Il contrasto alla diffusione dei contenuti terroristici *online* a seguito dell'adozione del Digital Services Act: riflessi sulla tutela della libertà di espressione

di Enrico Stella

Abstract: *The fight against the dissemination of terrorist content online after Digital Services Act coming into force: the effects on the protection of freedom of expression* - The following contribution analyses the European Union counter-terrorism legislation that applies to *social media*, focusing on the provisions addressing contents that incite the commission of terrorist offences and their effects on freedom of expression. After reconstructing the shift of the Eu counter-terrorism legislation from an *offline* dimension to a digital approach, the article describes the risks that might be caused by the definition of «public provocation to commit a terrorist offence». Then investigates the main measures provided by the regulation 784/2021 and how the *online* counter-terrorism legislative framework changes after DSA coming into force.

Keywords: Content moderation; Counter-terrorism legislation; DSA; Freedom of expression; Very large online platforms

1. Introduzione

La libertà di espressione è protetta, nell'ambito europeo, dall'art. 10 della Convenzione europea dei diritti dell'uomo (CEDU) e dall'art. 11 della Carta dei diritti fondamentali dell'Unione Europea (cd. Carta di Nizza). In una società democratica che possa qualificarsi come tale, tuttavia, tale diritto non può limitarsi a idee che sono accolte dalla comunità come favorevoli, inoffensive o indifferenti, ma deve includere anche esternazioni che potrebbero eventualmente offendere, sconvolgere o disturbare lo Stato o altro settore della popolazione[1]. Limitazioni alla libertà di espressione, di conseguenza, sono ammesse purché siano rispettate precise condizioni[2].

[1] Corte EDU, *Handyside c. Regno Unito*, 7-12-1976, par. 49.

[2] L'art. 10 CEDU stabilisce che «l'esercizio di [questa] libertà, poiché comporta doveri e responsabilità, può essere sottoposto alle formalità, condizioni, restrizioni o sanzioni che sono previste dalla legge e che costituiscono misure necessarie, in una società democratica, alla sicurezza nazionale, all'integrità territoriale o alla pubblica sicurezza, alla difesa dell'ordine e alla prevenzione dei reati, alla protezione della salute o della morale, alla protezione della reputazione o dei diritti altrui, per impedire la divulgazione di informazioni riservate o per garantire l'autorità e l'imparzialità del potere giudiziario». Relativamente al diritto dell'Unione, invece, l'art. 52 della Carta di Nizza prevede che «eventuali limitazioni all'esercizio dei diritti e delle libertà riconosciuti

DPCE online
ISSN: 2037-6677

Le misure legislative antiterrorismo dell'Unione rappresentano un chiaro esempio di risposta normativa che può essere opposta, per evidenti motivi di sicurezza, alla libertà in questione.

In tale ambito, la costante necessità di bilanciare la prima con quest'ultima, tuttavia, è resa più problematica in quanto la diffusione di contenuti terroristici, specialmente su *Internet* ed in particolare nel cd. *surface web*[3], siano essi messaggi, video o audio, è particolarmente pericolosa in quanto idonea a contribuire al fenomeno della radicalizzazione[4], incentivando, così, la commissione di reati terroristici[5] da parte sia di gruppi terroristici organizzati che dei cd. lupi solitari.

Con il progredire della tecnologia, soprattutto nell'ambito delle forme di comunicazione digitali, il legislatore europeo ha scelto di adattare la propria legislazione antiterrorismo provando a governare, sia con atti di *hard law* che di *soft law*, anche i canali di informazioni più "ontologicamente" difficili da normare: i *social media*[6].

Al riguardo va rilevato che il legislatore europeo, nei vari atti normativi relativi alla comunicazione digitale, non ha mai definito concetti, pur di uso comune, quali *social media* o *social networks*. In particolare, la normativa adottata ha avuto ad oggetto, almeno in un momento iniziale, i servizi della società dell'informazione offerti da un prestatore, piuttosto che quest'ultimo.

Nella prima normativa recante un regime di responsabilità per detti *providers*, la direttiva 2000/31/CE[7] (cd. direttiva sul commercio elettronico), infatti, si fa riferimento al «prestatore» solo in quanto «persona fisica o giuridica che presta un servizio della società dell'informazione» (art. 2 lett. b) (d'ora in poi prestatore di servizi). Quanto a tale servizio, esso è inteso nella disciplina in parola come qualsiasi servizio prestato normalmente dietro retribuzione, a distanza, per via elettronica e a richiesta individuale di un destinatario di servizi (art. 2 lett. a). E la stessa suddivisione che l'atto giuridico in parola compie tra i prestatori è operata unicamente in base alla tipologia di servizi che questi ultimi offrono. Esso distingue, in proposito, tra servizi di cd. *mere conduit*, *caching* e *hosting*[8].

dalla Carta devono essere previste dalla legge e rispettare il contenuto essenziale di detti diritti e libertà. Nel rispetto del principio di proporzionalità, possono essere apportate limitazioni solo laddove siano necessarie e rispondano effettivamente a finalità di interesse generale riconosciute dall'Unione o all'esigenza di proteggere i diritti e le libertà altrui».

[3] Da contrapporre al *dark web* inteso come spazio *online* non accessibile con gli ordinari motori di ricerca.

[4] Sulla definizione del concetto di "radicalizzazione" si veda C. Graziani, *Terrorismo internazionale, radicalizzazione e tecnologia*, in *Federalismi.it*, 2023, 12, 57-66.

[5] Reg. UE n. 784/2021 del P.E. e del Cons. del 29-4-2021 relativo al contrasto della diffusione di contenuti terroristici *online*, considerando 5.

[6] Sul concetto di *social media* o *social network* si veda S. Braschi, *Social media e responsabilità penale dell'Internet Service Provider*, in *Medialaws.eu*, 2020, 3, 161-162.

[7] Direttiva 2000/31/CE del P.E. e del Cons. dell'8-6-2000 relativa a taluni aspetti giuridici dei servizi della società dell'informazione, in particolare il commercio elettronico, nel mercato interno.

[8] I primi consistono nel «trasmettere, su una rete di comunicazione, informazioni fornite da un destinatario del servizio, o nel fornire un accesso alla rete di comunicazione» (art. 12). I secondi nel «trasmettere, su una rete di comunicazione, informazioni fornite da

Ai sensi della citata direttiva i *social media* rientrano nella categoria degli *hosting providers* in quanto prestano un servizio della società dell'informazione consistente nella memorizzazione di informazioni fornite da un loro destinatario del servizio[9], altresì, e più semplicemente, noto come «utente».

Solo con il regolamento sui servizi digitali 2022/2065 (d'ora in avanti DSA)[10] – il quale ha modificato la direttiva sul commercio elettronico e ripreso, ampliandola, la classificazione dei prestatori di servizi – il legislatore europeo si è focalizzato maggiormente su questi ultimi, enucleando definizioni normative, quali «piattaforme *online* di dimensioni molto grandi», che risultano maggiormente rispondenti ai caratteri dei cd. *social networks*.

Sin d'ora si rileva che, ai sensi del DSA, per piattaforme *online* di dimensioni molto grandi si intendono le piattaforme *online*[11] che hanno un numero medio mensile di destinatari attivi del servizio nell'Unione pari o superiore a 45 milioni, e che sono designate come tali dalla Commissione (art. 33 par.1).

Il DSA, è utile sottolineare preliminarmente, prevede un regime di responsabilità per tutti i prestatori di servizi basato su cerchi concentrici, secondo il quale gli obblighi previsti per i prestatori più grandi si aggiungono a quelli previsti per i prestatori più piccoli. Secondo un ordine di grandezza crescente, le figure di prestatori di servizi disciplinate dal DSA sono: *mere conduit providers*, *caching providers*, *hosting providers*, le piattaforme *online*, le piattaforme *online* di dimensioni molto grandi ed i motori di ricerca di dimensioni molto grandi[12]. Ai fini che qui rilevano, quindi, le piattaforme *online* di dimensioni molto grandi soggiacciono, oltre agli obblighi specificamente previsti per esse, anche a quelli previsti per gli *hosting providers*.

L'Unione Europea, nell'adeguare la sua legislazione antiterrorismo

un destinatario del servizio [che prevedano una] memorizzazione automatica, intermedia e temporanea di tali informazioni effettuata al solo scopo di rendere più efficace il successivo inoltro ad altri destinatari a loro richiesta» (art. 13). Gli ultimi nella «memorizzazione di informazioni fornite da un destinatario del servizio» (art. 14).

[9] Definito come «la persona fisica o giuridica che, a scopi professionali e non, utilizza un servizio della società dell'informazione, in particolare per ricercare o rendere accessibili delle informazioni» (art. 2 lett. b).

[10] Reg. UE n. 2065/2022 del P.E. e del Cons. del 19-10-2022 relativo a un mercato unico dei servizi digitali e che modifica la direttiva 2000/31/CE (regolamento sui servizi digitali). Sulle principali novità introdotte dal regolamento si veda L. Bolognini, E. Pelino, M. Scialdone (cur.), *Digital Services Act e Digital Markets Act. Definizioni e prime applicazioni dei nuovi regolamenti europei*, Milano, 2023, 3-234.

[11] Ai sensi dell'art. 3 lett. i) del DSA è considerato come piattaforma *online* «un servizio di memorizzazione di informazioni che, su richiesta di un destinatario del servizio, memorizza e diffonde informazioni al pubblico, tranne qualora tale attività sia una funzione minore e puramente accessoria di un altro servizio o funzionalità minore del servizio principale e, per ragioni oggettive e tecniche, non possa essere utilizzata senza tale altro servizio e a condizione che l'integrazione di tale funzione o funzionalità nell'altro servizio non sia un mezzo per eludere l'applicabilità del presente regolamento».

[12] Ai fini dell'economia dello scritto, non ci si soffermerà sulla nozione di motore di ricerca *online* né sull'analisi delle disposizioni riguardanti i prestatori di servizi che non siano *hosting providers* e piattaforme *online* di dimensioni molto grandi.

DPCE online
ISSN: 2037-6677

alle comunicazioni che avvengono sui *social media*, ha incluso, tra l'altro, norme atte a contrastare l'uso criminale di tali piattaforme consistente nella diffusione, da parte dei loro utenti, di contenuti terroristici. Tali disposizioni, in particolare, danno una definizione di questi ultimi e stabiliscono i comportamenti che i suddetti *providers* devono tenere in loro presenza.

L'attività di regolamentazione in questione, tuttavia, risulta alquanto complicata.

Tali giganti del *web*, infatti, nonostante facilitino il dibattito pubblico con la diffusione di idee, opinioni e informazioni fattuali che ospitano[13], e seppur, per questo, strumentali all'adeguata manifestazione del pensiero in un'epoca dove il dibattito civico si esprime prevalentemente *online*[14], rimangono, tuttavia, società private. E, in quanto tali, stipulano contratti, di natura prettamente privatistica, con i loro utenti, in cui, tra le relative clausole, modificabili unilateralmente, rientrano le regole comportamentali che questi ultimi si impegnano a rispettare (i cd. *community standards*)[15].

Nella moderazione dei contenuti generati dai loro utenti, dunque, i *social networks* seguono sia le norme previste, tra l'altro, dall'Unione Europea sia le regole di condotta da essi stessi predisposte.

La moderazione dei contenuti è definita dal DSA, in particolare, come «le attività, automatizzate o meno, svolte dai prestatori di servizi intermediari con il fine, in particolare, di individuare, identificare e contrastare contenuti illegali e informazioni incompatibili con le condizioni generali, forniti dai destinatari del servizio, comprese le misure adottate che incidono sulla disponibilità, sulla visibilità e sull'accessibilità di tali contenuti illegali o informazioni, quali la loro retrocessione, demonetizzazione o rimozione o la disabilitazione dell'accesso agli stessi, o che incidono sulla capacità dei destinatari del servizio di fornire tali informazioni, quali la cessazione o la sospensione dell'account di un destinatario del servizio» (art. 3 lett. t).

Nel presente lavoro, effettuata una breve ricostruzione dell'azione dell'Unione nella lotta alle attività terroristiche e dell'evoluzione determinatasi, in particolare, per contrastare il fenomeno del terrorismo *online*, ci si soffermerà su taluni aspetti di questa disciplina potenzialmente idonei a produrre riflessi sulla libertà di espressione. Libertà, quest'ultima, necessaria affinché la democrazia europea possa prosperare[16].

Segnatamente, sarà considerato, in particolare, il reato di pubblica provocazione di cui alla direttiva (UE) 2017/541 sulla lotta contro il terrorismo, dato, a nostro avviso, il suo potenziale e rilevante impatto sulla libertà di espressione. Verranno in linea di conto, successivamente, le normative relative alla responsabilità degli *hosting providers* e, infine, tra gli

[13] Reg. UE n. 784/2021 cit., considerando 5.
[14] Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni sul piano d'azione per la democrazia europea, COM(2020) 790 final, 2.
[15] Tale formula, pur coniata unicamente per le norme comportamentali di *Facebook*, viene usata, spesso, per indicare le regole di condotta previste da tutti *social media*, a mo' di sineddoche, sia perché il *social network* in questione è stato il primo creato al mondo, sia perché restituisce meglio l'idea di *social media* come comunità.
[16] Comunicazione della Commissione sul piano d'azione per la democrazia europea, cit., 1.

obblighi in materia di diligenza dei prestatori di servizi stabiliti dal DSA, le previsioni sulle condizioni generali per l'uso di tali servizi.

2. La legislazione antiterrorismo dell'Unione Europea e la sua evoluzione nell'era digitale: profili generali

Volendo operare una breve ricostruzione della legislazione adottata dall'Unione per contrastare il terrorismo, si deve necessariamente partire dal primo atto normativo in materia, e cioè la decisione quadro 2002/475/GAI sulla lotta al terrorismo[17]. Tale atto, emanato a seguito dell'attentato dell'11 settembre 2001, muovendo dalla considerazione che «il terrorismo costituisce una delle più gravi violazioni» dei principi «della democrazia [e dello] stato di diritto», i quali «sono patrimonio comune degli Stati membri» (considerando 1 e 2), si prefiggeva di ravvicinare la definizione dei reati terroristici negli Stati membri (considerando 6).

La disciplina sulla lotta contro il terrorismo introdotta dalla decisione quadro 2002/475/GAI è stata modificata dal legislatore europeo con la decisione quadro 2008/919/GAI[18]. Il nuovo intervento normativo riveste particolare rilevanza in quanto, differentemente da quello del 2002, evidenzia il ruolo che la tecnologia, ed in particolare l'uso di *Internet*, comincia a svolgere all'interno di tale contesto criminale (considerando 3, 4 e 8). Esso inserisce tra i reati connessi ad attività terroristiche la «pubblica provocazione per commettere reati di terrorismo» (art. 3 par. 1 lett. a). Inoltre, stabilisce una specifica previsione, nell'art. 2, concernente la delicata questione della possibile lesione dei principi fondamentali relativi alla libertà di espressione, chiarendo che la decisione quadro non ha l'effetto di imporre agli Stati membri di adottare misure che siano in contrasto con detti principi.

Il punto di svolta nella politica antiterrorismo dell'Unione, a partire dal quale i *social networks* incominciano a rivestire un ruolo fondamentale, tuttavia, si registra successivamente all'attentato terroristico avvenuto il 7 gennaio 2015 a Parigi contro la sede del giornale satirico "Charlie Hebdo". A seguito di tale attacco, infatti, il Parlamento europeo ha votato una risoluzione[19] in cui, preso atto che la diffusione della propaganda terroristica è facilitata dall'uso di *Internet* e dei *social media*, si è rivolto direttamente alle imprese operanti in tali settori chiedendo loro di cooperare con i governi, le autorità preposte all'applicazione della legge e la società civile per combattere il fenomeno terroristico, garantendo però, nel contempo, il rispetto in ogni circostanza della libertà di espressione e della tutela della vita privata[20].

La Commissione, successivamente, ha adottato un'agenda europea sulla sicurezza[21] in cui, fra l'altro, ha previsto il lancio di un *forum* a livello

[17] Decisione quadro del Cons. del 13-6-2002 sulla lotta contro il terrorismo (2002/475/GAI).
[18] Decisione quadro 2008/919/GAI del Cons. del 28-11-2008 che modifica la decisione quadro 2002/475/GAI sulla lotta contro il terrorismo.
[19] Risoluzione del P.E. dell'11-2-2015 sulle misure antiterrorismo (2015/2530(RSP)).
[20] Considerando lett. f) e art. 20.
[21] Commissione europea, *Agenda europea sulla sicurezza*, COM(2015) 185 final.

DPCE online
ISSN: 2037-6677

dell'UE, l'*European Union Internet Forum* (EUIF)[22]. L'EUIF, che vede coinvolte le società informatiche, le autorità di contrasto e la società civile, è finalizzato a sviluppare i migliori strumenti per contrastare la propaganda terroristica su *Internet* e sui *social media* e, in generale, l'uso improprio del *web* per fini terroristici, riducendo, in particolare, l'accessibilità ai contenuti terroristici e «increasing the volume of effective alternative narratives *online*»[23]. Tale *Forum*, oltre che aver instaurato un partenariato pubblico-privato che caratterizza il nuovo *modus operandi* di regolazione del *public speech*[24], è stato coinvolto nella creazione dell'unità addetta alle segnalazioni su *Internet* di Europol (EU IRU) volta a combattere la propaganda terroristica e le relative attività violente sulla rete[25].

Nel 2016, nuovamente in risposta ad un attentato terroristico avvenuto nel territorio europeo, questa volta a Bruxelles, l'Unione decide di adottare il Codice di condotta per lottare contro le forme illegali di incitamento all'odio *online* (di seguito, il Codice)[26]. In tale atto, seppur di *soft law*, le aziende informatiche aderenti[27] si impegnano a contrastare l'incitamento illegale all'odio *online*. Quest'ultimo viene descritto – conformemente alla decisione quadro 2008/913/GAI del 28 novembre 2008 sulla lotta contro talune forme ed espressioni di razzismo e xenofobia mediante il diritto penale (cd. *hate speech*)[28] – come «ogni comportamento consistente nell'istigazione pubblica alla violenza o all'odio nei confronti di un gruppo di persone, o di un suo membro, definito in riferimento alla razza, al colore, alla religione, all'ascendenza o all'origine nazionale o etnica».

Tale condotta criminosa è considerata dalle istituzioni europee strettamente legata alla diffusione di contenuti terroristici[29] in quanto questi ultimi presuppongono, e comunque fanno riferimento, a sentimenti di odio nei confronti di altri soggetti, prevalentemente, ma non unicamente, per motivi religiosi.

[22] Commissione europea, comunicato stampa, 3-12-2015 IP/15/6243.
[23] Cfr. Commissione europea, *Agenda europea sulla sicurezza*, cit., 15 e la *homepage* del *Forum* consultabile sul sito https://home-affairs.ec.europa.eu/networks/european-union-internet-forum-euif_en.
[24] Sui tratti essenziali di tale cambio di paradigma cfr. J. Balkin, *Old-school/new-school speech regulation*, in 127 *Harward Law review*, 2299 (2014).
[25] La *mission* di tale unità è consultabile al sito https://www.europol.europa.eu/media-press/newsroom/news/europol%e2%80%99s-internet-referral-unit-to-combat-terrorist-and-violent-extremist-propaganda.
[26] Il testo del Codice è visionabile al sito https://ec.europa.eu/newsroom/document.cfm?doc_id=42861.
[27] Le prime aziende aderenti, alle quali ne sono seguite altre, sono state Facebook, Microsoft Twitter e YouTube.
[28] Decisione quadro 2008/913/GAI del Cons. del 28-11-2008 sulla lotta contro talune forme ed espressioni di razzismo e xenofobia mediante il diritto penale.
[29] Si veda in proposto la Dichiarazione comune dei ministri della giustizia e degli interni dell'UE e dei rappresentanti delle istituzioni dell'UE sugli attentati terroristici di Bruxelles del 22 marzo 2016, ad evidenziare la volontà della Commissione di intensificare «i lavori presso le aziende informatiche, specie in sede di *Forum* dell'UE su *Internet*, per contrastare la propaganda terroristica e sviluppare, entro giugno 2016, un codice di condotta contro l'incitamento all'odio *online*». La Dichiarazione è consultabile al sito https://www.consilium.europa.eu/it/press/press-releases/2016/03/24/statement-on-terrorist-attacks-in-brussels-on-22-march/pdf/.

Tra le prescrizioni previste dal Codice, e successivamente riprese dal legislatore europeo[30], spicca, in particolare, il cd. meccanismo di *notice and take down*, in base al quale un utente della piattaforma può segnalare a quest'ultima la presenza di contenuti illegali postati da altri utenti.

Nel 2017 l'Unione è intervenuta nuovamente sulla legislazione antiterrorismo, con la direttiva (UE) 2017/541 sulla lotta contro il terrorismo[31] (d'ora in avanti, la direttiva 2017/541), ritenendo opportuno che la definizione dei reati considerati[32], ed in particolare dei «reati di terrorismo»[33], fosse oggetto di un'ulteriore armonizzazione e che le condotte incriminate fossero rese punibili anche se commesse attraverso l'uso di *Internet* e dei *social networks* (considerando 6).

Particolare rilevanza riveste, ai fini della nostra analisi, il reato di «pubblica provocazione per commettere reati di terrorismo», il quale, previsto all'art. 5 della direttiva, rientra tra i «reati connessi ad attività terroristiche» elencati nel Titolo III. In tale definizione, è importante notare, diversamente da quella prevista dalla decisione quadro del 2008/919/GAI,

[30] Tale meccanismo è stato previsto dal legislatore europeo, ai fini che qui rilevano, all'art. 16 del DSA e all'art. 5 del regolamento (UE) n. 784/2021.

[31] Direttiva (UE) 521/2017 del P.E. e del Cons. del 15-3-2017 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. Sulla direttiva 2017/541, cfr. G. De Minico, *La risposta europea al terrorismo del tempo ordinario: il lawmaker e il giudice*, in *Osservatorio sulle fonti*, 2017, 2; S. De Luca, *La direttiva 2017/541/UE e il difficile bilanciamento tra esigenze di pubblica sicurezza e rispetto dei diritti umani*, in *Eurojus*, 3 luglio 2017; V. Sachetti, *Il contrasto alla propaganda terroristica online nell'ambito dell'Unione europea: tutela attuale e prospettive future*, in *Eurojus*, 2019, 4.

[32] La direttiva contempla, oltre ai reati di seguito menzionati nel testo, i «Reati riconducibili a un gruppo terroristico» (Titolo II) ed i «Reati connessi ad attività terroristiche» (Titolo III).

[33] Si tratta dei seguenti reati: a) attentati alla vita di una persona che possono causarne il decesso; b) attentati all'integrità fisica di una persona; c) sequestro di persona o cattura di ostaggi; d) distruzioni di vasta portata di strutture governative o pubbliche, sistemi di trasporto, infrastrutture, compresi i sistemi informatici, piattaforme fisse situate sulla piattaforma continentale ovvero di luoghi pubblici o di proprietà private che possono mettere in pericolo vite umane o causare perdite economiche considerevoli; e) sequestro di aeromobili o navi o di altri mezzi di trasporto collettivo di passeggeri o di trasporto di merci; f) fabbricazione, detenzione, acquisto, trasporto, fornitura o uso di esplosivi o armi da fuoco, comprese armi chimiche, biologiche, radiologiche o nucleari, nonché ricerca e sviluppo di armi chimiche, biologiche, radiologiche o nucleari; g) rilascio di sostanze pericolose o il cagionare incendi, inondazioni o esplosioni i cui effetti mettano in pericolo vite umane; h) manomissione o interruzione della fornitura di acqua, energia o altre risorse naturali fondamentali il cui effetto metta in pericolo vite umane; i) interferenza illecita relativamente ai sistemi, ai sensi dell'articolo 4 della direttiva 2013/40/UE del Parlamento e del Consiglio nei casi in cui si applica l'articolo 9, paragrafo 3 o l'articolo 9, paragrafo 4, lettere b) o c), di tale direttiva in questione e interferenza illecita relativamente ai dati, di cui all'articolo 5 di tale direttiva nei casi in cui si applica l'articolo 9, paragrafo 4, lettera c), di tale direttiva; j) minaccia di commettere uno degli atti elencati alle lettere da a) a i) (art. 3, par. 1). Ciò quando hanno lo scopo di: a) intimidire gravemente la popolazione; b) costringere indebitamente i poteri pubblici o un'organizzazione internazionale a compiere o astenersi dal compiere un qualsiasi atto; c) destabilizzare gravemente o distruggere le strutture politiche, costituzionali, economiche o sociali fondamentali di un paese o di un'organizzazione internazionale (art. 3, par. 2).

DPCE online
ISSN: 2037-6677

si fa esplicito riferimento al compimento di tale reato non solo *offline*, ma anche *online*.

In particolare, viene considerata «pubblica provocazione per commettere reati di terrorismo», se compiuta intenzionalmente, «la diffusione o qualunque altra forma di pubblica divulgazione di un messaggio, con qualsiasi mezzo, sia *online* che *offline*, con l'intento di istigare la commissione di uno dei reati di terrorismo previsti all'articolo 3, paragrafo 1, lettere da a) a i), se tale comportamento, direttamente o indirettamente, ad esempio mediante l'apologia di atti terroristici, promuove il compimento di reati di terrorismo, creando in tal modo il pericolo che uno o più di tali reati possano essere commessi» (articolo 5).

Inoltre, nella motivazione della direttiva, tra i reati riconducibili alla pubblica provocazione si fa riferimento, tra gli altri, all'apologia e alla giustificazione del terrorismo o alla diffusione *online* e *offline* di messaggi o immagini, incluse quelle riguardanti le vittime del terrorismo, quale mezzo per raccogliere sostegno alle cause dei terroristi o intimidire gravemente la popolazione. E si precisa che, relativamente al rischio che possano essere commessi reati di terrorismo, devono essere esaminate, per ogni caso concreto, le specifiche circostanze di quest'ultimo (autore, destinatario e contesto), oltre che l'entità e la natura di siffatto pericolo (considerando 10). Inoltre, si chiarisce che la direttiva non dovrebbe in alcun modo essere interpretata come volta a limitare od ostacolare la diffusione di informazione a fini scientifici, accademici o di comunicazione e che l'espressione nel dibattito pubblico di opinioni radicali, polemiche o controverse in merito a questioni politiche sensibili non rientra nella definizione di pubblica provocazione per commettere reati di terrorismo (considerando 40).

La punibilità di questa condotta criminosa, come evidenziato dalla motivazione dell'atto normativo, costituisce un pilastro della politica legislativa antiterrorismo dell'Unione, soprattutto in ambito digitale. Un mezzo efficace per combattere il terrorismo sul *web*, infatti, consiste nel rimuovere alla fonte i contenuti *online* che costituiscono una pubblica provocazione per commettere un reato di terrorismo (considerando 22). E, a tal fine, è previsto che gli Stati membri adottino le misure che ritengono necessarie per assicurare la tempestiva rimozione dei contenuti *online* ospitati nel loro territorio che costituiscono una pubblica provocazione o, qualora ciò non fosse possibile, per bloccarne l'accesso (articolo 21).

Riguardo al reato di pubblica provocazione, tuttavia, va segnalato che esso è stato oggetto di considerazione nella relazione sull'impatto della direttiva 2017/541 sui diritti e sulle libertà fondamentali effettuata, su richiesta della Commissione, dall'Agenzia dell'Unione Europea per i diritti fondamentali (FRA)[34]. La relazione – le posizioni espresse nella quale riteniamo condivisibili - si sofferma, tra l'altro, su due aspetti critici di tale reato: il confine fra condotta criminale e libertà di espressione e l'individuazione dei due elementi necessari affinché la provocazione possa

[34] Agenzia dell'Unione Europea per i diritti fondamentali (FRA), *Directive (EU) 2017/541 on Combating Terrorism. Impact on Fundamental Rights and Freedoms Report*, 2021. La relazione è visionabile al seguente *link*: https://fra.europa.eu/sites/default/files/fra_uploads/fra-2021-directive-combating-terrorism_en.pdf.

determinarsi, ovvero l'intenzionalità di istigare un reato di terrorismo e il pericolo che questo possa essere commesso.

Relativamente al primo punto, la FRA, richiamando la giurisprudenza della Corte Europea dei Diritti dell'Uomo (CEDU), pur ricordando che la lotta al terrorismo costituisce una legittima limitazione alla libertà di espressione[35], sottolinea la difficoltà di delineare un chiaro confine tra quest'ultima e la pubblica provocazione[36]. L'Agenzia, inoltre, ricorda che, diversamente dalla formulazione prevista all'art. 5 della direttiva del 2017, il Relatore speciale delle Nazioni Unite, nella sua relazione sulle migliori pratiche per contrastare il terrorismo[37], aveva consigliato di sostituire riferimenti alla «direct or indirect provocation» con la formula «whether or not advocating terrorist offences»[38].

Per quanto riguarda l'intenzionalità, la FRA rileva che la mancanza di criteri specifici e pratiche armonizzate per determinare la suddetta volontà non può che lasciare un certo margine di discrezionalità in capo al giudice. Inoltre, a supporto della difficoltà di inquadrare l'intenzionalità di istigare la commissione di un reato di terrorismo dietro ogni messaggio di provocazione, il *report* menziona, a fini esemplificativi, quanto verificatosi in Francia. In proposito si rileva che nel 2019, e quindi tre anni dopo l'emanazione della direttiva, il 10% delle persone condannate per apologia di terrorismo – il 37% delle quali avevano espresso tali considerazioni *online* – era minorenne, e dunque con la possibilità di non essere pienamente consapevole delle proprie azioni[39].

Relativamente all'elemento del rischio, invece, la relazione sottolinea la possibilità che, per individuarne la presenza, gli organi giudicanti possano far ricorso all'influenza di colui che comunica il messaggio, disponendo, così, di un'arbitrarietà eccessiva[40].

Sul tema della rimozione dei contenuti *online* che costituiscano una pubblica provocazione per commettere reati di terrorismo è peraltro intervenuto il Consiglio europeo del 22-23 giugno 2017 il quale, nelle sue conclusioni, ha affermato che «anche il settore privato deve fare la sua parte per contribuire a combattere il terrorismo e la criminalità *online*. Prendendo le mosse dai lavori del *Forum* dell'Ue su *Internet*, [ci] si attende che le imprese del settore [...] sviluppino nuove tecnologie e nuovi strumenti al fine di migliorare la rilevazione automatica e la rimozione dei contenuti che incitano a compiere atti terroristici. Se necessario si dovrebbero completare tali iniziative con le pertinenti misure legislative a livello dell'Ue»[41].

---

[35] In proposito nella relazione si richiama la sentenza della Corte EDU, no. 36109/03, *Leroy v. France*, 2-10-2008, p.to 36.

[36] Tale rilievo si basa sulla *Guide on Article 10 of the European Convention on Human Rights. Freedom of expression* della Corte EDU del 31 agosto 2020 consultabile sul sito https://www.refworld.org/jurisprudence/caselawcomp/echr/2020/en/123515.

[37] Consiglio per i diritti umani delle Nazioni Unite, *Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Martin Scheinin*, A/HRC/16/51, 22-12-2010, 15-16.

[38] FRA, *Directive (EU) 2017/541*, cit., 52.

[39] *Ivi*, 57-58.

[40] *Ivi*, 60.

[41] Conclusioni del Cons. del 22/23-06-2017, https://www.consilium.europa.eu/media/23973/22-23-euco-final-conclusions-it.pdf.

DPCE online
ISSN: 2037-6677

Tali istanze hanno trovato riscontro nella Comunicazione della Commissione «Lotta ai contenuti illeciti *online*. Verso una maggiore responsabilizzazione delle piattaforme *online*»[42], alla quale è stata data applicazione con la Raccomandazione (UE) 2018/334 sulle misure per contrastare efficacemente i contenuti illegali *online*[43].

Nella Comunicazione anzidetta, la Commissione ha affermato la responsabilità gravante sulle piattaforme *online* di proteggere i loro utenti dalla possibilità che i servizi da esse offerti siano sfruttati da criminali e soggetti coinvolti in attività illegali e quindi di individuare, bloccare o rimuovere contenuti illeciti. Ha evidenziato, altresì, che la lotta contro tali contenuti va condotta assicurando la garanzia dei diritti fondamentali. In particolare, in considerazione del ruolo che le piattaforme rivestono per l'accesso alle informazioni, va evitata la rimozione dei contenuti leciti (cd. rimozione abusiva), la quale incide sulla libertà di espressione e sul pluralismo dei mezzi di comunicazione di massa[44].

Quanto alla raccomandazione 2018/334, va evidenziato che essa distingue tra raccomandazioni generali relative al contrasto di tutti i tipi di contenuti illegali (Capo II) e raccomandazioni specifiche relative a quelli terroristici (Capo III). Tale distinzione denota la consapevolezza del rilievo assunto da *Internet* nell'esercizio delle attività terroristiche e della necessità di una risposta più rapida ed efficace ai contenuti terroristici *online*, oltre all'esigenza che i prestatori di servizi di *hosting* aderenti al *Forum* dell'UE su *Internet* si attengano agli impegni assunti (considerando 31).

Le esigenze anzidette trovano un più incisivo riscontro nel regolamento (UE) 784/2021 relativo al contrasto della diffusione dei contenuti terroristici *online* (d'ora in avanti, il regolamento 784/2021)[45]. Nella motivazione di questo, rilevato che gli sforzi volti a contrastare tali contenuti sono stati avviati a livello dell'Unione dal 2015, nel quadro di una cooperazione volontaria tra Stati membri e *hosting providers*, si afferma che questi sforzi devono essere integrati da un quadro legislativo chiaro che possa contribuire a ridurre ulteriormente l'accessibilità a tali contenuti illegali (considerando 6).

Il regolamento, di conseguenza, stabilisce regole uniformi per contrastare la diffusione di contenuti terroristici ospitati sui servizi offerti dagli *hosting providers*, in particolare: obblighi che tali prestatori sono tenuti ad applicare nella moderazione di detti contenuti garantendone, eventualmente, la rimozione o la disabilitazione dell'accesso; misure che gli Stati sono tenuti ad adottare per individuare e assicurare la rapida rimozione dei contenuti e facilitare la cooperazione tra i vari attori coinvolti, quali le autorità nazionali dei Paesi membri, i prestatori di servizi interessati ed

[42] Comunicazione della commissione al P.E., al Cons., al Comitato economico e sociale europeo e al Comitato delle regioni, *Lotta ai contenuti illeciti online. Verso una maggiore responsabilizzazione delle piattaforme online*, COM (2017)555 final.
[43] Raccomandazione (UE) 2018/334 della Commissione dell'1-3-2018 sulle misure per contrastare efficacemente i contenuti illegali *online*.
[44] Comunicazione della Commissione lotta ai contenuti illeciti *online*, cit., 2-7.
[45] Reg. UE n. 784/2021 del P.E. e del Cons. del 29-4-2021, relativo al contrasto della diffusione di contenuti terroristici *online*. Sul regolamento (UE) n. 784/2021 si veda V. Mitsilegas e C. Salvi, *Digital Exceptionalism, Freedom of Expression and the Rule of Law: The Case of Targeting Terrorist Content Online*, in *Eurojus*, 2024, 2, 189-191.

Europol (art. 1 par. 1).

La normativa in questione, nella definizione di contenuti terroristici, include, tra gli altri, i «materiali che istigano alla commissione di uno dei reati di cui all'art. 3 par. 1, lettere da a) a i) della direttiva (UE) 2017/541, se tali materiali, direttamente o indirettamente, ad esempio mediante l'apologia di atti terroristici, incitano a compiere reati di terrorismo, generando in tal modo il pericolo che uno o più di questi crimini siano commessi» (art. 2 par. 7 lett. a).

Come si può notare, il regolamento 782/2021, nell'includere tra tali contenuti illegali anche quelli istigatori, riprende, quasi integralmente, la definizione di «pubblica provocazione per commettere reati di terrorismo» prevista dall'art. 5 della direttiva 2017/541[46]. In tal modo, dunque, persistono, anche a seguito del regolamento del 2021, le summenzionate criticità rilevate dalla relazione della FRA.

Nel contesto sin qui delineato si inserisce il regolamento sui servizi digitali. Il DSA, seppur di carattere orizzontale e non settoriale, riveste particolare rilevanza ai nostri fini in quanto, tra l'altro, introduce un quadro di responsabilità dei prestatori di servizi per le informazioni illegali ospitate. Inoltre, prevede procedure armonizzate in materia di ordini, emessi dalle autorità degli Stati membri, volti a rimuovere i contenuti illegali o a disabilitarne l'accesso. Regola la procedura di *notice and take down*, volta a segnalare la presenza di contenuti illeciti, già introdotta, come si è detto, dal Codice e pure prevista, come si vedrà, dal regolamento 784/2021. Infine, detta disposizioni relativamente alle condizioni generali predisposte dai prestatori di servizi.

Dal quadro sin qui tracciato, ci sembra emergere innanzitutto – come denota la disciplina della decisione quadro 2002/475/GAI – la consapevolezza del legislatore dell'Unione Europea della necessità di combattere il terrorismo. Inoltre, che l'azione dell'Unione subisce un'evoluzione correlativamente alle modalità di esercizio dell'azione terroristica. Da qui il richiamo specifico nella decisione quadro 2008/919/GAI, sia pure solo nella motivazione del provvedimento, all'uso di *Internet* a fini terroristici; il divieto della pubblica provocazione sia *offline* che *online* nella direttiva 2017/541, infine la previsione, con il regolamento 784/2021, di una disciplina specifica sul contrasto dei contenuti terroristici *online*.

Un altro aspetto che risulta emergere è il ruolo che viene riconosciuto ai privati in ordine all'impegno a contrastare la diffusione di contenuti terroristici e la loro rimozione. Ciò dapprima negli atti di *soft law* – quali la risoluzione del Parlamento europeo del 2015, il Codice di condotta e le conclusioni del Consiglio europeo del 2017 – e successivamente negli atti di carattere vincolante, come il regolamento 784/2021. Tendenza che, come si vedrà[47], trova un ulteriore sviluppo nella disciplina prevista dal DSA.

[46] Non c'è un richiamo testuale all'art. 5 della direttiva 2017/541 perchè quest'ultimo fa riferimento alla «diffusione di un messaggio […] sia *online* che *offline*», esplicitazione inutile nel quadro previsto dal regolamento del 2021 che, infatti, si occupa della diffusione dei contenuti terroristici effettuata unicamente *online*. Tuttavia, da un confronto delle disposizioni stabilite dalle due norme emerge la sostanziale sovrapponibilità dell'art. 2 par. 7 lett. a) del regolamento con l'art. 5 della direttiva.

[47] Cfr. *infra* par. 4.

DPCE online
ISSN: 2037-6677

Quanto alla libertà di espressione, fatto salvo quanto già detto in ordine alla disposizione contenuta nell'art. 2 della decisione quadro 2008/919/GAI, un esplicito riferimento alla tutela di tale diritto è contenuto nella motivazione di tutti gli atti normativi considerati[48].

E una puntuale previsione sul punto è stabilita dal regolamento 784/2021 all'art. 1 par. 4. In questa disposizione si statuisce che la normativa in parola non ha l'effetto di modificare l'obbligo di rispettare i diritti sanciti dalla Carta, facendo esplicito e chiaro riferimento, tra questi, al diritto alla libertà di espressione. Ciò evidenzia il rilievo del rispetto di questo diritto – di cui, nella motivazione, si sottolinea la fondamentale importanza in una società aperta e democratica (considerando 5) – anche quando si tratti di contrastare il fenomeno terroristico.

3. La responsabilità degli hosting providers: la disciplina del Regolamento (UE) 2065/2022 relativo a un mercato unico dei servizi digitali

Passando a considerare il quadro giuridico relativo alla responsabilità dei prestatori di servizi, al riguardo sono previsti, in particolare, due regimi.

Il primo, di natura settoriale, poiché relativo solamente ai contenuti terroristici *online*, stabilito dal regolamento 784/2021 e rivolto unicamente ai prestatori di servizi di *hosting* (art. 1 par. 1). Il secondo, di carattere orizzontale, in quanto avente ad oggetto tutti i contenuti illeciti, applicabile a tutte le categorie di *providers* e previsto dal DSA.

L'analisi riguarderà, in particolare, le disposizioni dettate dalle due normative nei confronti degli *hosting providers*.

Relativamente al primo regime giuridico, il regolamento 784/2021 prevede una pluralità di misure che i prestatori di servizi di *hosting* devono adottare al fine di contrastare la diffusione di contenuti terroristici *online* (sezione II)[49].

Il regolamento, inoltre, impone agli Stati membri di stabilire le sanzioni applicabili in caso di mancato rispetto, da parte dei suddetti prestatori, degli obblighi da esso previsti (art. 18).

Limitandoci alla considerazione delle misure che appaiono maggiormente rilevanti, in base all'atto normativo in parola ciascuno Stato membro designa un'autorità competente a emettere ordini di rimozione, nei confronti degli anzidetti *providers*, volti a rimuovere i contenuti terroristici presenti sui servizi di tali prestatori, o a disabilitarne l'accesso in tutti i Paesi membri (art. 3 par. 1 e art. 12 par. 1 lett. a). Gli *hosting providers* devono dare

[48] Direttiva 31/2000, considerando 9 e 46; decisione quadro n. 475/2002, considerando 10; decisione quadro n. 919/2008, considerando 13, 14 e art. 2; decisione quadro n. 913/2008, considerando 15 e art. 7; direttiva 2017/541, considerando 35 e 40; reg. n. 784/2021, considerando 1, 5, 10, 12, 23, 33, 49 e art. 1 e 5.

[49] Come si è rilevato *supra* par. 2, il regolamento include, tra i «contenuti terroristici», i «materiali che istigano alla commissione di uno dei reati di cui all'articolo 3, paragrafo 1, lettere da a) a i), della direttiva (UE) 2017/541, se tali materiali, direttamente o indirettamente, ad esempio mediante l'apologia di atti terroristici, incitano a compiere reati di terrorismo, generando in tal modo il pericolo che uno o più di tali reati siano commessi» (art. 2 par. 7 lett. a).

seguito a tale ordine, in considerazione della velocità con la quale i contenuti terroristici sono diffusi attraverso i servizi *online* (considerando 17), il prima possibile ed in ogni caso entro un'ora dal ricevimento dell'ordine (art. 3 par. 3). La sistematica o persistente inosservanza di tale obbligo, si prevede, deve essere punita dagli Stati membri con sanzioni pecuniarie fino al 4% del fatturato mondiale del *provider* (art. 18 par. 3).

I prestatori di servizi in questione informano l'autorità competente che ha emanato l'ordine, senza indebito ritardo, di aver dato seguito a quest'ultimo, indicando, inoltre, la data e l'ora della rimozione o della disabilitazione (art. 3 par. 6).

Tra gli obblighi che i prestatori di servizi di *hosting* devono rispettare, meritano particolare considerazione, a nostro avviso, le misure specifiche che devono essere adottate da un «prestatore di servizi di *hosting* esposto a contenuti terroristici». È tale, in particolare, ai sensi dell'art. 5 par. 4, il prestatore a cui l'autorità competente dello Stato membro ha notificato una decisione, basata su fattori oggettivi, come il ricevimento da parte del suddetto prestatore di due o più ordini di rimozione definitivi nei 12 mesi precedenti, che stabilisce che l'*hosting provider* è esposto a contenuti terroristici.

Il prestatore esposto, innanzitutto, è tenuto a includere, nelle sue condizioni contrattuali, disposizioni volte a contrastare l'uso improprio dei suoi servizi finalizzato a diffondere pubblicamente contenuti terroristici (art. 5 par. 1).

Inoltre, tra le misure specifiche che il *provider* esposto deve adottare per impedire la diffusione, nei suoi servizi, di tali contenuti, quest'ultimo può, tra l'altro, prevedere l'utilizzo della procedura di *notice and take down*. Consentire, cioè, l'uso di meccanismi, facilmente accessibili e utilizzabili, volti a consentire agli utenti di segnalare la presenza di tali contenuti criminali (art. 5 par. 2 lett. b).

Ai sensi del regolamento 784/2021, dunque, la responsabilità dei prestatori di servizi di *hosting* sorge qualora messi a conoscenza, a seguito della ricezione di un ordine di rimozione da parte dell'autorità nazionale di uno Stato membro, della presenza sui loro servizi di un contenuto terroristico, si rifiutino di adempiere agli obblighi previsti dalla normativa in parola.

Tale quadro giuridico settoriale in materia di responsabilità degli *hosting providers* appena descritto va letto in combinato disposto con quello orizzontale previsto dal DSA per tutti i contenuti illegali. Quest'ultimo, innanzitutto, prevede all'art. 6 par. 1 che «nella prestazione di un servizio [di *hosting*], il prestatore del servizio non è responsabile delle informazioni memorizzate su richiesta di un destinatario del servizio [cioè di un suo utente], a condizione che detto prestatore: non sia effettivamente a conoscenza delle attività o dei contenuti illegali e, per quanto attiene a domande risarcitorie, non sia consapevole di fatti o circostanze che rendono manifesta l'illegalità dell'attività o dei contenuti; oppure, non appena venga a conoscenza di tali attività o contenuti illegali o divenga consapevole di tali fatti o circostanze, agisca immediatamente per rimuovere i contenuti illegali

DPCE online
ISSN: 2037-6677

o per disabilitare l'accesso agli stessi»[50].

La responsabilità dell'*hosting provider*, dunque, sorge allorché questi venga a conoscenza del contenuto illegale condiviso sul loro servizio da un proprio utente.

Ciò può accadere, in particolare, qualora le autorità nazionali dei Paesi membri emanino, nei confronti degli *hosting providers*, degli ordini di rimozione dei contenuti illegali ai sensi dell'art. 9[51]. Possibilità analoga, seppure dettata per i soli contenuti terroristici, prevista, come in parte esaminato precedentemente, anche dal regolamento 784/2021 agli artt. 3 e 4[52].

Il DSA, tuttavia, introduce una nuova circostanza, oltre alla ricezione di un ordine di rimozione, in cui gli *hosting providers* possano venire a conoscenza della presenza di un contenuto illegale sui loro servizi: e cioè a seguito di un'apposita segnalazione fatta ad essi da parte di un loro utente.

L'art. 16, infatti, introduce il cd. *notice and take down mechanism* ponendo in capo ai prestatori di servizi di *hosting* l'obbligo di predisporre meccanismi volti a consentire, a qualsiasi loro destinatario del servizio, di notificare ad essi la presenza, nel suddetto servizio, di contenuti che tale utente ritiene essere illegali (cd. segnalazioni) (art. 16 par. 1). Gli *hosting providers*, in particolare, sono considerati a conoscenza dell'illegalità del contenuto trasmesso sui loro servizi, e quindi ritenuti responsabili ai sensi dell'art. 6 par. 1, qualora le segnalazioni siano tali da permettere ad un prestatore diligente di servizi di *hosting* di individuare, senza un esame giuridico dettagliato, l'illegalità del contenuto oggetto della segnalazione (art. 16 par. 3).

Con l'adozione del DSA, dunque, tali prestatori sono considerati a conoscenza della presenza di contenuti terroristici sui loro servizi, non più solo nei casi previsti dal regolamento 784/2021 agli artt. 3 e 4, e cioè a seguito dell'emanazione di un ordine di rimozione degli anzidetti contenuti da parte delle autorità nazionali degli Stati membri, ma anche ai sensi dell'art. 16 del DSA, e quindi a seguito del ricevimento di segnalazioni ben dettagliate circa la presenza di contenuti illegali. I contenuti terroristici, infatti, si pongono in un rapporto *species* a *genus* nei confronti dei contenuti illegali. Vengono fatte salve, tuttavia, le singole misure specifiche, previste dal regolamento del 2021, che gli *hosting providers* devono attuare per contrastare la diffusione di contenuti terroristici *online*, in quanto il DSA,

[50] L'art. 6 par. 1 del DSA, che ricalca l'art. 14 par. 1 della direttiva 31/2000 così come modificata dal regolamento in questione, fa salvi, dunque, i cd. *hosting providers* passivi. Infatti, come affermato dalla Corte di Giustizia dell'Unione Europea (CGUE) relativamente alla direttiva 31/2000, «le deroghe alla responsabilità previste dalla direttiva [e quindi anche quelle di cui all'art. 14 par. 1, le quali sono state riprese dall'art. 6 par. 1 del DSA] riguardano esclusivamente i casi in cui l'attività [degli *hosting providers*] sia di ordine meramente tecnico, automatico e passivo, con la conseguenza che detti prestatori non conoscono né controllano le informazioni trasmesse o memorizzate dalle persone alle quali forniscono i loro servizi». Corte giust., c-521/17, *Coöperatieve Vereniging SNB-REACT U.A./Deepak Mehta*, sent. 7-8-2018, p.to 47.

[51] L'art. 9 del DSA detta le tempistiche, i procedimenti e le condizioni che l'ordine di rimozione emesso dall'autorità nazionale dello Stato membro deve soddisfare.

[52] L'art. 4 del regolamento (UE) 784/2021 prevede una procedura specifica per gli ordini di rimozione transfrontalieri.

esplicitamente, non pregiudica le norme previste dal regolamento 784/2021 (art. 2 par. 4).

Venendo ai possibili riflessi della disciplina su esposta sulla libertà di espressione, potrebbe verificarsi il rischio che *i social media* si autotutelino al fine di non incorrere nelle responsabilità derivanti dall'ospitare, sui propri servizi, contenuti illegali ed in particolar modo terroristici. Nel caso di questi ultimi contenuti illegali infatti, una eventuale designazione, da parte degli anzidetti prestatori, di *hosting provider* esposto a contenuti terroristici potrebbe determinare un irreparabile discredito reputazionale. Discredito che potrebbe comportare, inoltre, possibili conseguenze economiche negative derivanti dall'eventuale reazione degli inserzionisti, i quali, non interessati a sponsorizzare il loro prodotto o servizio su un *social media* esposto a contenuti terroristici, potrebbero ritirare, da tale gigante del *web*, la loro pubblicità.

Pertanto, al fine di scongiurare l'eventualità di ospitare contenuti terroristici, le piattaforme potrebbero essere indotte ad utilizzare, nei loro *community standards*, formule ampie per definire contenuti pericolosi e/o illegali, quali l'istigazione all'odio o alla violenza, che possano essere correlati al fenomeno terroristico.

Ciò trova riscontro, ad esempio, nella posizione assunta da *Meta*, azienda statunitense che controlla 3 *social media* - *Facebook*, *Instagram* e *Threads* - e che, alla data del 6 febbraio 2025, detiene, di media, 259 milioni utenti attivi nel territorio dell'Unione Europea[53]. Tale azienda, nelle norme comportamentali che gli utenti si impegnano a rispettare al momento dell'iscrizione ad uno dei summenzionati *social networks*, dichiara di rimuovere un numero vario e considerevole di condotte riconducibili alla violenza e all'odio[54], come «qualunque contenuto che promuova o istighi alla violenza e minacce credibili alla sicurezza pubblica o personale», oltre a diversi contenuti riconducibili a «organizzazioni e persone pericolose»[55].

4. Il nuovo ruolo delle condizioni generali a seguito dell'adozione del DSA

Venendo all'ultimo degli aspetti da considerare, tra le novità introdotte dal DSA, rivestono particolare importanza le norme relative alle condizioni generali, anche note come «termini e condizioni d'utilizzo». Le condizioni generali, predisposte dai *providers* e modificabili da questi unilateralmente,

[53] I dati riportati sono consultabili al sito della Commissione europea https://digital-strategy.ec.europa.eu/en/policies/list-designated-vlops-and-vloses in cui quest'ultima elenca le piattaforme *online* designate come piattaforme *online* di dimensioni molto grandi fornendone i dati essenziali.

[54] L'elenco dei contenuti che *Meta* rimuove in quanto considerati istigazione alla violenza e incitamento all'odio è consultabile ai seguenti *link*: https://transparency.meta.com/it-it/policies/community-standards/violence-incitement/, https://transparency.meta.com/it-it/policies/community-standards/hate-speech/.

[55] Per il riferimento ai contenuti che l'azienda rimuove, al fine di «impedire e fermare gli atti di violenza nel mondo reale», si veda il link https://transparency.meta.com/it-it/policies/community-standards/dangerous-individuals-organizations/.

DPCE online
ISSN: 2037-6677

sono definite dalla normativa in parola come «tutte le clausole, comunque denominate e indipendentemente dalla loro forma, che disciplinano il rapporto contrattuale tra il prestatore dei servizi intermediari e il destinatario del servizio» (art. 3 lett. u).

Il regolamento sui servizi digitali prevede, a fini conoscitivi e di trasparenza, che tutti i prestatori di servizi includano, nelle loro condizioni generali, informazioni sulle restrizioni che impongono in relazione all'uso dei loro servizi. Tra tali informazioni rientrano le politiche, le procedure, le misure e gli strumenti utilizzati ai fini della moderazione dei contenuti, compresi il processo decisionale algoritmico e la verifica umana, nonché le regole procedurali del loro sistema interno di gestione dei reclami. I termini e le condizioni di utilizzo devono essere redatti in un linguaggio chiaro, semplice, comprensibile, facilmente fruibile e privo di ambiguità, oltre che essere rese disponibili al pubblico in un formato facilmente accessibile e leggibile meccanicamente (art. 14 par. 1).

Per le piattaforme *online* di dimensioni molto grandi, invece, viene previsto l'obbligo di una sintesi concisa delle suddette condizioni, di facile accesso e leggibile meccanicamente (art. 14 par. 5).

Il DSA, relativamente a tali prestatori, muove dalla considerazione che essi «possono comportare rischi per la società diversi in termini di portata ed effetti rispetto a quelli presentati dalle piattaforme più piccole». E, in ragione dell'impatto delle piattaforme *online* di dimensioni molto grandi sulla società, «i rischi sistemici posti [da queste ultime] possono avere un effetto sproporzionato sull'Unione» (considerando 76).

Ai sensi dell'art. 34 questi giganti del *web* sono tenuti ad effettuare una valutazione di tali rischi (art. 34 par. 1), i quali sono costituiti da: la diffusione di contenuti illegali tramite i servizi offerti dalle summenzionate piattaforme; eventuali effetti negativi, attuali o prevedibili, per l'esercizio dei diritti fondamentali (la dignità umana, il rispetto della vita privata e familiare, la tutela dei dati personali, la libertà di espressione e di informazione, la non discriminazione, il rispetto dei diritti del minore, la non discriminazione, l'elevata tutela del minore); eventuali effetti negativi, attuali o prevedibili, sul dibattito civico, sui processi elettorali e sulla sicurezza pubblica; qualsiasi effetto negativo, attuale o prevedibile, in relazione alla violenza di genere, alla protezione della salute pubblica e dei minori e alle gravi conseguenze negative per il benessere fisico e mentale della persona (art. 34 par. 1 lett. da a) a d).

Le piattaforme *online* di dimensioni molto grandi, nella valutazione, devono tenere conto di alcuni fattori che influenzano tali rischi, tra i quali, ai fini che qui interessano, rientrano: i sistemi di moderazione dei contenuti; le condizioni generali applicabili e la loro applicazione; l'amplificazione e la diffusione potenzialmente rapida e ampia di contenuti illegali e di informazioni incompatibili con le condizioni generali (art. 34 par. 2).

Nell'ipotesi in cui siano individuati rischi sistemici, l'art. 35 prevede l'adozione, da parte dei *providers*, di misure di attenuazione di tali rischi, tra le quali include: l'adeguamento delle condizioni generali e la loro applicazione, nonché l'adeguamento delle procedure di moderazione dei contenuti, compresa la velocità e la qualità del trattamento delle segnalazioni concernenti tipi specifici di contenuti illegali e, se del caso, la rapida rimozione dei contenuti segnalati o la disabilitazione del loro accesso, in

particolare in relazione all'incitamento illegale all'odio e alla violenza *online* (art. 35 par. 1 lett. b) e c).

Come si evince dal combinato disposto delle due norme, dunque, i sistemi di moderazione dei contenuti e le condizioni generali rappresentano tanto dei fattori che influenzano i rischi sistemici quanto misure volte alla loro attenuazione.

Il DSA, inoltre, prevede la (eventuale) necessità che le piattaforme *online* di grandi dimensioni adottino misure specifiche in caso di una crisi. Si è in presenza di quest'ultima, secondo il regolamento in questione, qualora si verifichino circostanze eccezionali che possano comportare una minaccia grave per la sicurezza pubblica o la salute pubblica nell'Unione o in sue parti significative (art. 36). Il rilievo che questa diposizione riveste con riguardo agli atti di terrorismo risulta dal fatto che nella motivazione del regolamento, tra le fattispecie da cui potrebbe derivare una crisi, si fa riferimento, in particolare, a tali atti.

In caso di crisi, la Commissione, dopo aver dichiarato tale stato di emergenza, può adottare una decisione che impone a una o più di tali piattaforme l'adozione di alcune misure. Tra queste ultime rientrano le stesse previste per contrastare i rischi sistemici, ed in particolare, ai fini che qui interessano, l'adeguamento delle condizioni generali e dei processi di moderazione (art. 36 par. 1).

La tutela della sicurezza pubblica dell'Unione, dunque, assume rilevanza, all'interno del DSA, sia in caso di rischi sistemici che di crisi. Qualora si verificassero eventi idonei a minare la pubblica sicurezza, quali incitamenti illegali all'odio o episodi terroristici, infatti, il regolamento permetterebbe a tali *providers* di intervenire (ulteriormente) sulle loro condizioni generali e sui processi di moderazione dei contenuti.

Ciò, con particolare riferimento alla libertà di espressione, potrebbe, a nostro parere, far sì che, soprattutto in caso di crisi, durante le quali le esigenze di sicurezza rivestono fondamentale rilevanza, i già severi *community standards* imposti dai *social media* vengano modificati sulla base di politiche aziendali volte sempre più ad impedire, alla radice, qualsiasi contenuto che possa astrattamente costituire una minaccia.

In ordine al ruolo che risulta assunto dai *social networks* a seguito dell'adozione del DSA, dalla normativa in parola sembra emergere, a nostro avviso, la scelta, da parte del legislatore europeo, di devolvere ad attori privati, e cioè alle *big-tech* della comunicazione, il compito di salvaguardare la sicurezza dell'ambiente digitale dell'Unione.

Ciò consegue, a noi pare, in primo luogo, dalla circostanza che ad esse è stato affidato l'onere di (auto)valutare i potenziali rischi sistemici posti dalle piattaforme stesse, senza una verifica compiuta in tal senso dalla Commissione. Questa, invece, può solo, tra l'altro, ottenere, su richiesta, la comunicazione dei documenti giustificatici della valutazione dei rischi (art. 34 par. 3), emanare orientamenti contenenti delle *best practices*, raccomandare l'adozione di alcune misure di attenuazione dei rischi (art. 35 par. 3) e, eventualmente, invitare le piattaforme *online* di dimensioni molto grandi a partecipare all'elaborazione di codici di condotta volontari (art. 45).

In secondo luogo, risulta dal fatto che è stata delegata ai *social networks* la scelta delle misure, da questi ritenute necessarie, che la Commissione impone loro di adottare in caso di crisi. La Commissione, può, eventualmente

DPCE online
ISSN: 2037-6677

e solo successivamente, revocare tale decisione (art. 36 par. 8) o incoraggiare detti *providers* a partecipare all'elaborazione e applicazione di protocolli di crisi volontari volti ad affrontare queste ultime (art. 48).

Inoltre, l'intero impianto normativo previsto in caso di crisi all'art. 36 del DSA, derubricato, per l'appunto, «meccanismo di risposta alle crisi», presenta delle criticità, espresse da parte della dottrina[56] e da noi condivise, consistenti nella circostanza che tale meccanismo vede come unici protagonisti le piattaforme *online* di dimensioni molto grandi e la Commissione. Quest'ultima, infatti, riferisce al Parlamento ed al Consiglio, in merito all'applicazione delle misure adottate dalle piattaforme, solo una volta all'anno dal momento in cui dichiara una crisi e, in ogni caso, tre mesi dopo la fine di quest'ultima (art. 36 par. 11).

5. Considerazioni finali

Riprendendo quanto fin qui detto, dall'analisi condotta si evince una convinta consapevolezza, da parte del legislatore europeo, della necessità di combattere tale fenomeno criminale, visti i valori messi a repentaglio dalle minacce terroristiche.

Tale obiettivo viene perseguito, in particolare, come emerge dagli atti normativi considerati, con un approccio di natura preventiva, volto ad impedire la commissione di atti terroristici, basato sul contrasto alla propaganda e alla radicalizzazione di tale fenomeno criminale.

Ciò trova riscontro, segnatamente, nel reato di «pubblica provocazione per commettere reati di terrorismo», così come armonizzato, e adattato all'ecosistema digitale, dalla direttiva 2017/541.

L'intento di orientare la legislazione antiterrorismo dell'Unione alla dimensione *online* viene confermato, inoltre, dall'adozione del regolamento 784/2021. Normativa finalizzata, in particolare, ad evitare, mediante una maggiore responsabilizzazione degli *hosting providers*, la diffusione di contenuti terroristici *online*, ed in particolare di quelli idonei a provocare la commissioni di reati terroristici, sui principali canali di informazioni dell'era digitale.

Tale quadro giuridico settoriale va letto in combinato disposto con le nuove previsioni dettate dal DSA sulla responsabilità degli *hosting providers*, ed in particolare con gli artt. 6 par. 1 e 16. Queste norme, infatti, prevedono che i prestatori in questione possano essere ritenuti responsabili - in quanto a conoscenza di un contenuto illegale diffuso sui loro servizi – a seguito di segnalazioni effettuate da altri utenti. Ciò è volto a creare un ecosistema digitale sempre più sicuro in cui l'utente stesso contribuisce alla salubrità dell'ambiente *online*.

Per quanto attiene alla tutela della libertà di espressione, l'esigenza di assicurare tale tutela è prevista, come pure si è detto, in tutta la normativa dell'Unione relativa, specificamente, al contrasto al terrorismo[57].

Ciò tuttavia non esclude, a nostro avviso, che tale diritto potrebbe essere limitato dalla nozione del reato di «pubblica provocazione per

[56] V. Colarocco, M. Cogode, *Gli obblighi applicabili a piattaforme online di dimensioni molto grandi (Artt. 33-43 – Capo III, Sezione 5)*, in *Dir. Internet*, 2023, 1, 32.
[57] Cfr. *supra* par. 2.

commettere reati di terrorismo» previsto all'art. 5 della direttiva 2017/541. Riguardo tale delitto, senza ritornare specificamente sul punto già considerato in precedenza, a noi sembrano condivisibili i rilievi effettuati dalla relazione della FRA[58]. Criticità che, in ragione del sostanziale rinvio operato dal regolamento 784/2021 alla direttiva del 2017, persistono nella definizione di materiali che istigano alla commissione di reati di terrorismo (art. 2 par. 7 lett. a).

Ed invero, il severo regime sanzionatorio stabilito dall'Unione, in cui i *social media* incorrerebbero qualora ospitassero contenuti, anche istigatori, di natura terroristica, potrebbe determinare la seguente conseguenza. E cioè che, al fine di evitare l'applicazione di tale regime, i *social networks* potrebbero adeguare le proprie condizioni generali e, in particolare, i propri *community standards*, attraverso una più severa politica di moderazione dei contenuti. Tale politica, determinando la rimozione o l'oscuramento di opinioni polemiche o controverse ritenute sia pure lontanamente riconducibili a materiali istigatori di reati di terrorismo, potrebbe incidere sul diritto alla libertà di espressione.

È senz'altro vero che quest'ultimo non è un diritto assoluto, e quindi può soggiacere alle condizioni previste, in particolare, nel caso di specie, dalla normativa antiterrorismo dell'Unione, dalla Carta di Nizza e, in ragione del richiamo ad essa effettuata, anche dalla Convenzione europea dei diritti dell'uomo.

Resta tuttavia il fatto che dalla normativa esaminata emerge che il bilanciamento tra l'esigenza di tutela del diritto fondamentale in parola e quella di contrasto alla diffusione di contenuti terroristici viene rimesso, in sostanza, alle piattaforme *online* le quali, come si è rilevato, potrebbero privilegiare politiche volte ad evitare l'applicazione di sanzioni piuttosto che ad assicurare la libertà di espressione dei propri utenti.

Sembrano corroborare la nostra tesi gli esiti della relazione effettuata dalla Commissione sull'attuazione del regolamento 784/2021[59]. Il *report*, infatti, segnala che, finora, nessun *hosting provider* ha impugnato un ordine di rimozione emanato dalle autorità nazionali degli Stati membri né è stato ritenuto esposto a contenuti terroristici ai sensi della normativa in parola[60]. Tale risultato, indubbiamente, depone a favore dell'efficacia, da parte del regolamento, di limitare, per quanto possibile, la diffusione di contenuti terroristici *online*. Questi dati, tuttavia, secondo una lettura alternativa, possono indicare una comprovata volontà, da parte dei summenzionati prestatori, di non incorrere in alcun modo nel regime sanzionatorio previsto dall'Unione. Intento raggiungibile, come dimostra il già citato caso dei *community standards* adottati da *Meta*, mediante l'adozione di condizioni generali molto severe che portino alla rimozione, preventiva, di contenuti polemici o controversi che possano essere, anche lontanamente, correlati al fenomeno terroristico.

Relativamente al ruolo delle condizioni generali, un considerevole

[58] Cfr. *supra* par. 2.
[59] Relazione della Commissione al Parlamento europeo e al Consiglio sull'attuazione del regolamento (UE) 784/2021 relativo al contrasto della diffusione di contenuti terroristici *online*, COM (2024) 64 final.
[60] *Ivi*, 8.

DPCE online
ISSN: 2037-6677

rischio per la libertà d'espressione è costituito, a noi pare, dal ruolo che queste hanno assunto a seguito dell'adozione del DSA.

Esse, infatti, vengono in rilievo in quanto possono costituire dei fattori che influenzano i rischi sistemici, misure volte alla loro attuazione e misure che, in caso di crisi, la Commissione può imporre alle piattaforme *online* di dimensioni molto grandi di adottare.

Ai nostri fini rileva, in particolare, la tutela della sicurezza pubblica dell'Unione. Quest'ultima, infatti, può essere messa a repentaglio da azioni quali incitamenti illegali all'odio o episodi terroristici. In presenza di tali pericoli, dunque, il DSA permetterebbe alle piattaforme *online* di dimensioni molto grandi di intervenire sulle condizioni generali.

Si può concludere, allora, relativamente al partenariato pubblico-privato reso necessario nella regolazione del dibattito civico *online*, condividendo le preoccupazioni di parte della dottrina. Quest'ultima, infatti, temendo un quadro giuridico che porti i *social media* ad agire secondo la logica del «shoot first, ask questions later»[61], ipotizza il rischio della legittimazione di una "privatizzazione" della censura[62] in favore dei grandi giganti del *web*, i quali dovrebbero ospitare il cd. *marketplace of ideas*[63], e che, invece, si potrebbero trovare a svolgere il ruolo di guardiani dello spazio *online*[64], in particolare in ragione del nuovo ruolo da essi assunto a seguito dell'emanazione del DSA.

Enrico Stella
Dipartimento di Giurisprudenza
Università degli Studi di Bari "Aldo Moro"
enrico.stella@uniba.it

[61] S.F. Kreimer, *Censorship by Proxy: The First Amendment, Internet Intermediaries, and the Problem of the Weakest Link*, in *U. Pa. L. Rev.*, 28 (2006), nota 52.
[62] Il concetto è spiegato da M. Monti, *Privatizzazione della censura e Internet platforms: la libertà di espressione e i nuovi censori dell'agorà digitale*, in *RIID*, 2019, 1, 35-51.
[63] Per una ricostruzione della definizione vedi G. De Gregorio, *The market place of ideas nell'era della post-verità: quali responsabilità per gli attori pubblici e privati online?*, in *Medialaws.eu*, 2017, 1, 91-105.
[64] T. Gilleispe, *Custodians of the Internet: platforms, content moderation, and the hidden decisions that shape social media*, New Haven-London, 2018, 5.