



Bruxelles, 14.2.2024
COM(2024) 64 final

**RELAZIONE DELLA COMMISSIONE AL PARLAMENTO EUROPEO E AL
CONSIGLIO**

**sull'attuazione del regolamento (UE) 2021/784 relativo al contrasto della diffusione di
contenuti terroristici online**

{SWD(2024) 36 final}

1. SINTESI

Il regolamento (UE) 2021/784 relativo al contrasto della diffusione di contenuti terroristici online offre agli Stati membri il quadro giuridico a livello europeo per proteggere i cittadini dall'esposizione a materiali terroristici online. Il regolamento cerca di garantire il buon funzionamento del mercato unico digitale contrastando l'uso improprio dei servizi di hosting per la diffusione di contenuti terroristici online al pubblico. Intende impedire ai terroristi di utilizzare Internet per diffondere messaggi allo scopo di intimidire, radicalizzare, reclutare e facilitare gli attacchi terroristici. Tutto questo acquista un'importanza particolare nell'attuale contesto di conflitti e instabilità, che compromette la sicurezza europea. La guerra di aggressione della Russia contro l'Ucraina e l'attacco terroristico sferrato da Hamas contro Israele il 7 ottobre 2023 hanno incrementato la diffusione di contenuti terroristici online.

Il quadro normativo per la lotta contro i contenuti terroristici online è stato rafforzato con l'entrata in vigore del regolamento sui servizi digitali, il 16 novembre 2022. Il regolamento disciplina gli obblighi dei servizi digitali che svolgono attività intermediarie collegando i clienti al contenuto, ai servizi e alle merci, in modo da proteggere meglio gli utenti online e contribuire a un ambiente online più sicuro.

Il regolamento relativo al contrasto della diffusione di contenuti terroristici online è entrato in applicazione il 7 giugno 2022. Ai sensi dell'articolo 22 del regolamento, la Commissione deve presentare al Parlamento europeo e al Consiglio una relazione sull'applicazione del regolamento ("relazione sull'applicazione").

La relazione sull'applicazione si fonda sulla valutazione delle informazioni comunicate dagli Stati membri, da Europol e dai prestatori di servizi di hosting conformemente agli obblighi stabiliti nel regolamento. Sulla base di tale valutazione, le principali conclusioni concernenti l'attuazione del regolamento si possono sintetizzare come illustrato qui di seguito.

- Al 31 dicembre 2023, **23 Stati membri** avevano designato una o più autorità competenti aventi facoltà di emettere ordini di rimozione come stabilito nel regolamento¹. L'elenco delle autorità degli Stati membri, disponibile sul sito web della Commissione, viene periodicamente aggiornato².
- Al 31 dicembre 2023 la Commissione aveva ricevuto informazioni su almeno 349 **ordini di rimozione di contenuti terroristici** emessi dalle autorità competenti di sei Stati membri (Spagna, Romania, Francia, Germania, Cechia e Austria), che nella maggior parte dei casi hanno dato luogo a rapide azioni di follow-up dei prestatori di servizi di hosting, tese a rimuovere i contenuti terroristici o a disabilitare l'accesso a essi. Ciò dimostra che gli strumenti offerti dal regolamento cominciano a essere utilizzati e si dimostrano efficaci nel garantire la rapida rimozione dei contenuti terroristici da parte dei prestatori di servizi di

¹ Il registro online istituito dalla Commissione ai sensi dell'articolo 12, paragrafo 4, del regolamento, elenca le autorità competenti di cui all'articolo 12, paragrafo 1, e il punto di contatto designato o istituito a norma dell'articolo 12, paragrafo 2, per ciascuna autorità competente. Viene periodicamente aggiornato in base alle notifiche ricevute dagli Stati membri. [Elenco delle autorità competenti nazionali e dei punti di contatto \(europa.eu\)](#).

² [Elenco delle autorità competenti nazionali e dei punti di contatto](#).

hosting ai sensi dell'articolo 3, paragrafo 3. Secondo le informazioni ricevute dalla Commissione, questi ordini di rimozione non sono stati impugnati.

- **Funziona bene il coordinamento** tra le autorità competenti degli Stati membri ed Europol, in particolare l'unità addetta alle segnalazioni su Internet di Europol (EU IRU), nell'applicazione del regolamento, soprattutto per quanto riguarda il trattamento degli ordini di rimozione.
- Lo strumento di Europol "**PERCI**"³ è diventato operativo il 3 luglio 2023; alcuni Stati membri lo hanno impiegato con successo per trasmettere ordini di rimozione e segnalazioni⁴. Le autorità competenti spagnole, tedesche, austriache, francesi e ceche lo hanno utilizzato per trasmettere ordini di rimozione. Nel complesso PERCI ha trattato almeno 14 615 segnalazioni tra il suo avvio il 3 luglio e il 31 dicembre 2023.
- Benché il regolamento non preveda misure particolari riguardo alle segnalazioni, secondo le informazioni ricevute dalla Commissione a partire dall'entrata in applicazione del regolamento si è registrato un **incremento della reattività alle segnalazioni** da parte dei prestatori di servizi di hosting.
- A quanto risulta alla Commissione, al 31 dicembre 2023 nessun prestatore di servizi di hosting risultava esposto a contenuti terroristici, secondo la definizione di cui all'articolo 5, paragrafo 4, del regolamento. L'individuazione dell'esposizione a contenuti terroristici è un prerequisito dell'applicazione delle misure specifiche delineate in tale articolo. Secondo le relazioni sulla trasparenza fornite dai prestatori di servizi di hosting, questi ultimi hanno però adottato misure tese a **contrastare l'uso improprio dei loro servizi** per la diffusione di contenuti terroristici, segnatamente con l'adozione di condizioni contrattuali specifiche e l'applicazione di altre disposizioni e misure per limitare la propagazione di contenuti terroristici.
- I prestatori di servizi di hosting hanno adottato altresì misure per informare in merito a **una minaccia imminente per la vita** ai sensi dell'articolo 14, paragrafo 5, del regolamento.

Per quanto riguarda i **prestatori di servizi di hosting di minori dimensioni**, nel 2021 la Commissione ha varato un invito a presentare proposte per sostenerli nell'attuazione del regolamento. Nel 2022 sono stati vincitori tre progetti (si veda alla sezione 4.8) che hanno iniziato a operare nel 2023 e hanno già ottenuto alcuni risultati, aiutando le piccole imprese a conformarsi al regolamento.

La Commissione ha avviato procedure di infrazione contro 22 Stati membri che non avevano designato le autorità competenti ai sensi dell'articolo 12, paragrafo 1, del regolamento, e non avevano adempiuto gli obblighi di cui all'articolo 12, paragrafi 2 e 3, e all'articolo 18, paragrafo 1,

³ PERCI (*Plateforme Européenne de Retraits des Contenus illégaux sur Internet*) è una piattaforma sviluppata e gestita da Europol per rimuovere i contenuti illegali online. Coadiuvata l'attuazione del regolamento offrendo, tra le altre funzionalità, una soluzione tecnica per il trattamento delle segnalazioni e degli ordini di rimozione inviati ai prestatori di servizi di hosting.

⁴ Le segnalazioni sono un meccanismo inteso ad allertare i prestatori di servizi di hosting, affinché possano su base volontaria esaminare la compatibilità di tali contenuti con le proprie condizioni contrattuali. Nel regolamento (considerando 40) si rileva che le segnalazioni si sono dimostrate uno strumento efficace e dovrebbero rimanere disponibili in aggiunta agli ordini di rimozione.

inviando **lettere di costituzione in mora** il 26 gennaio 2023⁵. Dopo l'avvio di tali procedure d'infrazione è aumentato il numero di Stati membri che hanno informato le autorità competenti, responsabili per il trattamento degli ordini di rimozione, come si può rilevare dalle informazioni pubblicate sul registro online⁶. Inoltre 11 delle procedure di infrazione aperte nel gennaio 2023 sono state chiuse entro il 21 dicembre 2023⁷.

Sulla base delle informazioni ricevute dagli Stati membri e da Europol e rese disponibili dai prestatori di servizi di hosting, la Commissione ha valutato che l'applicazione del regolamento abbia avuto un **impatto positivo** nel limitare la propagazione di contenuti terroristici online.

2. CONTESTO

Il regolamento, che è entrato in applicazione il 7 giugno 2022, cerca di garantire il buon funzionamento del mercato unico digitale contrastando l'uso improprio dei servizi di hosting per la diffusione di contenuti terroristici online al pubblico. Fornisce agli Stati membri strumenti mirati, sotto forma di ordini di rimozione, per lottare contro la diffusione di contenuti terroristici online e permette agli Stati membri di imporre ai prestatori di servizi di hosting di tutte le dimensioni di prendere misure specifiche per impedire che i loro servizi siano sfruttati da terroristi quando sono esposti ai contenuti terroristici.

Inoltre con l'entrata in vigore del regolamento sui servizi digitali, il 16 novembre 2022, il quadro normativo è stato esteso mediante una legislazione orizzontale di ampia portata volta a rendere lo spazio digitale più sicuro per i consumatori, con misure efficaci per contrastare i contenuti illegali e condizioni di servizio più trasparenti. Il regolamento dota la Commissione di ampi poteri di vigilanza, indagine ed esecuzione in relazione alle piattaforme online di dimensioni molto grandi e ai motori di ricerca online di dimensioni molto grandi. La Commissione può fra l'altro chiedere informazioni e indagare sulle azioni di moderazione dei contenuti svolte dalle società, e infliggere sanzioni pecuniarie.

Il regolamento sui servizi digitali autorizza ad affrontare ogni forma di contenuto illegale, permettendo alla Commissione di imporre alle piattaforme di fornire dati per dimostrare che rispettano i loro impegni relativi alla rimozione dei contenuti. Il regolamento sui contenuti terroristici online costituisce uno strumento ancora più potente per questa forma specifica di contenuto illegale, introducendo l'obbligo legale di rimuovere il contenuto entro un'ora dal ricevimento dell'ordine di rimozione e meccanismi efficaci di sanzionamento.

Come ha rilevato Europol nelle relazioni sulla situazione e le tendenze del terrorismo (TE-SAT)⁸ pubblicate negli ultimi anni, i terroristi fanno ampio ricorso a Internet per diffondere messaggi allo scopo di intimidire, radicalizzare, reclutare e facilitare gli attacchi terroristici. Sebbene le misure volontarie e le raccomandazioni non vincolanti si siano dimostrate proficue per limitare la

⁵ Cfr. comunicato stampa: [Contenuti terroristici online \(europa.eu\)](https://europa.eu/press-room/content/EN_IP-23-1000).

⁶ [Elenco delle autorità competenti nazionali e dei punti di contatto \(europa.eu\)](https://europa.eu/press-room/content/EN_IP-23-1000). Sul registro online sono reperibili informazioni sulle autorità competenti dei 23 Stati membri responsabili per l'emissione degli ordini di rimozione ai sensi dell'articolo 12, paragrafo 1, lettera a).

⁷ Finlandia, Malta, Cechia, Danimarca, Romania, Svezia, Lettonia, Spagna, Lituania, Austria e Slovacchia.

⁸ [Relazione TE-SAT di Europol 2023 https://www.europol.europa.eu/cms/sites/default/files/documents/Europol_TE-SAT_2023.pdf](https://www.europol.europa.eu/cms/sites/default/files/documents/Europol_TE-SAT_2023.pdf) e 2022 https://www.europol.europa.eu/cms/sites/default/files/documents/Tesat_Report_2022_0.pdf

disponibilità di contenuti terroristici online, alcune limitazioni, tra cui il ridotto numero di prestatori di servizi di hosting che hanno adottato meccanismi volontari⁹ e la frammentazione delle norme procedurali tra gli Stati membri, hanno limitato l'efficienza e l'efficacia della cooperazione tra gli Stati membri e i prestatori di servizi di hosting, rendendo così necessaria l'adozione di misure normative¹⁰. L'effettiva applicazione del regolamento è pertanto fondamentale per contrastare la diffusione di contenuti terroristici online. In tale processo la Commissione ha attivamente coadiuvato le autorità nazionali competenti.

Conformemente all'articolo 22 del regolamento la Commissione era tenuta a presentare una relazione sull'applicazione del regolamento ("relazione sull'applicazione") al Parlamento europeo e al Consiglio entro il 7 giugno 2023, sulla base delle informazioni fornite dagli Stati membri, fondate a loro volta in parte sulle informazioni fornite dai prestatori di servizi di hosting (articolo 21). Il ritardo nella presentazione della relazione sull'applicazione è dovuto, da un lato, alla ritardata trasmissione alla Commissione di informazioni essenziali da parte degli Stati membri e dei prestatori di servizi di hosting; dall'altro, si è stimato importante rispecchiare nella relazione sull'applicazione l'utilizzo di PERCI, che è diventato operativo il 3 luglio 2023 e da allora è stato impiegato per il trattamento degli ordini di rimozione conformemente al regolamento.

La presente relazione si propone unicamente di offrire una panoramica fattuale di questioni pertinenti all'applicazione del regolamento. Non contiene alcuna interpretazione del regolamento, né esprime opinioni su interpretazioni o altre misure adottate per applicare il regolamento.

Conformemente all'articolo 21, paragrafo 2, del regolamento, entro la stessa data (7 giugno 2023) la Commissione ha dovuto istituire un programma dettagliato per monitorare gli esiti, i risultati e gli effetti del regolamento. Più specificamente, il programma di monitoraggio dovrebbe definire gli indicatori e i mezzi da utilizzare per raccogliere i dati e gli altri elementi di prova necessari, nonché la periodicità di tali acquisizioni. Tale programma, che figura nel relativo documento di lavoro dei servizi della Commissione, 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 gli effetti del regolamento e valutarlo in applicazione del suo articolo 23.

3. OBIETTIVO E METODOLOGIA DELLA RELAZIONE

La presente relazione si propone l'obiettivo di valutare l'applicazione del regolamento e l'impatto che esso ha esercitato finora nel limitare la diffusione di contenuti terroristici online. Esamina quindi le azioni intraprese dagli Stati membri e dai prestatori di servizi di hosting, come le modifiche alle condizioni di servizio e agli orientamenti per la comunità, nonché il rispetto degli ordini di rimozione e la reattività a tali ordini.

A tal fine la Commissione ha raccolto informazioni dagli Stati membri, dall'unità addetta alle segnalazioni su Internet di Europol (EU IRU) e dai prestatori di servizi di hosting, tra cui le informazioni contenute nelle relazioni sulla trasparenza e il monitoraggio ai sensi degli articoli 7,

⁹ Commissione europea (2018), Valutazione d'impatto che accompagna la proposta di regolamento relativo alla prevenzione della diffusione di contenuti terroristici online (solo in EN), SWD(2018) 408 final, accesso effettuato il 4/5/2023 all'indirizzo:<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=SWD:2018:408:FIN>.

¹⁰ Ibidem.

8 e 21 del regolamento. 18 Stati membri hanno inviato informazioni a norma degli articoli 8 e 21. Le informazioni sulle azioni intraprese dai prestatori di servizi di hosting sono state raccolte tramite le loro relazioni annuali sulla trasparenza, tramite Europol e mediante comunicazioni volontarie dirette con i servizi della Commissione. La presente relazione sull'applicazione contiene le informazioni ricevute dalla Commissione entro il 31 dicembre 2023.

Obblighi di monitoraggio e trasparenza (articoli 21, 7 e 8)

Per elaborare la relazione sull'applicazione, a norma dell'articolo 21, paragrafo 1, del regolamento, gli Stati membri sono tenuti a raccogliere informazioni dalle loro autorità competenti e dai prestatori di servizi di hosting soggetti alla loro giurisdizione e a trasmetterle alla Commissione ogni anno entro il 31 marzo, comprese informazioni sulle azioni intraprese a norma del regolamento nell'anno civile precedente. L'articolo 21, paragrafo 1, indica il tipo di informazioni che gli Stati membri dovrebbero raccogliere in merito alle misure intraprese per conformarsi al regolamento, come i dettagli concernenti gli ordini di rimozione, il numero di richieste di accesso ai contenuti conservati per consentire lo svolgimento di indagini, procedimenti di reclamo e procedimenti di controllo amministrativo o giurisdizionale.

A norma dell'articolo 7, paragrafo 1, del regolamento, i prestatori di servizi di hosting definiscono chiaramente nelle loro condizioni contrattuali la loro politica volta a contrastare la diffusione di contenuti terroristici, che include, se del caso, una valida spiegazione del funzionamento delle misure specifiche.

Inoltre, conformemente all'articolo 7, paragrafo 2, del regolamento, un prestatore di servizi di hosting che, a norma del regolamento, abbia adottato misure contro la diffusione di contenuti terroristici in un determinato anno civile o sia stato tenuto a farlo, rende disponibile al pubblico una relazione sulla trasparenza in merito a tali azioni per tale anno. Tale relazione dev'essere pubblicata prima del 1° marzo dell'anno seguente.

L'articolo 7, paragrafo 3, del regolamento enumera le informazioni minime che tali relazioni sulla trasparenza dovrebbero contenere, come le misure intraprese per quanto concerne l'individuazione e la disabilitazione dell'accesso a contenuti terroristici, il numero di elementi che sono stati rimossi e/o ripristinati e l'esito dei reclami.

A norma dell'articolo 8 del regolamento le autorità competenti designate dagli Stati membri pubblicano relazioni annuali sulla trasparenza relative alle loro attività a norma del regolamento. L'articolo 8, paragrafo 1, indica le informazioni minime che tali relazioni dovrebbero contenere¹¹.

Al 31 dicembre 2023 18 Stati membri avevano trasmesso alla Commissione informazioni relative alle azioni intraprese in conformità del regolamento, mentre 23 Stati membri avevano designato una o più autorità aventi facoltà di emettere ordini di rimozione come stabilito nel regolamento.

¹¹ Cfr. il testo dell'articolo 8, paragrafo 1, del regolamento (UE) 2021/784 <https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:32021R0784>.

4. PUNTI SPECIFICI DI VALUTAZIONE

4.1. ORDINI DI RIMOZIONE (articolo 3)

In totale al 31 dicembre 2023 la Commissione era stata informata in merito ad almeno 349 ordini di rimozione inviati a Telegram, Meta, Justpaste.it, TikTok, DATA ROOM S.R.L., FLOKINET S.R.L., Archive.org, Soundcloud, X, Jumpshare.com, Krakenfiles.com, Top4Top.net e Catbox dalle autorità competenti di Spagna, Romania, Francia, Germania, Austria e Cechia.

L'autorità competente spagnola (CITCO - *Centro de Inteligencia contra el Terrorismo y el Crimen Organizado*) ha inviato 62 ordini di rimozione, l'autorità competente rumena (ANCOM – *Autoritatea Națională pentru Administrare și Reglementare în Comunicații*) ne ha inviati due e l'autorità competente francese (OCLCTIC – *Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication*) ne ha inviati 26. Dopo l'attacco terroristico perpetrato da Hamas contro Israele, l'autorità competente tedesca (BKA – *Bundeskriminalamt*) ha inviato 249 ordini di rimozione.

L'autorità spagnola competente ha trasmesso 62 ordini di rimozione, di cui 18 prima dell'avvio di PERCI e 44 tramite PERCI, fornendo una descrizione dettagliata della trasmissione e del follow-up degli ordini di rimozione emessi, assai importante per comprendere meglio le implicazioni e gli effetti del regolamento.

I primi due ordini di rimozione, emessi dall'autorità competente spagnola il 24 aprile 2023¹², riguardavano due messaggi con contenuto terroristico: l'uno opera del terrorismo di destra, l'altro opera del jihadismo. Il contenuto oggetto del primo ordine di rimozione era un documento PDF pubblicato su Telegram con accesso illimitato, che propugnava la violenza terroristica ed esaltava gli attentati terroristici di destra. Il messaggio con contenuto terroristico oggetto del secondo ordine di rimozione era un video caricato su Internet Archive, in cui comparivano immagini di jihadisti in combattimento, appartenenti all'organizzazione terroristica del cosiddetto Stato islamico. Questi due messaggi con contenuto terroristico sono stati rimossi da entrambe le piattaforme in meno di un'ora, e quindi nel rispetto dell'articolo 3, paragrafo 3, del regolamento. Nella valutazione fornita l'autorità competente spagnola ha spiegato di aver scelto un ordine di rimozione anziché una segnalazione essenzialmente per due motivi: il rispetto delle prescrizioni del regolamento in materia di ordini di rimozione e l'urgenza. L'autorità competente spagnola ha in seguito trasmesso altri ordini di rimozione.

Ha altresì evidenziato i problemi derivanti dal fatto che un prestatore di servizi di hosting (Meta) ha utilizzato un modulo web per ricevere gli ordini di rimozione anziché fornire un punto di contatto diretto. Questo modulo web ha causato anche problemi di comunicazione con l'autorità competente dello Stato membro in cui si trova lo stabilimento principale del prestatore di servizi di hosting.

L'autorità competente francese ha emesso il primo ordine di rimozione il 13 luglio 2023 nei confronti di una piattaforma di condivisione (Justpaste.it), che ha rimosso il contenuto terroristico entro un'ora. Il contenuto in questione era un messaggio propagandistico di Al Qaeda, proveniente

¹² [Ministerio del Interior | El CITCO culmina la retirada de Internet de dos contenidos que alentaban al terrorismo](#)

più specificamente dal suo organismo mediatico Rikan Ka Mamber della sezione indiana Al Qaeda Indian Sub continent (AQIS). La rimozione totale del contenuto è stata confermata sulla piattaforma PERCI di Europol.

L'autorità competente tedesca ha emesso sei, sedici e cinque ordini di rimozione, rispettivamente il 16, 18 e 24 ottobre 2023, nei confronti di messaggi propagandistici di Hamas e della Jihad islamica palestinese. L'accesso ai contenuti è stato disabilitato nell'UE conformemente all'articolo 3, paragrafo 3, del regolamento. L'autorità competente tedesca aveva dapprima inviato segnalazioni e poi emesso ordini di rimozione, dal momento che le segnalazioni non avevano avuto seguito. Dopo l'attacco sferrato da Hamas il 7 ottobre 2023, l'autorità competente tedesca ha trasmesso 249 ordini di rimozione, diretti in gran parte a Telegram¹³.

Le autorità competenti ceca e austriaca hanno trasmesso due e otto ordini di rimozione, rispettivamente a X e a Telegram.

Per quanto riguarda l'uso di un modulo web da parte di un prestatore di servizi di hosting per ricevere gli ordini di rimozione, le autorità spagnole hanno indicato due problemi: 1) nel contesto dell'articolo 3, paragrafo 2, del regolamento, un modulo web non consente alle autorità competenti degli Stati membri di trasmettere informazioni sulle procedure e sui termini applicabili prima di emettere il primo ordine di rimozione nei confronti del prestatore di servizi di hosting; 2) nel contesto dell'articolo 4, paragrafo 1, un modulo web non consente di trasmettere contemporaneamente una copia dell'ordine di rimozione all'autorità competente dello Stato membro in cui il prestatore di servizi di hosting ha lo stabilimento principale e al rappresentante legale del prestatore di servizi di hosting.

4.2 ORDINI DI RIMOZIONE TRANSFRONTALIERI (articolo 4)

Per i primi due ordini di rimozione emessi nell'aprile 2023, l'autorità competente spagnola non ha potuto inviare copie all'autorità dello Stato membro in cui il prestatore di servizi di hosting aveva lo stabilimento principale né al suo rappresentante legale, poiché nessuno dei due prestatori di servizi di hosting, in quel momento, aveva lo stabilimento principale né aveva designato un rappresentante legale nell'UE. Per gli ordini di rimozione successivi l'autorità competente spagnola ha inviato copie all'autorità competente dello Stato membro in cui il prestatore di servizi di hosting aveva lo stabilimento principale o aveva designato il proprio rappresentante legale.

Gli Stati membri avevano segnalato la difficoltà di trasmettere ordini di rimozione ai prestatori di servizi di hosting con sede in paesi terzi che non abbiano ancora adempiuto l'obbligo di nominare un rappresentante legale nell'Unione europea. In tale contesto la Commissione ha aiutato gli Stati membri ad assicurarsi che i prestatori di servizi di hosting adempiano l'obbligo di nominare un rappresentante legale nell'UE e di istituire un punto di contatto (articolo 15, paragrafo 1, del regolamento), come un indirizzo di posta elettronica, per assicurare un'azione immediata.

¹³ Secondo le informazioni di cui dispone la Commissione.

Inoltre la Commissione ha ricordato ai prestatori di servizi di hosting i loro obblighi in diverse sedi, tra cui il Forum dell'UE su Internet.

A quanto risulta alla Commissione, nessuna autorità competente dello Stato membro in cui il prestatore di servizi di hosting ha lo stabilimento principale ha finora esaminato un ordine di rimozione, ai sensi dell'articolo 4 del regolamento, per stabilire se esso abbia violato in modo grave o manifesto il regolamento o i diritti e le libertà fondamentali, poiché non è stata ancora presentata alcuna richiesta motivata di esame. Di conseguenza, finora nessuna autorità ha riscontrato che un ordine di rimozione violasse in tal modo il regolamento o i diritti fondamentali.

Finora nessun prestatore di servizi di hosting ha ripristinato i contenuti (o riabilitato l'accesso agli stessi) che erano stati oggetto di un ordine di rimozione a seguito dell'esame di cui all'articolo 4 del regolamento, poiché tale esame e le relative richieste di ripristino non hanno ancora avuto luogo. Di conseguenza non sono disponibili informazioni sul tempo solitamente necessario per ripristinare i contenuti o riabilitare l'accesso agli stessi, né sulle "misure necessarie" adottate dal prestatore di servizi di hosting per ripristinare i contenuti o riabilitare l'accesso agli stessi.

4.3. RICORSO EFFETTIVO (articolo 9)

Secondo le informazioni di cui dispone la Commissione, finora i prestatori di servizi di hosting non hanno impugnato ordini di rimozione o decisioni adottate ai sensi dell'articolo 5, paragrafo 4, dinanzi agli organi giurisdizionali competenti. Un prestatore di servizi di hosting ha tuttavia segnalato l'impossibilità di eseguire un ordine di rimozione.

Secondo le informazioni fornite dagli Stati membri¹⁴ almeno 12 Stati membri hanno messo in atto "procedure efficaci" per consentire ai prestatori di servizi di hosting e ai fornitori di contenuti di impugnare un ordine di rimozione emesso e/o una decisione adottata ai sensi dell'articolo 4, paragrafo 4, o dell'articolo 5, paragrafi 4, 6 o 7, dinanzi agli organi giurisdizionali dello Stato membro dell'autorità competente (articolo 9, paragrafi 1 e 2). Negli Stati membri in cui sono state messe in atto, tali procedure riguardano per lo più azioni legali. Sulla base dei dati attuali ricevuti dagli Stati membri, non è però possibile verificare se queste procedure siano "efficaci" o specificamente concernenti il regolamento, poiché fino ad oggi nessuna decisione è stata impugnata.

4.4. MISURE SPECIFICHE E RELATIVA TRASPARENZA (articoli 5 e 7)

Secondo le informazioni disponibili, fino a oggi nessun prestatore di servizi di hosting è stato ritenuto esposto a contenuti terroristici ai sensi dell'articolo 5, paragrafo 4, del regolamento. Di conseguenza l'obbligo di adottare le misure specifiche di cui a tale articolo non si applica (ancora) ad alcun prestatore di servizi di hosting.

Si noti tuttavia che, secondo le relazioni sulla trasparenza fornite dai prestatori di servizi di hosting, molti di questi ultimi hanno adottato misure tese a contrastare l'uso improprio dei loro servizi per la diffusione di contenuti terroristici, segnatamente l'adozione di condizioni contrattuali specifiche

¹⁴ Si osservi che le informazioni fornite non sono necessariamente complete. Sarebbero necessarie ulteriori valutazioni per tracciare un panorama esaustivo e interamente aggiornato del modo in cui gli Stati membri hanno dato attuazione all'obbligo di garantire la disponibilità di procedure di ricorso efficaci.

e l'applicazione di altre disposizioni e misure per limitare la propagazione di contenuti terroristici. Come si è osservato in precedenza, ai sensi dell'articolo 7 i prestatori di servizi di hosting devono garantire la trasparenza a tal proposito, non soltanto tramite relazioni sulla trasparenza ma anche inserendo nelle proprie condizioni contrattuali informazioni chiare.

4.5. MINACCIA IMMINENTE PER LA VITA (articolo 14, paragrafo 5)

Ai sensi dell'articolo 14, paragrafo 5, del regolamento, laddove sia a conoscenza di contenuti terroristici che comportano una minaccia imminente per la vita, il prestatore di servizi di hosting deve informarne immediatamente l'autorità competente per l'indagine e il perseguimento di reati negli Stati membri interessati. Ove non sia possibile individuare gli Stati membri interessati, il prestatore di servizi di hosting trasmette le informazioni a Europol, che vi darà adeguato seguito.

Al 31 dicembre 2023 la Commissione era stata informata di nove casi in cui l'unità UE addetta alle segnalazioni su Internet di Europol aveva ricevuto informazioni su contenuti terroristici che comportavano una minaccia imminente per la vita. Dal momento che l'articolo 14, paragrafo 5, del regolamento non prevede l'obbligo di informare Europol in tutti i casi, il numero delle notifiche potrebbe essere più elevato. La Spagna è l'unico Stato membro che ha fornito informazioni sull'applicazione dell'articolo 14, paragrafo 5. Il 18 aprile 2023 le autorità della Spagna hanno ricevuto una comunicazione da Amazon in merito a un presunto messaggio con contenuto terroristico, pubblicato sulla piattaforma videoludica Twitch, che comportava una minaccia imminente per la vita. Si è valutato che il contenuto non corrispondeva alle condizioni di un contenuto terroristico che comporti una minaccia imminente per la vita ai sensi del regolamento.

4.6. COOPERAZIONE TRA I PRESTATORI DI SERVIZI DI HOSTING, LE AUTORITÀ COMPETENTI E EUROPOL (articolo 14)

Come si è già osservato, Europol ha sviluppato una piattaforma denominata "PERCI" per coadiuvare l'attuazione del regolamento centralizzando, coordinando e favorendo la **trasmissione degli ordini di rimozione e delle segnalazioni** dagli Stati membri ai prestatori di servizi di hosting. La piattaforma è operativa dal 3 luglio 2023. Prima della piena attuazione di PERCI, Europol aveva messo in atto disposizioni contingenti per favorire la trasmissione manuale degli ordini di rimozione, la prevenzione di situazioni conflittuali relative ai contenuti per evitare interferenze con le indagini in corso e la risposta alle crisi in situazioni di "minaccia imminente per la vita".

PERCI è un sistema unico che consente la cooperazione tra le autorità competenti, i prestatori di servizi di hosting ed Europol, come prevede l'articolo 14 del regolamento per quanto riguarda le questioni trattate dal regolamento. Più concretamente PERCI:

- è una soluzione basata sul cloud concepita per garantire la sicurezza e la protezione dei dati nel cloud;
- è una piattaforma unica per la comunicazione e il coordinamento collaborativi in tempo reale, che agevola la rapida rimozione dei contenuti terroristici;

- favorisce il processo di esame degli ordini di rimozione transfrontalieri;
- rafforza la prevenzione di situazioni conflittuali, che è importante per evitare che l'autorità competente di uno Stato membro trasmetta un ordine di rimozione diretto a contenuti oggetto di un'indagine in corso in un altro Stato membro;
- consente ai prestatori di servizi di hosting di ricevere ordini di rimozione da un unico canale secondo criteri unificati e standardizzati.

Separatamente PERCI consente altresì la trasmissione delle segnalazioni.

Attualmente, a parte la sua rilevanza in relazione alle segnalazioni (si veda il considerando 40 del regolamento), PERCI favorisce la trasmissione degli ordini di rimozione (articoli 3 e 4), la presentazione di relazioni da parte degli Stati membri (articolo 8) e il coordinamento tra loro, nonché la prevenzione di situazioni conflittuali nel caso di conflitto con indagini in corso su contenuti per cui si intenda inviare un ordine di rimozione (articolo 14). PERCI è in fase di ulteriore sviluppo alla luce degli ulteriori compiti che dovrà svolgere in base al regolamento, come l'esame degli ordini di rimozione transfrontalieri (articolo 4)¹⁵.

Gli Stati membri hanno confermato che, ai sensi dell'articolo 14 del regolamento:

- le autorità competenti scambiano informazioni, si coordinano e cooperano tra loro;
- le autorità competenti scambiano informazioni, si coordinano e cooperano con Europol;
- esistono meccanismi per potenziare la cooperazione ed evitare qualsiasi interferenza con le indagini in corso negli altri Stati membri;
- la maggior parte degli Stati membri considera PERCI lo strumento preferito da utilizzare per trasmettere gli ordini di rimozione, giacché consente di coordinare l'azione tramite la prevenzione di situazioni conflittuali.

4.7. *EFFETTI SULLE SEGNALAZIONI*

Le segnalazioni di contenuti terroristici sono uno strumento volontario già utilizzato prima dell'adozione del regolamento. Benché il regolamento non contenga norme specifiche dedicate alle segnalazioni, conformemente al considerando 40 nessuna disposizione del regolamento impedisce agli Stati membri e a Europol di utilizzare le segnalazioni come strumento per contrastare i contenuti terroristici online.

¹⁵ Più dettagliatamente: - articoli 3 e 4: trasmissione di ordini di rimozione; - articolo 3, paragrafi da 6 a 8: riscontro dei prestatori di servizi di hosting; - articolo 4, paragrafi da 3 a 7: meccanismo di esame; - articolo 7: relazioni; - articolo 14, paragrafo 1: prevenire situazioni conflittuali, coordinare, evitare duplicazione di sforzi; - articolo 14, paragrafo 3 meccanismo di comunicazione sicuro; - articolo 14, paragrafo 4: utilizzo di un apposito strumento stabilito da Europol; - articolo 14, paragrafo 5: comunicazione di "minaccia imminente per la vita"; considerando 40: trasmissione di segnalazioni.

Fin dalla sua istituzione nel 2015, l'unità UE addetta alle segnalazioni su Internet di Europol opera per individuare i contenuti terroristici online e segnalarli ai prestatori di servizi di hosting; istituisce inoltre strumenti (PERCI e in precedenza IRMA¹⁶) per favorire la trasmissione delle segnalazioni.

Secondo le informazioni fornite alla Commissione, le autorità degli Stati membri continuano a utilizzare le segnalazioni con alcuni prestatori di servizi di hosting, ma potrebbero considerare l'opportunità di emettere ordini di rimozione nei confronti dei prestatori di servizi di hosting che non rispondono alle segnalazioni, oppure per altre ragioni come l'urgenza di rimuovere determinati contenuti.

4.8. SOSTEGNO AI PRESTATORI DI SERVIZI DI HOSTING DI MINORI DIMENSIONI PER L'ATTUAZIONE DEL REGOLAMENTO

Il regolamento contiene vari obblighi per i prestatori di servizi di hosting. Mentre i prestatori di servizi di hosting che sono grandi imprese hanno di solito capacità tecniche, capacità di controllo umano e conoscenze adeguate per attuare il regolamento, quelli che sono piccole imprese dispongono a tale scopo di risorse finanziarie, tecniche e umane e di competenze più limitate. Allo stesso tempo i prestatori di servizi di hosting di minori dimensioni sono presi di mira sempre più spesso da soggetti malintenzionati che vorrebbero sfruttarne i servizi. Questa tendenza si può attribuire anche agli efficaci sforzi di moderazione dei contenuti intrapresi dai prestatori di servizi di hosting di maggiori dimensioni; ciò mostra il successo delle misure di moderazione dei contenuti, ma anche l'esigenza di sostenere i prestatori di servizi di hosting di minori dimensioni per accrescerne la capacità e le conoscenze necessarie ad adempiere le prescrizioni del regolamento.

Per raccogliere questa sfida la Commissione ha varato un invito a presentare proposte nel quadro del Fondo Sicurezza interna, allo scopo di sostenere i prestatori di servizi di hosting di minori dimensioni nell'attuazione del regolamento¹⁷. La Commissione ha selezionato tre progetti¹⁸ che saranno sostenuti con un triplice approccio: in primo luogo con un'opera di informazione e sensibilizzazione relativa alle norme e alle prescrizioni del regolamento; in secondo luogo sviluppando, attuando e mettendo in opera gli strumenti e i quadri necessari per contrastare la diffusione di contenuti terroristici online; in terzo luogo condividendo esperienze e migliori pratiche in tutto il settore.

¹⁶ Europol ha istituito l'applicazione di gestione delle segnalazioni (IRMA) nel 2016 per favorire la segnalazione (flagging) di contenuti illegali ai prestatori di servizi online. Inizialmente l'accesso a IRMA è stato accordato al personale Europol e a unità specializzate (IRU) in sette Stati membri. IRMA è stata sostituita da PERCI il 3 luglio 2023.

¹⁷ https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/isf/wp-call/2021-2022/call-fiche_isf-2021-ag-teo_en.pdf

¹⁸ (1) Un quadro basato sull'intelligenza artificiale per sostenere i prestatori di servizi di hosting (microimprese e piccole imprese) nella segnalazione e nella rimozione di contenuti terroristici online (ALLIES), (2) Lotta ai contenuti terroristici online (FRISCO) e (3) Tecnologia contro il terrorismo in Europa (TATE). Per ulteriori informazioni consultare il link seguente: Finanziamenti e gare d'appalto (europa.eu).

I tre progetti hanno iniziato a operare nel 2023 e hanno già prodotto risultati preziosi. Ad esempio, nella sua relazione di mappatura il progetto FRISCO¹⁹ ha rilevato che i prestatori di servizi di hosting che sono microimprese e piccole imprese hanno tendenzialmente consapevolezza e conoscenze assai limitate del regolamento; la relazione sottolinea inoltre le potenziali difficoltà che questi prestatori di servizi di hosting potrebbero incontrare per rispondere agli ordini di rimozione entro un'ora, giacché spesso non dispongono di servizi attivi 24 ore su 24, sette giorni su sette. La carenza di risorse rappresenta un problema, così come l'istituzione di linee di comunicazione con le autorità di contrasto. Più della metà dei prestatori di servizi di hosting esaminati dai contraenti non moderano i contenuti generati dagli utenti e hanno affermato di non aver mai rilevato contenuti terroristici sulle proprie piattaforme. Questi prestatori di servizi di hosting adottano probabilmente misure ad hoc qualora tali contenuti appaiano sulle loro piattaforme.

Questi tre progetti coadiuvano i prestatori di servizi di hosting (piccole imprese) negli sforzi per conformarsi alle norme del regolamento, anche istituendo punti di contatto e meccanismi di attuazione per i reclami degli utenti.

Inoltre l'articolo 3, paragrafo 2, del regolamento - che impone di fornire tempestivamente informazioni sulle procedure e sui termini applicabili ai prestatori di servizi di hosting nei cui confronti non siano stati emessi in precedenza ordini di rimozione - può assumere importanza specialmente per i prestatori di servizi di hosting di minori dimensioni.

4.9. *SALVAGUARDIE A TUTELA DEI DIRITTI FONDAMENTALI*

Il regolamento comprende varie salvaguardie volte a rafforzare la responsabilità e la trasparenza in merito alle misure adottate per rimuovere i contenuti terroristici online. A tale proposito si fa riferimento a quanto si è già illustrato, specialmente alle informazioni fornite sui mezzi di ricorso, alle segnalazioni e al meccanismo speciale per gli ordini di rimozione transfrontalieri.

Ai sensi dell'articolo 23 del regolamento, inoltre, la Commissione trasmette una relazione sul funzionamento e l'efficacia dei meccanismi di salvaguardia, in particolare di quelli previsti dall'articolo 4, paragrafo 4, dall'articolo 6, paragrafo 3, e dagli articoli da 7 a 11, nel quadro della valutazione del regolamento. Tali salvaguardie riguardano i reclami, i mezzi di ricorso e i meccanismi di sanzione adottati e applicati contro il rischio di rimozione erronea di contenuti terroristici online per tutelare i fornitori di contenuti e i prestatori di servizi di hosting. La valutazione del funzionamento e dell'efficacia dei meccanismi di salvaguardia farà quindi parte della valutazione ai sensi dell'articolo 23.

A tal proposito il programma di monitoraggio di cui all'articolo 21, paragrafo 2, del regolamento contiene un quadro di indicatori per valutare gli effetti del regolamento sui diritti fondamentali, che confluirà nella valutazione del regolamento.

¹⁹ Effettuata nell'arco di sei mesi fino a maggio 2023. La relazione si basa sul riscontro fornito da 48 prestatori di servizi di hosting europei: 33 risposte alla nostra indagine online e 15 risposte tramite interviste. FRISCO, *D2.1: Relazione di mappatura sulle esigenze e gli ostacoli in relazione alla conformità. Comprendere le esigenze e la consapevolezza dei prestatori di servizi di hosting (microimprese e piccole imprese) per quanto riguarda l'adempimento delle prescrizioni del regolamento sui contenuti terroristici online* (non disponibile in IT), disponibile all'indirizzo [Deliverables | Frisco \(friscoprotect.eu\)](https://friscoprotect.eu).

Il programma di monitoraggio favorirà la valutazione del funzionamento e dell'efficacia dei meccanismi di salvaguardia attuati nel contesto del regolamento e delle loro conseguenze sui diritti fondamentali, che a sua volta fa parte della valutazione del regolamento. Questa sezione delle conseguenze corrisponde alle due sezioni citate all'articolo 23 del regolamento: a) il funzionamento e l'efficacia dei meccanismi di salvaguardia, in particolare di quelli previsti dall'articolo 4, paragrafo 4, dall'articolo 6, paragrafo 3, e dagli articoli da 7 a 11; b) le conseguenze dell'applicazione del presente regolamento sui diritti fondamentali, in particolare la libertà di espressione e di informazione, il rispetto della vita privata e la protezione dei dati personali.

4.10. AUTORITÀ COMPETENTI (articolo 13)

A norma dell'articolo 13 del regolamento, gli Stati membri devono assicurare che le autorità competenti dispongano di poteri necessari e di risorse sufficienti per conseguire gli obiettivi e adempiere gli obblighi loro incombenti a norma del regolamento. Alcuni Stati membri hanno applicato le misure seguenti per far sì che le autorità competenti dispongano di poteri necessari e di risorse sufficienti:

- istituzione di nuovi organismi/direzioni;
- assegnazione di fondi straordinari e di personale supplementare e
- introduzione di nuovi quadri legislativi.

5. CONCLUSIONI

È estremamente importante attuare senza riserva tutti gli strumenti e le misure a livello dell'UE per contrastare rapidamente la diffusione di contenuti illegali diffusi online, soprattutto in considerazione della vasta portata di tali contenuti, testimoniata di recente dalla diffusione di contenuti relativi all'attacco perpetrato da Hamas contro Israele.

Il regolamento contribuisce a rafforzare la sicurezza pubblica in tutta l'Unione per impedire che i terroristi utilizzino i prestatori di servizi di hosting operanti nel mercato interno per diffondere messaggi volti a intimidire, radicalizzare, reclutare e facilitare gli attacchi terroristici.

In seguito all'apertura di procedure di infrazione nel gennaio 2023, **sono stati compiuti alcuni progressi**. Al 31 dicembre 2023, come si ricava dal registro online, 23 Stati membri avevano designato autorità competenti ai sensi dell'articolo 12, paragrafo 1, il che ha permesso di usare in modo più sistematico le misure e gli strumenti offerti dal regolamento. Al 21 dicembre 2023 erano state chiuse 11 delle 22 procedure di infrazione aperte nel gennaio 2023. La Commissione esorta gli Stati membri rimanenti ad adottare le misure necessarie per designare le autorità competenti ai sensi dell'articolo 12, paragrafo 1, e ad adempiere gli obblighi di cui all'articolo 12, paragrafi 2 e 3, e all'articolo 18, paragrafo 1.

Complessivamente gli Stati membri hanno segnalato un'agevole trasmissione degli ordini di rimozione ai prestatori di servizi di hosting con il sostegno di Europol. Sulla base delle informazioni ricevute dagli Stati membri e da Europol, dall'entrata in applicazione del regolamento sono stati trasmessi almeno 349 **ordini di rimozione di contenuti terroristici**. In 10 casi i

contenuti terroristici non sono stati rimossi o l'accesso non è stato disabilitato dal prestatore di servizi di hosting entro il termine massimo di un'ora stabilito dal regolamento.

Secondo le informazioni ricevute dagli Stati membri e da Europol, benché il regolamento non contenesse norme a riguardo, dall'entrata in applicazione del regolamento si è registrata una maggiore reattività alle segnalazioni di contenuti terroristici. In nove casi inoltre Europol ha ricevuto dai prestatori di servizi di hosting informazioni su contenuti terroristici che comportavano una minaccia imminente per la vita, ai sensi dell'articolo 14, paragrafo 5.

Sono stati attuati procedure e canali di comunicazione più efficienti soprattutto dopo l'avvio della piattaforma PERCI il 3 luglio 2023, che ha dato luogo a un approccio più sistematico alla trasmissione di ordini di rimozione; PERCI viene inoltre utilizzata per trasmettere un maggior numero di segnalazioni. Gli Stati membri ed Europol si attendono che l'impiego di PERCI favorisca l'uso di questi strumenti volti a contrastare i contenuti terroristici online.

Su questa base la Commissione stima che, nel complesso, il regolamento abbia esercitato un **effetto positivo** nel limitare la diffusione di contenuti terroristici online. In 10 casi su 349, tuttavia, il prestatore di servizi di hosting ha superato il termine massimo di un'ora stabilito dal regolamento per rimuovere i contenuti terroristici o disabilitare l'accesso a essi.

La Commissione sostiene attivamente gli Stati membri e i prestatori di servizi di hosting, anche per mezzo di seminari tecnici organizzati prima dell'entrata in applicazione del regolamento e dopo di essa. L'ultimo seminario si è svolto il 24 novembre 2023. La Commissione sostiene in particolare i prestatori di servizi di hosting di minori dimensioni, per garantire una rapida e completa applicazione del regolamento e aiutarli ad affrontare i problemi che si sono presentati finora.

La Commissione continuerà a sorvegliare l'attuazione e l'applicazione del regolamento. La Commissione sorveglierà da vicino il funzionamento degli strumenti previsti dal regolamento tramite il programma di monitoraggio, che confluirà nella valutazione del regolamento ai sensi dell'articolo 23.