dossier

XIX Legislatura

22 maggio 2023

Adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2021/784 relativo al contrasto della diffusione di contenuti terroristici online

A.G. 45

Ai sensi dell'articolo 15
della legge 4 agosto 2022, n. 127

Senato della Repubblica

Camera dei deputati

Senato della Repubblica

SERVIZIO STUDI
Ufficio ricerche su questioni istituzionali, giustizia e cultura
TEL. 06 6706-2451 - ✉ studi1@senato.it - @SR_Studi
Dossier n. 98

Camera dei deputati

SERVIZIO STUDI
Dipartimento Giustizia
Tel. 066760-9253 ✉ st_giustizia@camera.it - @CD_giustizia
Atti del Governo n. 45

GI0023.docx

I N D I C E

Schede di lettura

Premessa

Lo schema di decreto legislativo, **AG. 45**, è adottato in attuazione delle disposizioni di cui all'articolo 15 della legge n. 127 del 2022 - delegazione europea 2021 (*vedi infra*), con cui il Governo è stato delegato all'emanazione di uno o più decreti legislativi per **l'adeguamento della normativa nazionale al Regolamento (UE) 2021/784** del Parlamento europeo e del Consiglio, del 29 aprile 2021, relativo al contrasto della diffusione di **contenuti terroristici online.**

Su di esso le Commissioni giustizia di Senato e Camera sono chiamate ad esprimere **parere entro il 25 giugno 2023**.

Il Governo deve esercitare la delega entro il 31 agosto 2023.

In sintesi lo schema di decreto:

- individua l**'oggetto** dell'intervento normativo, ovvero l'adozione di disposizioni di adeguamento della normativa nazionale al regolamento (UE) 2021/784 relativo al contrasto della **diffusione di contenuti terroristici online (art. 1);**
- reca alcune **definizioni**, che riguardano le strutture del Ministero dell'interno indicate nel provvedimento (**art. 2);**
- interviene con riguardo all'emissione degli **ordini di rimozione**, individuando l'Autorità competente e disciplinando la relativa procedura **(art. 3);**
- disciplina l'**esame degli ordini di rimozione transfrontalieri** individuando l'autorità competente in materia nel **giudice per le indagini preliminari**. La competenza sugli ordini di rimozione è attribuita a livello **distrettuale**, quindi al gip appartenente al tribunale del capoluogo del distretto **(art. 4);**
- conferisce all'Organo del Ministero dell'interno per la sicurezza e la regolarità dei servizi di telecomunicazione alcune attribuzioni che contribuiscono all'attuazione nazionale delle disposizioni del Regolamento **(art. 5);**
- disciplina il **regime sanzionatorio**, regolandone anche il procedimento di applicazione, prevedendo gruppi di illeciti amministrativi, di gravità crescente e configurabili solo quando il fatto non integri reato **(art. 6);**
- **reca le sanzioni penali,** prevedendo gruppi di illeciti, di gravità crescente e configurabili solo quando il fatto non integri più grave reato **(art. 7);**

- prevede **l'abrogazione della vigente disciplina** relativa alla rimozione dei contenuti pubblicati sui siti internet nell'ambito dell'attività investigativa finalizzata alla repressione dei reati con le finalità di terrorismo **(art. 8);**
- specifica che dall'attuazione del provvedimento non devono derivare nuovi o maggiori oneri a carico della finanza pubblica **(art. 9).**

LA NORMA DI DELEGA

Lo schema di decreto legislativo A.G. 45 dà attuazione all'**articolo 15** della legge n. 127 del 2022 – **Legge di delegazione europea 2021**, per l'adeguamento della normativa nazionale al regolamento (UE) 2021/784 relativo al contrasto della diffusione di contenuti terroristici *online*.

Per quanto riguarda il **procedimento per l'esercizio della delega**, il **comma 1** dell'articolo 15 prevede che il Governo debba adottare, entro il 31 maggio 2023, con le procedure di cui all'articolo 31 della legge n. 234 del 2012 e acquisito il parere delle competenti Commissioni parlamentari - **uno o più decreti legislativi** per l'adeguamento della normativa nazionale al regolamento (UE) n. 2021/784.

Si ricorda che il **termine per l'attuazione della delega** è stato fissato al 13 maggio 2023 dall'art. 1, comma 4 della legge n. 14 del 2023 (*Conversione in legge, con modificazioni, del decreto-legge 29 dicembre 2022, n. 198, recante disposizioni urgenti in materia di termini legislativi. Proroga di termini per l'esercizio di deleghe legislative).* La formulazione originaria dell'art. 15 della legge n. 127 del 2022 non prevedeva alcun termine per l'attuazione della delega.

Il Governo ha trasmesso lo schema alle Camere il 16 maggio 2023. Per effetto dell'art. 31, comma 3, della legge n. 234 del 2012, il termine per l'esercizio della delega è prorogato di 3 mesi per consentire alle competenti commissioni parlamentari di esprimere il parere e al Governo di poterne tenere conto (c.d. **scorrimento dei termini**); pertanto, **il decreto legislativo dovrà essere adottato entro il 31 agosto 2023**.

Il medesimo comma 1 contiene gli specifici **princìpi e criteri di esercizio della delega** che vanno ad affiancarsi ai princìpi e criteri direttivi generali di cui all'articolo 32, della legge n. 234 del 2012 *(v. infra schede di lettura sui singoli articoli del provvedimento).*

Il **comma 2** specifica che dall'attuazione della delega non devono derivare nuovi o maggiori oneri a carico della finanza pubblica e che le amministrazioni interessate provvedono all'adempimento dei compiti derivanti dall'esercizio della delega con le risorse umane, strumentali e finanziarie disponibili a legislazione vigente.

IL CONTENUTO DELLO SCHEMA

Articolo 1
(Oggetto)

L'**articolo 1** individua il contenuto del decreto, ovvero l'adozione di disposizioni di adeguamento della normativa nazionale al regolamento (UE) 2021/784 del Parlamento europeo e del Consiglio, del 29 aprile 2021, relativo al contrasto della **diffusione di contenuti terroristici online.**

Il Regolamento UE/2021/784: contrasto della diffusione di contenuti terroristici online

Il **Regolamento (UE) 2021/784**, in vigore dal 7 giugno 2022, stabilisce norme a livello dell'Unione per contrastare **l'uso improprio dei servizi di hosting** per la diffusione al pubblico di contenuti terroristici online.

Il Regolamento si fonda su una combinazione di misure legislative, non legislative e volontarie basate sulla collaborazione tra le autorità e i prestatori di servizi di hosting, nel rispetto dei diritti fondamentali.

Al riguardo, le norme UE prevedono (art. 2):

- obblighi di diligenza ragionevoli e proporzionati che i prestatori di servizi di hosting sono tenuti ad applicare per contrastare la diffusione al pubblico di contenuti terroristici tramite i propri servizi e a garantire, ove necessario, la rimozione o la disabilitazione dell'accesso a tali contenuti;
- le misure che gli Stati membri dell'Unione debbono mettere in atto in conformità al diritto dell'Unione e subordinate alle salvaguardie dei diritti fondamentali, al fine di:

individuare e garantire la rimozione tempestiva dei contenuti terroristici da parte dei prestatori di servizi di hosting;

agevolare la cooperazione tra le autorità competenti degli Stati membri, i prestatori di servizi di hosting e, ove opportuno, l'Europol.

Il Regolamento si applica ai prestatori di servizi di hosting che offrono servizi nell'Unione, indipendentemente dal fatto di disporre di una sede principale negli Stati membri. Il materiale diffuso al pubblico per scopi educativi, giornalistici, artistici o di ricerca o a fini di prevenzione o di lotta al terrorismo, non è considerato come contenuto terroristico.

La definizione fornita dal Regolamento (art. 2, par. 7) dei contenuti terroristici, è piuttosto ampia considerandosi tali i materiali che

- istigano alla commissione di uno dei reati di terrorismo 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;

- sollecitano una persona o un gruppo di persone a commettere o a contribuire a commettere uno dei reati di terrorismo;
- sollecitano una persona o un gruppo di persone a partecipare alle attività di un gruppo terroristico, ai sensi dell'articolo 4, lettera b), della direttiva (UE) 2017/541;
- impartiscono istruzioni per la fabbricazione o l'uso di esplosivi, armi da fuoco o altre armi o sostanze nocive o pericolose, ovvero altri metodi o tecniche specifici allo scopo di commettere o contribuire alla commissione di uno dei reati di terrorismo;
- costituiscono una minaccia di commissione di uno dei reati di terrorismo.

Si ricorda che, ai sensi della **Direttiva (UE) 2017/541** (art. 3) sono **reati di terrorismo** i seguenti atti intenzionali, che, per la loro natura o per il contesto in cui si situano, possono arrecare grave danno a un paese o a un'organizzazione internazionale, quando sono commessi con uno degli scopi elencati al paragrafo 2:

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, comprese armi chimiche, biologiche, radiologiche o nucleari, nonché ricerca e sviluppo di armi chimiche, biologiche, radiologiche o nucleari; (21)

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 (20) 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).

2. Gli scopi di cui al paragrafo 1 sono:

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.

In sintesi, il Regolamento, all'art. 3, prevede la facoltà per gli Stati membri di emettere a carico dei prestatori di servizi un **ordine di rimozione di contenuti terroristici in tutti gli Stati membri.** Una volta ricevuto tale ordine, gli hosting providers dovranno provvedere alla rimozione del contenuto il prima possibile, e in ogni caso entro un'ora dal ricevimento dell'ordine. I contenuti rimossi dovranno poi essere conservati dagli intermediari per 6 mesi ai fini delle indagini.

Inoltre, il Regolamento prevede, all'art. 5, che i prestatori di servizi di hosting adottino misure specifiche, efficaci e proporzionate, fondate su meccanismi automatici e automatizzati ma anche garantendo verifiche umane, laddove ritenute necessarie, per **proteggere i propri servizi** dalla diffusione al pubblico di contenuti terroristici. Potendo dunque i prestatori di servizi di hosting provvedere autonomamente alla rimozione dei contenuti ospitati sulle proprie piattaforme, il Regolamento evidenzia che, per poter garantire una tutela giurisdizionale effettiva, i fornitori di contenuti devono essere posti in grado di conoscere il motivo per cui i contenuti che essi forniscono è stato rimosso o il cui accesso è stato disabilitato. A tal fine, i prestatori di servizi di hosting devono mettere a disposizione del fornitore di contenuti informazioni concernenti la rimozione, nonché predisporre un meccanismo di reclamo.

In caso invece di contenuti terroristici che comportino una minaccia imminente per la vita o un presunto reato di terrorismo, quale definito dalla direttiva 541/2017 *(v. sopra),* i prestatori dovranno informare tempestivamente le autorità competenti.

Gli Stati membri dovranno designare le autorità competenti (anche tra quelle esistenti) a emettere e valutare gli ordini di rimozione, controllare l'adozione delle misure specifiche, così come irrogare sanzioni. Tali autorità dovranno poi coordinarsi e cooperare tra loro a livello sovranazionale.

Vengono fatte salve disposizioni contenute nella direttiva 31/2000, per cui rimane fermo il divieto di imporre un obbligo generale di ricerca attiva di contenuti terroristici a carico dei prestatori di servizi. Inoltre, le diverse misure adottate da questi ultimi non dovranno comportare automaticamente la perdita del beneficio dell'esenzione di responsabilità previsto in tale direttiva.

Infine, per quanto riguarda il trattamento sanzionatorio, gli Stati membri dovranno stabilire le norme relative alle sanzioni applicabili alle violazioni del Regolamento da parte dei prestatori di servizi di hosting, che potranno essere di natura amministrativa o penale

Si ricorda che, ai sensi dell'art. 24 del regolamento, le disposizioni in esso contenute si applicano a decorrere dal 7 giugno 2022. Con nota 137 final del 26 gennaio 2023, la Commissione europea ha aperto una **procedura di infrazione** nei confronti dell'Italia ai sensi dell'art. 258 TFUE, per non aver provveduto, entro la suddetta data, all'individuazione delle autorità competenti a emettere ed esaminare gli ordini di rimozione dei contenuti terroristici, nonché alla predisposizione delle norme volte a sanzionare le violazioni delle disposizioni del regolamento.

Articolo 2
(Definizioni)

L'**articolo 2** reca alcune definizioni, che riguardano le strutture del Ministero dell'interno indicate nel provvedimento.

In particolare, la disposizione si riferisce a:

a) **Comitato di analisi strategica antiterrorismo (C.A.S.A.)** per indicare il Comitato istituito presso il Dipartimento della pubblica sicurezza del Ministero dell'interno con decreto del Ministero dell'interno 6 maggio 2004, che ha disciplinato il Piano nazionale per la gestione dei eventi di natura terroristica.

   Il Comitato opera come tavolo permanente, nel cui ambito vengono condivise e valutate le informazioni sulla minaccia terroristica interna ed internazionale. È presieduto dal Direttore Centrale della Polizia di Prevenzione e vi prendono parte le forze di polizia a competenza generale (Polizia di Stato e Arma dei Carabinieri); i Servizi di Intelligence (AISE ed AISI) e, per i contributi specialistici, la Guardia di Finanza ed il Dipartimento dell'Amministrazione penitenziaria.

   Ai sensi dell'articolo 12, comma 3, della legge 3 agosto 2007, n. 124, il CASA fornisce ogni possibile cooperazione al Sistema di informazione per la sicurezza della Repubblica per lo svolgimento dei compiti a questo affidati.

b) **Dipartimento della pubblica sicurezza** per indicare il Dipartimento del Ministero dell'interno che, ai sensi dell'articolo 4 della legge 1° aprile 1981, n. 121, provvede secondo le direttive del Ministro all'attuazione della politica dell'ordine e della sicurezza pubblica; al coordinamento tecnico-operativo delle forze di polizia; alla direzione e amministrazione della Polizia di Stato, nonché alla direzione e gestione dei supporti tecnici, anche per le esigenze generali del Ministero dell'interno.

   Il Dipartimento della Pubblica Sicurezza è organizzato in Direzioni Centrali e in Uffici di pari livello, anche a carattere interforze, ai sensi dell'art. 4, D.P.C.M. n. 78/2019.

c) **Organo del Ministero dell'interno per la sicurezza e la regolarità dei servizi di telecomunicazione** per indicare il l'organo del Ministero previsto dall'articolo 1, comma 13, della legge 13 luglio 1997, n. 249 e dal decreto interministeriale del 19

gennaio 1999 in sostituzione del Servizio polizia postale e delle comunicazioni.
A livello operativo e funzionale il Servizio è organizzato in **numerose aree di intervento** che riguardano, in particolare, la pedopornografia on line (articolo 14, comma 2, della legge 3 agosto 1998, n. 269) e i reati commessi ai danni dei minori e delle fasce più esposte della cittadinanza nonché, più in generale, dei delitti contro la persona commessi attraverso la rete (quali minacce, diffamazioni, *cyberstalking*, ecc); il cyberterrorismo, nell'ottica della prevenzione e del contrasto ai fenomeni di radicalizzazione, propaganda, addestramento e pianificazione di attentati attraverso la rete; il copyright: la tutela delle reti di comunicazione e la protezione delle infrastrutture critiche informatizzate, in funzione del contenimento e del contrasto delle violazioni dei dati e dei sistemi informatici (*hacking*), attraverso il C.N.A.I.P.I.C. – Centro Nazionale Anticrimine Informatico per la protezione delle Infrastrutture Critiche; il crimine finanziario-informatico (*Financial Cybercrime*); i reati postali e la tutela del diritto d'autore.

Articolo 3
(Emissione degli ordini di rimozione)

L'**articolo 3** concerne l'emissione degli **ordini di rimozione**, individuando l'Autorità competente e disciplinando la relativa procedura, in attuazione degli specifici principi e criteri direttivi di cui all'art. 15, comma 1, lettere *a*, *b* ed *e* della legge 127/2022 (Legge di delegazione europea 2021).

La lett. *a* reca, quale principio e criterio direttivo, quello di individuare delle Autorità competenti ad emettere ed esaminare gli ordini di rimozione ai sensi dell'articolo 12, paragrafo 1, lettere *a* e *b* del Regolamento (UE) 2021/784, disciplinando il procedimento per l'adozione delle predette misure in modo da prevedere l'immediata informativa del Procuratore nazionale antimafia e antiterrorismo e l'acquisizione di elementi informativi e valutativi anche presso il Comitato di analisi strategica antiterrorismo.

La lett. *b* reca, quale principio e criterio direttivo, quello di individuare l'Organo del Ministero dell'interno per la sicurezza e la regolarità dei servizi di telecomunicazione, tra l'altro, quale struttura di supporto tecnico al punto di contatto designato ai sensi dell'articolo 12, paragrafo 2, del regolamento.

La lett. *c* reca, quale principio e criterio direttivo, quello di prevedere effettivi strumenti di tutela in favore dei prestatori di servizi di *hosting* e dei fornitori di contenuti nei casi previsti dall'articolo 9 del regolamento (UE) 2021/784, che riconosce ai prestatori di servizi di *hosting* che hanno ricevuto un ordine di rimozione o una decisione il diritto a un ricorso effettivo

Il **comma 1** concerne l'**individuazione dell'Autorità competente** a emettere gli ordini di rimozione di contenuti terroristici *on line* ai sensi dell'art. 3, paragrafo 1, del regolamento (UE) 2021/784 - in attuazione del criterio di delega di cui all'art. 15, comma 1, lett. *a* della legge 127/2022 - individuandola nell'**ufficio del pubblico ministero** presso il tribunale del capoluogo di distretto di corte d'appello (**procura distrettuale**) competente per i delitti con finalità di terrorismo riconducibili ai contenuti *on line* o che per primo ha acquisito la notizia relativa alla presenza dei contenuti terroristici *on line*.

L'art. 3, paragrafo 1, del regolamento (UE) 2021/784 prevede che l'Autorità competente di ogni Stato membro abbia la facoltà di emettere un ordine di rimozione imponendo ai prestatori di servizi di rimuovere contenuti terroristici o di disabilitare l'accesso a contenuti terroristici in tutti gli Stati membri.

La **definizione di "contenuti terroristici"** è recata dall'art. 2, punto 7, del regolamento citato.

In tale definizione rientrano:

- materiali che istigano a compiere un reato di terrorismo se tali materiali incitano direttamente o indirettamente, ad esempio attraverso l'apologia di terrorismo, a compiere reati di terrorismo, generando il pericolo che tali reati siano commessi;
- materiali che sollecitano una persona o un gruppo a commettere un reato di terrorismo;
- materiali che sollecitano una persona o un gruppo a partecipare alle attività di un gruppo terroristico;
- materiali che impartiscano istruzioni per la fabbricazione o l'uso di esplosivi, armi o sostanze nocive o pericolose o concernenti metodi o tecniche per la commissione di reati di terrorismo;
- materiali che costituiscano una minaccia di commissione di un reato di terrorismo.

I **reati di terrorismo** cui si fa riferimento sono quelli di cui all'art. 3, paragrafo 1, lett. da *a* a *i* della direttiva (UE) 2017/541. Si tratta degli atti seguenti, qualora commessi al fine di intimidire gravemente la popolazione, di costringere i poteri pubblici o un'organizzazione internazionale a compiere od omettere determinati atti o di destabilizzare gravemente o distruggere le strutture politiche, costituzionali, economiche o sociali fondamentali di un Paese o di un'organizzazione internazionale: attentati alla vita e all'integrità fisica delle persone; sequestro di persona o cattura di ostaggi; distruzioni di vasta portata di strutture governative o pubbliche o di proprietà private o di infrastrutture, compresi i sistemi informatici, in modo da mettere in pericolo vite umane o da causare perdite economiche considerevoli; sequestro di navi, aerei o altri mezzi di trasporto; reati concernenti esplosivi e armi, anche chimiche, biologiche, radiologiche o nucleari; rilascio di sostanze pericolose, incendi, inondazioni o esplosioni in modo da mettere in pericolo vite umane; manomissione o interruzione della fornitura di acqua, energia o altre risorse fondamentali in modo da mettere in pericolo vite umane; gravi attacchi a sistemi di informazione.

Si ricorda infine che, ai sensi dell'art. 13 del regolamento (UE) 2021/784 gli Stati membri assicurano che le Autorità competenti dispongano di poteri necessari e risorse sufficienti per svolgere le loro funzioni (paragrafo 1). Gli Stati membri provvedono altresì affinché le Autorità competenti svolgano i loro compiti in modo obiettivo, discriminatorio e nel pieno rispetto dei diritti fondamentali e non sollecitino né accettino istruzioni da alcun altro organismo (paragrafo 2).

In particolare la competenza all'emissione degli ordini di rimozione spetta:

- alla **procura competente ai sensi del codice di procedura penale** qualora i contenuti terroristici *on line* siano riconducibili a un **delitto con finalità di terrorismo**;

- alla **procura presso il tribunale del capoluogo di distretto di corte d'appello** che ha acquisito per prima la notizia della presenza dei contenuti terroristici *on line*, negli altri casi.

Si ricorda che, ai sensi dell'art. 51, comma 3-*quater*, c.p.p. nei procedimenti per i delitti consumati o tentati con finalità di terrorismo le funzioni del pubblico ministero sono esercitate dal procuratore della Repubblica presso il tribunale del capoluogo del distretto di corte d'appello nel cui ambito ha sede il giudice competente.

Ne consegue che, in ogni caso, la competenza a emettere l'ordine di rimozione spetta all'ufficio del pubblico ministero presso il tribunale capoluogo del distretto (procura distrettuale).

Il **comma 2** riguarda l'**individuazione del punto di contatto** da parte dell'Autorità competente, ai sensi dell'art. 12, paragrafo 2, del regolamento.

L'art. 12, paragrafo 2, del regolamento (UE) 2021/784 prevede che ciascuno Stato membro si assicuri che sia designato o istituito un punto di contatto in seno all'Autorità competente per trattare le richieste di chiarimenti e di riscontro relative agli ordini di rimozione e che le informazioni sul punto di contatto siano rese pubbliche.

In particolare, il comma in commento stabilisce che i procuratori distrettuali, entro quindici giorni dalla data di entrata in vigore del decreto legislativo, individuino il **punto di contatto** tra il **personale addetto alle sezioni di polizia giudiziaria** e assicurino **adeguata pubblicità** alle informazioni relative. Si prevede che il punto di contatto, nell'assolvimento dei suoi compiti, possa avvalersi del **supporto tecnico** dell'Organo del Ministero dell'interno per la sicurezza e la regolarità dei servizi di telecomunicazione (*sul quale vedi scheda relativa all'art. 2*); in tal modo viene data attuazione al criterio di delega di cui all'art. 15, comma 1, lett. *b* della legge 127/2022.

Il pubblico ministero informa immediatamente il **procuratore nazionale antimafia e antiterrorismo** della ricezione della notizia relativa alla presenza di contenuti terroristici *on line* (**comma 3**) e informa altresì il medesimo procuratore nazionale antimafia e antiterrorismo prima di adottare i decreti con i quali è emesso l'ordine di rimozione o ne viene ritardata l'emissione (**comma 7**). Ai fini dell'emissione dell'ordine di rimozione il pubblico ministero acquisisce, anche presso il Comitato di analisi strategica antiterrorismo (CASA, *sul quale vedi scheda relativa all'art. 2*), ogni necessario elemento informativo e valutativo (**comma 4**). Le predette norme danno attuazione a specifici criteri di delega previsti dall'art. 15, comma 1, lett. *a* della legge 127/2022.

Ai sensi del **comma 5** il pubblico ministero può, con decreto motivato, **ritardare l'emissione dell'ordine di rimozione** quando ciò si renda necessario per l'acquisizione di rilevanti elementi probatori ovvero per l'individuazione o la cattura dei responsabili dei delitti con finalità di terrorismo cui i contenuti terroristici *on line* siano riconducibili.

Il **comma 6** prevede che l'ordine di rimozione sia emesso con **decreto motivato** e che sia portato a conoscenza dei destinatari preferibilmente per il tramite di agenti o ufficiali di polizia giudiziaria appartenenti all'Organo del Ministero dell'interno per la sicurezza e la regolarità dei servizi di telecomunicazioni (*sul quale vedi scheda relativa all'art. 2*). Il medesimo comma prevede che nel caso di contenuti generati dagli utenti su piattaforme di soggetti terzi l'ordine di rimozione riguardi **i soli specifici contenuti illeciti**.

Ai sensi dell'art. 3, paragrafo 3, del regolamento (UE) 2021/784 i prestatori di servizi di *hosting* rimuovono i contenuti terroristici o disabilitano 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.

Il prestatore di servizi informa senza ritardo l'Autorità competente della rimozione dei contenuti o della disabilitazione dell'accesso (paragrafo 6). Il prestatore informa altresì senza ritardo l'Autorità competente nel caso in cui non sia stato in grado di conformarsi all'ordine di rimozione per causa di forza maggiore o per impossibilità di fatto a lui non imputabile, compresi motivi tecnici od operativi obiettivamente giustificabili (paragrafo 7). Il prestatore informa, inoltre, l'Autorità competente e chiede i chiarimenti necessari qualora non sia in grado di conformarsi all'ordine di rimozione in quanto quest'ultimo è viziato da errori manifesti o non contiene informazioni sufficienti (paragrafo 8).

Ai sensi dell'art. 11 del regolamento (UE) 2021/784 il prestatore di servizi di *hosting* mette a disposizione del fornitore di contenuti informazioni sulla rimozione o sulla disabilitazione (paragrafo 1) e, qualora richiesto dal fornitore, comunica i motivi della disabilitazione o rimozione e lo informa dei diritti di ricorso (paragrafo 2). Il prestatore di servizi si astiene tuttavia dal divulgare qualsiasi informazione qualora l'Autorità competente, per motivi di pubblica sicurezza, disponga che la motivazione non sia divulgata per il tempo necessario, non superiore a sei settimane, prorogabili di ulteriori sei settimane (paragrafo 3).

Il **comma 8** stabilisce che, nel caso di **mancato adempimento**, ferma restando l'applicazione delle sanzioni cui all'articolo 7 (*vedi infra*), sia disposta, nelle forme e con le modalità di cui all'art. 321 c.p.p., l'**interdizione dell'accesso al dominio internet**, garantendo comunque, ove tecnicamente possibile, la fruizione dei contenuti estranei alle attività illecite.

L'art. 321 c.p.p. disciplina il sequestro preventivo, prevedendo, al comma 1, che esso sia disposto con decreto motivato dal giudice competente per il merito (prima dell'esercizio dell'azione penale dal giudice per le indagini preliminari) su richiesta del pubblico ministero.

Il sequestro è immediatamente revocato, a richiesta del pubblico ministero o dell'interessato, quando risultano mancanti, anche per fatti sopravvenuti, le condizioni di applicabilità; nel corso delle indagini preliminari alla revoca provvede il pubblico ministero con decreto motivato (comma 3).

Nel corso delle indagini preliminari, quando non sia possibile, per la situazione di urgenza, attendere il provvedimento del giudice, il sequestro è disposto dal pubblico ministero con decreto motivato; negli stessi casi, prima dell'intervento del pm, al sequestro procedono ufficiali di polizia giudiziaria i quali, entro 48 ore, trasmettono il verbale al pm, che, se non dispone la restituzione delle cose sequestrate, richiede al giudice la convalida e l'emissione del decreto di cui al comma 1 entro 48 ore dal sequestro, se disposto dal pm medesimo, o dalla ricezione del verbale, se al sequestro ha proceduto la polizia giudiziaria (comma 3-*bis*).

Il sequestro perde efficacia se non sono osservati i termini di cui al comma 3-*bis* o se il giudice non lo convalida entro 10 giorni dalla ricezione della richiesta (comma 3-*ter*).

Il **comma 9** disciplina l'**opposizione all'ordine di rimozione**, in attuazione del criterio di delega di cui all'art. 15, comma 1, lett. *c* della legge 127/2022, prevedendo che:

- i soggetti legittimati a proporre opposizione siano i **prestatori di servizi di *hosting*** che hanno ricevuto l'ordine di rimozione o i **fornitori dei contenuti** rimossi o resi inaccessibili (*sui prestatori di servizi di* hosting, *vedi* infra *approfondimento specifico)*;
- il **termine** per la presentazione dell'opposizione sia di **dieci giorni** dalla conoscenza del provvedimento;
- l'opposizione sia presentata innanzi al **giudice per indagini preliminari**, che provvede con ordinanza in camera di consiglio;
- avverso l'ordinanza sia ammesso **ricorso per cassazione** unicamente per **violazione di legge**.

Articolo 4
(Esame degli ordini di rimozione transfrontalieri)

L'articolo 4 disciplina l'**esame degli ordini di rimozione transfrontalieri** individuando, in attuazione del principio di delega di cui all'art. 15, comma 1, lett. a), della legge comunitaria 2021, l'autorità competente in materia nel **giudice per le indagini preliminari**. La competenza sugli ordini di rimozione è attribuita a livello **distrettuale**, quindi al gip appartenente al tribunale del capoluogo del distretto:

- in cui è situato lo **stabilimento principale del prestatore di servizi di *hosting***
  o
- in cui **risiede o è stabilito il rappresentante legale** del prestatore di servizi di *hosting*.

Dal punto di vista sostanziale, la competenza del giudice per le indagini preliminari riguarda:

- l'**esame degli ordini di rimozione emessi dall'autorità competente di un altro Stato membro** nel quale il prestatore di servizi di *hosting* non abbia lo stabilimento principale o il rappresentante legale;
- l'assunzione di **decisioni motivate** che stabiliscano **se l'ordine di rimozione violi in modo grave o manifesto il regolamento o i diritti e delle libertà fondamentali** garantiti dalla Carta, previste dall'art. 4, par. 3 e 4, del regolamento.

La **procedura** relativa agli ordini di rimozione transfrontalieri è stabilita dall'art. 4 del regolamento, in base al quale **l'autorità di uno Stato membro** che ha adottato un ordine di rimozione rivolto ad un prestatore di servizi di *hosting* che non ha lo stabilimento principale o il rappresentante legale in tale Stato **è tenuto a trasmetterne una copia**, nel momento stesso dell'adozione dell'ordine, **all'autorità competente dello Stato nel quale si trovano lo stabilimento principale o il rappresentante legale del prestatore** medesimo.

Ferma restando l'immediata precettività dell'ordine di rimozione nei confronti del prestatore di servizi di *hosting*, che è tenuto ad adottare le misure indicate dall'art. 3 del regolamento (v. *supra*, art. 3), l'ordine di rimozione è esaminato da quest'ultima autorità al fine di **stabilire se esso violi in modo grave o manifesto il regolamento o i diritti e delle libertà fondamentali garantiti dalla Carta**:

- **di propria iniziativa, entro 72 ore** dal ricevimento della copia dell'ordine di rimozione; in caso sia riscontrata la violazione, l'autorità nel medesimo termine adotta una decisione motivata;

- **su richiesta del prestatore di servizi di *hosting* o del fornitore di contenuti**, presentata rispettivamente **entro 48 ore** dal ricevimento dell'ordine di rimozione o dalla comunicazione ricevuta da parte del prestatore di servizi di *hosting* circa i motivi della rimozione; anche in questo caso, **l'autorità decide entro 72 ore** dal ricevimento della richiesta, esponendo nella decisione le proprie conclusioni sull'esistenza di una violazione.

In entrambi i casi, l'autorità competente deve **comunicare** tempestivamente **la decisione motivata all'autorità dell'altro Stato membro** che ha emesso l'ordine di rimozione, **al prestatore di servizi di *hosting***, eventualmente **al fornitore di contenuti**, qualora questi abbia proposto richiesta di esame, e **ad Europol**.

Qualora la decisione accerti la sussistenza di una violazione, l'ordine di rimozione cessa di avere effetti giuridici; in tal caso il prestatore di servizi di *hosting* ripristina immediatamente i contenuti o l'accesso agli stessi.

Sempre in attuazione del citato principio di delega di cui all'art. 15, comma 1, lett. a), **il gip trasmette** immediatamente **copia dell'ordine di rimozione transfrontaliero al Procuratore nazionale antimafia** e antiterrorismo o, comunque, prima di assumere le decisioni motivate che accertano la sussistenza di violazioni gravi o manifeste del presente regolamento o dei diritti e delle libertà fondamentali, previste dall'art. 4, par. 3 e 4, del regolamento.

Le decisioni, ai sensi del comma 2, sono adottate con decreto motivato, sentito il pubblico ministero. Qualora il decreto sia stato adottato a seguito di richiesta presentata dal prestatore di servizi di *hosting* o dal fornitore di contenuti, i medesimi soggetti hanno facoltà, entro 10 giorni dal deposito, di proporre **ricorso per cassazione** esclusivamente **per violazione di legge**. Tale disposizione attua il principio di delega di cui all'art. 15, comma 1, lett. e), secondo cui devono essere previsti effettivi strumenti di tutela in favore dei prestatori di servizi di *hosting* e dei fornitori di contenuti.

Articolo 5
(Prestatori di servizi di hosting esposti a contenuti terroristici)

L'**articolo 5** conferisce all'Organo del Ministero dell'interno per la sicurezza e la regolarità dei servizi di telecomunicazione (su cui, si v. *supra*, *l*a scheda dell'articolo 2) alcune attribuzioni che contribuiscono all'attuazione nazionale delle disposizioni del regolamento (UE) 2021/784.

In particolare, l'organo del Ministero dell'interno viene individuato come l'autorità nazionale competente ad:

- **adottare le decisioni con cui**, ai sensi dell'art. 5, par. 4 del regolamento, **si accerta che il prestatore di servizi di hosting è «esposto a contenuti terroristici»**. La decisione deve essere basata su fattori oggettivi, come richiede il regolamento, come ad esempio il ricevimento da parte del prestatore di servizi di hosting di due o più ordini di rimozione definitivi nei 12 mesi precedenti. Una volta adottata la decisione va notificata al prestatore di servizi;
- **sorvegliare l'attuazione delle misure** specifiche che, a seguito dell'accertamento svolto, il prestatore di servizi di hosting è tenuto ad adottare;
- emettere le **ulteriori decisioni** previste dal regolamento ai sensi del medesimo articolo 5, paragrafi 6 e 7, nei casi di insufficienza delle misure poste in essere dal prestatore di servizi ovvero nei casi di riesame, modifica e revoca delle decisioni già adottate.

In proposito, l'articolo 5, paragrafo 6 del regolamento stabilisce che ove, sulla base di fattori oggettivi, l'autorità competente ritiene che le misure specifiche adottate non soddisfino le prescrizioni di cui ai paragrafi 2 e 3, tale autorità competente indirizza al prestatore di servizi di hosting una decisione che gli impone di adottare ulteriori misure specifiche
Il paragrafo 7 prevede che il prestatore di servizi di hosting può, in qualsiasi momento, chiedere all'autorità competente il riesame e, eventualmente, la modifica o la revoca delle decisioni già adottate. Entro tre mesi dal ricevimento della richiesta, l'autorità competente adotta una decisione motivata in merito alla richiesta basata su fattori oggettivi e la notifica al prestatore di servizi di hosting.

Ai sensi del **comma 2**, le decisioni assunte dall'Organo del Ministero dell'interno possono essere impugnate dal prestatore di servizi di *hosting* dinanzi al competente **tribunale amministrativo regionale** entro sessanta giorni dalla notifica.

Articolo 6
(Sanzioni amministrative)

L'articolo 6 disciplina il **regime sanzionatorio**, regolandone anche il procedimento di applicazione, prevedendo gruppi di illeciti, di gravità crescente e configurabili solo quando il fatto non integri reato.

Più nel dettaglio **l'articolo 6**, in attuazione dei **criteri di delega di cui alle lett. c) e d)** del comma 1, dell'articolo 15 della legge n. 127 del 2022, disciplina le **sanzioni amministrative**.

Le lettere c) e d) del comma 1 dell'articolo 15 della legge di delegazione europea 2021, impongono al Governo nell'esercizio della delega di prevedere, per le violazioni delle disposizioni indicate all'articolo 18 del Regolamento (UE) 2021/784, **sanzioni efficaci**, **dissuasive e proporzionate** alla gravità delle violazioni medesime, nonché di individuare le **Autorità competenti a irrogare le sanzioni** e a vigilare sull'osservanza delle disposizioni del Regolamento (UE) 2021/784.

Per garantire l'efficacia delle disposizioni del Regolamento, l'art. 18 dello stesso Regolamento impone agli Stati di imporre sanzioni a carico degli *hosting providers* per la violazione delle principali decisioni delle autorità nazionali. Tali sanzioni debbono essere effettive, proporzionate e dissuasive, e la loro entità deve tener conto di una serie di circostanze. Infine, in caso di sistematica o persistente inosservanza delle decisioni di rimozione, molto efficace è prevista la possibilità di imporre sanzioni pecuniarie a carico del prestatore inadempiente fino al 4% del fatturato mondiale del precedente esercizio finanziario. Occorre ricordare con riguardo alla **tipologia delle sanzioni da imporre**, che il *considerando n. 45* del Regolamento precisi che tali **sanzioni** possono **essere sia di natura amministrativa che penale**.

Il **comma 1** assoggetta alla **sanzione amministrativa pecuniaria da 25.000 a 100.000 euro** il prestatore di servizi di *hosting* che:

a) **non informa tempestivamente**, mediante il modello di cui all'allegato II del Regolamento, **l'autorità che ha emesso l'ordine di rimozione dell'avvenuta esecuzione dell'ordine**, indicandone in particolare la data e l'ora, secondo quanto previsto dall'art.3 del Regolamento;

L'articolo 18 del Regolamento impone agli Stati membri di sanzionare, tra gli altri le violazioni di cui all'art. 3, par. 6, del Regolamento. Tale disposizione impone, per l'appunto, al prestatore di servizi di *hosting* di informare senza

indebito ritardo l'autorità competente utilizzando il modello di cui all'allegato II del Regolamento, della rimozione dei contenuti terroristici o della disabilitazione dell'accesso ai contenuti in tutti gli Stati membri, indicando, in particolare, la data e l'ora della rimozione o disabilitazione.

b) **rimuove i contenuti terroristici** o disabilita l'accesso ai contenuti terroristici (la rimozione o la disabilitazione - occorre ricordare – deve avvenire il prima possibile e in ogni caso entro un'ora dal ricevimento dell'ordine di rimozione), **omettendo di adottare le misure necessarie per ripristinare i contenuti** o riabilitare l'accesso agli stessi (art. 4, par. 2, seconda ipotesi, del Regolamento);

c) dopo aver ricevuto una decisione emessa dall'autorità competente ai sensi dell'articolo 4, par. 6, del Regolamento, **omette di ripristinare immediatamente i contenuti o l'accesso agli stessi**, fatta salva la possibilità di applicare le proprie condizioni contrattuali conformemente al diritto dell'Unione e nazionale (art. 4, par. 7, del Regolamento);

L'articolo 18 del Regolamento impone agli Stati membri di sanzionare le violazioni di cui all'art. 4, par. 2 e 7, del Regolamento. L'articolo 4 del Regolamento disciplina la **procedura per gli ordini di rimozione transfrontalieri**. Come accennato ai sensi dell'art. 3, le autorità nazionali competenti possono emettere ordini di rimozione a carico dei prestatori dei servizi di *hosting* presenti sul proprio territorio, i quali devono essere eseguiti al massimo entro un'ora dal loro ricevimento. In caso di procedura transfrontaliera ex art. 4, par.3 del Regolamento, invece, l'ordine andrà trasmesso anche all'autorità nazionale competente per territorio la quale potrà esaminarlo entro 72 ore per stabilire se viola in modo grave o manifesto il Regolamento o la Carta di Nizza. Per gli stessi motivi, gli *hosting providers* colpiti dall'ordine di rimozione e i fornitori dei contenuti considerati terroristici hanno facoltà di ricorrere all'autorità competente per territorio entro 48 ore affinché adotti una decisione entro le successive 72 ore (par. 4). L'accertamento della contrarietà dell'ordine di rimozione transfrontaliero con il Regolamento 2021/784 o la Carta di Nizza comporta la cessazione dei suoi effetti giuridici e il ripristino dei contenuti prima rimossi o disabilitati. E' comunque fatta salva la possibilità di applicare le proprie condizioni contrattuali conformemente al diritto dell'Unione e nazionale (par. 6 e 7).

d) non osserva le disposizioni di cui all'articolo 6 del Regolamento nella **conservazione dei contenuti terroristici rimossi** o il cui accesso è stato disabilitato, ovvero **nella conservazione dei relativi dati**;

dinanzi alle giurisdizioni dello Stato competente avverso tutte le decisioni assunte dalle autorità nazionali (art. 9). A loro volta, l'art. 10 del Regolamento riconosce agli utenti fornitori dei contenuti rimossi o disabilitati il diritto di poter presentare un **reclamo** interno diretto alla reintegrazione di quanto rimosso o disabilitato (par. 1). Ai sensi del par. 2 dell'art. 10, ciascun *hosting provider* deve esaminare tempestivamente ogni reclamo e ripristinare i contenuti o il relativo accesso senza indebito ritardo se la rimozione o la disabilitazione si rivela ingiustificata. L'autore del reclamo delle conclusioni del reclamo deve essere informato entro due settimane dal ricevimento del reclamo. Qualora il reclamo sia rigettato, il prestatore di servizi di hosting fornisce al reclamante i motivi della propria decisione. Il ripristino dei contenuti o dell'accesso allo stesso non osta all'avvio di procedimenti di controllo amministrativi o giurisdizionali che impugnino la decisione del prestatore di servizi di hosting o dell'autorità competente.

g) fuori dei casi di cui all'articolo 11, par. 3, del Regolamento, **omette di comunicare al fornitore di contenuti le informazioni sui motivi delle decisioni** assunte dai *providers* di rimozione o disabilitazione di determinati contenuti (ex par. 1 e 2 art. 11);

L'articolo 18 del Regolamento impone agli Stati membri di sanzionare le violazioni di cui all'art. 11 del Regolamento, il quale riconosce agli utenti fornitori dei contenuti rimossi o disabilitati il diritto di ricevere informazioni sui motivi di siffatte decisioni assunte dai *providers*. Il par.1 dell'art. 11, nello specifico prevede che il prestatore di servizi di *hosting*, quando rimuove o disabilita l'accesso a contenuti terroristici, deve mettere a disposizione del fornitore di contenuti informazioni concernenti tale rimozione o disabilitazione. Ai sensi del par. 2 dell'art. 11, su richiesta del fornitore di contenuti, il prestatore di servizi di *hosting* comunica i motivi della rimozione o della disabilitazione al fornitore di contenuti e lo informa dei diritti di ricorso contro l'ordine di rimozione o gli fornisce copia dell'ordine di rimozione. Il par. 3 esonera l'*hosting provider* da tali obblighi informativi, nei casi in cui l'autorità competente che emette l'ordine di rimozione decide che è necessario e proporzionato, che la motivazione non sia divulgata per motivi di pubblica sicurezza, quali la prevenzione, l'indagine, l'accertamento e il perseguimento di reati di terrorismo, per il tempo necessario, ma non superiore a sei settimane dalla suddetta decisione. In tal caso, il prestatore di servizi di *hosting* si astiene dal divulgare qualsiasi informazione concernente la rimozione o la disabilitazione dell'accesso a contenuti terroristici. L' autorità competente può prorogare tale termine di ulteriori sei settimane, ove tale non divulgazione continui a essere giustificata.

h) omette di informare l'Organo del Ministero dell'interno per la sicurezza e la regolarità dei servizi di telecomunicazione e la

competente Direzione Generale del Ministero delle imprese e del *made in Italy* (attualmente la Direzione generale per i servizi di comunicazione elettronica, di radiodiffusione e postali e, in particolare, gli Ispettorati territoriali) della **designazione del rappresentante legale**, comunicando la relativa accettazione, o di rendere pubbliche le informazioni relative al rappresentante legale designato (art. 17, par. 4, del Regolamento).

L'articolo 18 del Regolamento impone agli Stati membri di sanzionare le violazioni di cui all'art. 17 del Regolamento, che disciplina la figura del **rappresentante legale**. Il prestatore che non ha il proprio stabilimento principale nell'UE ha l'obbligo, infatti, di designare una persona fisica o giuridica quale suo rappresentante legale ai fini del ricevimento, dell'attuazione e dell'esecuzione degli ordini di rimozione nonché di tutte le altre decisioni emesse dalle autorità competenti (art. 17, par. 1). Il prestatore di servizi di *hosting* conferisce al proprio rappresentante legale i poteri e le risorse necessari per ottemperare a tali ordini di rimozione e decisioni e per cooperare con le autorità competenti. Il rappresentante legale risiede o è stabilito in uno degli Stati membri in cui il prestatore di servizi di *hosting* offre i propri servizi (art. 17, par. 2). Il rappresentante legale può essere ritenuto responsabile per le violazioni del presente Regolamento, fatte salve le responsabilità e le azioni legali del prestatore di servizi di hosting. (art. 17, par.3). Il par. 4 dell'art. 17 del Regolamento impone al prestatore di servizi di *hosting* di informare della designazione l'autorità competente dello Stato membro in cui il suo rappresentante legale risiede o è stabilito. Il prestatore di servizi di hosting rende pubbliche le informazioni relative al rappresentante legale.

Il **comma 2** punisce invece con la **sanzione amministrativa pecuniaria** da 50.000 a 200.000 euro il **prestatore di servizi di *hosting* esposto a contenuti terroristici** che:

- **non include nelle sue condizioni contrattuali** o non applica disposizioni volte a contrastare l'uso improprio dei suoi servizi per la diffusione al pubblico di contenuti terroristici (art. 5, par. 1, co. 1, del Regolamento);
- **non osserva taluno degli obblighi di condotta** di cui all'articolo 5, par.1, del Regolamento (art. 5, par. 1, co. 2, del Regolamento);
- adotta misure specifiche prive di taluno dei requisiti di cui all'articolo 5, par. 3, del Regolamento;
- dopo aver ricevuto una decisione di cui all'articolo 5, par. 4 o 6, del Regolamento, **omette di comunicare** all'Organo del Ministero dell'interno per la sicurezza e la regolarità dei servizi di telecomunicazione, nei tre mesi dal ricevimento della decisione o ad una delle successive cadenze annuali, **le misure specifiche che ha adottato** e che intende adottare per conformarsi alle

disposizioni di cui ai par. 2 e 3 del medesimo articolo 5 (art. 5, par. 5, del Regolamento).

L'articolo 18 del Regolamento impone agli Stati membri di sanzionare le violazioni di cui all'art. 5 del Regolamento, il quale prevede **obblighi di autoregolamentazione** a carico degli ***hosting providers*** **particolarmente esposti a contenuti terroristici**. **Un *provider* identificato come "esposto"** da parte dell'autorità nazionale competente (in quanto, nei 12 mesi precedenti, ha ricevuto due o più ordini di rimozione definitivi) deve prevedere nelle proprie condizioni di servizio e applicare disposizioni per contrastare l'uso improprio dei servizi per la diffusione al pubblico di contenuti terroristici. Le specifiche **misure di protezione** possono comprendere misure o capacità tecnico-operative, meccanismi di segnalazione da parte degli utenti, meccanismi di moderazione dei contenuti e qualsiasi altra misura idonea. Tali misure devono essere comunicate all'autorità nazionale competente, la quale, se le reputa insufficienti, gliene impone di proprie (senza tuttavia poter stabilire obblighi generali di sorveglianza e di accertamento attivo dei contenuti terroristici nonché l'obbligo di utilizzare strumenti automatizzati). La decisione di esposizione e quelle contenenti le misure ritenute necessarie dall'autorità nazionali possono essere riesaminate, modificate o revocate.

Il **comma 3**, infine, prevede l'applicazione della sanzione amministrativa pecuniaria da 75.000 a 300.000 euro nei confronti del **prestatore di servizi di *hosting* esposto a contenuti terroristici** che:

- omette di adottare misure specifiche per proteggere i propri servizi dalla **diffusione al pubblico** di contenuti terroristici ai sensi dell'articolo 5, par. 2, del Regolamento;
- dopo aver ricevuto una decisione di cui all'articolo 5, par. 6, omette di adottare le misure imposte dalla decisione per garantire il rispetto delle disposizioni di cui ai paragrafi 2 e 3 del medesimo articolo 5 (art. 5, par. 6, del Regolamento).

Nello specifico il par. 2 dell'art. 5, come già ricordato, impone al prestatore di servizi di *hosting* esposto a contenuti terroristici di adottare misure specifiche per proteggere i propri servizi dalla diffusione al pubblico di contenuti terroristici. La decisione in merito alla scelta delle misure specifiche spetta al prestatore di servizi di *hosting*. Il par. 6 dell'art. 5 prevede invece che le misure debbano essere comunicate all'autorità nazionale competente, la quale, se le reputa insufficienti, può imporne di proprie.

Il **comma 4** individua le **autorità competenti ad irrogare le sanzioni**, negli Ispettorati territoriali della competente Direzione Generale del Ministero delle imprese e del *made in Italy* (attualmente la Direzione generale per i servizi di comunicazione elettronica, di radiodiffusione e

postali e, in particolare, gli Ispettorati territoriali), che procedono ai sensi della legge 24 novembre 1981, n. 689, a seguito delle comunicazioni da parte dell'Organo del Ministero dell'interno per la sicurezza delle telecomunicazioni, al quale compete invece l'accertamento e la contestazione delle violazioni. La medesima disposizione prevede, inoltre, che – fatta salva l'ipotesi di cui all'articolo 24 della legge n. 689/81 – il rapporto di accertamento e di contestazione delle violazioni sia presentato al Ministero delle imprese e del *Made in Italy* e che, in deroga all'articolo 8-*bis* della legge n. 689/81, la **reiterazione delle violazioni** operi anche nel caso di pagamento in misura ridotta.

L'articolo 8 della legge n. 689 del 1981, rubricato "Reiterazione delle violazioni" è stato introdotto nell'originario impianto della legge n. 689 dall'articolo 94 del decreto legislativo n. 507 del 1999. La norma fornisce la nozione di reiterazione stabilendo che essa sussiste quando nei 5 anni successivi alla commissione di una violazione amministrativa, accertata con provvedimento esecutivo lo stesso soggetto commette un'altra violazione della stessa indole. Il comma 5 dell'art. 8 precisa che la reiterazione non operi in caso di pagamento in misura ridotta.

Il **comma 5**, trasponendo quanto previsto dall'articolo 18, par. 2, del Regolamento, dispone che nella **determinazione della sanzione** si debba aver riguardo a tutte le circostanze rilevanti, tra cui:

- ✓ la natura, la gravità e la durata della violazione;
- ✓ il carattere doloso o colposo della violazione;
- ✓ le precedenti violazioni commesse dal prestatore di servizi di *hosting*;
- ✓ le condizioni patrimoniali, economiche e finanziarie del prestatore di servizi di *hosting* (Il Regolamento, art. 18, par. 1, lett. d) richiama la "solidità finanziaria" del prestatore di servizi);
- ✓ la cooperazione del prestatore di servizi di *hosting* con le autorità competenti
- ✓ l'attività svolta dal prestatore di servizi di *hosting* per l'eliminazione o attenuazione delle conseguenze della violazione (tale circostanza non è espressamente richiamata nell'elenco – un elenco di carattere esemplificativo – di cui al par.2 dell'art. 18 del Regolamento);
- ✓ la natura e le dimensioni del prestatore di servizi di hosting;
- ✓ il grado di colpa del prestatore di servizi di hosting, tenuto conto delle misure tecniche e organizzative adottate dal prestatore di servizi di hosting per conformarsi al Regolamento e al presente decreto.

Il **comma 6** stabilisce che i proventi derivanti dalle **sanzioni amministrative pecuniarie** in esame debbano essere versati in un apposito capitolo dell'entrata del bilancio dello Stato, per essere riassegnate, in egual misura, con decreto del Ministero dell'economia e delle finanze, al Ministero dell'interno e al Ministero delle imprese e del *Made in Italy*, ai fini dell'integrazione delle risorse già destinate a legislazione vigente all'attuazione delle disposizioni di cui al presente articolo.

Il **comma 7** prevede infine che l'Organo del Ministero dell'Interno per la sicurezza e la regolarità dei servizi di telecomunicazione coopera con il Ministero delle Imprese e del *Made in Italy* per gli aspetti relativi ai precedenti commi, sulla base di una convenzione operativa sottoscritta dal Ministero dell'Interno e dal Ministero delle imprese e del *Made in Italy*, entro novanta giorni dall'entrata in vigore del presente decreto legislativo.

Articolo 7
(Sanzioni penali)

L'articolo 7 reca le sanzioni penali, prevedendo gruppi di illeciti, di gravità crescente e configurabili solo quando il fatto non integri più grave reato.

La disciplina delle sanzioni penali è stabilita dal presente articolo in attuazione del criterio di delega di cui alla lettera *c)* del comma 1, dell'articolo 15 della legge n. 127 del 2022 (Legge di delegazione europea 2021).

Come già ricordato in sede di commento all'articolo 6 inerente alle sanzioni amministrative, la citata lettera *c)* del comma 1 dell'articolo 15 della legge di delegazione europea 2021, impone al Governo, nell'esercizio della delega, di prevedere **sanzioni efficaci** per le violazioni delle disposizioni indicate all'articolo 18 del regolamento (UE) 2021/784.

Per garantire l'efficacia delle disposizioni del Regolamento, il suo art. 18 impone agli Stati di prevedere sanzioni a carico degli *hosting providers* per la violazione delle principali decisioni delle autorità nazionali. Tali sanzioni debbono essere effettive, proporzionate e dissuasive, e la loro entità deve tener conto di una serie di circostanze. Inoltre, in caso di sistematica o persistente inosservanza delle decisioni di rimozione, molto efficace sembra la possibilità di imporre sanzioni pecuniarie a carico del prestatore inadempiente fino al 4% del fatturato mondiale del precedente esercizio finanziario (par. 3 dell'art. 18). Occorre infine ricordare con riguardo alla **tipologia delle sanzioni da imporre**, che il *considerando n. 45* del Regolamento precisi che tali **sanzioni potranno essere sia di natura amministrativa che penale**.

Il **comma 1** punisce con l'**arresto fino a sei mesi oppure con** l'**ammenda da 100.000 a 400.000 euro** il **prestatore di servizi di *hosting*** che, salvo che il fatto costituisca più grave reato:

i) omette di designare o istituire, violando l'art. 15, par. 1, del Regolamento, un **punto di contatto** per la ricezione e l'immediata esecuzione degli **ordini di rimozione** in via telematica, oppure omette di fornire al pubblico le informazioni inerenti ai medesimi punti di contatto istituiti o designati;

j) omette, quando non abbia lo stabilimento principale nell'Unione europea, di designare per iscritto una persona fisica o giuridica quale **rappresentante legale** all'interno dell'Unione al fine di ricevere e dare seguito agli ordini di rimozione impartiti o alle altre decisioni assunte dalle autorità competenti; le medesime sanzioni si applicano quando il rappresentante legale designato non risieda o non sia stabilito in uno degli Stati membri in cui il prestatore di servizi di *hosting* offre i propri servizi oppure quando il rappresentante legale non abbia ricevuto i poteri o le risorse necessari per ottemperare agli ordini di rimozione e

a collaborare con le autorità (violazioni di quanto previsto dall'art. 17 del Regolamento).

L'articolo 18 del Regolamento impone agli Stati membri di sanzionare, tra l'altro, le violazioni di cui all'art. 15, par. 1, e 17, del Regolamento medesimo.
L'articolo 15, par. 1, impone ai servizi di *hosting* di designare o istituire un **punto di contatto** per la ricezione degli ordini di rimozione per via elettronica e per il rapido adempimento degli ordini secondo quanto previsto dagli articoli 3 e 4 del Regolamento medesimo. Il prestatore di servizi di *hosting* - prosegue il paragrafo 1 – deve provvedere a rendere disponibili al pubblico le informazioni relative al punto di contatto medesimo.
L'articolo 17 del Regolamento reca la disciplina inerente al **rappresentante legale**. Tale articolo 17, ai paragrafi 1 e 2, prevede che il prestatore di servizi di *hosting* che non abbia il proprio stabilimento principale nell'Unione europea designi, per iscritto, una persona fisica o giuridica quale suo rappresentante legale nell'Unione ai fini del ricevimento, dell'attuazione e dell'esecuzione degli ordini di rimozione e delle altre decisioni emesse dalle autorità competenti. La disposizione pone esplicitamente in capo al prestatore di servizi di *hosting* conferisca al proprio rappresentante legale i poteri e le risorse necessari per ottemperare a tali ordini di rimozione e decisioni e per cooperare con le autorità competenti.

Nei suddetti casi previsti dal comma 1, il **comma 4** prevede che l'autorità giudiziaria possa disporre l'**interdizione dell'accesso al dominio *internet*** al prestatore di servizi di *hosting* che non provveda agli adempimenti omessi nei **15 giorni** successivi all'accertamento e alla contestazione delle violazioni. Si applica l'art. 321 del codice di procedura penale.

Si rammenta che l'art. 321 c.p.p. (concernente l'oggetto del sequestro preventivo) prevede che il giudice competente a pronunciarsi nel merito dispone con decreto motivato il sequestro, a richiesta del PM, della cosa pertinente al reato, quando vi sia pericolo che la libera disponibilità della medesima possa aggravare o protrarre le conseguenze del reato ovvero agevolare la commissione di altri reati.

Il **comma 2** punisce con l'**arresto fino a sei mesi e con** l'**ammenda da 100.000 a 400.000 euro** il **prestatore di servizi di *hosting*** e il **rappresentante legale** che, salvo che il fatto costituisca più grave reato:

a) omettono di ottemperare all'**ordine di rimozione** del contenuto terroristico entro un'ora dal ricevimento o di **disabilitare l'accesso** a tali contenuti entro il medesimo termine;
b) **forniscono informazioni riguardanti la rimozione o la disabilitazione** in parola, in violazione dell'art. 11, par. 3, del Regolamento;

c) **non informano** immediatamente l'autorità giudiziaria o altra autorità competente circa la **presenza *online* di contenuti terroristici**, in violazione dell'art. 14, par. 5, del Regolamento.

L'articolo 18 del Regolamento impone agli Stati membri di sanzionare, tra l'altro, le violazioni di cui all'art. 11 e all'art. 14, par. 5, del Regolamento medesimo.
L'art. 11 richiamato, ai paragrafi 1 e 2, reca disciplina concernente le informazioni ai fornitori di contenuti terroristici in caso di rimozione o disabilitazione dell'accesso. L'omessa comunicazione è punita ai sensi dell'art. 6, comma 1, lettera g), dello schema di decreto in esame, in materia di sanzioni amministrative (si rinvia alla relativa scheda). Il par. 3 del medesimo articolo 11 stabilisce che tali obblighi di comunicazione non si applichino quando l'autorità competente ad emettere l'ordine di rimozione decide che le informazioni relativa alla rimozione o disabilitazione all'accesso non siano divulgata, per motivi di pubblica sicurezza ivi specificati, per un tempo necessario, non superiore a sei settimane dalla suddetta decisione. Tale termine è prorogabile di ulteriori sei settimane ove la non divulgazione continui ad essere giustificata. In tali circostanze, il prestatore di servizi di *hosting* deve quindi astenersi dal divulgare qualsiasi informazione concernente la rimozione o la disabilitazione dell'accesso a contenuti terroristici.
L'art. 14, par. 5, dispone invece che il prestatore di servizi di *hosting* deve informare immediatamente l'autorità competente della presenza di contenuti terroristici *online* di cui sia venuto a conoscenza. Il medesimo par. 5 disciplina i casi in cui non sia possibile individuare gli Stati membri interessati.

Il **comma 3** disciplina la sanzione applicabile al **prestatore di servizi di *hosting*** e al **rappresentante legale** quando l'omessa rimozione o disabilitazione entro un'ora abbia carattere **sistematico** e **persistente**.

In tali casi la sanzione consiste nell'**arresto fino a un anno** e nell'**ammenda** pari ad una somma **da 250.000 a 1.000.000 euro** oppure pari al **4% del fatturato realizzato a livello mondiale dal prestatore di servizi di *hosting*, nell'ultimo esercizio chiuso anteriormente all'accertamento della violazione, se superiore**.

Come sopra accennato, la possibilità di irrogare la sanzione pecuniaria fino al 4% del fatturato mondiale del prestatore di servizi di *hosting* del precedente esercizio finanziario è esplicitamente prevista dall'art. 18, par. 3, del Regolamento.

Per il **comma 4**, v. *sopra*.

Il **comma 5** stabilisce che le disposizioni del presente articolo non si applichino al rappresentante legale che abbia comunicato, entro 15 giorni dalla sua designazione, di non disporre dei poteri e delle risorse necessari al corretto svolgimento delle proprie funzioni. Tale comunicazione è effettuata

all'organo del Ministero dell'interno per la sicurezza delle telecomunicazioni e alla competente Direzione Generale del Ministero delle imprese e del *made in Italy* (attualmente la Direzione generale per i servizi di comunicazione elettronica, di radiodiffusione e postali e, in particolare, gli Ispettorati territoriali).

Articolo 8
(Abrogazioni)

L'articolo 8 prevede l'abrogazione dell'articolo 2, comma 4, del decreto-legge 18 febbraio 2015, n. 7, convertito, con modificazioni, dalla legge 17 aprile 2015, n. 43 recante disciplina del decreto di rimozione dei contenuti pubblicati sui siti internet adottato dal PM nell'ambito dell'attività investigativa finalizzata alla repressione dei reati di cui agli articoli 270-bis e ss. c.p. commessi con le finalità di terrorismo.

Più nel dettaglio **l'articolo 8** abroga il comma 4 dell'articolo 2, del decreto-legge 18 febbraio 2015, n. 7, in quanto la disciplina ivi contenuta risulta assorbita da quanto previsto dai commi 5 e 8 dell'articolo 3 (*si veda la scheda di lettura*) del provvedimento in esame proprio con riferimento all'**ordine di rimozione emesso dal PM** e all'interdizione dell'accesso al dominio *internet* in conseguenza del mancato adempimento del predetto ordine**.**

A tal proposito nella **Analisi tecnico normativa** si precisa con riferimento alla disposizione abroganda che la nuova regolamentazione: " contempla anche l'ipotesi in cui non sia ravvisabile una *notitia criminis* o il contenuto terroristico da rimuovere non sia comunque riferibile a un'indagine in corso, e purtuttavia si pone l'esigenza di rimozione di contenuti terroristici all'infuori di un'indagine in corso; in tal caso, in deroga rispetto alla previsione generale che riferita alle disposizioni del codice di procedura penale, la competenza viene radicata nell'ufficio del pubblico ministero del tribunale del capoluogo del distretto che ha acquisito per primo la notizia relativa alla presenza sulle reti di telecomunicazioni disponibili al pubblico dei contenuti terroristici; il precedente riferimento al termine di quarantotto ore dalla ricezione della notifica del decreto di rimozione per l'esecuzione del medesimo viene ora riallineato dalla disposizione sanzionatoria di cui all'articolo 7, comma 2, lettera a) del decreto legislativo al termine di un'ora previsto dall'art. 3, paragrafo 3, del Regolamento; mantiene la possibilità di disporre, in caso di inadempimento dell'ordine di rimozione, l'interdizione dell'accesso al dominio internet («garantendo comunque, ove tecnicamente possibile, la fruizione dei contenuti estranei alle condotte illecite») nelle forme e con le modalità di cui all'articolo 321 del codice di procedura penale (articolo 3, comma 8)".

Articolo 9
(Clausola di invarianza finanziaria)

L'**articolo 9** reca la **clausola di invarianza finanziaria**, prevedendo che dall'attuazione del decreto non derivino nuovi o maggiori oneri a carico della finanza pubblica e che le amministrazioni interessate provvedano agli adempimenti previsti dal decreto con le risorse umane, strumentali e finanziarie disponibili a legislazione vigente.

PRESTATORI DI SERVIZI DI *HOSTING* E FORNITORI DI CONTENUTI *ONLINE*

(definizione, normativa e giurisprudenza)

I **prestatori di servizi di hosting** (c.d. ***hosting provider***) e i **fornitori di contenuti *online*** sono solo alcune delle figure professionali che operano nel settore della comunicazione via internet. Al proposito, occorre innanzitutto ricordare che la nozione di **sito *Internet*** è piuttosto generica, potendosi - in via di approssimazione – individuarsi:

- **siti di soggetti che esercitano un controllo sulle proprie pagine** (il sito di un ente pubblico, di un'impresa commerciale, di un'associazione, eccetera);
- **siti che fungono da servizio per contenuti altrui** (i c.d. ***provider***: per esempio, i motori di ricerca, Youtube, Facebook, eccetera);
- **siti che – senza essere *provider* – producono contenuti propri ma consentono l'inserimento di messaggi pubblici degli utenti** (per esempio: commenti, *likes*, eccetera). In tali casi si parla anche di **piattaforme di condivisione.**

Con specifico riferimento ai **prestatori di servizi di *hosting***, essi sono – come spiega la stessa etimologia del termine, dall'inglese ***to host,* ospitare** - soggetti che mettono a disposizione, dietro corrispettivo, piattaforme *online* destinate ad essere riempite di contenuti da utenti o fornitori di contenuti *online*.

In una fattispecie nella quale coesistono le due figure di colui che mette a disposizione uno spazio vuoto (l'*hosting provider*) e di colui che vi immette dei contenuti (l'utente o il fornitore di contenuti *online*) il primo e principale problema è, all'evidenza, l'identificazione del soggetto cui imputare eventuali **responsabilità** per la diffusione di contenuti illeciti, ad esempio perché in violazione della normativa in materia di tutela del **diritto d'autore.**

Su tale aspetto si sono concentrati, soprattutto negli ultimi anni, gli interventi normativi, nonché diverse pronunce giurisprudenziali.

Il punto di partenza nella ricostruzione normativa è il **decreto legislativo n. 70 del 2003** (di attuazione della direttiva 2000/31/CE relativa a taluni aspetti giuridici dei servizi della società dell'informazione nel mercato interno, con particolare riferimento al commercio elettronico), il cui **articolo 17 esclude** l'esistenza di un obbligo generale, per il *provider*, di sorvegliare sulle informazioni che trasmette o memorizza, come pure di ricercare attivamente fatti o circostanze che indichino la presenza di attività illecite.

Con specifico riferimento all'attività di memorizzazione di informazioni (*hosting*), l'**articolo 16** analogamente **esclude** che, nella prestazione di un servizio della società dell'informazione, consistente nella memorizzazione di

informazioni fornite da un destinatario del servizio, il prestatore sia responsabile delle informazioni memorizzate a richiesta di un destinatario del servizio, **a condizione che** detto prestatore:

a) **non sia effettivamente a conoscenza** del fatto che l'attività o l'informazione è illecita e, per quanto attiene ad azioni risarcitorie, non sia al corrente di fatti o di circostanze che rendono manifesta l'illiceità dell'attività o dell'informazione;
b) non appena a conoscenza di tali fatti, su comunicazione delle autorità competenti, **agisca immediatamente** per rimuovere le informazioni o per disabilitarne l'accesso.

Nel corso di questa Legislatura è stata presentata una proposta di legge (**A.C. 891,** qui il *dossier* di documentazione) in materia di prevenzione e contrasto del fenomeno del cyberbullismo che, agli articoli da 2 a 5, regola alcuni aspetti tecnici riferiti ai siti *Internet* al fine di consentire l'individuazione chiara delle responsabilità.

Più nel dettaglio, l'articolo 2 prescrive – al comma 1 - che ogni sito *Internet* debba avere un **amministratore responsabile**, individuato tra soggetti in possesso di requisiti stabiliti con regolamento dell'AGCOM. La figura del responsabile del sito ha lo scopo di assicurare la **libera, trasparente e responsabile utilizzazione della rete** e sostanzialmente richiama l'applicazione, nella più generale comunicazione *online*, di principi analoghi a quelli vigenti per la **stampa** (art. 57 c.p. e legge n. 47 del 1948) – validi, secondo taluna giurisprudenza (v. Cassazione, sez. V penale, 11 dicembre 2017, n. 13398) anche per le testate *online* di giornali cartacei registrati.

Oltre a dover predisporre nella pagina principale del sito una **sezione** dedicata e facilmente individuabile e un indirizzo PEC, che consentano una comunicazione certa ed efficace con gli utenti, l'amministratore responsabile del sito ha anche gli **obblighi** di:

- fornire alle autorità competenti in materia di prevenzione e contrasto del cyberbullismo le **informazioni** che consentano l'identificazione dell'utente dei suoi servizi, al fine di individuare e prevenire attività illecite;
- **rimuovere**, entro 96 ore dalla pubblicazione, contenuti illeciti o gravemente lesivi della dignità della persona che siano segnalati o di cui sia venuto a conoscenza;
- adottare gli strumenti di **filtraggio** di contenuti offensivi della dignità e gli altri *standard* tecnologici individuati con proprio regolamento dall'AGCOM.

A sua volta, l'articolo 3 della proposta n. 891 prevede **misure interdittive** per gli utenti che si rendano responsabili di condotte illecite o gravemente

lesive della dignità delle persone. Viene stabilito che, nei confronti di tali utenti, i fornitori di servizi di comunicazione elettronica adottino **misure adeguate, proporzionate ed effettive** per interdire, su richiesta dell'autorità giudiziaria, l'accesso e la consultazione di siti *Internet*. A tal fine l'AGCOM – d'intesa con il Garante per i dati personali – adotta un apposito regolamento.

L'articolo 4, in particolare, contempla degli **obblighi per gli operatori telefonici,** stabilendo che i contratti degli utenti stipulati con i fornitori di servizi di comunicazione e di informazione offerti mediante reti di comunicazione elettronica devono espressamente richiamare le disposizioni di cui all'**articolo 2048 del codice civile** in materia di responsabilità dei genitori per i danni cagionati dai figli minori, in conseguenza di atti illeciti posti in essere attraverso l'uso della rete. La disposizione è volta – evidentemente – a sollecitare negli adulti che acquistano apparecchi cellulari per i figli una maggiore vigilanza sull'uso che questi ne facciano, collegandosi a *Internet*.

L'articolo 5 – a sua volta – prevede che la Presidenza del Consiglio dei ministri promuova periodiche **campagne informative** di prevenzione e di sensibilizzazione sull'uso consapevole di *Internet* e sui suoi rischi.

Come già anticipato, la materia è stata altresì oggetto di numerose **pronunce** giurisprudenziali.

In sede di **Consiglio d'Europa**, sono degne di nota le sentenze della Corte europea dell'uomo:

- *Delfi c. Estonia* del 16 giugno 2015, nella quale un sito *Internet* è stato ritenuto responsabile di contenuti offensivi caricati da terzi;
- *Magyar Tartalomszolgáltatók c. Ungheria* del 2 febbraio 2016, in cui viceversa è stata accertata la violazione dell'art. 10 CEDU (libertà di espressione) a carico dell'Ungheria per avere condannato un sito *Internet* per i commenti apparsi a opera di utenti;
- *Magyar Jeti Zrt c. Ungheria* del 4 dicembre 2018, in cui – analogamente – l'Ungheria è stata condannata per violazione dell'art. 10 CEDU, in ragione delle condanne inflitte a una testata *online* per aver inserito un *link* a un altro sito;
- *Standard Verlagsgellschaft c. Austria* n. 3 del 7 dicembre 2021, in cui a carico dell'Austria è stata accertata la violazione dell'art. 10 CEDU per avere costretto una testata giornalistica *online* a rivelare dati idonei a risalire all'identità di commentatori, i cui *post* erano stati ritenuti offensivi da un partito politico.

Per l'**Unione europea**, v., per esempio, la sentenza della Corte di giustizia del Lussemburgo, sez. V, 2 aprile 2020, n. 567.

Per l'**Italia**, le pronunzie intervenute paiono esprimere un prevalente indirizzo nel senso di **escludere la responsabilità, a patto che** il gestore del sito:

- ✓ **non intervenga sui contenuti** medesimi (cioè non diventi "attivo") e, comunque,
- ✓ **non sia informato della loro natura illecita** (vuoi perché offensiva, vuoi perché in violazione del diritto d'autore o - ancora – perché costituente pratica commerciale scorretta: v., tra le tante, Corte di cassazione, sez. III penale, 17 dicembre 2013, n. 5107; Corte di cassazione, sez. I civile, 19 marzo 2019, n. 7708; Consiglio di Stato, sez. VI, 17 febbraio 2020, n. 1217; Tribunale civile di Roma, 20 gennaio 2021; proprio di recente (il 2 marzo 2023) – peraltro – risulta emanata una sentenza del tribunale civile di Milano che ha ritenuto Meta – *id est*: Facebook – responsabile di diffamazione nei riguardi di dirigenti della società SNAITECH per non aver rimosso un commento offensivo).

Inoltre, merita di esser menzionata la sentenza della **Corte di Cassazione, sez. I civ., 19/03/2019 n. 7708**, dalla quale è possibile trarre le seguenti statuizioni:

- l'***hosting provider* attivo** è il prestatore dei servizi della società dell'informazione il quale svolge un'attività che esula da un servizio di ordine meramente tecnico, automatico e passivo, e pone, invece, in essere una condotta attiva, **concorrendo con altri nella commissione dell'illecito, onde resta sottratto al regime generale di esenzione** di cui al l'articolo 16 del decreto legislativo.n. 70 del 2003, dovendo la sua responsabilità civile atteggiarsi secondo le regole comuni;
- nell'ambito dei servizi della società dell'informazione, la **responsabilità** dell'*hosting provider*, prevista dal citato articolo 16 del decreto legislativo n. 70 del 2003 sussiste in capo al prestatore dei servizi che **non abbia provveduto alla immediata rimozione dei contenuti illeciti,** nonché che abbia continuato a pubblicarli, pur quando ricorrano congiuntamente le seguenti condizioni:
  - **sia a conoscenza legale dell'illecito** perpetrato dal destinatario del servizio, per averne avuto notizia dal titolare del diritto leso oppure *aliunde*;
  - **l'illiceità dell'altrui condotta sia ragionevolmente constatabile**, onde egli sia in colpa grave per non averla positivamente riscontata, alla stregua del grado di diligenza che è ragionevole attendersi da un operatore professionale della rete in un determinato momento storico;

- **abbia la possibilità di attivarsi utilmente,** in quanto reso edotto in modo sufficientemente specifico dei contenuti illecitamente immessi da rimuovere.

Da ultimo, si segnala che, con specifico riferimento al tema della **tutela del diritto d'autore** dei contenuti abusivamente diffusi *online*, è stata approvata in prima lettura alla Camera la **proposta di legge A.C. 217-648-A** (Disposizioni per la prevenzione e la repressione della diffusione illecita di contenuti tutelati dal diritto d'autore mediante le reti di comunicazione elettronica; qui il *dossier* di documentazione)

L'articolo 2, in particolare, attribuisce all'Autorità per le garanzie nelle comunicazioni (**AGCOM**) il potere di ordinare ai prestatori di servizi di d**isabilitare l'accesso a contenuti diffusi in maniera illecita**, anche adottando a tal fine provvedimenti cautelari in via d'urgenza. Più nel dettaglio, l'AGCOM può ordinare ai prestatori di servizi, ivi inclusi i prestatori di accesso alla rete, di disabilitare l'accesso a contenuti illeciti mediante il **blocco della risoluzione DNS dei nomi di dominio e il blocco all'instradamento del traffico di rete verso gli indirizzi IP univocamente destinati ad attività illecite**. In sede di adozione di tale provvedimento, l'AGCOM ordina **anche il blocco di ogni altro futuro nome di dominio, sottodominio, ove tecnicamente possibile, o indirizzo IP, a chiunque riconducibili,** comprese le variazioni del nome o della semplice declinazione o estensione (c.d. *top level domain*), che consenta l'accesso ai medesimi contenuti abusivamente diffusi o a contenuti della stessa natura (commi 1 e 2).

Nei casi di gravità e urgenza, in cui la violazione abbia ad oggetto contenuti trasmessi in **diretta**, prime visioni di opere cinematografiche e audiovisive o programmi di intrattenimento, contenuti audiovisivi, anche sportivi o altre opere dell'ingegno assimilabili, eventi sportivi nonché eventi di interesse sociale o di grande interesse pubblico, l'AGCOM ordina ai prestatori di servizi, compresi i prestatori di servizi di accesso alla rete, di disabilitare l'accesso ai contenuti trasmessi abusivamente mediante blocco dei nomi di dominio e degli indirizzi IP, adottando a tal fine un **provvedimento cautelare abbreviato, senza contraddittorio**.

I fornitori di servizi della società dell'informazione coinvolti a qualsiasi titolo nell'accessibilità del sito *web* o dei servizi illegali eseguono il provvedimento dell'Autorità **senza alcun indugio e comunque entro 30 minuti** dalla notificazione, disabilitando la risoluzione DNS dei nomi di dominio e l'instradamento del traffico di rete verso gli indirizzi IP indicati nell' elenco di cui al comma 4 o comunque adottando le misure tecnologiche e organizzative necessarie per rendere non fruibili da parte degli utilizzatori finali i contenuti trasmessi abusivamente.