri sono tenuti ad attuare per individuare i contenuti terroristici, consentirne la rapida rimozione da parte dei prestatori di servizi di hosting, *conformemente alla legislazione dell'Unione che prevede salvaguardie adeguate in materia di libertà di espressione e di libertà di ricevere e diffondere informazioni e idee in una società aperta e democratica*, e facilitare la cooperazione con le autorità competenti di altri Stati membri, i prestatori di servizi di hosting e, se del caso, gli organismi pertinenti dell'Unione. **[Em. 43]**

2. Il presente regolamento si applica ai prestatori di servizi di hosting che offrono servizi *al pubblico* nell'Unione, indipendentemente dal luogo del loro stabilimento principale. [Em. 44]
- 2 bis. Il presente regolamento non si applica ai contenuti diffusi per scopi educativi, artistici, giornalistici o di ricerca o per finalità di sensibilizzazione, né ai contenuti che rappresentano l'espressione di opinioni polemiche o controverse nell'ambito di dibattiti pubblici. [Em. 45]*
- 2 ter. 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 del trattato sull'Unione europea e si applica fatti salvi i principi fondamentali sanciti nel diritto nazionale e dell'Unione per quanto concerne la libertà di parola, la libertà di stampa nonché la libertà e il pluralismo dei media. [Em. 46]*
- 2 quater. Il presente regolamento non pregiudica la direttiva 2000/31/CE. [Em. 47]*

Articolo 2
Definizioni

Ai fini del presente regolamento si applicano le seguenti definizioni:

- 1) ***"servizi della società dell'informazione": i servizi di cui all'articolo 2, lettera a), della direttiva 2000/31/CE; [Em. 48]***
- 1) "prestatore di servizi di hosting": un prestatore di servizi della società dell'informazione che consistono nel memorizzare informazioni fornite dal fornitore di contenuti su richiesta di quest'ultimo e nel rendere le informazioni memorizzate disponibili a terzi ***al pubblico. Tale definizione si applica esclusivamente ai servizi forniti al pubblico al livello applicazioni. I fornitori di infrastrutture cloud e i fornitori di cloud non sono considerati prestatori di servizi di hosting. Analogamente, tale definizione non si applica ai servizi di comunicazione elettronica di cui alla direttiva (UE) 2018/1972; [Em. 49]***
- 2) "fornitore di contenuti": un utilizzatore che ha fornito informazioni che sono (o sono state) memorizzate ***o rese disponibili al pubblico***, su sua richiesta, da un prestatore di servizi di hosting; **[Em. 50]**

- 3) "offrire servizi nell'Unione": consentire a persone fisiche o giuridiche in uno o più Stati membri di utilizzare i servizi del prestatore di servizi di hosting che presenta un collegamento sostanziale con tale Stato membro o con tali Stati membri, ad esempio:
- a) lo stabilimento del prestatore di servizi di hosting nell'Unione;
 - b) un numero significativo di utenti in uno o più Stati membri;
 - c) orientamento delle attività verso uno o più Stati membri;
- 4) ~~"reati di terrorismo": i reati ai sensi dell'articolo 3, paragrafo 1, della direttiva (UE) 2017/541;~~ **[Em. 51]**
- 5) "contenuto terroristico": uno o più dei seguenti ~~messaggi~~ **materiali**: **[Em. 52]**
- a) istigazione, ~~anche~~ ***alla commissione di uno dei reati di cui all'articolo 3, paragrafo 1, lettere da a) a i), della direttiva (UE) 2017/541, se tale comportamento, direttamente o indirettamente, ad esempio*** mediante l'apologia del terrorismo ***di atti terroristici***, ~~alla commissione di~~ ***inciti a compiere*** reati di terrorismo, generando in tal modo il pericolo che ***uno o più di*** tali reati siano effettivamente ***possano essere*** commessi ***intenzionalmente***; **[Em. 53]**

- b) ~~incitamento a~~ *sollecitazione nei confronti di un'altra persona o di un altro gruppo di persone a commettere o contribuire a* ~~alla commissione di uno dei reati di terrorismo~~ *cui all'articolo 3, paragrafo 1, lettere da a) a i), della direttiva (UE) 2017/541, generando in tal modo il pericolo che uno o più di tali reati possano essere commessi intenzionalmente;* [Em. 54]
- c) ~~promozione delle~~ *sollecitazione nei confronti di un'altra persona o di un altro gruppo di persone a prendere parte alle* attività di un gruppo terroristico, ~~in particolare incoraggiando la partecipazione o il sostegno a un,~~ *ivi compreso fornendo informazioni o risorse materiali o finanziando in qualsiasi modo le attività di tale* gruppo terroristico ~~ai sensi dell'articolo 2, paragrafo 3, 4 della direttiva (UE) 2017/541,~~ *generando in tal modo il pericolo che uno o più di tali reati possano essere commessi intenzionalmente;* [Em. 55]
- d) *l'atto di impartire* istruzioni ~~su~~ *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;* [Em. 56]

d bis) descrizione della commissione di uno o più dei reati di cui all'articolo 3, paragrafo 1, lettere da a) a i), della direttiva (UE) 2017/541, generando in tal modo il pericolo che uno o più di tali reati possano essere commessi intenzionalmente; [Em. 57]

- 6) "diffusione di contenuti terroristici": il fatto di rendere accessibili a terzi **al pubblico** i contenuti terroristici tramite i servizi dei prestatori di servizi di hosting; [Em. 58]
- 7) "condizioni contrattuali": tutte le modalità, le condizioni e le clausole che, indipendentemente dalla loro denominazione o forma, disciplinano il rapporto contrattuale tra il prestatore di servizi di hosting e gli utilizzatori di tali servizi;
- ~~8) "segnalazione": un avviso trasmesso da un'autorità competente o, se del caso, da un pertinente organismo dell'Unione a un prestatore di servizi di hosting in merito a contenuti che possono essere considerati contenuti terroristici, affinché il prestatore proceda, su base volontaria, alla verifica della compatibilità con le proprie condizioni contrattuali al fine di prevenire la diffusione di contenuti terroristici; [Em. 59]~~
- 9) "stabilimento principale": la sede centrale o la sede legale nella quale sono esercitate le principali funzioni finanziarie ed eseguiti i controlli operativi.

9 bis) "autorità competente": un'unica autorità giudiziaria designata o un'autorità amministrativa indipendente dal punto di vista funzionale nello Stato membro.
[Em. 60]

SEZIONE II

Misure volte a prevenire la diffusione di contenuti terroristici online

Articolo 3

Obblighi di diligenza

1. I prestatori di servizi di hosting ~~adottano~~, **agiscono** in conformità al presente regolamento, ~~misure adeguate, ragionevoli e proporzionate~~, per ~~prevenire la diffusione di contenuti terroristici~~ e proteggere gli utilizzatori ~~da tali~~ **dai** contenuti **terroristici**. ~~In tale contesto~~, Essi agiscono in modo diligente, proporzionato e non discriminatorio, prestano il debito rispetto **in tutte le circostanze** ai diritti fondamentali degli utilizzatori e tengono conto della fondamentale importanza che ~~riveste~~ **rivestono** la libertà di espressione e **la libertà** di ~~informazione~~ **ricevere e trasmettere informazioni e idee** in una società aperta e democratica, **al fine di evitare l'eliminazione dei contenuti non terroristici**. [Em. 61]

- 1 bis. Tali obblighi di diligenza non costituiscono un obbligo generale per i prestatori di servizi di hosting di sorvegliare le informazioni che trasmettono o memorizzano né un obbligo generale di ricercare attivamente fatti o circostanze che indichino la presenza di attività illecite. [Em. 62]***
- ~~2. I prestatori di servizi di hosting includono nelle loro condizioni contrattuali disposizioni volte a prevenire la diffusione di contenuti terroristici e ne assicurano l'applicazione. [Em. 63]~~
- 2 bis. Laddove siano a conoscenza o siano consapevoli dell'esistenza di contenuti terroristici nei loro servizi, i prestatori di servizi di hosting ne informano le autorità competenti ed eliminano tali contenuti rapidamente. [Em. 64]***
- 2 ter. I prestatori di servizi di hosting che soddisfano i criteri della definizione di fornitori di piattaforme per la condivisione di video a norma della direttiva (UE) 2018/1808 adottano misure appropriate per contrastare la diffusione di contenuti terroristici conformemente all'articolo 28 ter, paragrafo 1, lettera c), e paragrafo 3, della direttiva (UE) 2018/1808. [Em. 65]***

Articolo 4

Ordini di rimozione di contenuti

1. L'autorità competente *dello Stato membro in cui il prestatore di servizi di hosting ha il suo stabilimento principale* ha facoltà di adottare ~~una decisione~~ *un ordine di rimozione* che imponga al prestatore di servizi di hosting di rimuovere contenuti terroristici o di disabilitarne l'accesso *in tutti gli Stati membri*. [Em. 66]
- 1 bis.* *L'autorità competente di uno Stato membro in cui il prestatore di servizi di hosting non ha la sua sede principale o un rappresentante legale può chiedere che l'accesso ai contenuti terroristici sia disabilitato e dare esecuzione a tale richiesta all'interno del suo territorio.* [Em. 67]
- 1 ter.* *Se l'autorità competente interessata non ha rilasciato in precedenza un ordine di rimozione a un prestatore di servizi di hosting, contatta il prestatore di servizi di hosting, fornendo informazioni sulle procedure e i termini applicabili, almeno 12 ore prima del rilascio di un ordine di rimozione.* [Em. 68]

2. I prestatori di servizi di hosting rimuovono i contenuti terroristici o ne disabilitano l'accesso *il prima possibile e* entro un'ora dal ricevimento dell'ordine di rimozione. **[Em. 69]**
3. Gli ordini di rimozione recano i seguenti elementi in conformità al modello di cui all'allegato I:
 - a) l'identificazione, *tramite firma elettronica*, dell'autorità competente che emette l'ordine di rimozione e l'autenticazione dell'ordine di rimozione da parte dell'autorità competente; **[Em. 70]**
 - b) la motivazione *dettagliata* per cui il contenuto è considerato contenuto terroristico, ~~almeno con~~ *e un* riferimento *specifico* alle categorie di contenuti terroristici elencati all'articolo 2, paragrafo 5; **[Em. 71]**
 - c) un indirizzo URL (Uniform Resource Locator) *esatto* e, se necessario, ulteriori informazioni che consentano di individuare il contenuto in questione; **[Em. 72]**
 - d) un riferimento al presente regolamento come base giuridica dell'ordine di rimozione;

- e) la data e l'ora dell'emissione dell'ordine;
- f) informazioni *facilmente comprensibili* sui mezzi di ricorso a disposizione del prestatore di servizi di hosting e del fornitore di contenuti, *ivi compresi il ricorso all'autorità competente nonché il ricorso a un organo giurisdizionale e i termini per il ricorso*; [Em. 73]
- g) ~~se del caso~~ *ove necessario e proporzionato*, la decisione di cui all'articolo 11 di non divulgare informazioni sulla rimozione dei contenuti terroristici o sulla disabilitazione dell'accesso a tali contenuti. [Em. 74]

~~4. Su richiesta del prestatore di servizi di hosting o del fornitore di contenuti, l'autorità competente trasmette una motivazione dettagliata, fermo restando l'obbligo del prestatore di servizi di hosting di conformarsi all'ordine di rimozione entro il termine di cui al paragrafo 2. [Em. 75]~~

5. ~~Le autorità competenti indirizzano~~ *L'autorità competente indirizza* l'ordine di rimozione allo stabilimento principale del prestatore di servizi di hosting o al rappresentante legale designato dal prestatore di servizi di hosting ai sensi dell'articolo 16 e lo ~~trasmettono~~ *trasmette* al punto di contatto di cui all'articolo 14, paragrafo 1. Tali ordini sono trasmessi con mezzi elettronici che producano una traccia scritta in condizioni che consentano di stabilire l'autenticazione del mittente, compresa l'esattezza della data e dell'ora di invio e di ricezione dell'ordine. **[Em. 76]**

6. I prestatori di servizi di hosting ~~accusano ricevuta e~~ informano senza indebito ritardo l'autorità competente della rimozione dei contenuti terroristici o della disabilitazione dell'accesso agli stessi, indicando, in particolare, la data e l'ora dell'intervento, utilizzando il modello di cui all'allegato II. **[Em. 77]**

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, ***anche per motivi tecnici o operativi***, il prestatore di servizi di hosting ne informa, senza indebito ritardo, l'autorità competente e ne spiega i motivi, utilizzando il modello di cui all'allegato III. La scadenza di cui al paragrafo 2 si applica non appena i motivi addotti vengono meno. **[Em. 78]**
8. ~~Se non è in grado~~ ***Il prestatore di servizi di hosting può rifiutare*** di conformarsi all'ordine ~~eseguire l'ordine~~ di rimozione, ~~in quanto il~~ ***se tale*** provvedimento è viziato da errori manifesti o non contiene informazioni sufficienti ~~per l'esecuzione dell'ordine~~, il prestatore di servizi di hosting ne informa, senza indebito ritardo, l'autorità competente e chiede i chiarimenti necessari, utilizzando il modello di cui all'allegato III. La scadenza di cui al paragrafo 2 si applica non appena sono forniti i chiarimenti. **[Em. 79]**

9. L'autorità competente che ha emesso l'ordine di rimozione informa l'autorità competente che vigila sull'attuazione delle misure ~~proattive~~ *specifiche* di cui all'articolo 17, paragrafo 1, lettera c), quando l'ordine di rimozione diventa definitivo. Un ordine di rimozione diventa definitivo se non è oggetto di ricorso entro il termine stabilito in conformità al diritto nazionale applicabile o se è stato confermato in esito al ricorso. **[Em. 80]**

Articolo 4 bis

Procedura di consultazione per gli ordini di rimozione

- 1. L'autorità competente che emette un ordine di rimozione a norma dell'articolo 4, paragrafo 1 bis, trasmette una copia dell'ordine di rimozione all'autorità giudiziaria competente di cui all'articolo 17, paragrafo 1, lettera a), dello Stato membro nel quale il prestatore di servizi di hosting ha lo stabilimento principale nel momento stesso in cui l'ordine è trasmesso al prestatore di servizi di hosting conformemente all'articolo 4, paragrafo 5.*

- 2. Qualora l'autorità competente dello Stato membro in cui è situato lo stabilimento principale del prestatore di servizi di hosting abbia fondati motivi di ritenere che l'ordine di rimozione possa incidere sugli interessi fondamentali di tale Stato membro, essa informa al riguardo l'autorità di emissione competente. L'autorità di emissione tiene conto di tali circostanze e, se necessario, ritira o adegua l'ordine di rimozione. [Em. 81]*

Articolo 4 ter

Procedura di cooperazione per il rilascio di un ordine di rimozione supplementare

- 1. Se un'autorità competente ha emesso un ordine di rimozione a norma dell'articolo 4, paragrafo 1 bis, tale autorità può contattare l'autorità competente dello Stato membro in cui il prestatore di servizi di hosting ha il suo stabilimento principale al fine di chiedere che quest'ultima autorità competente emetta altresì un ordine di rimozione di cui all'articolo 4, paragrafo 1.*

- 2. L'autorità competente dello Stato membro in cui si trova lo stabilimento principale del prestatore di servizi di hosting emette un ordine di rimozione o rifiuta di emettere un ordine quanto prima ma non oltre un'ora dal momento in cui è stata contattata a norma del paragrafo 1 e informa l'autorità competente che ha emesso il primo ordine della sua decisione.*

3. *Laddove un'autorità competente di uno Stato membro di stabilimento principale necessita di più di un'ora per effettuare la propria valutazione del contenuto, essa presenta al prestatore di servizi di hosting interessato la richiesta di disabilitare temporaneamente l'accesso al contenuto per un massimo di 24 ore e in tale periodo l'autorità competente esegue la valutazione e invia l'ordine di rimozione o ritira la richiesta di disabilitare l'accesso. [Em. 82]*

Articolo 5

Segnalazioni

1. ~~L'autorità competente o l'organismo competente dell'Unione può inviare una segnalazione a un prestatore di servizi di hosting.~~
2. ~~I prestatori di servizi di hosting mettono in atto misure operative e tecniche per agevolare la rapida valutazione dei contenuti che le autorità competenti e, se del caso, gli organismi pertinenti dell'Unione segnalano loro affinché provvedano, su base volontaria, ad esaminarli.~~

- ~~3. La segnalazione è indirizzata allo stabilimento principale del prestatore di servizi di hosting o al rappresentante legale designato dal prestatore di servizi di hosting ai sensi dell'articolo 16 e trasmessa al punto di contatto di cui all'articolo 14, paragrafo 1. Tali segnalazioni sono trasmesse per via elettronica.~~
- ~~4. La segnalazione contiene informazioni sufficientemente dettagliate, segnatamente i motivi per i quali il contenuto è considerato contenuto terroristico, un URL e, se necessario, ulteriori informazioni che consentano di individuare il contenuto terroristico oggetto della segnalazione.~~
- ~~5. Il prestatore di servizi di hosting procede, in via prioritaria, a valutare il contenuto individuato nella segnalazione rispetto alle proprie condizioni contrattuali e decide se rimuovere tale contenuto o disabilitarne l'accesso.~~
- ~~6. Il prestatore di servizi di hosting informa rapidamente la competente autorità o l'organismo competente dell'Unione dell'esito della valutazione e della tempistica di eventuali misure prese a seguito della segnalazione.~~

~~7. Se ritiene che la segnalazione non contenga informazioni sufficienti per valutare il contenuto in oggetto, il prestatore di servizi di hosting ne informa senza indugio l'autorità competente o l'organismo dell'Unione competente, precisando quali ulteriori informazioni o chiarimenti sono necessari. [Em. 83]~~

Articolo 6

Misure proattive *specifiche* [Em. 84]

1. ~~Fatte salve la direttiva (UE) 2018/1808 e la direttiva 2000/31/CE, i~~ prestatori di servizi di hosting ~~adottano, se del caso, possono adottare~~ misure proattive *specifiche* per proteggere i loro servizi dalla diffusione *pubblica* di contenuti terroristici. Tali misure sono efficaci, *mirate* e proporzionate, ~~in considerazione del~~ *e prestano particolare attenzione al* rischio e ~~del~~ *al* livello di esposizione a contenuti terroristici, ~~dei~~ *ai* diritti fondamentali degli utilizzatori e ~~dell'importanza~~ *all'importanza* fondamentale che ~~riposte~~ *rivestono* la libertà di espressione e *la libertà* di ~~informazione~~ *ricevere e trasmettere informazioni e idee* in una società aperta e democratica. [Em. 85]

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

- ~~a) prevenire che siano nuovamente caricati online i contenuti che erano stati rimossi o il cui accesso era stato disattivato perché considerati contenuti terroristici;~~
- ~~b) individuare, identificare e rimuovere prontamente i contenuti terroristici o disabilitarne l'accesso.~~

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

La relazione contiene tutte le informazioni pertinenti che consentano all'autorità competente di cui all'articolo 17, paragrafo 1, lettera c), di valutare se le misure proattive sono efficaci e proporzionate, anche per valutare il funzionamento degli strumenti automatizzati utilizzati nonché la sorveglianza umana e i meccanismi di verifica applicati. [Em. 86]

3. Se ritiene che le misure proattive adottate e trasmesse a norma del paragrafo 2 non siano sufficienti per attenuare e gestire il rischio e il livello di esposizione, l'autorità competente di cui all'articolo 17, paragrafo 1, lettera c), può richiedere al prestatore di servizi di hosting di adottare specifiche misure proattive supplementari. A tal fine, il prestatore di servizi di hosting coopera con l'autorità competente di cui all'articolo 17, paragrafo 1, lettera c), al fine di individuare le misure specifiche che è tenuto ad attuare, definire i principali obiettivi e criteri di riferimento, nonché il calendario dell'attuazione. [Em. 87]

4. Se non è possibile raggiungere *Dopo aver accertato che* un accordo entro tre mesi dalla richiesta *prestatore di servizi di hosting ha ricevuto un numero significativo* di cui al paragrafo 3 *ordini di rimozione*, l'autorità competente di cui all'articolo 17, paragrafo 1, lettera c), può emettere *inviare* una decisione *richiesta di misure specifiche necessarie, proporzionate ed efficaci aggiuntive che il prestatore di servizi di hosting dovrà attuare. L'autorità competente non* impone l'adozione di ~~specifiche misure proattive supplementari necessarie e proporzionate~~ *un obbligo generale di sorveglianza né l'utilizzo di strumenti automatizzati*. La decisione *richiesta* tiene conto, in particolare, della *fattibilità tecnica delle misure, delle dimensioni e della* capacità economica del prestatore di servizi di hosting, delle ripercussioni di tali misure sui diritti fondamentali degli utilizzatori e dell'importanza fondamentale della libertà di espressione e *della libertà di informazione-ricevere e trasmettere informazioni e idee in una società aperta e democratica*. La ~~decisione~~ *richiesta* è indirizzata allo stabilimento principale del prestatore di servizi di hosting o al rappresentante legale designato dal prestatore di servizi di hosting. Il prestatore di servizi di hosting rende periodicamente conto dell'attuazione di tali misure, secondo le indicazioni dell'autorità competente di cui all'articolo 17, paragrafo 1, lettera c). [Em. 88]

5. Il prestatore di servizi di hosting può, in qualsiasi momento, chiedere un riesame all'autorità competente di cui all'articolo 17, paragrafo 1, lettera c), e, eventualmente, la revoca della richiesta ~~o della decisione~~ di cui, rispettivamente, ~~ai paragrafi 2, 3 e~~ **al paragrafo 4**. L'autorità competente adotta una decisione motivata entro un termine ragionevole dopo aver ricevuto la richiesta del prestatore di servizi di hosting. **[Em. 89]**

Articolo 7

Conservazione del contenuto e dei relativi dati

1. Il prestatore di servizi di hosting conserva i contenuti terroristici rimossi o disabilitati a seguito di un ordine di rimozione, ~~di una segnalazione~~ o di misure ~~proattive~~ **specifiche** in conformità degli articoli ~~4, 5~~ e 6 e i relativi dati rimossi in conseguenza della rimozione del contenuto terroristico e che sono necessari per: **[Em. 90]**
- a) i procedimenti di riesame ~~amministrativo~~ **o ricorso amministrativi** o ~~giudiziario~~ **giudiziari**; **[Em. 91]**
 - b) la prevenzione, l'accertamento, l'indagine o il perseguimento di reati di terrorismo **da parte delle autorità di contrasto**. **[Em. 92]**

2. I contenuti terroristici e i relativi dati di cui al paragrafo 1, **lettera a)**, sono conservati per un periodo di sei mesi **e cancellati al termine di tale periodo**. Su richiesta dell'autorità competente o di un organo giurisdizionale, i contenuti terroristici sono conservati per un periodo ~~più lungo~~ **successivamente specificato soltanto in caso di necessità** e per tutto il tempo necessario per il procedimento di riesame **o ricorso amministrativo o giudiziario** in corso di cui al paragrafo 1, lettera a). **I prestatori di servizi di hosting conservano i contenuti terroristici e i relativi dati di cui al paragrafo 1, lettera b), finché l'autorità di contrasto non reagisce alla notifica effettuata dal prestatore di servizi di hosting in conformità dell'articolo 13, paragrafo 4, ma non oltre sei mesi.** [Em. 93]

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

Tali salvaguardie tecniche e organizzative assicurano che i contenuti terroristici e i relativi dati conservati siano consultati e trattati solo per le finalità di cui al paragrafo 1, e garantiscono un elevato livello di sicurezza dei dati personali in questione. I prestatori di servizi di hosting riesaminano e aggiornano tali salvaguardie ogniqualvolta sia necessario.

SEZIONE III
SALVAGUARDIE E RENDICONTAZIONE

Articolo 8

Obblighi di trasparenza *per i prestatori di servizi di hosting* [Em. 94]

1. ***Ove applicabile, i*** prestatori di servizi di hosting definiscono nelle loro condizioni contrattuali la loro politica volta ad impedire la diffusione di contenuti terroristici, che include, se del caso, una valida spiegazione del funzionamento delle misure proattive, compreso l'uso di strumenti automatizzati *specifiche*. [Em. 95]
2. I prestatori di servizi di hosting ~~pubblicano~~ ***che sono o sono stati soggetti a un ordine di rimozione nell'anno di riferimento rendono pubblicamente disponibili*** relazioni annuali sulla trasparenza in merito alle misure intraprese contro la diffusione di contenuti terroristici. [Em. 96]
3. Le relazioni sulla trasparenza contengono almeno le seguenti informazioni:
 - a) informazioni sulle misure intraprese dal prestatore di servizi di hosting per quanto concerne l'individuazione, l'identificazione e la rimozione di contenuti terroristici;

- b) informazioni sulle misure intraprese dal prestatore di servizi di hosting per prevenire che siano nuovamente caricati online i contenuti che erano stati rimossi o ai quali l'accesso era stato disabilitato perché considerati contenuti terroristici, ***in particolare se sono state utilizzate tecnologie automatizzate***; [Em. 97]
- c) il numero di messaggi con contenuto terroristico che sono stati rimossi o ai quali l'accesso è stato disattivato, a seguito, rispettivamente, di ordini di rimozione, segnalazioni o misure proattive ***o misure specifiche e il numero di ordini il cui contenuto non è stato rimosso a norma dell'articolo 4, paragrafi 7 e 8, congiuntamente alle motivazioni del rifiuto***; [Em. 98]
- d) ~~un quadro sintetico~~ ***il numero*** e i risultati dei procedimenti di reclamo ***e azioni di riesame giudiziario, compreso il numero di casi in cui è stato accertato che i contenuti sono stati erroneamente identificati come contenuti terroristici.*** [Em. 99]

Articolo 8 bis

Obblighi di trasparenza delle autorità competenti

- 1. Le autorità competenti pubblicano relazioni annuali sulla trasparenza che includono almeno le seguenti informazioni:*
 - a) il numero di ordini di rimozione emessi, il numero di rimozioni e il numero di ordini di rimozione rifiutati o ignorati;*
 - b) il numero di contenuti terroristici individuati che hanno portato all'indagine e al perseguimento di reati e il numero di vasi di contenuti erroneamente individuati come terroristici;*
 - c) una descrizione delle misure richieste dalle autorità competenti a norma dell'articolo 6, paragrafo 4. [Em. 100]*

Articolo 9

Salvaguardie specifiche per quanto riguarda l'uso e l'attuazione di misure ~~proattive~~ **specifiche**

[Em. 101]

1. Laddove utilizzino, ~~in conformità al presente regolamento,~~ strumenti automatizzati in relazione ai contenuti che memorizzano, i prestatori di servizi di hosting predispongono misure di salvaguardia efficaci e appropriate per garantire l'accuratezza e la fondatezza delle decisioni relative a tali contenuti, in particolare delle decisioni di rimuovere i contenuti considerati terroristici o di disabilitarne l'accesso. **[Em. 102]**
2. Tali misure di salvaguardia comprendono, in particolare, la sorveglianza umana e meccanismi di verifica ~~ove opportuno e~~ ***dell'adeguatezza della decisione di rimuovere un contenuto o di negarvi l'accesso,*** in ogni caso, ~~quando sia necessaria una valutazione dettagliata del contesto pertinente al fine di determinare se i~~ contenuti siano da considerare terroristici ***particolare per quanto riguarda il diritto alla libertà di espressione e alla libertà di ricevere e trasmettere informazioni e idee in una società aperta e democratica.*** **[Em. 103]**

Articolo 9 bis
Ricorso effettivo

1. *I fornitori di contenuti i cui contenuti sono stati rimossi o ai quali l'accesso è stato disabilitato a seguito di un ordine di rimozione e i prestatori di servizi di hosting che hanno ricevuto un ordine di rimozione hanno il diritto a un ricorso effettivo. Gli Stati membri mettono in atto procedure efficaci per l'esercizio di tale diritto.*
[Em. 104]

Articolo 10
Meccanismi di reclamo

1. I prestatori di servizi di hosting predispongono ~~meccanismi efficaci~~ **un meccanismo efficace** e ~~accessibili~~ **accessibile** che ~~consentono~~ **consente** ai fornitori di contenuti il cui contenuto è stato rimosso o reso inaccessibile a seguito di una segnalazione a ~~norma dell'articolo 5~~ o di misure ~~proattive~~ **specifiche** a norma dell'articolo 6, di presentare un reclamo nei confronti della misura adottata dal prestatore di servizi di hosting, chiedendo la reintegrazione del contenuto. [Em. 105]

2. I prestatori di servizi di hosting esaminano tempestivamente ogni reclamo che ricevono e ripristinano il contenuto senza indebito ritardo quando la rimozione o la disabilitazione dell'accesso si rivela ingiustificata. Essi informano l'autore del reclamo delle conclusioni del loro esame ***entro due settimane dal ricevimento del reclamo, fornendo una spiegazione laddove decidano di non ripristinare il contenuto. Il ripristino del contenuto non osta all'adozione di ulteriori misure giudiziarie nei confronti della decisione del prestatore di servizi di hosting o dell'autorità competente.*** [Em. 106]

Articolo 11

Informazioni ai fornitori di contenuti

1. Quando rimuove contenuti terroristici o ne disabilita l'accesso, il prestatore di servizi di hosting mette a disposizione del fornitore di contenuti informazioni ***complete e concise*** concernenti la rimozione o la disabilitazione dell'accesso a tali contenuti ***e le possibilità di impugnare la decisione e fornisce, su richiesta, una copia dell'ordine di rimozione emesso a norma dell'articolo 4.*** [Em. 107]

- ~~2. Su richiesta del fornitore di contenuti, il prestatore di servizi di hosting gli comunica i motivi della rimozione o della disabilitazione dell'accesso e lo informa delle possibilità di ricorso. [Em. 108]~~
3. L'obbligo previsto ai paragrafi *al paragrafo 1 e 2* non si applica se l'autorità competente decide, *sulla base di prove oggettive e tenuto conto della proporzionalità e necessità di tale decisione*, che la motivazione non sia divulgata per ragioni di pubblica sicurezza, quali la prevenzione, l'indagine, l'accertamento e il perseguimento di reati di terrorismo, per il tempo necessario, ma non superiore a {quattro} settimane da tale decisione. In tal caso, il prestatore di servizi di hosting si astiene dal divulgare qualsiasi informazione concernente la rimozione o la disabilitazione dell'accesso a contenuti terroristici. [Em. 109]

SEZIONE IV

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

Articolo 12

Capacità delle autorità competenti

Gli Stati membri assicurano che le autorità competenti dispongano della capacità necessaria e di risorse sufficienti per conseguire gli obiettivi e adempiere gli obblighi loro incombenti a norma del presente regolamento, *con solide garanzie di indipendenza*. [Em. 110]

Articolo 13

Cooperazione tra i prestatori di servizi di hosting, le autorità competenti e, se del caso, gli organismi ~~pertinenti~~ *competenti* dell'Unione **[Em. 111]**

1. Le autorità competenti degli Stati membri scambiano informazioni, si coordinano e cooperano tra loro e, se del caso, con ~~i pertinenti organismi dell'Unione quali~~ Europol, per quanto riguarda gli ordini di rimozione ~~e le segnalazioni~~, in modo da evitare duplicazioni, potenziare il coordinamento ed evitare qualsiasi interferenza con indagini in corso nei diversi Stati membri. **[Em. 112]**
2. Le autorità competenti degli Stati membri scambiano informazioni, si coordinano e cooperano con l'autorità competente di cui all'articolo 17, paragrafo 1, lettere c) e d), per quanto riguarda le misure adottate a norma dell'articolo 6, e i provvedimenti sanzionatori a norma dell'articolo 18. Gli Stati membri provvedono a che l'autorità competente di cui all'articolo 17, paragrafo 1, lettere c) e d), sia in possesso di tutte le informazioni pertinenti. A tal fine, gli Stati membri predispongono canali e meccanismi di comunicazione adeguati *e sicuri* per garantire che le informazioni pertinenti siano condivise tempestivamente. **[Em. 113]**

3. Gli Stati membri e i prestatori di servizi di hosting possono scegliere di avvalersi di appositi strumenti, inclusi, se del caso, quelli stabiliti dagli organismi pertinenti dell'Unione quali *da* Europol, per facilitare in particolare: **[Em. 114]**
- a) il trattamento dei dati e il feedback relativi agli ordini di rimozione a norma dell'articolo 4;
 - b) ~~il trattamento dei dati e il feedback relativi alle segnalazioni a norma dell'articolo 5;~~ **[Em. 115]**
 - c) la cooperazione allo scopo di individuare ed attuare misure proattive *specifiche* a norma dell'articolo 6. **[Em. 116]**

4. Laddove sia a conoscenza di eventuali ~~prove di reati di terrorismo~~ **contenuti terroristici**, il prestatore di servizi di hosting ne informa immediatamente l'autorità competente per le indagini e il perseguimento di reati nello Stato membro interessato. ***Ove non sia possibile individuare lo Stato membro interessato, il prestatore di servizi di hosting informa*** il punto di contatto di cui all'articolo 14 17, paragrafo 2, dello Stato membro in cui ha lo stabilimento principale o un rappresentante legale. ~~In caso di dubbi, il prestatore di servizi di hosting può trasmettere~~ ***e trasmette inoltre*** tali informazioni a Europol, che vi darà adeguato seguito. [Em. 117]

4 bis. I prestatori di servizi di hosting cooperano con le autorità competenti. [Em. 118]

Articolo 14

Punti di contatto

1. I prestatori di servizi di hosting ***che hanno precedentemente ricevuto uno o più ordini di rimozione*** istituiscono un punto di contatto incaricato di ricevere gli ordini di rimozione e ~~le segnalazioni~~ per via elettronica e di assicurarne il rapido trattamento ai sensi degli articoli ***dell'articolo 4 e 5***. Essi provvedono affinché tali informazioni siano rese pubbliche. [Em. 119]

2. Le informazioni di cui al paragrafo 1 precisano la lingua o le lingue ufficiali dell'Unione, elencate al regolamento 1/58, nelle quali è possibile rivolgersi al punto di contatto e nelle quali avvengono gli ulteriori scambi relativi agli ordini di rimozione e alle segnalazioni a norma degli articoli *dell'articolo* 4 e 5. Tali lingue comprendono almeno una delle lingue ufficiali dello Stato membro in cui il prestatore di servizi di hosting ha lo stabilimento principale o in cui risiede o è stabilito il suo rappresentante legale ai sensi dell'articolo 16. **[Em. 120]**

3. ~~Gli Stati membri istituiscono un punto di contatto per trattare le richieste di chiarimenti e di feedback in relazione agli ordini di rimozione e alle segnalazioni che hanno emesso. Le informazioni relative al punto di contatto sono rese pubbliche.~~
[Em. 121]

SEZIONE V
ATTUAZIONE E ESECUZIONE

Articolo 15
Competenza

1. Lo Stato membro nel quale il prestatore di servizi di hosting ha lo stabilimento principale è competente ai fini degli articoli 6, 18 e 21. Il prestatore di servizi di hosting che non ha lo stabilimento principale in uno degli Stati membri è considerato soggetto alla giurisdizione dello Stato membro in cui risiede o è stabilito il rappresentante legale di cui all'articolo 16.
2. Laddove il prestatore di servizi di hosting *che non ha lo stabilimento principale in uno degli Stati membri* ometta di designare un rappresentante legale, tutti gli Stati membri sono competenti. *Uno Stato membro, qualora decida di esercitare tale competenza, ne informa tutti gli altri Stati membri.* [Em. 122]

~~3. Se l'autorità di un altro Stato membro ha emesso un ordine di rimozione a norma dell'articolo 4, paragrafo 1, tale Stato membro è competente ad adottare misure coercitive conformemente alla legislazione nazionale, al fine di dare esecuzione all'ordine di rimozione. [Em. 123]~~

Articolo 16

Rappresentante legale

1. Il prestatore di servizi di hosting che non è stabilito nell'Unione, ma offre servizi nell'Unione, designa, per iscritto, una persona fisica o giuridica quale suo rappresentante legale nell'Unione per la ricezione, l'attuazione e l'esecuzione degli ordini di rimozione, ~~delle segnalazioni, delle richieste e delle decisioni~~ *richieste* emessi dalle autorità competenti sulla base del presente regolamento. Il rappresentante legale risiede o è stabilito in uno degli Stati membri in cui il prestatore di servizi offre i propri servizi. [Em. 124]

2. Il prestatore di servizi di hosting incarica il rappresentante legale di ricevere, attuare ed eseguire, per suo conto, gli ordini di rimozione, ~~le segnalazioni, le richieste e le decisioni~~ *richieste* di cui al paragrafo 1. Il prestatore di servizi di hosting conferisce al proprio rappresentante legale i poteri e le risorse necessari per cooperare con le autorità competenti e per ottemperare a tali decisioni e ordini. **[Em. 125]**
3. Il rappresentante legale designato può essere ritenuto responsabile per il mancato rispetto degli obblighi derivanti dal presente regolamento, fatte salve le responsabilità del prestatore di servizi di hosting e le azioni legali che possono essere promosse nei confronti di quest'ultimo.
4. Il prestatore di servizi di hosting informa della designazione l'autorità competente di cui all'articolo 17, paragrafo 1, lettera d), dello Stato membro in cui il rappresentante legale risiede o è stabilito. Le informazioni relative al rappresentante legale sono rese pubbliche.

SEZIONE VI
DISPOSIZIONI FINALI

Articolo 17

Designazione delle autorità competenti

1. Ciascuno Stato membro designa la *un'autorità giudiziaria* o le autorità competenti *amministrativa indipendente dal punto di vista funzionale competente* per:
[Em. 126]
 - a) emanare ordini di rimozione a norma dell'articolo 4;
 - b) ~~individuare, identificare e segnalare contenuti terroristici ai prestatori di servizi di hosting a norma dell'articolo 5;~~ [Em. 127]
 - c) sorvegliare l'attuazione delle misure ~~proattive~~ *specifiche* a norma dell'articolo 6; [Em. 128]
 - d) far rispettare gli obblighi stabiliti dal presente regolamento mediante sanzioni a norma dell'articolo 18.

- 1 bis. *Gli Stati membri designano un punto di contatto all'interno delle autorità competenti per trattare le richieste di chiarimenti e di feedback in relazione agli ordini di rimozione che hanno emesso. Le informazioni relative al punto di contatto sono rese pubbliche. [Em. 129]***
2. Entro [sei mesi dopo l'entrata in vigore del presente regolamento] gli Stati membri notificano alla Commissione le autorità competenti di cui al paragrafo 1. La Commissione ***istituisce un registro online di tutte le autorità competenti e del punto di contatto designato per ciascuna autorità competente. La Commissione pubblica la notifica e le eventuali modifiche della stessa nella Gazzetta ufficiale dell'Unione europea. [Em. 130]***

Articolo 18

Sanzioni

1. Gli Stati membri stabiliscono le norme relative alle sanzioni applicabili in caso di violazione *sistematica e persistente* da parte dei prestatori di servizi di hosting degli obblighi derivanti dal presente regolamento e adottano tutte le misure necessarie per assicurarne l'applicazione. Tali sanzioni sono limitate a violazioni degli obblighi sanciti dai seguenti articoli: **[Em. 131]**
 - a) ~~articolo 3, paragrafo 2 (condizioni contrattuali dei prestatori di servizi di hosting);~~ **[Em. 132]**
 - b) articolo 4, paragrafi 2 e 6 (attuazione degli ordini di rimozione e relativo feedback);
 - c) ~~articolo 5, paragrafi 5 e 6 (valutazione delle segnalazioni e relativo feedback);~~ **[Em. 133]**
 - d) articolo 6, ~~paragrafi 2 e~~ *paragrafo* 4 (relazioni sulle misure proattive *specifiche* e adozione di misure a seguito di una decisione *richiesta* che impone specifiche misure proattive *specifiche supplementari*); **[Em. 134]**

- e) articolo 7 (conservazione dei dati);
- f) articolo 8 (trasparenza *per i prestatori di servizi di hosting*); [Em. 135]
- g) articolo 9 (salvaguardie ~~in relazione a~~ *relative all'attuazione di* misure ~~proattive~~ *specifiche*); [Em. 136]
- h) articolo 10 (procedure di reclamo);
- i) articolo 11 (informazioni ai fornitori di contenuti);
- j) articolo 13, paragrafo 4 (informazioni relative ~~alle prove di reati di terrorismo~~ *ai contenuti terroristici*); [Em. 137]
- k) articolo 14, paragrafo 1, (punti di contatto);
- l) articolo 16 (designazione di un rappresentante legale).

2. Le sanzioni ~~previste~~ *di cui al paragrafo 1* sono efficaci, proporzionate e dissuasive. Gli Stati membri notificano alla Commissione, entro [sei mesi dall'entrata in vigore del presente regolamento], le norme e misure adottate al riguardo nonché ogni modifica ad esse apportata successivamente. **[Em. 138]**

3. Gli Stati membri provvedono a che, nel determinare il tipo e il livello delle sanzioni, le autorità competenti tengano conto di tutte le circostanze pertinenti, tra cui:
 - a) la natura, la gravità e la durata della violazione;
 - b) il carattere doloso o colposo della violazione;
 - c) precedenti violazioni da parte della persona giuridica ritenuta responsabile;
 - d) la solidità finanziaria della persona giuridica ritenuta responsabile;
 - e) il livello di cooperazione del prestatore di servizi di hosting con le autorità competenti.; **[Em. 139]**

*e bis) la natura e le dimensioni dei prestatori di servizi di hosting, in particolare le microimprese o le piccole imprese quali definite nella raccomandazione 2003/361/CE della Commissione*¹³. [Em. 140]

4. Gli Stati membri provvedono a che la sistematica *e persistente* inosservanza degli obblighi ai sensi dell'articolo 4, paragrafo 2 sia passibile di sanzioni pecuniarie fino al 4 % del fatturato mondiale del prestatore di servizi di hosting dell'ultimo esercizio finanziario. [Em. 141]

Articolo 19

Requisiti tecnici, *criteri di valutazione della rilevanza* e modifiche ai modelli da utilizzare per gli ordini di rimozione [Em. 142]

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. [Em. 143]

¹³

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

1 bis. Alla Commissione è conferito il potere di adottare atti delegati in conformità all'articolo 20 al fine di integrare il presente regolamento con criteri e dati che le autorità competenti utilizzeranno per stabilire quando la quantità di ordini di rimozione di contenuti non impugnati costituisca un numero significativo secondo il presente regolamento. [Em. 144]

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

Articolo 20

Esercizio della delega

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

2. Il potere di adottare gli atti delegati di cui all'articolo 19, è conferito alla Commissione per un periodo di tempo indeterminato a decorrere [dalla data di applicazione del presente regolamento].
3. La delega di potere di cui all'articolo 19 può essere revocata in qualsiasi momento dal Parlamento europeo o dal Consiglio. La decisione di revoca pone fine alla delega di potere ivi specificata. Gli effetti della decisione decorrono dal giorno successivo alla pubblicazione della decisione nella *Gazzetta ufficiale dell'Unione europea* o da una data successiva ivi specificata. Essa non pregiudica la validità degli atti delegati già in vigore.
4. Prima dell'adozione dell'atto delegato la Commissione consulta gli esperti designati da ciascuno Stato membro nel rispetto dei principi stabiliti nell'accordo interistituzionale "Legiferare meglio" del 13 aprile 2016.
5. Non appena adotta un atto delegato, la Commissione ne dà contestualmente notifica al Parlamento europeo e al Consiglio.

6. L'atto delegato adottato ai sensi dell'articolo 19 entra in vigore solo se né il Parlamento europeo né il Consiglio hanno sollevato obiezioni entro il termine di due mesi dalla data in cui esso è stato loro notificato o se, prima della scadenza di tale termine, sia il Parlamento europeo che il Consiglio hanno informato la Commissione che non intendono sollevare obiezioni. Tale periodo è prorogato di due mesi su iniziativa del Parlamento europeo o del Consiglio.

Articolo 21

Monitoraggio

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

- a) informazioni sul numero di ordini di rimozione e segnalazioni, il numero di messaggi con contenuto terroristico che sono stati rimossi o il cui accesso è stato disabilitato, comprese le corrispondenti tempistiche a norma degli articoli *dell'articolo 4 e 5, nonché informazioni sul numero dei relativi casi in cui l'individuazione, l'indagine e il perseguimento dei reati terroristici hanno avuto un esito positivo*; [Em. 145]
- b) informazioni sulle specifiche misure proattive adottate a norma dell'articolo 6, compresa la quantità di contenuti terroristici che è stata rimossa o il cui accesso è stato disabilitato, comprese le corrispondenti tempistiche;
- b bis) informazioni sul numero di richieste di accesso emesse dalle autorità competenti riguardanti i contenuti conservati dai prestatori di servizi di hosting a norma dell'articolo 7*; [Em. 146]
- c) informazioni sul numero di procedimenti di reclamo avviati e le azioni intraprese dai prestatori di servizi di hosting a norma dell'articolo 10;

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

2. Entro [un anno dalla data di applicazione del presente regolamento], la Commissione istituisce un programma dettagliato per monitorare gli esiti, i risultati e gli effetti del presente regolamento. Il programma di monitoraggio definisce gli indicatori e i mezzi da utilizzare per raccogliere i dati e gli altri elementi di prova necessari, nonché la periodicità di tali acquisizioni. Esso specifica le misure che la Commissione e gli Stati membri sono tenuti ad adottare ai fini della raccolta e dell'analisi dei dati e di altri elementi di prova per monitorare i progressi e valutare il presente regolamento, in applicazione dell'articolo 23.

Articolo 22

Relazione sull'applicazione

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

Articolo 23

Valutazione

Non prima di ~~[tre anni]~~ **A un anno** dalla data di applicazione del presente regolamento}, la Commissione procede a una valutazione del presente regolamento e trasmette una relazione al Parlamento europeo e al Consiglio sull'applicazione del presente regolamento, compreso il funzionamento e l'efficacia dei meccanismi di salvaguardia, ***nonché l'impatto sui diritti fondamentali e in particolare sulla libertà di espressione, la libertà di ricevere e trasmettere informazioni e il diritto al rispetto della vita privata. Nel quadro di tale valutazione, la Commissione riferisce inoltre in merito alla necessità, alla fattibilità e all'efficacia di un'eventuale piattaforma europea sui contenuti terroristici online, che consentirebbe a tutti gli Stati membri di utilizzare un unico canale di comunicazione sicuro per inviare ordini di rimozione relativi ai contenuti terroristici ai prestatori di servizi di hosting.*** Se opportuno, la relazione è accompagnata da proposte legislative. Gli Stati membri trasmettono alla Commissione le informazioni necessarie per la preparazione della relazione. **[Em. 147]**

Articolo 24

Entrata in vigore

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

Esso si applica a decorrere dal [~~6~~ **12** mesi dopo l'entrata in vigore]. **[Em. 148]**

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

Il presidente

Per il Consiglio

Il presidente

ALLEGATO I

ORDINE DI RIMOZIONE DI UN CONTENUTO TERRORISTICO (articolo 4 del regolamento (UE) xxx)

A norma dell'articolo 4 del regolamento (UE) ...¹⁵, entro un'ora dal ricevimento di un ordine di rimozione dall'autorità competente, il destinatario di detto ordine rimuove i contenuti terroristici o ne disabilita l'accesso.

A norma dell'articolo 7 del regolamento (UE) ...¹⁶, 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.

L'ordine di rimozione dovrebbe essere inviato in una delle lingue indicate dal destinatario a norma dell'articolo 14, paragrafo 2.

SEZIONE A:

Stato membro di emissione:

.....

NB: i dettagli relativi all'autorità di emissione vanno indicati oltre (sezioni E e F)

Destinatario (rappresentante legale):

.....

Destinatario (punto di contatto):

.....

Stato membro di competenza del destinatario: [se diverso dallo Stato di emissione]

.....

¹⁵ Regolamento del Parlamento europeo e del Consiglio sulla prevenzione della diffusione di contenuti terroristici online (*GUL...*).

¹⁶ Regolamento del Parlamento europeo e del Consiglio sulla prevenzione della diffusione di contenuti terroristici online (*GUL...*).

Data e ora di emissione dell'ordine di rimozione:

.....

Numero di riferimento dell'ordine di rimozione:

.....

SEZIONE B: Contenuto da rimuovere o accesso da disabilitare ~~entro un'ora~~ **senza indebito ritardo**: [Em. 162]

Indirizzo URL e ulteriori informazioni necessarie che consentano di individuare e localizzare con esattezza il contenuto in questione:

.....

Motivi per cui il contenuto è considerato contenuto terroristico ai sensi dell'articolo 2, paragrafo 5 del regolamento (UE) xxx. Il contenuto (spuntare le caselle pertinenti):

- ~~istiga, anche mediante l'apologia del~~ **alla commissione di reati di** terrorismo, ~~alla commissione di reati di terrorismo~~ **di cui all'articolo 3, paragrafo 1, lettere da a) a i) della direttiva (UE) 2017/541**(articolo 2, paragrafo 5, lettera a)); [Em. 149]
- ~~incita~~ **sollecita un'altra persona o un gruppo di persone** a contribuire a **alla commissione di reati di terrorismo di cui all'articolo 3, paragrafo 1, lettere da a) a i) della direttiva (UE) 2017/541** (articolo 2, paragrafo 5, lettera b)); [Em. 150]
- ~~promuove le~~ **sollecita un'altra persona o un gruppo di persone a partecipare alle** attività di un gruppo terroristico, ~~incoraggiando la partecipazione o il sostegno a tale gruppo~~ **di cui all'articolo 3, paragrafo 1, lettere da a) a i) della direttiva (UE) 2017/541** (articolo 2, paragrafo 5, lettera c)); [Em. 151]
- ~~impartisce istruzioni su metodi~~ **o tecniche per la fabbricazione o l'uso di esplosivi, armi da fuoco o altre armi o sostanze nocive o pericolose ovvero altre** tecniche ~~alle scop~~ **o metodi specifici al fine** di commettere reati di terrorismo **di cui all'articolo 3, paragrafo 1, lettere da a) a i), della direttiva (UE) 2017/541**(articolo 2, paragrafo 5, lettera d)); [Em. 152]
- descrive la commissione di reati di cui all'articolo 3, paragrafo 1, lettere da a) a i) della direttiva (UE) 2017/541** (articolo 2, paragrafo 5, lettera e)). [Em. 153]

Informazioni supplementari sui motivi per i quali il contenuto è considerato terroristico (facoltativo):

.....
.....

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** i cui contenuti sono stati rimossi o ne è stato disabilitato l'accesso.

Altrimenti: Precisazioni relative alla possibilità di impugnare l'ordine di rimozione nello Stato membro di emissione (che possono essere trasmesse al fornitore di contenuti, su sua richiesta) in base al diritto nazionale; cfr. sezione G.

SEZIONE D: Informazioni allo Stato membro competente

- Spuntare la casella se lo Stato di competenza del destinatario è diverso dallo Stato membro di emissione
- Una copia dell'ordine di rimozione è inviata all'autorità competente dello Stato di competenza

SEZIONE E: Dettagli relativi all'autorità che ha emesso l'ordine di rimozione

Tipo di autorità che ha emesso l'ordine di rimozione (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 di emissione e/o al suo rappresentante che certifica che l'ordine di rimozione è accurato e corretto:

Denominazione dell'autorità:

Nome del suo rappresentante:

Funzione (titolo/grado):

Numero di fascicolo:.....

Indirizzo:.....

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

Fax: (prefisso internazionale) (prefisso urbano).....

E-mail:

Data:

Timbro ufficiale (se disponibile) e firma¹⁷:

SEZIONE F: Dati di contatto per il follow-up

Indirizzo dell'autorità di emissione da utilizzare per la richiesta di un riscontro sull'ora della rimozione o della disabilitazione dell'accesso o per la trasmissione di ulteriori chiarimenti:

.....

Dati di contatto dell'autorità dello Stato di competenza del destinatario [se diverso dallo Stato membro di emissione]

.....

SEZIONE G: Informazioni sulle possibilità di ricorso

Informazioni relative all'organismo o all'organo giurisdizionale competente, ai termini e alle procedure, ***compresi i requisiti formali*** per impugnare l'ordine di rimozione: **[Em. 154]**

Organismo o organo giurisdizionale competente per impugnare l'ordine di rimozione:

.....

Termine per impugnare la decisione:

XXX mesi a decorrere dal xxxx

Link alle disposizioni della legislazione nazionale:

.....

ALLEGATO II

MODULO PER IL FEEDBACK DA INVIARE A SEGUITO DELLA RIMOZIONE O
DELLA DISABILITAZIONE DI CONTENUTI TERRORISTICI
(articolo 4, paragrafo 5, del regolamento (UE) xxx)

SEZIONE A:

Destinatario dell'ordine di rimozione:

.....

Autorità che ha emesso l'ordine di rimozione:

.....

Riferimento del fascicolo dell'autorità di emissione:

.....

Riferimento del fascicolo del destinatario:

.....

Data e ora di ricevimento dell'ordine di rimozione:

.....

SEZIONE B:

Il contenuto terroristico/l'accesso al contenuto terroristico oggetto dell'ordine di rimozione è stato (spuntare la casella pertinente):

- rimosso
- disabilitato

Ora e data di rimozione o disabilitazione dell'accesso:

SEZIONE C: Identificazione del destinatario

Nome del prestatore di servizi di hosting/del rappresentante legale:

.....

Stato membro di stabilimento principale o di stabilimento del rappresentante legale:

.....

Nome della persona autorizzata:

.....

Informazioni sul punto di contatto (e-mail):

.....

Data:

.....

ALLEGATO III

INFORMAZIONI SULL'IMPOSSIBILITÀ DI ESEGUIRE UN ORDINE DI RIMOZIONE (articolo 4, paragrafi 6 e 7, del regolamento (UE) xxx)

SEZIONE A:

Destinatario dell'ordine di rimozione:

.....

Autorità che ha emesso l'ordine di rimozione:

.....

Riferimento del fascicolo dell'autorità di emissione:

.....

Riferimento del fascicolo del destinatario:

.....

Data e ora di ricevimento dell'ordine di rimozione:

.....

SEZIONE B: Motivi della mancata esecuzione di un ordine:

i) l'ordine di rimozione non può essere eseguito o non può essere eseguito entro il termine prescritto per la seguente ragione:

cause di forza maggiore o impossibilità di fatto non imputabile al destinatario o al prestatori di servizi, ***anche per motivi tecnici o operativi [Em. 155]***

l'ordine di rimozione è viziato da errori manifesti

l'ordine di rimozione non contiene informazioni sufficienti

ii) fornire ulteriori informazioni sui motivi della mancata esecuzione:

.....

iii) 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 richiesti:

.....

SEZIONE C: Informazioni sul prestatore di servizi/sul suo rappresentante legale

Nome del prestatore di servizi/del suo rappresentante legale:

.....

Nome della persona autorizzata:

.....

Dati di contatto (e-mail):

.....

Firma:

.....

Data e ora:

.....