Il Regolamento dell'Unione sul contrasto della diffusione di contenuti terroristici online: le principali novità e le potenziali criticità

06/10/2022 DIRITTO EUROPEO E DELLA CONCORRENZA, IT&TMT, PROSPETTIVE

Andrea Palumbo

In data 7 giugno 2022, ha cominciato a trovare applicazione il Regolamento relativo al contrasto della diffusione di contenuti terroristici online[1] (conosciuto come «*Terrorist Content Regulation*»), che rappresenta un'iniziativa di fondamentale importanza sia per la lotta al terrorismo che per l'evoluzione del diritto europeo dei media. Il Regolamento, che è direttamente applicabile in tutti gli Stati membri dell'Unione, impone obbligazioni di ampia portata per i prestatori di servizi di *hosting*[2] stabiliti nell'Unione e fuori dall'Unione. Il Regolamento è stato molto discusso per l'incisività degli obblighi imposti ai prestatori di servizi di *hosting* e per i rischi che la sua applicazione pone per i diritti alla libertà di espressione e alla privacy.

Il Regolamento si caratterizza per avere un ambito di applicazione particolarmente ampio, ed una portata extraterritoriale. Difatti, trova applicazione per tutti i prestatori di servizi di *hosting*, a prescindere dal loro luogo di stabilimento fintantoché prestano servizi agli utenti nell'Unione, e quindi anche per i prestatori stabiliti fuori dall'Unione. Vi

[1] Regolamento (UE) 2021/784 del Parlamento europeo e del Consiglio del 29 aprile 2021 relativo al contrasto della diffusione di contenuti terroristici online, GUUE L 172 del 17.05.2021.
[2] Gli *host providers*, o prestatori di servizi di *hosting*, sono una categoria di prestatore di servizi della società dell'informazione le cui attività sono destinatarie di una disciplina *ad hoc* in molti testi legislativi europei. Ai sensi dell'articolo 2, punto 1), del Regolamento in esame, il prestatore di servizi di hosting è definito come "*un prestatore di servizi di cui all'articolo 1, lettera b), della direttiva (UE) 2015/1535 del Parlamento europeo e del Consiglio che consistono nel memorizzare le informazioni fornite dal fornitore di contenuti su richiesta di quest'ultimo*".

sono poi specifici ed ulteriori obblighi imposti per i prestatori che le autorità nazionali considerano essere esposti a contenuti terroristici.

Per quanto riguarda i nuovi obblighi del Regolamento, questi si suddividono i tre principali categorie, e si declinano diversamente a seconda che il prestatore sia o meno designato come esposto a contenuti terroristici.

La prima categoria riguarda gli obblighi di rimozione del contenuto e di predisposizione di un meccanismo di reclamo, applicabili indistintamente a tutti i prestatori. In primo luogo, l'autorità competente di ogni Stato membro ha la facoltà di emettere un ordine di rimozione richiedendo ai prestatori di rimuovere contenuti terroristici o di disabilitare l'accesso a contenuti terroristici in tutti gli Stati membri. Con la ricezione dell'ordine, i prestatori sono conseguentemente tenuti a rimuovere i contenuti terroristici o a disabilitare l'accesso ai contenuti terroristici in tutti gli Stati membri il prima possibile, e in ogni caso entro un'ora dal ricevimento dell'ordine di rimozione[3]. Tuttavia, se il prestatore non ha mai ricevuto un ordine di rimozione in precedenza, riceverà, 12 ore prima che l'ordine sia emesso, una comunicazione ufficiale contenente informazioni sulle procedure e le scadenze applicabili in relazione all'ordine. Al contempo, come salvaguardia per la tutela della libertà di espressione degli utenti in connessione agli ordini di rimozione, è previsto che i prestatori predispongono un meccanismo efficace e accessibile che consenta ai fornitori di contenuti i cui contenuti siano stati rimossi, o l'accesso ai quali sia stato disabilitato, di presentare un reclamo nei confronti di tale rimozione o disabilitazione, chiedendo la reintegrazione dei contenuti o del relativo accesso[4]. I prestatori sono tenuti ad esaminare tempestivamente ogni reclamo ricevuto tramite il suddetto meccanismo, e a ripristinare i contenuti o l'accesso senza ritardo qualora la rimozione o la disabilitazione appaiono ingiustificate. In caso di rigetto del reclamo, il prestatore deve fornire una motivazione per la propria decisione.

La seconda categoria riguarda gli obblighi di notifica dei prestatori, che si declinano diversamente a seconda del livello di esposizione a contenuti terroristici del singolo prestatore. Vi sono tre obblighi applicabili indistintamente a tutti i prestatori. In primo luogo, ogni prestatore deve informare l'autorità competente senza ritardo dell'avvenuta rimozione o blocco di contenuti terroristici a seguito dell'emissione di un ordine di rimozione. In secondo luogo, i prestatori devono notificare l'avvenuta rimozione o blocco agli utenti il cui contenuto è stato rimosso o bloccato. In terzo luogo, qualora i prestatori vengano a conoscenza dell'esistenza di contenuti terroristici che comportano una minaccia imminente per la vita, sono tenuti a darne comunicazione all'autorità competente ad avviare azioni penali. Infine, per i soli prestatori esposti a contenuti terroristici, vige l'obbligo di comunicare all'autorità competente le misure specifiche intraprese per contrastare l'uso improprio dei loro servizi per la diffusione al pubblico di contenuti terroristici.

La terza categoria riguarda gli obblighi imposti ai prestatori esposti a contenuti terroristici di adottare misure specifiche per contrastarne la diffusione al pubblico[5]. Tali ulteriori obblighi trovano la loro giustificazione nei maggiori rischi posti dai servizi offerti da tali prestatori per la disseminazione di contenuti terroristici. In particolare, questi prestatori devono implementare misure volte a contrastare l'uso improprio dei loro servizi per la diffusione al pubblico di contenuti terroristici. Le misure da implementare non sono determinate a priori dal Regolamento, e possono essere liberamente scelte dai prestatori sulla base delle caratteristiche dei propri servizi, tenendo in considerazione il livello di esposizione dei servizi, le capacità tecniche e operative, la solidità

[3] Si veda l'articolo 3 del Regolamento.
[4] Si veda l'articolo 10 del Regolamento.
[5] Si veda l'articolo 5 del Regolamento.

finanziaria, il numero di utilizzatori del prestatore e la quantità di contenuti forniti. Le misure devono inoltre essere implementate nel rispetto dei diritti e degli interessi legittimi degli utilizzatori, in particolare dei diritti fondamentali relativi alla libertà di espressione e di informazione, al rispetto della vita privata e alla protezione dei dati personali.

Nonostante il Regolamento non imponga le misure specifiche da scegliere, sono forniti alcuni esempi di misure considerate idonee per adempiere agli obblighi del Regolamento, la cui adeguatezza deve tuttavia essere sempre accertata sulla base delle circostanze del caso concreto. In particolare, il Regolamento elenca le seguenti misure specifiche[6]: i) adeguate misure o capacità tecniche e operative, quali personale o mezzi tecnici adeguati per individuare e rimuovere rapidamente o disabilitare l'accesso a contenuti terroristici, ii) meccanismi facilmente accessibili e di facile uso per consentire agli utenti di segnalare o indicare al prestatore presunti contenuti terroristici, iii) qualsiasi altro meccanismo per sensibilizzare maggiormente in merito ai contenuti terroristici nei suoi servizi, quali i meccanismi di moderazione per l'utente, iv) qualsiasi altra misura che il prestatore ritenga appropriata per contrastare la disponibilità di contenuti terroristici nei suoi servizi.

Il Regolamento predispone salvaguardie per mitigare i rischi che gli utenti siano sottoposti a decisioni erronee prese interamente da strumenti automatizzati. E' infatti richiesto che, qualora le misure specifiche comportino l'uso di misure tecniche, sono fornite salvaguardie adeguate ed efficaci, in particolare attraverso la sorveglianza e le verifiche umane, per garantire l'accuratezza ed evitare la rimozione di materiale che non sono contenuti terroristici. Inoltre, il Regolamento chiarisce che l'obbligo di adottare misure specifiche non comporta l'obbligo per i prestatori di servizi di hosting di utilizzare strumenti automatizzati.

Inoltre, e sempre in relazione alle misure specifiche da adottare, il Regolamento fa un'importante precisazione: l'obbligo di adottare misure specifiche lascia impregiudicato l'articolo 15, paragrafo 1, della direttiva 2000/31/CE[7] ("Direttiva E-Commerce") e non comporta l'obbligo generale per i prestatori di servizi di hosting di sorvegliare le informazioni che trasmettono o memorizzano, né l'obbligo generale di ricercare attivamente fatti o circostanze che indichino la presenza di attività illecite. Pertanto, i prestatori sono tutelati dal rischio di perdere l'esenzione di responsabilità prevista in via generale per tutti i prestatori di servizi di hosting dalla Direttiva E-Commerce, e permane il divieto per le autorità pubbliche di imporre a tali prestatori una c.d. *general monitoring obligation*.

Si può osservare come l'impostazione degli obblighi del Regolamento sull'adozione di misure specifiche è simile a quella scelta dal legislatore europeo per il *Digital Services Act* ("DSA"), ed in particolare all'articolo 27 di quest'ultimo. Anche il DSA impone obblighi ulteriori e specifici per operatori le cui attività comportano più alti rischi sistemici per la diffusione di contenuto illegale o dannoso, come la disinformazione, ed in particolare per le piattaforme di grandi dimensioni. Anche nel DSA, questi obblighi impongono l'adozione di specifiche misure volte a contrastare l'uso improprio dei servizi delle piattaforme, parimenti lasciando alle piattaforme la scelta sulle misure più appropriate da implementare nel caso concreto, seppur fornendo una lista con esempi di misure che potrebbero essere idonee.

Il Regolamento impone anche degli obblighi di trasparenza per i prestatori, di due tipi. Vi sono obblighi di trasparenza verso gli utenti, che impongono ai

[6] Si veda l'articolo 5, comma 2, del Regolamento.
[7] 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, GUUE L 178 del 17.7.2000.

prestatori di indicare nelle proprie condizioni contrattuali la loro strategia per contrastare la disseminazione di contenuti terroristici, e vi sono obblighi di trasparenza verso l'esterno di pubblicare un resoconto annuale sulle azioni intraprese contro i contenuti terroristici.

Il Regolamento rappresenta un importante passo avanti nella lotta all'utilizzo di internet per finalità terroristiche. Il processo legislativo che ha portato alla sua adozione è stato lungo e travagliato, dopo che molti *stakeholders* hanno espresso preoccupazioni sui rischi che avrebbe comportato per i diritti fondamentali. In particolare, era stato evidenziato il rischio che i prestatori avrebbero dovuto usare strumenti automatizzati per rilevare i contenuti da rimuovere, con l'alto rischio di rimuovere erroneamente contenuti leciti, data l'imprecisione degli strumenti automatizzati nel comprendere il contesto ed il significato di contenuti condivisi online. L'uso di strumenti automatizzati sarebbe stato necessario, per i prestatori, alla luce del poco tempo a disposizione per adempiere agli ordini di rimozione. Inoltre, un altro rischio lamentato riguarda il fatto che gli Stati membri non sono obbligati a coinvolgere le autorità giudiziarie nell'emissione degli ordini di rimozione, così potenzialmente privando gli utenti di adeguate tutele del proprio diritto alla libertà di espressione.

Nel testo finale del Regolamento, queste preoccupazioni sono state in parte accolte, con l'inserimento della precisazione che i prestatori non sono obbligati ad usare strumenti automatizzati, e che opportune verifiche devono essere condotte sul funzionamento di tali strumenti. Tuttavia, non è stata recepita la richiesta di imporre un controllo da parte dell'autorità giudiziaria sull'emissione degli ordini di rimozione.
A tre mesi dalla data in cui il Regolamento ha cominciato a trovare applicazione, resta da vedere se la sua attuazione a livello nazionale comporterà rischi per i diritti fondamentali degli utenti.

Andrea Palumbo

ASSOCIATE

a.palumbo@dejalex.com

+32 (0)26455670

Chaussée de La Hulpe 187
1170 - Bruxelles

MILANO
Via San Paolo, 7 · 20121 Milano, Italia
T. +39 02 72554.1 · F. +39 02 72554.400
milan@dejalex.com

ROMA
Via Vincenzo Bellini, 24 · 00198 Roma, Italia
T. +39 06 809154.1 · F. +39 06 809154.44
rome@dejalex.com

BRUXELLES
Chaussée de La Hulpe 187 · 1170 Bruxelles, Belgique
T. +32 (0)26455670 · F. +32 (0)27420138
brussels@dejalex.com

MOSCOW
Ulitsa Bolshaya Ordynka 37/4 · 119017, Moscow, Russia
T. +7 495 792 54 92 · F. +7 495 792 54 93
moscow@dejalex.com