Consiglio dell'Unione europea

Bruxelles, 3 dicembre 2018
(OR. en)

14978/18

Fascicolo interistituzionale: 2018/0331(COD)

CT 194
ENFOPOL 595
JAI 1232
COTER 170
CYBER 303
TELECOM 440
FREMP 216
AUDIO 112
DROIPEN 189
CODEC 2160

NOTA

Origine:	presidenza
Destinatario:	Consiglio
n. doc. prec.:	14570/18
Oggetto:	Proposta di regolamento del Parlamento europeo e del Consiglio relativo alla prevenzione della diffusione di contenuti terroristici online - Orientamento generale

I. INTRODUZIONE

1. Il 12 settembre 2018 la Commissione ha presentato al Consiglio una proposta di regolamento relativo alla prevenzione della diffusione di contenuti terroristici online[1], che dà seguito alla richiesta formulata dal Consiglio europeo del giugno 2018 di elaborare una proposta legislativa che migliori l'individuazione e la rimozione di contenuti che incitano all'odio e a compiere atti terroristici. La proposta fa parte del pacchetto di proposte sulla sicurezza che accompagna il discorso sullo stato dell'Unione pronunciato dal presidente della Commissione.

[1] Doc. 12129/18 + ADD 1-3

2. La base giuridica della proposta è l'articolo 114 del trattato sul funzionamento dell'Unione europea (mercato interno). Il regolamento proposto introduce il concetto di ordine di rimozione che obbliga i prestatori di servizi di hosting che operano nel territorio dell'Unione a rimuovere i contenuti terroristici o a disabilitane l'accesso entro un'ora. In caso di mancato rispetto possono essere imposte sanzioni. L'attuale testo del progetto di proposta contiene forti salvaguardie intese a tutelare i diritti e i principi fondamentali, in particolare la libertà di espressione e il diritto al ricorso legale.

3. Proseguirà l'attuale regime di cooperazione volontaria, che è stato creato nell'ambito del Forum dell'UE su Internet, istituito nel dicembre 2015.

II. LAVORI IN SEDE DI CONSIGLIO

4. Il Gruppo "Terrorismo" (TWP) ha esaminato il progetto di regolamento nelle riunioni del 25 settembre, 5 e 25 ottobre e 6 e 15 novembre 2018. A seguito di questo esame approfondito del progetto di regolamento a livello di esperti, i Consiglieri GAI hanno discusso alcune delle restanti questioni il 22 novembre 2018. Il progetto di regolamento è stato inoltre esaminato in sede di CATS il 18 settembre 2018.

5. Il Comitato dei rappresentanti permanenti (COREPER) ha tenuto un primo dibattito durante la colazione il 26 settembre, ha scambiato opinioni in materia di lotta al terrorismo, anche sulla presente proposta, con il coordinatore antiterrorismo dell'UE durante la colazione del COREPER del 21 novembre e ha esaminato l'ultima proposta di compromesso della presidenza il 28 novembre 2018 con il presidente, che ha concluso che tale proposta aveva il necessario sostegno della maggioranza.

III. PRINCIPALI QUESTIONI AFFRONTATE

6. Il testo di compromesso della presidenza affronta la maggior parte delle questioni sollevate dagli Stati membri introducendo una serie di modifiche, precisate in appresso nell'ordine degli articoli.

– In tema di diritti fondamentali e di necessità di tutelare i contenuti giornalistici, il testo sui diritti fondamentali in generale, e sulla libertà di stampa in particolare, è stato rafforzato con l'aggiunta del nuovo paragrafo 3 all'articolo 1 e con la sostanziale modifica della fine del considerando 9, per tenere conto delle norme giornalistiche previste dalla regolamentazione della stampa o dei media.

– In termini di ambito di applicazione, la definizione di "*contenuto terroristico*", di cui all'articolo 2, paragrafo 5, è stata maggiormente allineata alla direttiva sulla lotta contro il terrorismo. La definizione di "*prestatore di servizi di hosting*" è stata ulteriormente chiarita al considerando 10, che definisce nei particolari i diversi elementi costitutivi della definizione, spiegando quali prestatori di servizi non rientrano nell'ambito di applicazione e fornendo esempi di prestatori di servizi di hosting contemplati.

– Quanto ai principali strumenti intesi a prevenire la diffusione di contenuti terroristici online (articoli 4 e 5), il testo chiarisce all'articolo 4, paragrafi 3 bis e 4, oltre che nel corrispondente considerando 13 bis, quali informazioni sono fornite al prestatore di servizi di hosting nell'ordine di rimozione. È stato aggiunto un nuovo articolo 4 bis che espone la procedura di consultazione per gli ordini di rimozione. Al considerando 25 è stato aggiunto un riferimento supplementare al diritto a un ricorso effettivo per gli ordini di rimozione, oltre al riferimento generale di cui al considerando 8.

– In merito alle misure proattive, le modifiche all'articolo 6, paragrafi 2 bis e 4, precisano ora che spetta agli Stati membri scegliere la natura e la portata delle misure, all'atto di decidere le misure proattive da imporre.

– In risposta al possibile onere a carico delle piccole e medie imprese, l'articolo 8, paragrafo 2, e il corrispondente considerando 24, precisano che l'obbligo di pubblicare relazioni sulla trasparenza è limitato ai prestatori di servizi di hosting esposti a contenuti terroristici.

– Se, per motivi di sicurezza pubblica, l'obbligo di divulgare informazioni sulla rimozione di contenuti terroristici al fornitore di contenuti non dovesse applicarsi immediatamente, il periodo previsto dall'articolo 11, paragrafo 3, durante il quale le informazioni possono essere trattenute, è stato prolungato da 4 + 4 settimane a 6+ 6 settimane.

– In merito alla cooperazione, l'articolo 13, paragrafo 3 e i considerando 27 e 30 sono stati modificati per fare in modo che gli Stati membri si coordinino prima di emettere ordini di rimozione e segnalazioni (chiarendo come evitare duplicazioni e interferenze con le indagini) e per incentivare l'uso degli strumenti di Europol. L'articolo 13, paragrafo 4 è stato modificato per fare in modo che qualsiasi notifica di minaccia grave giunga all'autorità competente quanto prima possibile.

– Oltre a ciò, sono state introdotte modifiche per ridurre l'onere a carico dei prestatori di servizi di hosting, chiarendo, al considerando 33, che il punto di contatto ai sensi dell'articolo 14, per il trattamento degli ordini di rimozione può essere esternalizzato e limitando la disponibilità 24 ore su 24 e 7 giorni su 7 di un punto di contatto ai prestatori di servizi di hosting esposti a contenuti terroristici.

– L'articolo 15, paragrafo 3, e il corrispondente considerando 34 bis, sulle misure coercitive sono stati soppressi.

– All'articolo 24, il periodo di attuazione è stato prolungato da sei a dodici mesi.

Per quanto riguarda la giurisdizione e l'eventuale ruolo dello Stato membro in cui il prestatore di servizi di hosting è stabilito, anche in relazione ai ricorsi giurisdizionali, sono state introdotte varie modifiche. Il testo attuale precisa all'articolo 15, paragrafo 1 e al considerando 34, che per motivi di efficacia dell'attuazione, di urgenza e di ordine pubblico, qualsiasi Stato membro è competente a emettere ordini di rimozione e segnalazioni a qualunque prestatore di servizi di hosting, a prescindere dallo Stato membro in cui esso è stabilito o in cui ha designato un rappresentante legale. Il considerando 27 precisa che non dovrebbero essere emesse duplicazioni degli ordini di rimozione. È stato inoltre aggiunto l'articolo 4 bis che prevede la consultazione dell'autorità competente dello Stato membro in cui il prestatore di servizi di hosting è stabilito o ha il suo rappresentante legale. Infine, il considerando 38 chiarisce che lo Stato membro deve garantire il pieno rispetto dei diritti fondamentali prima di emanare sanzioni.

IV. ALTRE QUESTIONI

7. La Repubblica ceca, la Danimarca e la Finlandia mantengono una riserva d'esame parlamentare sulla proposta.

8. Il Comitato economico e sociale europeo è stato consultato dal Consiglio con lettera del 24 ottobre 2018 e formulerà il suo parere nella sessione plenaria di dicembre.

9. Il Parlamento europeo ha nominato quale relatore Helga Stevens (ECR, BE), commissione per le libertà civili, la giustizia e gli affari interni (LIBE).

V. CONCLUSIONE

10. Si invita il Consiglio ad adottare un orientamento generale sul testo che figura nell'allegato della presente nota.

11. Le modifiche rispetto alla proposta della Commissione (doc. 12129/18) sono indicate come segue: il testo nuovo è in ***grassetto corsivo***, mentre le parti soppresse della proposta iniziale della Commissione sono contrassegnate da [...].

ALLEGATO

2018/0331 (COD)

Proposta di

REGOLAMENTO DEL PARLAMENTO EUROPEO E DEL CONSIGLIO

relativo alla prevenzione della diffusione di contenuti terroristici online

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

IL PARLAMENTO EUROPEO E IL CONSIGLIO DELL'UNIONE EUROPEA,

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

vista la proposta della Commissione europea,

previa trasmissione del progetto di atto legislativo ai parlamenti nazionali,

visto il parere del Comitato economico e sociale europeo[2],

deliberando secondo la procedura legislativa ordinaria,

considerando quanto segue:

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

[2] GU C del , pag. .

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

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

(4) Gli sforzi volti a contrastare i contenuti terroristici online sono stati avviati a livello dell'Unione nel 2015 nel quadro della cooperazione volontaria tra gli Stati membri e i prestatori di servizi di hosting; essi dovrebbero essere integrati da un quadro legislativo chiaro al fine di ridurre l'accessibilità dei contenuti terroristici online e affrontare in modo adeguato un fenomeno in rapida evoluzione. Tale quadro legislativo poggerebbe su iniziative volontarie, che sono state rafforzate dalla raccomandazione (UE) 2018/334[3], e risponde alla richiesta del Parlamento europeo di rafforzare le misure volte ad affrontare i contenuti illegali e nocivi e a quella del Consiglio europeo di migliorare l'individuazione automatizzata e la rimozione dei contenuti che incitano a compiere atti terroristici.

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

(5) L'applicazione del presente regolamento non dovrebbe pregiudicare l'applicazione dell'articolo 14 della direttiva 2000/31/CE[4]. In particolare, tutte le misure adottate dal prestatore di servizi di hosting conformemente al presente regolamento, comprese le eventuali misure proattive, non dovrebbero comportare automaticamente la perdita, per il prestatore di servizi, del beneficio dell'esenzione di responsabilità prevista in tale disposizione. Il presente regolamento lascia impregiudicata la competenza delle autorità e degli organi giurisdizionali nazionali a stabilire la responsabilità dei prestatori di servizi di hosting in determinati casi se non sono soddisfatte le condizioni di cui all'articolo 14 della direttiva 2000/31/CE per beneficiare dell'esenzione di responsabilità. ***Il presente regolamento non si applica alle attività connesse alla sicurezza nazionale, che rimane di esclusiva competenza di ciascuno Stato membro.***

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

---

[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 alla protezione della pubblica sicurezza, attuando nel contempo adeguate e solide salvaguardie per garantire la tutela dei diritti fondamentali in gioco. Ciò include i diritti al rispetto della vita privata e alla protezione dei dati personali, il diritto ad una tutela giurisdizionale effettiva, il diritto alla libertà di espressione, compresa la libertà di ricevere e trasmettere informazioni, la libertà d'impresa e il principio di non discriminazione. Le autorità competenti e i prestatori di servizi di hosting dovrebbero adottare solo le misure che sono necessarie, adeguate e proporzionate in una società democratica, tenendo conto della particolare importanza rivestita dalla libertà di espressione e di informazione***, come pure dalla libertà di stampa e dal pluralismo dei media***, che costituiscono […] [...] i fondamenti essenziali di una società democratica e pluralista e uno dei valori su cui si fonda l'Unione. Le misure che costituiscano un'ingerenza nella libertà di espressione e d'informazione dovrebbero essere rigorosamente mirate, nel senso che devono servire a prevenire la diffusione di contenuti terroristici, ma senza pregiudicare il diritto di ricevere e diffondere informazioni in modo lecito, tenuto conto del ruolo centrale dei prestatori di servizi di hosting nel facilitare il dibattito pubblico e la diffusione e la ricezione di informazioni, pareri e idee nel rispetto della legge.

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

(9) Onde chiarire le misure che i prestatori di servizi di hosting e le autorità competenti dovrebbero adottare per prevenire la diffusione di contenuti terroristici online, è opportuno che il presente regolamento stabilisca una definizione dei contenuti terroristici per fini di prevenzione sulla base della definizione dei reati di terrorismo ai sensi della direttiva (UE) 2017/541 del Parlamento europeo e del Consiglio[5]. Data la necessità di contrastare la propaganda terroristica online più perniciosa, la definizione dovrebbe ricomprendere il materiale [...] che incita, incoraggia o appoggia la commissione di reati di terrorismo e il contributo agli stessi, […] o promuove la partecipazione alle attività di un gruppo terroristico. ***[...] Nella definizione rientrano i contenuti che forniscono indicazioni per la fabbricazione o l'uso di esplosivi, armi da fuoco o altre armi o sostanze nocive o pericolose, nonché sostanze CBRN, ovvero***
altri metodi e tecniche, compresa la selezione degli obiettivi, al fine 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 [...] educativi, ***di controargomentazione*** o di ricerca***, garantendo un giusto equilibrio tra i diritti fondamentali, tra cui in particolare la libertà di espressione e di informazione e le esigenze di sicurezza pubblica***. ***Qualora il materiale diffuso sia pubblicato sotto la responsabilità editoriale del fornitore di contenuti, qualsiasi decisione relativa alla rimozione di tale contenuto dovrebbe tener conto delle norme giornalistiche previste dalla regolamentazione della stampa o dei media in conformità del diritto dell'Unione nonché del diritto alla libertà di espressione e del diritto alla libertà e al pluralismo dei media sanciti all'articolo 11 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.

---

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).

(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 ***e materiali*** forniti da un destinatario del servizio su sua richiesta e che rendono disponibili a terzi tali informazioni ***e materiali*** memorizzati, indipendentemente dalla natura meramente tecnica, automatica o passiva di tale attività. […] ***La memorizzazione dei contenuti consiste nella detenzione dei dati nella memoria di un server fisico o virtuale; ciò esclude dall'ambito di applicazione il semplice trasporto ("mere conduit") e altri servizi di comunicazione elettronica ai sensi del [codice europeo delle comunicazioni elettroniche] o i prestatori di servizi di memorizzazione temporanea ("caching"), ovvero altri servizi forniti in altri strati dell'infrastruttura di Internet, quali registri e autorità di registrazione, DNS (domain name system - sistema dei nomi di dominio) o servizi adiacenti, quali i servizi di pagamento o di protezione contro gli attacchi distribuiti di negazione del servizio (DDoS). Inoltre le informazioni devono essere memorizzate su richiesta del fornitore di contenuti; rientrano nell'ambito di applicazione solo i servizi relativamente ai quali il fornitore di contenuti è il destinatario diretto. Infine, le informazioni memorizzate sono messe a disposizione di terzi, intesi come qualunque utente terzo che non sia il fornitore di contenuti. Non rientrano nell'ambito di applicazione i servizi di comunicazione interpersonale che consentono lo scambio interpersonale e interattivo diretto di informazioni tra un numero limitato di persone, in cui le persone che danno inizio o partecipano alla comunicazione ne stabiliscono i destinatari.*** Ad esempio, i prestatori di servizi […] ***di hosting*** includono le piattaforme dei social media, i servizi di streaming video, i servizi di condivisione di video, audio e immagini, i servizi di condivisione di file e altri servizi di cloud ***e di memorizzazione*** […]. ***Il presente regolamento si applica all'attività di prestazione di servizi di hosting anziché al prestatore specifico o alla sua attività prevalente, che potrebbe combinare servizi di hosting con altri servizi che non rientrano nell'ambito di applicazione del presente regolamento***.

(10 bis) Il regolamento dovrebbe inoltre applicarsi ai prestatori di servizi di hosting che offrono servizi nell'Unione, ma che sono stabiliti al di fuori di essa, dal momento che una quota significativa dei prestatori di servizi di hosting esposti a contenuti terroristici che possono essere diffusi tramite i loro servizi sono stabiliti in paesi terzi. Ciò dovrebbe garantire che tutte le imprese operanti nel mercato unico digitale si conformino agli stessi obblighi a prescindere dal paese di stabilimento. Per determinare se offre servizi nell'Unione, è necessario verificare se il prestatore di servizi consente alle persone fisiche o giuridiche di uno o più Stati membri di usufruire dei suoi servizi. Tuttavia, la semplice accessibilità del sito Internet di un prestatore di servizi o di un indirizzo di posta elettronica e di altri dati di contatto in uno o più Stati membri non dovrebbe di per sé costituire una condizione sufficiente per l'applicazione del presente regolamento.

(11) L'esistenza di un collegamento sostanziale con l'Unione dovrebbe essere presa in considerazione al fine di determinare l'ambito di applicazione del presente regolamento. Tale collegamento sostanziale con l'Unione dovrebbe considerarsi presente quando il prestatore di servizi è stabilito nell'Unione o, in caso contrario, sulla base dell'esistenza di un numero considerevole di utilizzatori in uno o più Stati membri o dell'orientamento delle sue attività verso uno o più Stati membri. L'orientamento delle attività verso uno o più Stati membri può essere determinato sulla base di tutte le circostanze pertinenti, tra cui l'uso di una lingua o di una moneta generalmente usata nello Stato membro in questione o la possibilità di ordinare prodotti o servizi. L'orientamento delle attività verso uno Stato membro potrebbe anche desumersi dalla disponibilità di un'applicazione nell'apposito negozio online ("app store") nazionale, dalla diffusione di pubblicità a livello locale o nella lingua usata nello Stato membro in questione, o dalla gestione dei rapporti con la clientela, ad esempio la fornitura di assistenza alla clientela nella lingua generalmente parlata in tale Stato membro. Un collegamento sostanziale dovrebbe essere presunto anche quando le attività di un prestatore di servizi sono dirette verso uno o più Stati membri come previsto all'articolo 17, paragrafo 1, lettera c), del regolamento (UE) n. 1215/2012 del Parlamento europeo e del Consiglio[6]. Al contrario, non si può considerare che la prestazione del servizio al solo scopo di conformarsi al divieto di discriminazione imposto dal regolamento (UE) 2018/302 del Parlamento europeo e del Consiglio[7] comprovi, di per sé, che le sue attività sono dirette o orientate verso un dato territorio all'interno dell'Unione.

---

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

(13) Occorre armonizzare la procedura e gli obblighi che discendono dagli ordini giuridici che ingiungono ai prestatori di servizi di hosting di rimuovere contenuti terroristici o di disabilitarne l'accesso, in esito a una valutazione delle autorità competenti. Gli Stati membri dovrebbero designare le autorità competenti, assegnando tale compito alle autorità amministrative, esecutive o giudiziarie di loro scelta. In considerazione della velocità alla quale i contenuti terroristici sono diffusi attraverso i servizi online, la presente disposizione impone ai prestatori di servizi di hosting l'obbligo di provvedere a che i contenuti terroristici oggetto di un ordine di rimozione siano rimossi o che l'accesso sia disabilitato entro un'ora dal ricevimento del provvedimento. ***Fatto salvo l'obbligo di conservare i dati a norma dell'articolo 7 del presente regolamento, ovvero del [progetto di normativa relativa alle prove elettroniche], s***petta ai prestatori di servizi di hosting decidere se rimuovere il contenuto in questione o disabilitarne l'accesso per gli utilizzatori nell'Unione. ***Ciò dovrebbe avere l'effetto di impedire o almeno di rendere difficile l'accesso e di scoraggiare seriamente gli utenti di Internet che ricorrono ai loro servizi dall'accedere ai contenuti per cui l'accesso è stato disabilitato.***

(13 bis) L'ordine di rimozione dovrebbe includere la classificazione dei contenuti pertinenti quali contenuti terroristici e contenere informazioni sufficienti per localizzare i contenuti, fornendo un URL e ogni altra informazione aggiuntiva quale ad esempio una copia della schermata (screenshot) dei contenuti in questione. Su richiesta, l'autorità competente dovrebbe trasmettere una motivazione supplementare contenente i motivi per cui il contenuto è considerato contenuto terroristico. Le motivazioni fornite non devono contenere informazioni sensibili che potrebbero compromettere le indagini. Le motivazioni dovrebbero tuttavia consentire al prestatore di servizi di hosting e, in ultima istanza, al fornitore di contenuti di esercitare effettivamente il loro diritto al ricorso giurisdizionale.

(14) L'autorità competente dovrebbe trasmettere l'ordine di rimozione direttamente al destinatario e al punto di contatto con ogni mezzo elettronico che consenta di conservare una traccia scritta in condizioni che permettano al prestatore di stabilirne l'autenticità, compresa l'esattezza della data e dell'ora di invio e ricevimento dell'ordine, quali posta elettronica protetta e piattaforme o altri canali protetti, compresi quelli messi a disposizione dal prestatore di servizi, in conformità delle norme in materia di protezione dei dati personali. Segnatamente, tale obbligo può essere assolto usando servizi elettronici di recapito certificato qualificati ai sensi del regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio[8].

[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) […] ***Il*** meccanismo ***di segnalazione*** inteso ad allertare i prestatori di servizi di hosting nei confronti delle informazioni ***e dei materiali*** che possono essere considerati contenuti terroristici, che permette loro su base volontaria di esaminare la compatibilità ***con*** le proprie condizioni contrattuali***, costituisce uno strumento particolarmente efficace, rapido e proporzionato per mettere i prestatori di servizi di hosting a conoscenza di contenuti specifici che possono essere diffusi tramite i loro servizi*** **[…].** 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) 2016/794[9], resta invariato.

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

---

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 (GU L 135 del 24.5.2016, pag. 53).

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

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

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

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

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

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

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

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

(25) Le procedure di reclamo costituiscono una tutela necessaria contro la rimozione erronea ***- in conseguenza di misure adottate a norma delle condizioni contrattuali dei prestatori di servizi di hosting -*** di contenuti protetti nell'ambito della libertà di espressione e di informazione. I prestatori di servizi di hosting dovrebbero pertanto predisporre meccanismi di facile uso per i reclami, assicurando che siano trattati tempestivamente e in piena trasparenza nei confronti del fornitore di contenuti. L'obbligo di ripristinare il contenuto rimosso erroneamente non pregiudica la possibilità che il prestatore di servizi di hosting applichi le proprie condizioni contrattuali per altri motivi. ***Inoltre i fornitori di contenuti i cui contenuti siano stati rimossi a seguito di un ordine di rimozione dovrebbero avere diritto a un ricorso effettivo conformemente all'articolo 19 del TUE e all'articolo 47 della Carta dei diritti fondamentali dell'Unione europea.***

(26) ***Più in generale, l***[...]'articolo 19 del TUE e l'articolo 47 della Carta dei diritti fondamentali dell'Unione europea sanciscono il diritto a una tutela giurisdizionale effettiva, in forza del quale le persone devono essere in grado di conoscere il motivo per cui il contenuto da loro caricato è stato rimosso o il relativo accesso disabilitato. A tal fine, il prestatore di servizi di hosting dovrebbe mettere a disposizione del fornitore di contenuti utili informazioni che gli consentano di impugnare la decisione. Può tuttavia non essere necessario inviare una notifica al fornitore di contenuti. A seconda delle circostanze, i prestatori di servizi di hosting possono sostituire il contenuto considerato terroristico con un messaggio indicante che il contenuto è stato rimosso o disabilitato 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 al fornitore di contenuti la rimozione del contenuto o la disabilitazione dell'accesso al contenuto.

(27) Al fine di evitare duplicazioni ed eventuali interferenze con le indagini, le autorità competenti dovrebbero scambiarsi informazioni, coordinarsi e cooperare reciprocamente e, se del caso, con Europol, […] ***prima di emettere*** ordini di rimozione ***o al momento di trasmettere*** segnalazioni ai prestatori di servizi di hosting. Nel decidere in merito all'emissione dell'ordine di rimozione, l'autorità competente dovrebbe prendere in debita considerazione qualsiasi notifica di un'interferenza con gli interessi di un'indagine ("prevenzione di conflittualità"). Qualora un'autorità competente sia informata, da parte di un'autorità competente di un altro Stato membro, dell'esistenza di un ordine di rimozione, non dovrebbe essere emesso un secondo ordine. ***Nel decidere in merito all'emissione di un ordine di rimozione, l'autorità competente dovrebbe prendere in debita considerazione qualsiasi notifica di un'interferenza con gli interessi di un'indagine ("prevenzione di conflittualità"). Qualora un'autorità competente sia informata, da parte di un'autorità competente di un altro Stato membro, dell'esistenza di un ordine di rimozione, non dovrebbe essere emesso un secondo ordine.*** Europol potrebbe sostenere l'attuazione delle disposizioni del presente regolamento, nel rispetto del suo attuale mandato e del quadro giuridico esistente.

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

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

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

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

(32) Le autorità competenti degli Stati membri dovrebbero essere autorizzate a utilizzare tali informazioni per adottare le misure investigative previste dalla legislazione dello Stato membro o dell'Unione europea, ivi inclusa l'emissione di un ordine europeo di produzione ai sensi del regolamento relativo agli ordini europei di produzione e di conservazione di prove elettroniche in materia penale[10].

(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***, interni o esternalizzati,*** che permettono di trasmettere per via elettronica gli ordini di rimozione e le segnalazioni e delle risorse tecniche […] ***o*** personali che consentono di trattarli rapidamente. Il punto di contatto del prestatore di servizi di hosting non deve necessariamente essere situato nell'Unione 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 disabilitato entro un'ora dal ricevimento di un ordine di rimozione, ***i prestatori di servizi di hosting esposti a contenuti terroristici, attestati dal ricevimento di un ordine di rimozione,*** dovrebbero far sì che il punto di contatto sia accessibile 24 ore su 24 e 7 giorni su 7. Le informazioni sul punto di contatto dovrebbero comprendere informazioni sulla lingua in cui il punto di contatto può essere contattato. Per facilitare la comunicazione tra i prestatori di servizi di hosting e le autorità competenti, i prestatori di servizi di hosting sono incoraggiati ad ammettere la comunicazione in una delle lingue ufficiali dell'Unione nella quale sono disponibili le loro condizioni contrattuali.

(34) In assenza di un obbligo generale per i prestatori di servizi di assicurare la presenza fisica all'interno del territorio dell'Unione, è necessario determinare in modo chiaro lo Stato membro nella cui giurisdizione ricade il prestatore di servizi di hosting che offre servizi all'interno dell'Unione. Generalmente, il prestatore di servizi di hosting ricade nella giurisdizione dello Stato membro in cui ha lo stabilimento principale o in cui ha designato un rappresentante legale. ***Tuttavia, per motivi di efficacia dell'attuazione, di urgenza e di ordine pubblico, qualsiasi Stato membro dovrebbe essere competente per quanto riguarda ordini di rimozione e segnalazioni.***

---

10 COM(2018)225 final.

(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.***

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

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

(38) Le sanzioni sono necessarie per garantire che i prestatori di servizi di hosting diano effettiva attuazione agli obblighi previsti dal presente regolamento. Occorre che gli Stati membri adottino norme relative alle sanzioni, ***che possono essere di natura amministrativa o penale,*** comprese, eventualmente, linee guida per il calcolo delle stesse. Sanzioni particolarmente severe dovrebbero essere inflitte nel caso in cui il prestatore di servizi di hosting ometta sistematicamente di rimuovere contenuti terroristici o di disabilitarne l'accesso entro un'ora dal ricevimento di un ordine di rimozione. La mancata conformità in casi individuali potrebbe essere sanzionata nel rispetto del principio *ne bis in idem* e del principio di proporzionalità, assicurando che tali sanzioni tengano conto dell'inosservanza sistematica. Al fine di garantire la certezza del diritto, il regolamento dovrebbe stabilire in che misura gli obblighi pertinenti possano essere soggetti a sanzioni. Sanzioni in caso di mancato rispetto dell'articolo 6 dovrebbero essere adottate solo in relazione agli obblighi derivanti dalla richiesta di riferire a norma dell'articolo 6, paragrafo 2, o da una decisione che impone misure proattive supplementari a norma dell'articolo 6, paragrafo 4. ***Nel valutare la natura della violazione e nel decidere in merito all'applicazione di sanzioni, dovrebbero essere pienamente rispettati i diritti fondamentali quali la libertà di espressione.*** Nel determinare se debbano essere inflitte sanzioni pecuniarie si dovrebbe tenere debito conto delle risorse finanziarie del prestatore. Gli Stati membri assicurano che le sanzioni non incoraggino la rimozione di contenuti che non hanno natura terroristica.

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

(40) Per poter modificare rapidamente, se necessario, il contenuto del modello da utilizzare ai fini del presente regolamento, è opportuno delegare alla Commissione il potere di adottare atti conformemente all'articolo 290 del trattato sul funzionamento dell'Unione europea riguardo alla modifica degli allegati I, II e III del presente regolamento. Per tenere conto dello sviluppo tecnologico e del relativo quadro giuridico, alla Commissione dovrebbe essere inoltre conferito il potere di adottare atti delegati al fine di integrare il presente regolamento con requisiti tecnici per gli strumenti elettronici destinati ad essere utilizzati dalle autorità competenti per trasmettere gli ordini di rimozione. È di particolare importanza che durante i lavori preparatori la Commissione svolga adeguate consultazioni, anche a livello di esperti, nel rispetto dei principi stabiliti nell'accordo interistituzionale "Legiferare meglio" del 13 aprile 2016[11]. 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. ***Gli Stati membri possono utilizzare le relazioni sulla trasparenza dei prestatori di servizi di hosting integrandole, ove necessario, con informazioni più dettagliate.*** 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.

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

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

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

HANNO ADOTTATO IL PRESENTE REGOLAMENTO:

SEZIONE I
DISPOSIZIONI GENERALI

Articolo 1

Oggetto e ambito di applicazione

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

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

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

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

3. ***Il presente regolamento non pregiudica l'obbligo di rispettare i diritti fondamentali e i principi giuridici fondamentali sanciti dall'articolo 6 del trattato sull'Unione europea.***

Articolo 2

Definizioni

Ai fini del presente regolamento si applicano le seguenti definizioni:

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

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

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

In assenza di tale stabilimento, la valutazione del collegamento sostanziale si basa su specifici criteri di fatto quali:

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

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

4) "reati di terrorismo": ***uno degli atti intenzionali di cui all'***[...] articolo 3, paragrafo 1, […] della direttiva (UE) 2017/541;

5) "contenuto terroristico": […] ***materiale che può contribuire alla commissione di atti intenzionali di cui all'articolo 3, paragrafo 1, lettere da a) a i), della direttiva (UE) 2017/541 mediante***:

a bis) la minaccia di commettere un reato di terrorismo;

a) l'istigazione, […] ***ad esempio*** mediante l'apologia ***degli atti terroristici***, alla commissione di reati di terrorismo, generando in tal modo il pericolo che tali reati siano effettivamente commessi;

b) ***la sollecitazione nei confronti di persone o di un gruppo di persone a commettere reati di terrorismo o*** […] a contribuire a reati di terrorismo;

c) la promozione delle attività di un gruppo terroristico, in particolare ***sollecitando persone o un gruppo di persone a partecipare alle attività criminose di un gruppo terroristico o a sostenere le attività criminose di*** […] un gruppo terroristico ai sensi dell'articolo 2, paragrafo 3, della direttiva (UE) 2017/541;

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

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

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

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

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

SEZIONE II

MISURE VOLTE A PREVENIRE LA DIFFUSIONE DI CONTENUTI TERRORISTICI ONLINE

Articolo 3

Obblighi di diligenza

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

2. I prestatori di servizi di hosting includono nelle loro condizioni contrattuali ***disposizioni relative al fatto che non memorizzeranno contenuti terroristici, come pure*** disposizioni volte a prevenire la diffusione di contenuti terroristici, e ne assicurano l'applicazione.

Articolo 4

Ordini di rimozione di contenuti

1. L'autorità competente ha facoltà di adottare un […] ***ordine di rimozione di contenuti*** che imponga al prestatore di servizi di hosting di rimuovere contenuti terroristici o di disabilitarne l'accesso.

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

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

   a) l'identificazione dell'autorità competente che emette l'ordine di rimozione e l'autenticazione dell'ordine di rimozione da parte dell'autorità competente; […] ***una valutazione del contenuto***, almeno con riferimento alle ***pertinenti*** categorie di contenuti terroristici elencati all'articolo 2, paragrafo 5;

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

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

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

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

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

4. Su richiesta del prestatore di servizi di hosting o del fornitore di contenuti, l'autorità competente trasmette una motivazione […] ***supplementare in cui sono spiegati i motivi per i quali il contenuto è considerato contenuto terroristico***, fermo restando l'obbligo del prestatore di servizi di hosting di conformarsi all'ordine di rimozione entro il termine di cui al paragrafo 2.

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

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

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

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

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

Articolo 4 bis

Procedura di consultazione per gli ordini di rimozione

1. L'autorità di emissione presenta una copia dell'ordine di rimozione all'autorità competente di cui all'articolo 17, paragrafo 1, lettera a), dello Stato membro in cui è situato lo stabilimento principale del prestatore di servizi di hosting contemporaneamente alla trasmissione al prestatore di servizi di hosting in conformità dell'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.

3. L'autorità di emissione tiene conto di tali circostanze e, se necessario, ritira o adegua l'ordine di rimozione.

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 sufficienti […] ***su***i motivi per i quali il contenuto è considerato contenuto terroristico ***e fornisce*** 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 ***senza indebito ritardo*** […] la competente autorità o l'organismo competente dell'Unione dell'esito della valutazione e della tempistica di eventuali misure prese a seguito della segnalazione.

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

Articolo 6

Misure proattive

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

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

   a) […] ***contrastare in maniera efficace la ricomparsa d***i contenuti che erano stati rimossi o il cui accesso era stato disabilitato perché considerati contenuti terroristici;

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

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

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

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

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

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

Articolo 7

Conservazione del contenuto e dei relativi dati

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

   a) i procedimenti di riesame amministrativo o giudiziario;

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

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

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

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

SEZIONE III
SALVAGUARDIE E RENDICONTAZIONE

Articolo 8

Obblighi di trasparenza

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

2. I prestatori di servizi di hosting […] ***esposti a contenuti terroristici*** pubblicano relazioni annuali sulla trasparenza in merito alle misure intraprese contro la diffusione di contenuti terroristici.

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

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

   b) informazioni sulle misure intraprese dal prestatore di servizi di hosting per […] ***contrastare in maniera efficace la ricomparsa d***i contenuti che erano stati rimossi o ai quali l'accesso era stato disabilitato perché considerati contenuti terroristici;

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

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

Articolo 9

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

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

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

Articolo 10

Meccanismi di reclamo

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

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

Articolo 11

Informazioni ai fornitori di contenuti

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

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

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

SEZIONE IV

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

Articolo 12

Capacità delle autorità competenti

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

Articolo 13

Cooperazione tra i prestatori di servizi di hosting, le autorità competenti e, se del caso, gli organismi […] ***competenti*** *dell'Unione*

1. Le autorità competenti degli Stati membri scambiano informazioni, si coordinano e cooperano tra loro e, se del caso, con gli […] organismi ***competenti*** dell'Unione quali Europol, per quanto riguarda gli ordini di rimozione e le segnalazioni, in modo da evitare duplicazioni, potenziare il coordinamento ed evitare qualsiasi interferenza con indagini in corso nei diversi Stati membri.

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

3. ***Ai fini dell'efficace attuazione del presente regolamento, nonché per evitare duplicazioni, g***li Stati membri e i prestatori di servizi di hosting possono scegliere di avvalersi di appositi strumenti, inclusi […] quelli stabiliti dagli organismi […] ***competenti*** dell'Unione quali Europol, per facilitare in particolare:

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

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

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

4. Laddove sia a conoscenza di eventuali prove di reati di terrorismo, il prestatore di servizi di hosting ne informa immediatamente l'autorità competente per le indagini e il perseguimento di reati nello Stato membro ***o negli Stati membri*** interessati [...]. ***Ove non sia possibile individuare lo Stato membro o gli Stati membri interessati, il prestatore di servizi di hosting informa*** [...] ***il punto di contatto di cui all'articolo 14, paragrafo 3, dello Stato membro in cui ha lo stabilimento principale o un rappresentante legale e trasmette inoltre*** tali informazioni a Europol, che vi darà adeguato seguito.

Articolo 14

Punti di contatto

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

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

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

SEZIONE V
ATTUAZIONE E ESECUZIONE

Articolo 15
Competenza

1. Lo Stato membro nel quale il prestatore di servizi di hosting ha lo stabilimento principale è competente ai fini degli articoli 6, 18 e 21. Il prestatore di servizi di hosting che non ha lo stabilimento principale in uno degli Stati membri è considerato soggetto alla giurisdizione dello Stato membro in cui risiede o è stabilito il rappresentante legale di cui all'articolo 16. ***Qualsiasi Stato membro è competente ai fini degli articoli 4 e 5, a prescindere dal luogo in cui il prestatore di servizi di hosting ha lo stabilimento principale o in cui ha designato un rappresentante legale.***

2. Laddove il prestatore di servizi di hosting ometta di designare un rappresentante legale, tutti gli Stati membri sono competenti. ***Uno Stato membro, qualora decida di esercitare la propria competenza, ne informa tutti gli altri Stati membri.***

Articolo 16

Rappresentante legale

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

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

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

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

SEZIONE VI
DISPOSIZIONI FINALI

Articolo 17

Designazione delle autorità competenti

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

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

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

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

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

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

Articolo 18

Sanzioni

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

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

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

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

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

e) articolo 7 (conservazione dei dati);

f) articolo 8 (trasparenza);

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

h) articolo 10 (procedure di reclamo);

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

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

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

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

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

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

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

b) il carattere doloso o colposo della violazione;

c) precedenti violazioni da parte della persona giuridica ***o fisica*** ritenuta responsabile;

d) la solidità finanziaria della persona giuridica ***o fisica*** ritenuta responsabile;

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

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

Articolo 19

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

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

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

Articolo 20

Esercizio della delega

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

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

3. La delega di potere di cui all'articolo 19 può essere revocata in qualsiasi momento dal Parlamento europeo o dal Consiglio. La decisione di revoca pone fine alla delega di potere ivi specificata. Gli effetti della decisione decorrono dal giorno successivo alla pubblicazione della decisione nella Gazzetta ufficiale dell'Unione europea o da una data successiva ivi specificata. Essa non pregiudica la validità degli atti delegati già in vigore.

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

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

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

Articolo 21

Monitoraggio

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

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

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

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

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

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

Articolo 22

Relazione sull'applicazione

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

Articolo 23

Valutazione

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

Articolo 24

Entrata in vigore

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

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

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

Fatto a Bruxelles, il

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