

## RELAZIONE ILLUSTRATIVA

Con il presente decreto legislativo si dà attuazione all'articolo 15 della legge 4 agosto 2022, n. 127 (Legge di delegazione europea 2021), con cui il Governo è stato delegato ad adottare le disposizioni necessarie ad adeguare l'ordinamento nazionale al Regolamento (UE) 2021/784, relativo al contrasto della diffusione di contenuti terroristici *online* (di seguito: il Regolamento).

In base all'articolo 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 data suddetta – 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.

Il decreto legislativo si compone di 9 articoli.

L'**articolo 1** individua l'oggetto del decreto.

L'**articolo 2** reca talune definizioni volte a semplificare la formulazione delle disposizioni del decreto. Nello specifico, è parso opportuno definire:

- a) il *Comitato di analisi strategica antiterrorismo (C.A.S.A.)*: il Comitato di cui all'articolo 12, comma 3, della legge 3 agosto 2007, n. 124, istituito presso il Dipartimento della pubblica sicurezza con decreto del Ministro dell'interno che ne definisce anche la composizione e le modalità di funzionamento;
- b) il *Dipartimento della pubblica sicurezza*: il Dipartimento della pubblica sicurezza di cui all'articolo 4, della legge 1° aprile 1981, n. 121;
- c) l'*Organo del Ministero dell'interno per la sicurezza e la regolarità dei servizi di telecomunicazione*: l'organo di cui all'articolo 14, comma 2, della legge 3 agosto 1998, n. 269.

L'**articolo 3** individua l'autorità competente per l'emissione degli ordini di rimozione ai sensi dell'articolo 3, paragrafo 1, del regolamento, nonché la relativa procedura, in attuazione dei criteri di delega *sub a), b) ed e)* (che concernono anche le procedure di esame degli ordini di rimozione emessi dagli altri Stati UE).

L'autorità competente è stata indicata nell'ufficio del pubblico ministero competente in base alle disposizioni del codice di procedura penale, se – come di regola avviene – i contenuti terroristici risultino riconducibili a un delitto con finalità di terrorismo. Fuori di tali ipotesi, e cioè quando non sia ravvisabile una *notitia criminis* o il contenuto terroristico da rimuovere non sia comunque riferibile a un'indagine in corso, l'ordine di rimozione è emesso dall'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 (**comma 1**).

Quanto all'individuazione del *punto di contatto*, che l'articolo 12, paragrafo 2, del regolamento richiede agli Stati membri di designare «in seno all'autorità competente» allo specifico fine di «trattare le richieste di chiarimenti e di riscontro in relazione agli ordini di rimozione emessi da tale



autorità competente», i procuratori della Repubblica degli uffici distrettuali dovranno individuarlo entro quindici giorni dall'entrata in vigore del decreto tra il personale addetto alle sezioni di polizia giudiziaria, provvedendo altresì ad «assum[ere] le iniziative necessarie ad assicurare adeguata pubblicità alle informazioni ad esso relative». Conformemente alla precisa indicazione contenuta nella disposizione di delega, si è previsto che, nell'assolvimento dei propri compiti, il punto di contatto potrà avvalersi del supporto tecnico dell'Organo del Ministero dell'interno per la sicurezza e la regolarità dei servizi di telecomunicazione (**comma 2**).

Dal punto di vista procedurale, si è stabilito:

- che della ricezione della notizia relativa alla presenza dei contenuti terroristici in rete, così come dell'intenzione di emettere un ordine di rimozione (o del suo eventuale differimento), il pubblico ministero competente debba informare immediatamente il Procuratore nazionale antimafia e antiterrorismo (**commi 3 e 6**);
- che, ai fini della emissione dell'ordine di rimozione, il pubblico ministero acquisisca ogni necessario elemento informativo e valutativo, anche presso il su menzionato C.A.S.A. (**comma 4**);
- che l'ordine di rimozione sia adottato con decreto motivato e portato a conoscenza dei destinatari preferibilmente per il tramite del personale di polizia giudiziaria appartenente all'Organo del ministero dell'interno per la sicurezza e la regolarità dei servizi di telecomunicazione (**comma 6, primo periodo**);
- che, in caso di contenuti generati dagli utenti e ospitati su piattaforme riconducibili a soggetti terzi, possa disporsi «la rimozione dei soli specifici contenuti illeciti» (**comma 6, secondo periodo**).

Quando risulti necessario al fine di acquisire rilevanti elementi probatori ovvero di individuare o catturare i responsabili di delitti con finalità di terrorismo, il pubblico ministero potrà, con decreto motivato, ritardare l'emissione dell'ordine di rimozione (**comma 5**).

Per l'ipotesi in cui il prestatore di servizi di hosting non ottemperi all'ordine di rimozione, oltre a trovare applicazione le sanzioni di cui all'articolo 7, potrà essere disposta «l'interdizione dell'accesso al dominio internet nelle forme e con le modalità di cui all'articolo 321 del codice di procedura penale, garantendo comunque, ove tecnicamente possibile, la fruizione dei contenuti estranei alle condotte illecite» (**comma 8**).

Tale previsione, così come quella del comma 6, riprende quella già contenuta nell'articolo 2, comma 4, del decreto-legge 18 febbraio 2015, n. 7 (convertito con modificazioni dalla legge 17 aprile 2015, n. 144), che viene pertanto abrogata dal successivo **articolo 8** dello schema di decreto.

Quanto ai rimedi giurisdizionali, di cui all'articolo 9 del Regolamento (lettera *e*) della delega), s'è previsto che i prestatori di servizi di hosting destinatari di un ordine di rimozione e i fornitori dei contenuti rimossi o resi inaccessibili, nei dieci giorni successivi alla conoscenza del provvedimento, possano presentare opposizione innanzi al giudice per le indagini preliminari, che provvede con ordinanza in camera di consiglio a norma dell'articolo 127 del codice di procedura penale, ricorribile per cassazione unicamente per violazione di legge (**comma 9**).

L'**articolo 4**, che – per quanto s'è anticipato – attua anch'esso i criteri di delega *sub a), b) ed e)*, individua nel giudice per le indagini preliminari l'autorità competente per l'esame degli ordini di rimozione transfrontalieri trasmessi dalle autorità competenti degli altri Stati membri, nonché per



l'assunzione delle decisioni ( motivate) attraverso le quali – in base all'articolo 4, paragrafi 3 e 4 del Regolamento – gli ordini in questione possono essere privati dell'efficacia giuridica loro propria qualora si accerti che essi «viol[no] in modo grave o manifesto il presente regolamento o i diritti e delle libertà fondamentali garantiti dalla Carta». Anche in questo caso la competenza è stata concentrata a livello distrettuale (e, cioè, «presso il tribunale del capoluogo del distretto in cui il prestatore di servizi di hosting ha lo stabilimento principale o in cui il rappresentante legale del prestatore di servizi di hosting risiede o è stabilito»). Si prevede, inoltre, che copia dell'ordine di rimozione debba essere trasmesso dal giudice al Procuratore nazionale antimafia e antiterrorismo immediatamente e, comunque, prima di assumere le decisioni di cui sopra (**comma 1**).

Per le decisioni di cui all'articolo 4, paragrafi 3 e 4 del Regolamento, si prevede che esse vadano adottate sentito il pubblico ministero e nella forma del decreto motivato e che, quando siano state assunte a seguito di istanza del prestatore di servizi di hosting o del fornitore di contenuti, possano essere impugnate – nei dieci giorni dal deposito – a mezzo di ricorso per cassazione unicamente per violazione di legge (**comma 2**).

L'**articolo 5** attribuisce all'Organo del Ministero dell'interno per la sicurezza e la regolarità dei servizi di telecomunicazione la competenza:

- a emettere la decisione con cui, ai sensi dell'articolo 5, paragrafo 4, del regolamento, si accerta che il prestatore di servizi di hosting è «esposto a contenuti terroristici»;
- a sorvegliare l'attuazione delle misure specifiche che, a seguito di detto accertamento, il prestatore di servizi di hosting è tenuto ad adottare;
- a emettere le ulteriori decisioni di cui ai paragrafi 6 e 7 del medesimo articolo 5 (**comma 1**).

Per l'impugnazione delle decisioni assunte dall'Organo del Ministero dell'interno per la sicurezza e la regolarità dei servizi di telecomunicazione al prestatore di servizi di hosting è riconosciuta la possibilità di ricorrere al competente tribunale amministrativo regionale entro sessanta giorni dalla notifica.

Gli **articoli 6 e 7** danno attuazione ai **criteri di delega sub c) e d)**, con cui si richiedeva al Governo – rispettivamente – 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» e di «individuare le autorità competenti a irrogare le sanzioni [...] e a vigilare sull'osservanza delle disposizioni del regolamento (UE) 2021/784, diverse dalle misure [specifiche]».

L'**articolo 6** è dedicato alle sanzioni amministrative.

I primi tre commi della disposizione individuano altrettanti gruppi di illeciti, suddivisi per gravità crescente e configurabili solo quando il fatto non integri reato.

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 (art. 3, par. 6, del Regolamento);
- b) rimuove i contenuti terroristici o disabilita l'accesso ai contenuti terroristici ai sensi dell'articolo 3, paragrafo 3, del regolamento, omettendo di adottare le misure necessarie



- per ripristinare i contenuti o riabilitare l'accesso agli stessi, in conformità dell'articolo 4, paragrafo 7, del regolamento (art. 4, par. 2, seconda ipotesi, del Regolamento);
- c) dopo aver ricevuto una decisione emessa dall'autorità competente ai sensi dell'articolo 4, paragrafo 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);
  - d) nella conservazione dei contenuti terroristici rimossi o il cui accesso è stato disabilitato, ovvero nella conservazione dei relativi dati, non osserva le disposizioni di cui all'articolo 6 del regolamento;
  - e) non rispetta gli obblighi di trasparenza di cui all'articolo 7 del regolamento;
  - f) non predispone il meccanismo di reclamo di cui all'articolo 10, paragrafo 1, del regolamento o, nell'esame, nella decisione e nella gestione dei reclami, non rispetta le disposizioni di cui al paragrafo 2 del medesimo articolo 10;
  - g) fuori dei casi di cui all'articolo 11, paragrafo 3, del regolamento, omette di comunicare al fornitore di contenuti le informazioni di cui ai paragrafi 1 e 2 del medesimo articolo 11;
  - 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).

Il **comma 2** prevede la sanzione amministrativa pecuniaria da 50.000 a 200.000 euro nei confronti del prestatore di servizi di hosting esposto a contenuti terroristici che:

- a) 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);
- b) fuori dei casi di cui alla lettera a), non osserva taluno degli obblighi di condotta di cui all'articolo 5, paragrafo 1, del regolamento (art. 5, par. 1, co. 2, del Regolamento);
- c) adotta misure specifiche prive di taluno dei requisiti di cui all'articolo 5, paragrafo 3, del regolamento;
- d) dopo aver ricevuto una decisione di cui all'articolo 5, paragrafi 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 scadenze annuali, le misure specifiche che ha adottato e che intende adottare per conformarsi alle disposizioni di cui ai paragrafi 2 e 3 del medesimo articolo 5 (art. 5, par. 5, del Regolamento).

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:

- a) omette di adottare misure specifiche per proteggere i propri servizi dalla diffusione al pubblico di contenuti terroristici ai sensi dell'articolo 5, paragrafo 2, del regolamento;
- b) dopo aver ricevuto una decisione di cui all'articolo 5, paragrafo 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).



Quanto alle autorità competenti ad irrogare le sanzioni, il **comma 4** le individua 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, cui si rimette di accertare e contestare le 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.

Il **comma 5** traspone l'articolo 18, par. 2, del Regolamento, disponendo che nella determinazione della sanzione si debba aver riguardo a tutte le circostanze rilevanti, tra cui:

- a) la natura, la gravità e la durata della violazione;
- b) il carattere doloso o colposo della violazione;
- c) le precedenti violazioni commesse dal prestatore di servizi di hosting;
- d) le condizioni patrimoniali, economiche e finanziarie del prestatore di servizi di hosting;
- e) la cooperazione del prestatore di servizi di hosting con le autorità competenti
- f) l'attività svolta dal prestatore di servizi di hosting per l'eliminazione o attenuazione delle conseguenze della violazione;
- g) la natura e le dimensioni del prestatore di servizi di hosting;
- h) 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** dispone in merito ai proventi derivanti dalle sanzioni amministrative pecuniarie di cui al presente articolo, stabilendo che essi siano da versarsi a 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** stabilisce 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.

L'**articolo 7** si occupa delle sanzioni penali.

Anche in questo caso, come già visto per l'articolo 6 in relazione alle sanzioni amministrative, i commi da 1 a 3 della norma individuano tre distinti gruppi di illeciti, suddivisi per gravità crescente e configurabili solo quando non ricorrano gli estremi di altro più grave reato.

Al **comma 1** si prevede la pena alternativa dell'arresto fino a sei mesi o dell'ammenda da 100.000 a 400.000 euro per il prestatore di servizi di hosting che:

- a) in violazione dell'articolo 15, paragrafo 1, del regolamento, omette di designare o istituire un punto di contatto per la ricezione degli ordini di rimozione in via telematica e per l'immediata esecuzione dei medesimi ai sensi degli articoli 3 e 4 del regolamento, oppure



omette di rendere disponibili al pubblico le informazioni relative al punto di contatto designato o istituito;

- b) non avendo lo stabilimento principale nell'Unione, omette di designare, 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 decisioni emesse dalle autorità competenti, oppure designa un rappresentante legale che non risiede o non è stabilito in uno degli Stati membri in cui il prestatore di servizi di hosting offre i propri servizi, oppure omette di conferire al rappresentante legale i poteri e le risorse necessari per ottemperare agli ordini di esecuzione e per cooperare con le autorità competenti.

Poiché si tratta di condotte che, di fatto, ove protratte nel tempo, possono addirittura mettere in crisi il funzionamento degli stessi meccanismi giuridici "di base" predisposti dal Regolamento, è parso opportuno prevedere che, quando il prestatore di servizi di hosting, nei quindici giorni successivi all'accertamento e alla contestazione delle violazioni, non provvede agli adempimenti omessi, l'autorità giudiziaria possa disporre l'interdizione dell'accesso al dominio internet nelle forme e con le modalità di cui all'articolo 321 del codice di procedura penale (**comma 4**).

Al **comma 2** si comminano, in questo caso in forma congiunta, le pene dell'arresto fino a sei mesi e dell'ammenda da 100.000 a 400.000 euro al prestatore di servizi di hosting che:

- a) omette di rimuovere i contenuti terroristici entro un'ora dal ricevimento dell'ordine di rimozione o di disabilitare l'accesso ad essi entro il medesimo termine (art. 3, par. 3, e art. 4, par. 2, del Regolamento);
- b) nel caso di cui all'articolo 11, paragrafo 3, del regolamento, fornisce informazioni riguardanti la rimozione o la disabilitazione dell'accesso a contenuti terroristici;
- c) nel caso di cui all'articolo 14, paragrafo 5, del regolamento, non informa immediatamente della presenza di contenuti terroristici l'autorità giudiziaria o altra autorità che a quella abbia l'obbligo di riferire.

Per l'ipotesi in cui la violazione di cui al comma 2, lettera a), sia sistematica o persistente, s'è prevista l'applicazione della pena dell'arresto fino a un anno e dell'ammenda da euro 250.000 sino ad euro 1.000.000 o, laddove superiore, sino ad un importo pari al quattro per cento del fatturato realizzato a livello mondiale dal prestatore di servizi di hosting nell'ultimo esercizio chiuso anteriormente all'accertamento della violazione. Tale ultima previsione, in particolare, è stata inserita per ottemperare a quanto disposto dall'articolo 18, paragrafo 3, del Regolamento (**comma 3**).

In ragione della gravità, nonché della natura delle violazioni di cui ai commi 2 e 3, esse sono state estese al rappresentante legale che, ai sensi dell'articolo 17 del Regolamento, i prestatori di servizi di hosting sono tenuti a designare quando non abbiano il proprio stabilimento legale nell'Unione «ai fini del ricevimento, dell'attuazione e dell'esecuzione degli ordini di rimozione, e delle decisioni emesse dalle autorità competenti».

In correlazione a tale estensione è parso tuttavia opportuno mandare esente da pena il rappresentante legale che, entro quindici giorni dalla sua designazione, comunichi all'Organo del Ministero dell'interno per la sicurezza e la regolarità dei servizi di telecomunicazione 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) di non disporre dei poteri e delle risorse necessari al corretto e integrale adempimento dei suoi compiti (**comma 5**).



All' **articolo 8**, per le ragioni a suo tempo esposte, si 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.

Con l' **articolo 9**, infine, è prevista la neutralità finanziaria del provvedimento.

Si segnala che con riferimento al presente schema di decreto legislativo è stata chiesta dal Ministero della giustizia e concessa dal DAGL, in data 3 maggio 2023, l'esenzione dall'AIR, in relazione al ridotto impatto dell'intervento, in presenza delle seguenti condizioni, congiuntamente considerate:

a) costi di adeguamento attesi di scarsa entità in relazione ai singoli destinatari, tenuto anche conto della loro estensione temporale. Si è osservato - in sintesi- che la natura sostanzialmente ordinamentale e procedurale dell'intervento porta ad escludere la configurazione di costi di adeguamento in capo ai cittadini, mentre gli adempimenti eventualmente connessi all'implementazione delle previsioni introdotte (così come le misure organizzative descritte dall'articolo 3, comma 2) costituiscono esercizio delle competenze istituzionali proprie degli apparati giudiziari ed amministrativi interessati e, pertanto, afferiscono all'esercizio di funzioni nell'ambito di istituti e moduli procedurali già noti all'ordinamento, che non richiedono lo sviluppo ovvero l'esercizio di ulteriori e diverse competenze rispetto a quelle già in essere.

Ai relativi adempimenti, pertanto, le amministrazioni interessate provvederanno con le risorse umane, strumentali e finanziarie disponibili a legislazione vigente.

b) numero esiguo dei destinatari dell'intervento. Dai dati forniti dalla Polizia postale (sito - sezione cyberterrorismo) è emerso come, a fronte dei numerosi siti monitorati, soltanto un esiguo numero di casi sia stato poi sottoposto al vaglio giudiziale con successiva rimozione dei contenuti. La disciplina introdotta è dunque destinata ad operare in un numero limitato di casi, attesa la specificità della fattispecie e le stigmatizzate modalità della condotta.

c) risorse pubbliche impiegate di importo ridotto. Le disposizioni del presente intervento normativo, configurandosi come norme di carattere definitorio, di coordinamento ordinamentale, ovvero di natura procedimentale e precettiva, non determinano nuovi o maggiori oneri a carico della finanza pubblica, potendo essere attuate con le risorse umane, strumentali e finanziarie disponibili a legislazione vigente.

d) limitata incidenza sugli assetti concorrenziali del mercato. L'intervento normativo non impatta sugli assetti concorrenziali del mercato e non presenta aspetti di interferenza o di incompatibilità con l'ordinamento europeo, anzi è volto a consentire l'adeguamento dell'ordinamento nazionale al Regolamento (UE) 2021/784.



## RELAZIONE TECNICA

La presente relazione tecnica è volta a valutare gli effetti finanziari concernenti il completo 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, attraverso il decreto legislativo in esame, da emanarsi ai sensi dell'articolo 15 della legge 4 agosto 2022, n. 127 (Legge di delegazione europea 2021).

Obiettivo del presente provvedimento è, infatti, l'adeguamento della normativa interna alle disposizioni europee che si occupano di sicurezza nazionale per il contrasto e la lotta ad attività estreme e radicalizzanti quali il terrorismo, che costituisce una minaccia alla sicurezza, ai valori delle società democratiche e ai diritti e alle libertà dei cittadini europei. Come noto, la lotta al terrorismo passa dalle misure adottate per impedire ai terroristi di acquistare armi o costruire bombe, fino agli sforzi volti a cercare di contrastare la radicalizzazione, che attualmente è diventata una minaccia sempre più grave. Le tecnologie di comunicazione *online* hanno reso più facile per i terroristi comunicare a livello transfrontaliero, oltre ad amplificare la propaganda terroristica e incrementare la diffusione dell'estremismo. Nell'aprile 2021 il Consiglio d'Europa ha adottato il regolamento UE 2021/784 relativo al contrasto della diffusione di contenuti terroristici online, che dispone riguardo alla facoltà delle autorità competenti degli Stati membri di emettere ordini di rimozione nei confronti di prestatori di servizi, imponendo loro di rimuovere i contenuti terroristici o di disabilitarne l'accesso in tutti gli Stati membri per un'efficace condivisione delle informazioni tra le autorità di contrasto, giudiziarie e di *intelligence* per permettere di rintracciare i terroristi stranieri e contrastare la criminalità organizzata.

Il fulcro della materia, secondo quanto previsto dal citato regolamento, è di rimuovere l'allocatione delle pagine di un sito o di un'applicazione *web* su un *server* così da non permettere al sito o all'applicazione di essere raggiungibili e visibili agli utenti in rete. Il decreto legislativo è costituito di **nove articoli** incluse le disposizioni finanziarie (articolo 9).

L'**articolo 1** individua l'oggetto del decreto, che procede all'adeguamento dell'ordinamento interno alle disposizioni contenute nel regolamento (UE) 2021/784 per il contrasto della diffusione di contenuti terroristici online.

La norma, stante il suo carattere ordinamentale, non determina nuovi o maggiori oneri a carico della finanza pubblica.

L'**articolo 2** contiene le definizioni delle strutture del Ministero dell'interno indicate nel provvedimento; ha natura ordinamentale e, come tale, non produce effetti negativi per la finanza pubblica.

L'**articolo 3** contiene l'indicazione dell'autorità competente per l'emissione degli ordini di rimozione individuata: a) nell'ufficio del pubblico ministero competente in base alle disposizioni del codice di procedura penale quando i contenuti terroristici di cui all'articolo 2, numero 7) del citato Regolamento sono riconducibili a un delitto con finalità di terrorismo; b) nei casi residuali, la competenza è del pubblico ministero del tribunale del capoluogo del distretto in cui è acquisita la



notizia relativa alla presenza sulle reti di telecomunicazioni disponibili al pubblico di contenuti terroristici.

I suddetti procuratori della Repubblica individuano il punto di contatto di cui all'articolo 12, paragrafo 2, del Regolamento, tra il personale addetto alle sezioni di polizia giudiziaria e assumono le iniziative necessarie ad assicurare adeguata pubblicità alle informazioni ad esso relative.

Nell'assolvimento dei propri compiti, il punto di contatto può avvalersi del supporto tecnico dell'Organo del Ministero dell'interno per la sicurezza e la regolarità dei servizi di telecomunicazione (comma 2).

Con particolare riferimento a tale attività, che rientra tra i compiti e le funzioni istituzionalmente demandate ai soggetti interessati dalla previsione in esame, si segnala che la stessa potrà essere assicurata con le risorse umane, strumentali e finanziarie disponibili a legislazione vigente.

Si segnala che il pubblico ministero è tenuto ad informare immediatamente il Procuratore nazionale antimafia e antiterrorismo della notizia relativa alla presenza dei contenuti terroristici in rete, sia dell'intenzione di emettere un ordine di rimozione (o del suo eventuale differimento) (comma 3). Analoga comunicazione è prevista in sede di emissione dell'ordine di rimozione (comma 7), come pure si prevede che il pubblico ministero acquisisca ogni necessario elemento informativo e valutativo, anche presso il Comitato di analisi strategica antiterrorismo (C.A.S.A.) istituito presso il Dipartimento della pubblica sicurezza con decreto del Ministro dell'interno, che ne definisce anche la composizione e le modalità di funzionamento.

Al riguardo, si rappresenta che gli adempimenti informativi inseriti – i quali potranno essere svolti con modalità telematiche attraverso le strumentazioni e le piattaforme dei sistemi telematici già operativi - rientrano tra le attività di rilevazione e monitoraggio dei fenomeni criminali correntemente già svolte dagli uffici e la loro raccolta è funzionale alle attività informative necessarie alla gestione efficiente delle procedure e dei carichi di lavoro che tanto la DNAA che le altre articolazioni del Ministero della giustizia sono chiamate ad assolvere.

Con il comma 6 dell'articolo in esame si stabilisce che l'ordine di rimozione sia adottato con decreto motivato e portato a conoscenza dei destinatari preferibilmente per il tramite del personale di polizia giudiziaria appartenente all'Organo del ministero dell'interno per la sicurezza e la regolarità dei servizi di telecomunicazione e che possa essere disposta la rimozione dei soli specifici contenuti illeciti nel caso di contenuti generati dagli utenti e ospitati su piattaforme riconducibili a soggetti terzi.

Si segnala la disposizione contenuta nel comma 8, secondo la quale nel caso in cui il prestatore di servizi di hosting non ottemperi all'ordine di rimozione, oltre a trovare applicazione le sanzioni penali previste dal successivo articolo 7, potrà essere disposta l'interdizione dell'accesso al dominio internet nelle forme e con le modalità di cui all'articolo 321 del codice di procedura penale, garantendo comunque, ove tecnicamente possibile, la fruizione dei contenuti estranei alle condotte illecite.

Nel comma 9 vengono disciplinati i rimedi giurisdizionali per i prestatori di servizi di hosting destinatari di un ordine di rimozione e i fornitori dei contenuti rimossi o resi inaccessibili, i quali, possono presentare opposizione innanzi al giudice per le indagini preliminari, che provvede con ordinanza in camera di consiglio, ricorribile avanti alla Corte di cassazione unicamente per violazione di legge, entro dieci giorni dalla conoscenza del provvedimento impugnato.



In termini generali, va osservato che le disposizioni in esame introducono nuove fattispecie delittuose, volte al contrasto di un fenomeno in crescente espansione e rispetto al quale allo stato non sono disponibili elementi informativi utili a delinearne la consistenza, si assicura che gli adempimenti declinati nelle medesime norme, sono di natura istituzionale e potranno essere fronteggiati nell'ambito delle risorse umane, strumentali e finanziarie disponibili a legislazione vigente, trattandosi di attività rientranti nei compiti e nelle funzioni ordinarie previste dall'ordinamento giudiziario e sono eseguiti con modalità già dettate dal diritto interno.

Per tali ragioni, dalle disposizioni in esame non derivano nuovi o maggiori oneri per la finanza pubblica.

L'**articolo 4** individua nel Giudice per le indagini preliminari presso il tribunale del capoluogo del distretto in cui il prestatore di servizi di hosting ha lo stabilimento principale o in cui il rappresentante legale del prestatore di servizi di hosting risiede o è stabilito, l'autorità competente per l'esame degli ordini di rimozione transfrontalieri trasmessi dalle autorità competenti degli altri Stati membri. Lo stesso giudice è competente ad emettere decreto motivato sia ex officio che su richiesta della parte interessata nel caso di violazione grave o manifesta delle disposizioni del Regolamento UE 784/2021 o della Carta europea dei diritti fondamentali.

Si segnala che il Giudice per le indagini preliminari è tenuto a trasmettere copia degli ordini di rimozione al Procuratore nazionale antimafia e antiterrorismo e che avverso i decreti emessi dallo stesso GIP è possibile ricorrere per cassazione unicamente per violazione di legge.

Come sopra rappresentato con riferimento alle disposizioni contenute nell'articolo 3, per gli aspetti di competenza dell'Amministrazione della giustizia, si rileva l'assenza di oneri aggiuntivi, in quanto le attività giudiziarie previste rientrano tra gli adempimenti di natura istituzionale ordinariamente espletati e fronteggiabili nell'ambito degli stanziamenti di bilancio dell'amministrazione giudiziaria destinati al funzionamento degli uffici giudiziari.

L'**articolo 5** attribuisce all'Organo del Ministero dell'interno per la sicurezza e la regolarità dei servizi di telecomunicazione la competenza:

- a emettere la decisione con cui, ai sensi dell'articolo 5, paragrafo 4, del regolamento, si accerta che il prestatore di servizi di hosting è «esposto a contenuti terroristici»;
- a sorvegliare l'attuazione delle misure specifiche che, a seguito di detto accertamento, il prestatore di servizi di hosting è tenuto ad adottare;
- a emettere le ulteriori decisioni di cui ai paragrafi 6 e 7 del medesimo articolo 5 (comma 1).

Tale Organo, previsto dall'articolo 1, comma 13, della legge 13 luglio 1997, n. 249 e dal decreto del Ministro dell'interno, di concerto con il Ministro delle comunicazioni e con il Ministro del tesoro, del bilancio e della programmazione economica del 19 gennaio 1999, attualmente svolge, nell'ambito dei compiti di polizia delle telecomunicazioni, attività di contrasto nei confronti della prostituzione minorile, della pornografia minorile e delle iniziative turistiche volte allo sfruttamento della prostituzione minorile, ai sensi dell'articolo 14, comma 2, della legge 3 agosto 1998, n. 269 nonché del traffico di stupefacenti via internet, ai sensi dell'articolo 12 del decreto-legge 21 ottobre 2020, n. 130 convertito, con modificazioni, dalla legge 18 dicembre 2020, n. 173.

In tale contesto, con specifico riferimento ai profili di competenza dell'Organo del Ministero dell'interno, giova richiamare anche la legge 31 luglio 2005 n. 155, che ha convertito con modificazioni il decreto legge 27 luglio 2005 n. 144, recante *“Misure urgenti per il contrasto del*



*terrorismo internazionale*”, che, all’art. 7-bis, attribuisce agli Ufficiali di Polizia Giudiziaria dell’organo del Ministero dell’interno per la sicurezza e per la regolarità dei servizi di telecomunicazione, per le finalità di prevenzione e repressione delle attività terroristiche o di agevolazione del terrorismo condotte con i mezzi informatici, la possibilità di svolgere le attività sotto copertura, di cui all’articolo 4, commi 1 e 2, del D.L. 18 ottobre 2001, n. 374, nonché la legge 4 agosto 2021, n. 109, di conversione del decreto-legge 14 giugno 2021, n. 82, recante disposizioni urgenti in materia di cybersicurezza, definizione dell’architettura nazionale di cybersicurezza e istituzione dell’Agenzia per la cybersicurezza nazionale.

Per l’esercizio dei compiti previsti dall’articolo in commento, che rientrano comunque tra le azioni di contrasto al "cybercrime" di competenza della specialità della Polizia postale e delle comunicazioni della Polizia di Stato, esso si avvale di una infrastruttura informatica già esistente e sufficientemente capiente, risultando, inoltre, già operativo anche il canale di comunicazione con i fornitori di connettività alla rete internet (cd. provider) chiamati ad adempiere al connesso obbligo di filtraggio. Si rileva, pertanto, l’assenza di oneri aggiuntivi, in quanto le attività descritte rientrano tra gli adempimenti di natura istituzionale ordinariamente espletati e fronteggiabili nell’ambito degli stanziamenti di bilancio dell’amministrazione destinati al funzionamento degli uffici in argomento. L’articolo in esame prevede, inoltre, che per l’impugnazione delle decisioni assunte dall’Organo del Ministero dell’interno per la sicurezza e la regolarità dei servizi di telecomunicazione al prestatore di servizi di hosting è possibile ricorrere al competente tribunale amministrativo regionale entro sessanta giorni dalla notifica (comma 2).

La citata disposizione analizzata, stante il carattere ordinamentale e procedimentale non determina nuovi o maggiori oneri a carico della finanza pubblica.

L’**articolo 6** disciplina il regime sanzionatorio prevedendo, ai primi tre commi, gruppi di illeciti, suddivisi per gravità crescente e configurabili solo quando il fatto non integri reato.

I commi 4 e 5 stabiliscono il procedimento di applicazione delle sanzioni amministrative pecuniarie, prevedendo l’applicazione, in via generale, delle disposizioni di cui alla legge 24 novembre 1981, n. 689.

L’attività di vigilanza e di accertamento, ai fini dell’irrogazione delle sanzioni è esercitata dall’Organo del Ministero dell’interno per la sicurezza delle telecomunicazioni che provvede ad accertare, contestare/notificare estremi della violazione sia al trasgressore che all’obbligato in solido.

Tale cooperazione sarà disciplinata tramite una convenzione, che verrà sottoscritta tra il Ministero delle imprese e del made in Italy e il Ministero dell’Interno entro 90 giorni dall’entrata in vigore del presente decreto, e che ne definirà i termini organizzativi senza oneri di spesa.

All’irrogazione delle sanzioni provvede 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), a seguito delle comunicazioni da parte dell’Organo del Ministero dell’interno per la sicurezza delle telecomunicazioni, che accerta e contesta le violazioni. Il sistema sanzionatorio assicura l’effettività e la proporzionalità della singola sanzione, tenendo conto della natura, della gravità e della durata della violazione, dell’eventuale sua reiterazione ( La reiterazione delle violazioni, di cui all’articolo 8-bis della legge 24 novembre 1981, n. 689, opera anche nel caso di pagamento in misura ridotta) e del carattere doloso o colposo, con graduazione commisurata alle misure tecniche e organizzative



adottate dal prestatore di servizi di hosting in relazione alla sua solidità finanziaria ed alla sua organizzazione.

L'obiettivo perseguito tramite l'irrogazione della sanzione amministrativa è duplice: reprimere adeguatamente la condotta illecita e prevenirne la reiterazione, non soltanto da parte del trasgressore, ma altresì da parte della generalità degli operatori del mercato.

La sanzione, in tal guisa, rappresenta un provvedimento avente carattere afflittivo che assume, al contempo, la finalità di prevenzione della reiterazione della condotta avendo previsto che quest'ultima opera anche nel caso di pagamento in misura ridotta.

L'attività sanzionatoria 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) è esercitata secondo i principi generali di cui alla L. n. 689/81 (legalità, irretroattività, soggettività) dalla quale gli stessi mutuano anche i criteri per la determinazione degli importi sanzionatori, fissati, a sua volta dall'articolo 6, tra un limite minimo ed un limite massimo, ed irrogate tenuto conto del combinato disposto dell'articolo 11 della legge 689/81 e del comma 5 dell'articolo 6 della presente norma.

L'ordinanza ingiunzione, di cui al secondo comma dell'articolo 18 della legge 24 novembre 1981, n. 689, è adottata nel termine di 180 giorni dalla scadenza del termine indicato nel primo comma dell'articolo 16 della medesima legge, ai sensi dell'articolo 32 ter del decreto legislativo n. 300/1999.

Le attività descritte saranno svolte senza la necessità di costituire alcuna nuova struttura, bensì con le risorse umane e strumentali disponibili, senza nuovi o maggiori oneri per la finanza pubblica. Le sanzioni introdotte con il presente schema di decreto legislativo riguardano l'inosservanza degli obblighi derivanti dagli articoli 3,4,5, 6,7,10,11,14,15 e 17 del Regolamento (UE) 2021/784 e costituiscono un sistema sanzionatorio interamente nuovo, che non presenta carattere ricognitivo di preesistenti sanzioni, non essendo già previsto, a legislazione vigente, un apparato sanzionatorio per i casi di violazione degli obblighi di cui al citato Regolamento. Infine, si prevede che i proventi delle sanzioni sono versati ad apposito capitolo dell'entrata del bilancio dello Stato, per essere riassegnati, in egual misura, con decreto del Ministro 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.

Per quanto attiene alla cooperazione tra l'organo del Ministero dell'interno per la sicurezza e la regolarità dei servizi di telecomunicazione ed il Ministero delle Imprese e del made in Italy, regolamentata, secondo quanto fissato dal comma 7, da una convenzione operativa sottoscritta tra il Ministero dell'Interno e il Ministero delle imprese e del made in Italy entro novanta giorni dalla data di entrata in vigore del presente decreto legislativo, si segnala che i compiti che deriveranno per effetto della citata convenzione, relativi a funzioni istituzionali, non determinano effetti negativi per la finanza pubblica, e potranno essere assicurati nell'ambito delle risorse umane, strumentali e finanziarie disponibili a legislazione vigente.

Si conferma, pertanto, che dall'attuazione del presente articolo non derivano nuovi o maggiori oneri a carico della finanza pubblica.

L'**articolo 7** reca le sanzioni penali suddivise in tre categorie di illeciti ordinati per gravità crescente.

La prima categoria di illeciti riguarda il solo presentatore dei servizi di hosting punito in via alternativa con l'arresto fino a sei mesi o l'ammenda da 100.000 a 400.000 euro per condotte omissive



come la mancata designazione o individuazione del punto di contatto per la ricezione e immediata esecuzione degli ordini di rimozione (comma 1).

La seconda categoria (comma 2) di illeciti, per i quali viene prevista congiuntamente la pena dell'arresto fino a sei mesi o l'ammenda da 100.000 a 400.000 euro, prevede l'estensione della responsabilità al rappresentante legale che, ai sensi dell'articolo 17 del Regolamento, i prestatori di servizi di hosting sono tenuti a designare quando non abbiano il proprio stabilimento legale nell'Unione, per il ricevimento, l'attuazione e l'esecuzione degli ordini di rimozione, e delle decisioni emesse dalle autorità competenti.

Con il comma 3 si intende punire, con l'applicazione della pena dell'arresto fino a un anno e dell'ammenda da euro 250.000 sino ad euro 1.000.000 o, laddove superiore, sino ad un importo pari al quattro per cento del fatturato realizzato a livello mondiale dal prestatore di servizi di hosting nell'ultimo esercizio chiuso anteriormente all'accertamento della violazione, la sistematica e persistente violazione dell'obbligo di designare o istituire un punto di contatto per la ricezione e immediata esecuzione degli ordini di rimozione.

Si segnala il contenuto del comma 4 del presente articolo, che, inserito nella linea ispiratrice del Regolamento per cui è fondamentale adottare misure di contrasto al fenomeno della diffusione di contenuti terroristici online anche in fase prodromica, prevede che l'autorità giudiziaria può disporre l'interdizione dell'accesso al dominio internet - nelle forme e con le modalità previste per il sequestro preventivo come regolato dall'articolo 321 del codice di procedura penale - quando il prestatore di servizi di hosting, nei quindici giorni successivi all'accertamento e alla contestazione delle violazioni, non provvede agli adempimenti omessi ed indicati dal comma 1 dell'articolo in esame.

Sotto il profilo finanziario, è da evidenziare che le disposizioni qui esaminate, che prevedono la punibilità di condotte illecite con pene pecuniarie, producono un gettito d'entrata per le casse dell'Erario, determinando effetti positivi per la finanza pubblica, sebbene allo stato non quantificabili. Al tempo stesso si segnala che gli adempimenti connessi alle norme appena illustrate rientrano nella tipologia di quelli ordinariamente espletati a regime e sono correlati a compiti istituzionalmente svolti dagli organi e dal personale preposto.

Per quanto indicato, è possibile dare attuazione alle attività indicate nell'ambito delle competenze del Ministero della giustizia avvalendosi delle risorse umane, strumentali e finanziarie disponibili a legislazione vigente, trattandosi di compiti e funzioni istituzionali che vengono già ordinariamente espletati.

Si rappresenta, altresì, la natura ordinamentale e procedurale delle disposizioni tese alla regolamentazione unitaria delle condotte illecite al cui contrasto è preordinato il regolamento (UE) 2021/784, nonché della previsione di introdurre sanzioni efficaci, dissuasive e proporzionate alla gravità delle violazioni delle disposizioni indicate all'articolo 18 del medesimo regolamento.

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, dal momento che le disposizioni contenute risultano assorbite e superate da quanto previsto dai commi 5 e 8 dell'articolo 3 del provvedimento in esame con riferimento all'ordine di rimozione emesso dal pubblico ministero e all'interdizione dell'accesso al dominio internet in conseguenza del mancato adempimento del predetto ordine.

La previsione ha carattere ordinamentale e non determina effetti negativi per la finanza pubblica.



L'**articolo 9** contiene la clausola di invarianza finanziaria relativa al presente provvedimento con cui si prevede che dall'attuazione delle norme non devono derivare nuovi e maggiori oneri a carico della finanza pubblica dal momento che le amministrazioni pubbliche interessate provvedono con le risorse umane, strumentali e finanziarie disponibili a legislazione vigente.





# Ministero dell'Economia e delle Finanze

DIPARTIMENTO DELLA RAGIONERIA GENERALE DELLO STATO

## **VERIFICA DELLA RELAZIONE TECNICA**

La verifica della presente relazione tecnica, effettuata ai sensi e per gli effetti dell'art. 17, comma 3, della legge 31 dicembre 2009, n. 196 ha avuto esito Positivo.

Il Ragioniere Generale dello Stato

Firmato digitalmente



## ANALISI TECNICO-NORMATIVA (ATN)

### **SCHEMA DI DECRETO LEGISLATIVO RECANTE ADEGUAMENTO DELLA NORMATIVA NAZIONALE ALLE DISPOSIZIONI DEL REGOLAMENTO (UE) 2021/784, RELATIVO AL CONTRASTO DELLA DIFFUSIONE DI CONTENUTI TERRORISTICI ONLINE**

**Amministrazioni proponenti:** Ministro per gli affari europei, il Sud, le politiche di coesione e il PNRR, Ministero della giustizia, Ministero dell'interno e Ministero delle imprese e del Made in Italy.

**Referente ATN:** Ufficio legislativo del Dicastero della giustizia.

#### **PARTE I - ASPETTI TECNICO-NORMATIVI DI DIRITTO INTERNO**

##### ***1) Obiettivi e necessità dell'intervento normativo. Coerenza con il programma di governo.***

L'intervento normativo persegue l'obiettivo di definire misure di adeguamento, ordinamentale ed organizzativo, alle misure definite dalla normativa eurounitaria per contrastare l'uso improprio dei servizi di hosting ai fini della diffusione al pubblico di contenuti terroristici on line.

Con lo schema di decreto legislativo in esame si dà quindi attuazione all'articolo 15 della legge 4 agosto 2022, n. 127 (Legge di delegazione europea 2021), con cui il Governo è stato delegato a adottare le disposizioni necessarie a adeguare l'ordinamento nazionale al Regolamento (UE) 2021/784 (di seguito: Regolamento), relativo al contrasto della diffusione di contenuti terroristici *online*.

Il presente schema di decreto legislativo è volto, pertanto, ad adeguare l'ordinamento giuridico nazionale alle previsioni del Regolamento e provvedere alla 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. La completa definizione delle descritte misure di attuazione si rende ancor più impellente in ragione dell'apertura di procedura di infrazione nei confronti dell'Italia ai sensi dell'art. 258 TFUE per non aver adempiuto agli obblighi derivanti dal Regolamento, avviata dalla Commissione europea con nota C (2023) 137 *final* del 26 gennaio 2023.

In base all'articolo 24 del citato Regolamento, le disposizioni in esso contenute si applicano a decorrere dal 7 giugno 2022.

##### ***2) Analisi del quadro normativo nazionale.***

L'intervento normativo si pone a completamento del quadro degli istituti e delle misure normative già definite dall'ordinamento per contrastare il fenomeno terrorismo con particolare riferimento alla diffusione e la propaganda di contenuti criminali attraverso l'uso della rete internet.

L'attuale normativa di contrasto al terrorismo internazionale prevista nel nostro ordinamento, innovando la precedente regolamentazione parametrata in funzione dei fenomeni di terrorismo interno riconducibili al periodo dei c.d. "anni di piombo" (l. 15 dicembre 1979, n. 625), ed intervenendo in parte ad innestare nel corpo del Codice penale e di procedura penale specifiche disposizioni di contrasto, nasce in risposta ai gravi attentati terroristici avvenuti all'estero dal 2001:

- **articoli 270-bis e segg. del Codice penale**, come integrati e modificati con successivi interventi normativi;
- **articoli 302 e 414 comma 4 del Codice penale**;
- il **d.l. 18 ottobre 2001 n. 374** (convertito con modifiche nella legge 15 dicembre 2001 n. 438) come successivamente modificato, emanato all'indomani degli attentati di New York dell'11 settembre 2001 in danno delle Torri Gemelle, recante "Disposizioni urgenti per contrastare il terrorismo internazionale";
- il **d.l. 27 luglio 2005 n. 144** (convertito con modifiche nella legge 31 luglio 2005 n. 155), come successivamente modificato, emanato a seguito agli attentati di Londra del 7 luglio 2005 in danno della rete dei trasporti pubblici, recante "Misure urgenti per il contrasto del terrorismo internazionale";
- il **d.l. 18 febbraio 2015 n. 7** (convertito con modifiche nella legge 17 aprile 2015 n. 43), come successivamente modificato, emanato in seguito agli attentati di Parigi del 7 gennaio 2015 in danno della sede del settimanale satirico Charlie Hebdo, recante "Misure urgenti per il contrasto del terrorismo, anche di matrice internazionale, nonché proroga delle missioni internazionali delle Forze armate e di polizia, iniziative di cooperazione allo sviluppo e sostegno ai processi di ricostruzione e partecipazione alle iniziative delle Organizzazioni internazionali per il consolidamento dei processi di pace e di stabilizzazione";
- il **d.l. 30 ottobre 2015 n. 174**, convertito con modificazioni dalla L. 11 dicembre 2015, n. 198, come successivamente modificato, che all'articolo 7-ter prevede "Misure di *intelligence* di contrasto in ambito cibernetico";
- la **legge 28 luglio 2016 n. 153**, recante norme per il contrasto del terrorismo, che ha introdotto nuove fattispecie penali in modo da rafforzare il contrasto al fenomeno del terrorismo internazionale;

- la **legge 20 novembre 2017, n. 167**, recante “Disposizioni per l’adempimento degli obblighi derivanti dall’appartenenza dell’Italia all’Unione europea (in particolare, art. 24).

Con riferimento invece ai moduli organizzativi che si pongono a cornice dell’odierno provvedimento, si segnalano:

- la **legge 269 del 1998** recante “*Norme contro lo sfruttamento della prostituzione, della pornografia, del turismo sessuale in danno di minori, quali nuove forme di riduzione in schiavitù*” che, all’articolo 14, individua nell’organo del Ministero dell’interno per la sicurezza e la regolarità dei servizi di telecomunicazione l’articolazione pubblica deputata a svolgere le attività occorrenti per il contrasto dei delitti di cui agli articoli 600-bis, primo comma, 600-ter, commi primo, secondo e terzo, e 600-quinquies del codice penale commessi mediante l’impiego di sistemi informatici o mezzi di comunicazione telematica ovvero utilizzando reti di telecomunicazione disponibili al pubblico.

A detta articolazione si estende ora la competenza a emettere la decisione di cui all’articolo 5, paragrafo 4, del regolamento, a sorvegliare l’attuazione delle misure specifiche adottate dai prestatori di servizi di hosting esposti a contenuti terroristici e a emettere le ulteriori decisioni di cui ai paragrafi 6 e 7 del medesimo articolo 5;

- la **legge 3 agosto 2007 n. 124**, recante “Sistema di informazione per la sicurezza della Repubblica e nuova disciplina del segreto” che, all’articolo 12, comma 3, definisce i compiti del Comitato di analisi strategica antiterrorismo (C.A.S.A.), istituito presso il Ministero dell’interno, estesi dall’attuale provvedimento all’attività di cooperazione istruttoria con gli organi del pubblico ministero, ai fini della emissione dell’ordine di rimozione (articolo 3 comma 4).

Con specifico riferimento alle misure di contrasto al fenomeno della diffusione di contenuti terroristici attraverso la rete internet, occorre precisare che già dal 2015 la legislazione italiana prevede la possibilità, per l’autorità giudiziaria, di ordinare la rimozione di contenuti digitali dalla rete o bloccare l’accesso a siti internet per prevenire e contrastare la propaganda terroristica *on line* e altre condotte criminose di natura terroristica perpetrate attraverso il *web*.

**L’articolo 2 del citato d.l. 7/2015, ai commi 2 e 3**, attribuisce alla Polizia postale e delle comunicazioni il compito di formulare ed aggiornare costantemente una *black-list* dei siti internet utilizzati per finalità terroristiche e prevede che, su richiesta dell’autorità giudiziaria procedente, i prestatori di servizi internet inibiscano l’accesso a tali siti.

Inoltre, **al successivo comma 4**, prevede la possibilità per il pubblico ministero che procede per i delitti di terrorismo (e in particolare per quelli previsti dagli articoli 270 *bis*, 270 *ter*, 270 *quater* e 270 *quinquies* del codice penale commessi con le finalità di terrorismo di cui all'articolo 270 *sexies*) e che abbia concreti elementi per ritenere che le attività criminose vengono perpetrate per via telematica di ordinare ai *service providers*, con decreto motivato, la rimozione dei contenuti entro e non oltre le 48 ore dalla ricezione della notifica dell'ordine, pena l'interdizione dell'accesso al dominio internet disposta dal giudice competente nelle forme e con le modalità del sequestro preventivo (articolo 321 c.p.p.), garantendo comunque, ove tecnicamente possibile, la fruizione dei contenuti estranei alle condotte illecite.

A completare il vigente quadro normativo concorrono altresì le seguenti disposizioni:

- **l'articolo 16 del Decreto legislativo 9 aprile 2003, n. 70** (di recepimento dell'articolo 14 della Direttiva 2000/31/CE sul commercio elettronico), dedicato ai prestatori di servizi di *hosting*, nel quale viene in linea di principio sancita l'esenzione della responsabilità del provider per le informazioni memorizzate a richiesta di un destinatario del servizio, salvo che sia a conoscenza del fatto che l'attività o l'informazione è illecita o che – non appena a conoscenza di tali circostanze, su comunicazione delle autorità competenti – non agisca immediatamente per rimuovere le informazioni o per disabilitarne l'accesso. Viene anche previsto, al comma 3 della medesima disposizione, che l'autorità giudiziaria o quella amministrativa competente possa esigere, anche in via d'urgenza, che il prestatore di servizi di *hosting* impedisca o ponga fine alle violazioni commesse;
- **l'articolo 17 del medesimo Decreto legislativo n. 70** (che attua l'articolo 15 della Direttiva 2000/31/CE), con il quale si precisa che il prestatore di servizi di hosting non è assoggettato ad un obbligo generale di sorveglianza sulle informazioni che memorizza, né ad un obbligo generale di ricercare attivamente fatti o circostanze che indichino la presenza di attività illecite, ma è comunque tenuto ad informare senza indugio l'autorità giudiziaria o quella amministrativa avente funzioni di vigilanza, qualora sia a conoscenza di presunte attività o informazioni illecite riguardanti un utilizzatore del suo servizio, nonché a fornire senza indugio, a richiesta delle autorità competenti le informazioni in suo possesso che ne consentano l'identificazione, al fine di individuare e prevenire attività illecite. Il *provider* è civilmente responsabile del contenuto di tali servizi nel caso in cui, richiesto dall'autorità giudiziaria o amministrativa avente funzioni di vigilanza, non abbia agito prontamente per

impedire l'accesso a detto contenuto, ovvero se – avendo avuto conoscenza del carattere illecito o pregiudizievole per un terzo del contenuto di un servizio al quale assicura l'accesso – non abbia provveduto ad informarne l'autorità competente.

### 3) *Incidenza delle norme proposte sulle leggi e i regolamenti vigenti.*

Il disegno di decreto legislativo incide sull'**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 pubblico ministero nell'ambito dell'attività investigativa finalizzata alla repressione dei reati di cui agli articoli 270-bis e segg. c.p. commessi con le finalità di terrorismo), che viene ora abrogato dall'articolo 8.

Con riferimento alla disposizione abrogata occorre precisare 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).

Il decreto legislativo detta inoltre una previsione che **deroga all'articolo 8-bis della legge 689/1981**.

Infatti, mentre il richiamato articolo 8-bis prevede, al comma 5, che gli effetti che la legge stabilisce per le ipotesi di reiterazione del reato non operino nel caso di pagamento in misura ridotta, l'articolo 6, comma 4, dell'adottando decreto legislativo stabilisce - in linea generale - che «[l]a reiterazione

delle violazioni, di cui all'articolo 8-bis della legge 24 novembre 1981, n. 689, opera anche nel caso di pagamento in misura ridotta».

#### **4) *Analisi della compatibilità dell'intervento con i principi costituzionali.***

Non si rilevano profili di incompatibilità con i principi costituzionali.

Giova precisare che seppur la Corte costituzionale, sin dalla sentenza n. 24 del 1973, abbia attribuito alla libertà della corrispondenza e di ogni altro mezzo di comunicazione il rango di diritto dell'individuo rientrante tra i valori supremi costituzionali, tanto da essere espressamente qualificato dall'art. 15 della Costituzione come diritto inviolabile, ha pur sempre pacificamente riconosciuto che *«la libertà di manifestazione del pensiero, garantita dall'art. 21, primo comma, della Costituzione»*, che attraverso il libero accesso ai mezzi di comunicazione si estrinseca, *«trova i suoi limiti non soltanto nella tutela del buon costume, ma anche nella necessità di proteggere altri beni di rilievo costituzionale e nell'esigenza di prevenire e far cessare turbamenti della sicurezza pubblica, la cui tutela costituisce una finalità immanente del sistema (sentenze n. 19 dell'8 marzo 1962, n. 87 del 6 luglio 1966, n. 84 del 2 aprile 1969)»* (Corte Costituzionale, sent. n. 65 del 1970).

È pienamente conforme ai principi costituzionali, pertanto, un intervento normativo finalizzato ad una regolamentazione della diffusione on line di contenuti che possano attentare all'ordine pubblico e alla sicurezza della collettività, quest'ultima considerata bene inerente al vigente sistema costituzionale il cui mantenimento *«rappresenta una finalità immanente dello stesso sistema»* (Corte costituzionale, sent. n. 15 del 1973)<sup>1</sup>.

#### **5) *Analisi delle compatibilità dell'intervento con le competenze e le funzioni delle regioni ordinarie e a statuto speciale nonché degli enti locali.***

Il presente schema di decreto legislativo non presenta aspetti di interferenza o di incompatibilità con le competenze costituzionali delle regioni, incidendo su materie riservate alla competenza legislativa esclusiva dello Stato (art. 117, lettere *l*) ed *h*) della Costituzione), riferendosi ad attività di prevenzione del terrorismo nel perseguimento di interessi costituzionali relativi alla sicurezza,

---

<sup>1</sup> Nello stesso senso Corte Costituzionale, sent. n. 19 del 1962: *«Se per turbamento dell'ordine pubblico bisogna intendere l'insorgere di un concreto ed effettivo stato di minaccia per l'ordine legale mediante mezzi illegali idonei a scuoterlo - ed è da escludere che possa intendersi altro -, è perciò chiaro che non possono esser considerate in contrasto con la Costituzione le disposizioni legislative che effettivamente, e in modo proporzionato, siano volte a prevenire e reprimere siffatti turbamenti. Né può costituire impedimento all'emanazione di disposizioni del genere l'esistenza di diritti costituzionalmente garantiti. Infatti, la tutela costituzionale dei diritti ha sempre un limite insuperabile nella esigenza che attraverso l'esercizio di essi non vengano sacrificati beni, ugualmente garantiti dalla Costituzione. Il che tanto più vale, quando si tratti di beni che - come l'ordine pubblico - sono patrimonio dell'intera collettività. Occorre perciò concludere che anche la libertà di manifestazione del pensiero (come del resto questa Corte già ha avuto occasione di affermare nelle sentenze n. 1 del 1956, e nn. 33, 120 e 121 del 1957) incontra un limite nell'esigenza di prevenire o far cessare turbamenti dell'ordine pubblico»*.

all'ordine pubblico e alla pacifica convivenza, che l'art. 117, secondo comma, lettera h), riserva allo Stato in quanto afferente le funzioni primariamente dirette a tutelare «beni fondamentali, quali l'integrità fisica o psichica delle persone, la sicurezza dei possessi ed ogni altro bene che assume prioritaria importanza per l'esistenza stessa dell'ordinamento» (sentenza n. 105 del 2006, con richiamo a sentenza n. 290 del 2001).

**6) *Verifica della compatibilità con i principi di sussidiarietà, differenziazione ed adeguatezza sanciti dall'articolo 118, primo comma, della Costituzione.***

Le disposizioni contenute nel disegno di decreto legislativo esaminato sono compatibili e rispettano i principi di cui all'art. 118 della Costituzione, in quanto non prevedono né determinano, sia pure in via indiretta, nuovi o più onerosi adempimenti a carico degli Enti locali.

**7) *Verifica dell'assenza di rilegificazioni e della piena utilizzazione delle possibilità di delegificazione e degli strumenti di semplificazione normativa.***

L'intervento normativo attiene a materia regolata da disposizioni di rango primario e, come tale, non pone possibilità di delegificazione od ulteriori possibilità di semplificazione normativa.

**8) *Verifica dell'esistenza di progetti di legge vertenti su materia analoga all'esame del Parlamento e relativo stato dell'iter.***

Non risultano pendenti in Parlamento iniziative normative in materia analoga a quella trattata nella proposta qui analizzate.

**9) *Indicazioni delle linee prevalenti della giurisprudenza ovvero della pendenza di giudizi di costituzionalità sul medesimo o analogo progetto.***

Le disposizioni contenute nel provvedimento non contrastano con i principi fissati in materia dalla giurisprudenza anche costituzionale, così come ampiamente rappresentato al punto 4 che precede. Non risultano giudizi di costituzionalità pendenti sul medesimo oggetto.

## **PARTE II. CONTESTO NORMATIVO COMUNITARIO E INTERNAZIONALE**

**10) *Analisi della compatibilità dell'intervento con l'ordinamento comunitario.***

Il provvedimento non presenta aspetti di interferenza o di incompatibilità con l'ordinamento europeo. Anzi, è volto ad implementare nell'ordinamento nazionale tutte le misure organizzative ed ordinamentali definite dal Regolamento (UE) 2021/784.

L'iniziativa legislativa si basa sull'articolo 114 del Trattato sul funzionamento dell'Unione europea (TFEU), dedicato al ravvicinamento delle normative degli Stati membri in materia di funzionamento del mercato interno.

La Commissione europea mira, invero, a stabilire un quadro giuridico chiaro e armonizzato per prevenire l'uso improprio dei servizi di hosting per la diffusione di contenuti terroristici on line, garantendo il corretto funzionamento del mercato unico digitale attraverso condizioni di parità per tutti i service provider che offrano i propri servizi sul territorio dell'Unione, tutelando altresì la fiducia e la sicurezza dei cittadini.

***11) Verifica dell'esistenza di procedure d'infrazione da parte della Commissione europea sul medesimo o analogo oggetto.***

Come già segnalato, con nota C (2023) 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 adempiuto agli obblighi derivanti dal Regolamento. La finalità dello schema di decreto è, pertanto, quella di dare piena attuazione alle misure organizzative ed ordinamentali che si rendono necessarie per garantire la piena operatività della normativa eurounitaria e consentire la chiusura della procedura di infrazione attualmente pendente.

***12) Analisi della compatibilità dell'intervento con gli obblighi internazionali.***

Per quanto appena notato, l'intervento è imposto dal rispetto degli obblighi internazionali derivanti dall'appartenenza dell'Italia all'Unione europea.

***13) Indicazioni delle linee prevalenti della giurisprudenza ovvero della pendenza di giudizi innanzi alla Corte di Giustizia delle Comunità europee sul medesimo o analogo oggetto.***

Non risultano giudizi pendenti innanzi alla Corte di Giustizia delle Comunità europee sul medesimo o analogo oggetto.

Si segnala peraltro che la piena compatibilità delle misure introdotte con i principi generali enunciati dalla Corte di Giustizia in precedenti pronunce.

Nella sentenza *Glawischnig-Piesczek* del 3 ottobre 2019 la Corte di Giustizia, adita con domanda di pronuncia pregiudiziale avente ad oggetto l'interpretazione dell'articolo 14, paragrafi 1 e 3 della Direttiva 2000/31/CE, ha ritenuto legittima la previsione che consente ai giudici nazionali di imporre misure di rimozione o di blocco di contenuti d'odio dichiarati illeciti «*al fine di poter ottenere dal prestatore di servizi di hosting di cui trattasi che egli impedisca qualsiasi ulteriore danno agli interessi in causa, è legittimo che il giudice competente possa esigere da tale prestatore di servizi di hosting di bloccare l'accesso alle informazioni memorizzate, il cui contenuto sia identico a quello precedentemente dichiarato illecito, o di rimuovere tali informazioni, qualunque sia l'autore della richiesta di memorizzazione delle medesime. Orbene, tenuto conto, in particolare, di tale identità di contenuto delle informazioni di cui trattasi, non si può ritenere che l'ingiunzione*

*all'uopo emessa ponga a carico del prestatore di servizi di hosting un obbligo di sorveglianza, in via generale, sulle informazioni da esso memorizzate, né un obbligo generale di ricercare attivamente fatti o circostanze che indichino la presenza di attività illecite, ai sensi dell'articolo 15, paragrafo 1, della direttiva 2000/31».*

***14) Indicazioni delle linee prevalenti della giurisprudenza ovvero della pendenza di giudizi innanzi alla Corte Europea dei Diritti dell'uomo sul medesimo o analogo oggetto.***

Non risultano giudizi pendenti innanzi alla Corte Europea dei Diritti dell'uomo sul medesimo o analogo oggetto.

Si segnala peraltro che la piena compatibilità delle misure introdotte con i principi generali enunciati dalla Corte Europea dei Diritti dell'Uomo in precedenti pronunce che, seppur facenti riferimento ad altre fattispecie, possono essere analogicamente estesi anche alla pubblicazione di contenuti terroristici.

Nel caso Delfi c. Estonia, si è affermata la responsabilità dei prestatori che svolgono un ruolo attivo ma non contrastano la diffusione di contenuti manifestamente illeciti, caricati da terzi, di cui abbiano il controllo, ovvero, qualora non ne abbiano il controllo e laddove l'illiceità dei contenuti non sia manifesta, che omettano di contrastarla pure a seguito di ingiunzioni specifiche (Prima sezione, sent. 10 ottobre 2013; Grande Camera, sent. 16 giugno 2015). La Corte EDU ha ritenuto che, nei casi in cui i commenti degli utenti assumono la forma di incitamento all'odio e di minacce dirette all'integrità fisica delle persone, i diritti e gli interessi di altri e della società nel suo insieme possono autorizzare gli Stati contraenti a imporre responsabilità ai portali di notizie su Internet che non adottano misure atte a rimuovere senza indugio i commenti palesemente illeciti, senza che ciò costituisca una violazione dell'articolo 10 della Convenzione.

***15) Eventuali indicazioni sulle linee prevalenti della regolamentazione sul medesimo oggetto da parte di altri Stati membri dell'Unione Europea.***

Non risultano indicazioni da parte di altri Stati membri dell'Unione Europea.

### **PARTE III. ELEMENTI DI QUALITÀ SISTEMATICA E REDAZIONALE DEL TESTO**

***1) Individuazione delle nuove definizioni normative introdotte dal testo, della loro necessità, della coerenza con quelle già in uso.***

L'**articolo 2** reca talune definizioni volte a semplificare la formulazione delle disposizioni del decreto. Nello specifico, si riepilogano le seguenti definizioni utilizzate, in parte mutate da ulteriori vigenti disposizioni normative:

- a) il *Comitato di analisi strategica antiterrorismo (C.A.S.A.)*: il Comitato di cui all'articolo 12, comma 3, della legge 3 agosto 2007, n. 124, istituito presso il Dipartimento della pubblica sicurezza con decreto del Ministro dell'interno che ne definisce anche la composizione e le modalità di funzionamento;
- b) il *Dipartimento della pubblica sicurezza*: il Dipartimento della pubblica sicurezza di cui all'articolo 4, della legge 1° aprile 1981, n. 121;
- c) l'*Organo del Ministero dell'interno per la sicurezza e la regolarità dei servizi di telecomunicazione*: l'organo di cui all'articolo 14, comma 2, della legge 3 agosto 1998, n. 269;

**2) *Verifica della correttezza dei riferimenti normativi contenuti nel progetto, con particolare riguardo alle successive modificazioni e integrazioni subite dai medesimi.***

I riferimenti normativi che figurano nello schema di atto normativo sono corretti.

**3) *Ricorso alla tecnica della novella legislativa per introdurre modificazioni ed integrazioni a disposizioni vigenti.***

Il provvedimento in esame introduce disposizioni normative autonome di adattamento dell'ordinamento giuridico nazionale alle previsioni del Regolamento, non facendo quindi ricorso alla tecnica della novella.

**4) *Individuazione di effetti abrogativi impliciti di disposizioni dell'atto normativo e loro traduzione in norme abrogative espresse nel testo normativo.***

Come già segnalato, il disegno di decreto legislativo abroga espressamente l'articolo 2, comma 4, del decreto-legge 18 febbraio 2015, n. 7, convertito, con modificazioni, dalla legge 17 aprile 2015, n. 43. L'intervento normativo non comporta, per contro, effetti abrogativi impliciti.

**5) *Individuazione di disposizioni dell'atto normativo aventi effetto retroattivo o di reviviscenza di norme precedentemente abrogate o di interpretazione autentica o derogatorie rispetto alla normativa vigente.***

Si è già segnalato il carattere derogatorio della previsione di cui all'articolo 6, comma 4, del emanando decreto legislativo rispetto all'articolo 8-bis della legge 689/1981 (v. Parte I, *sub* 3).

**6) *Verifica della presenza di deleghe aperte sul medesimo oggetto, anche a carattere integrativo o correttivo.***

Non vi sono norme di delega aperte relative alla medesima materia.

**7) *Indicazione degli eventuali atti successivi attuativi; verifica della congruenza dei termini previsti per la loro adozione.***

Il provvedimento non prevede successivi interventi attuativi. Deve peraltro rammentarsi che, secondo quanto previsto dall'articolo 6, comma 7, la cooperazione tra l'Organo del Ministero dell'interno per la sicurezza e la regolarità dei servizi di telecomunicazione e il Ministero delle Imprese e del Made in Italy si svolgerà sulla base di una convenzione operativa che i due Dicasteri sottoscriveranno entro novanta giorni dall'entrata in vigore del decreto legislativo. Il termine indicato appare congruo, avuto anche riguardo a pregressi analoghi rapporti collaborativi delle due amministrazioni.

**8) *Verifica della piena utilizzazione e dell'aggiornamento di dati e di riferimenti statistici attinenti alla materia oggetto del provvedimento, ovvero indicazione della necessità di commissionare all'Istituto nazionale di statistica apposite elaborazioni statistiche con correlata indicazione nella relazione economico-finanziaria della sostenibilità dei relativi costi.***

Per la predisposizione dell'intervento normativo sono stati utilizzati dati e riferimenti statistici già in possesso presso l'Amministrazione proponente.

6022/10.3.140  
355



*Ministero della Giustizia*  
*Ufficio Legislativo*

**Alla Presidenza del Consiglio dei Ministri  
Capo del Dipartimento per gli Affari Giuridici e Legislativi**

**RICHIESTA DI ESENZIONE DALL'AIR**

Si richiede, ai sensi dell'articolo 7 co. 1 del d.p.c.m. 15 settembre 2017, n. 169, l'esenzione dall'obbligo di redazione della AIR con riferimento allo schema di decreto legislativo recante **"Adeguamento della normativa nazionale alle disposizioni del Regolamento (UE) 2021/784, relativo al contrasto della diffusione di contenuti terroristici *online*"** (di seguito: il Regolamento),

in relazione al ridotto impatto dell'intervento in presenza delle seguenti condizioni, congiuntamente considerate:

- a) costi di adeguamento attesi di scarsa entità in relazione ai singoli destinatari;
- b) numero esiguo dei destinatari dell'intervento;
- c) risorse pubbliche impiegate nell'ambito degli ordinari stanziamenti di bilancio;
- d) impatto non rilevante sugli assetti concorrenziali del mercato.

A tal fine, si rappresenta quanto segue.

**a) Costi di adeguamento attesi di scarsa entità in relazione ai singoli destinatari**

Con il presente schema di decreto legislativo si dà attuazione all'articolo 15 della legge 4 agosto 2022, n. 127 (Legge di delegazione europea 2021), con cui il Governo è stato delegato ad adottare le disposizioni necessarie ad adeguare l'ordinamento nazionale al Regolamento (UE) 2021/784, relativo al contrasto della diffusione di contenuti terroristici *online*, anche in esito alla lettera della Commissione di *messa in mora* dell'Italia per non aver adempiuto agli obblighi derivanti dal sopra citato Regolamento sul contrasto della diffusione di contenuti

terroristici online.

Il Regolamento è volto a garantire il buon funzionamento del mercato unico digitale in tutta l'Unione contrastando l'uso improprio dei servizi di hosting a fini terroristici e contribuendo alla sicurezza pubblica.

In particolare, col presente intervento normativo, si **provvede alla 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.**

Le norme in esame non comportano costi di adeguamento e, quanto agli oneri amministrativi, si nota che essi si ricollegano essenzialmente al Regolamento, atto che - per sua natura - è obbligatorio in tutti i suoi elementi e direttamente applicabile in ciascuno degli Stati membri (a decorrere dal 7 giugno 2022). È dunque alla sovraordinata fonte eurounitaria, e non al decreto legislativo recante mere norme di adattamento interno, che detti oneri debbono ritenersi in via immediata ricollegabili.

Inoltre, come la stessa Commissione europea ha evidenziato nella valutazione di impatto del Regolamento, *«[s]ulla base del numero di fornitori di servizi attualmente identificati come possibili host di contenuti terroristici, gli obblighi relativi alle misure proattive e alla conservazione dei dati riguarderebbero in linea di principio tra 150 e 400 società, quindi tra l'1,5% e il 4% dei 10.000 fornitori di servizi di hosting sopra menzionati»*<sup>1</sup>. Conseguentemente, gli obblighi definiti dalla normativa risultano essere ampiamente mitigati sia dalla garanzia che si tratta di misure proporzionate e facilmente attuabili grazie a risorse già internalizzate, sia dal fatto che ricadono su pochissimi destinatari.

Nel dettaglio, si osserva quanto segue.

Gli **articoli 1, 2 ed 8** sono norme, rispettivamente, di inquadramento normativo e definitorio, nonché di coordinamento ordinamentale, per loro natura non suscettibili di comportare costi di adeguamento in capo ai destinatari delle disposizioni.

Gli **articoli 3, 4, 6 e 7** recano, invece, la disciplina dell'emissione degli ordini di rimozione, dell'esame degli ordini di rimozione transfrontalieri e delle sanzioni penali e amministrative applicabili. Dette norme si configurano come disposizioni di natura ordinamentale, sostanziale e processuale, che non comportano costi amministrativi di adeguamento in capo ai destinatari, se non di modesta entità.

In particolare, sia articolo 3, comma 1, sia l'articolo 4, comma 1, stabiliscono i criteri per l'individuazione dell'autorità giudiziaria competente a procedere.

La restante parte dell'articolato, invece, reca descrizione degli istituti e dei moduli processuali applicabili alle fattispecie incriminatrici introdotte dal provvedimento.

---

<sup>1</sup> *European commission - Proposal for a Regulation of the European Parliament and of the Council on preventing the dissemination of terrorist content online - Impact assessment (COM(2018) 640 final) - paragrafo 6.1.2.*

L'articolo 5, infine, attribuisce all'Organo del Ministero dell'interno per la sicurezza e la regolarità dei servizi di telecomunicazione la competenza:

- a emettere la decisione con cui, ai sensi dell'articolo 5, paragrafo 4, del regolamento, si accerta che il prestatore dei servizi di hosting è "esposto a contenuti terroristici";
- a sorvegliare l'attuazione delle misure specifiche che, a seguito di detto accertamento, il prestatore di servizi di hosting è tenuto ad adottare;
- a emettere le ulteriori decisioni di cui ai paragrafi 6 e 7 del medesimo articolo 5.

Prevede, inoltre, che per l'impugnazione delle decisioni assunte dall'Organo del Ministero dell'interno per la sicurezza e la regolarità dei servizi di telecomunicazione al prestatore di servizi di hosting è possibile ricorrere al competente tribunale amministrativo regionale entro sessanta giorni dalla notifica.

In conclusione, la natura ordinamentale e procedurale dell'intervento porta ad escludere la configurazione di costi di adeguamento in capo ai cittadini, mentre gli adempimenti eventualmente connessi all'implementazione delle previsioni introdotte (così come le misure organizzative descritte dall'articolo 3, comma 2) costituiscono esercizio delle competenze istituzionali proprie degli apparati giudiziari ed amministrativi interessati e, pertanto, afferiscono all'esercizio di funzioni nell'ambito di istituti e moduli procedurali già noti all'ordinamento, che non richiedono lo sviluppo ovvero l'esercizio di ulteriori e diverse competenze rispetto a quelle già in essere.

Ai relativi adempimenti, pertanto, le amministrazioni interessate provvederanno con le risorse umane, strumentali e finanziarie disponibili a legislazione vigente.

#### **b) Numero esiguo dei destinatari dell'intervento**

La disciplina introdotta è destinata ad operare in un numero limitato di casi, attesa la specificità della fattispecie e le stigmatizzate modalità della condotta.

Orbene, per quanto di interesse, dai dati forniti dalla Polizia postale (sito - *sezione cyberterrorismo*) emerge come, a fronte dei numerosi siti monitorati, soltanto un esiguo numero di casi sia stato poi sottoposto al vaglio giudiziale con successiva rimozione dei contenuti.

#### **A titolo esemplificativo:**

- **Anno 2018** su circa 36mila spazi web monitorati (siti, blog, forum, portali di social network) sono stati rimossi circa 250 contenuti;
- **Anni 2021-2022**

<b>Cyberterrorismo<sup>2</sup></b>	<b>2021</b>	<b>2022*</b>
<b>Casi trattati</b>	1.321	1.193
<b>Persone indagate</b>	80	66
<b>Spazi virtuali monitorati</b>	126.998	173.306
/ Estremismo internazionale religioso / estremismo razziale, antagonista ed anarchico		
* Dati rilevati il 27/12/2022		

Peraltro, il dato numerico relativo alle persone indagate, che ammonta a poche decine di unità, conferma quanto assunto dalla scrivente amministrazione circa l'esiguità del numero dei destinatari dell'intervento.

Ulteriore conferma di detto assunto si ritrae dai dati relativi alla - anch'essa assai limitata - diffusione dei delitti con finalità di terrorismo nel nostro paese, rappresentata con buona approssimazione nel seguente grafico tratto dal "*Terrorism Situation e and Trend report*" del 2020 dell'Unione Europea-Europol, dal quale emerge il numero limitato di processi istruiti e di condanne irrogate:

<sup>2</sup> Fonte dati: Ministero dell'Interno – Commissariato di P.S. on line – "Resoconto attività 2022 della polizia postale e delle comunicazioni e dei centri operativi sicurezza cibernetica" del 03.01.2023 (<https://www.commissariatodips.it/notizie/articolo/resoconto-attivita-2022-della-polizia-postale-e-delle-comunicazioni-e-dei-centri-operativi-sicurezza/index.html>)

## annex 4

## Convictions and penalties

This annex contains statistical information on the concluded court proceedings for terrorist offences in 2019, as reported to Eurojust. It highlights some key figures and, where relevant, compares those with the figures for previous years.

table / Number of convictions and acquittals for terrorist offences per EU Member State in 2017, 2018<sup>1</sup> and 2019<sup>2</sup>, as reported to Eurojust.

Member State	2017	2018	2019
Austria	18	36	40
Belgium	85	80	91
Bulgaria		1	
Czechia	8	7	
Denmark	4	6	4
Estonia	2		
Finland	2	1	
France	122	141	105
Germany	34	57	53
Greece	10	34	48
Hungary		3	6
Italy	23	15	17
Lithuania	2	10	
Netherlands	46	37	56
Poland	4		
Portugal	1		1
Slovenia		1	
Spain	71	120	97
Sweden	3	1	5
UK	125	115	
<b>Total</b>	<b>569</b>	<b>664</b>	<b>520</b>

<sup>1</sup> The data for the previous years corresponds to the data reported in the respective TE-SAT reports.

<sup>2</sup> Eurojust received contributions containing information on terrorist related court decisions in 2019 from the following EU Member States: Austria, Belgium, Denmark, France, Germany, Greece, Hungary, Italy, the Netherlands, Portugal, Spain and Sweden. In case a verdict pronounced in 2019 was appealed and the appeal was concluded before the end of the year, Eurojust reports only on the final verdict.

- › Eurojust was informed of concluded court proceedings for terrorist offences in 2019 that took place in 12 EU Member States and resulted in 520 convictions and acquittals.
- › In 2019 the greatest number of convictions and acquittals was reported to Eurojust by France (105), Spain (97) and Belgium (91).

table / Number of convictions and acquittals per EU Member State in 2019, as reported to Eurojust.

Member State	Convictions	Acquittals	Total	Acquittals in %
Austria	29	11	40	28
Belgium	85	6	91	7
Denmark	4	-	4	0
France	105	-	105	0
Germany	50	3	53	6
Greece	31	14	45	31
Hungary	6	-	6	0
Italy	12	5	17	29
Netherlands	43	13	56	23
Portugal	1	-	1	0
Spain	79	18	97	19
Sweden	4	1	5	20
<b>Total</b>	<b>449</b>	<b>71</b>	<b>520</b>	<b>14</b>

**c) Risorse pubbliche impiegate nell'ambito degli ordinari stanziamenti di bilancio**

Con riferimento all'impatto finanziario dell'intervento, si specifica che le disposizioni del presente intervento normativo, configurandosi come norme di carattere definitorio, di coordinamento ordinamentale, ovvero di natura procedimentale e precettiva, non determinano nuovi o maggiori oneri a carico della finanza pubblica, potendo essere attuate con le risorse umane, strumentali e finanziarie disponibili a legislazione vigente, conformemente a quanto precisato dall'**articolo 9, comma 1**.

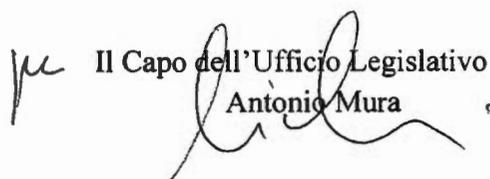
**d) Impatto non rilevante sugli assetti concorrenziali del mercato.**

Le disposizioni sopra esaminate non impattano per loro intrinseca natura sugli assetti concorrenziali del mercato e non presentano aspetti di interferenza o di incompatibilità con l'ordinamento europeo, anzi sono volte all'adeguamento dell'ordinamento nazionale al Regolamento (UE) 2021/784.

L'intervento normativo, oltre che volto a salvaguardare la libertà di espressione (compresa la libertà di ricevere e comunicare informazioni e idee in una società aperta e democratica) e la libertà e il pluralismo dei media, si può ritenere anche proiettato a garantire un miglioramento del funzionamento del mercato unico digitale, da perseguirsi tramite un rafforzamento non solo della certezza del diritto per i prestatori di servizi di *hosting* ma anche e soprattutto della fiducia degli utilizzatori nell'ambiente *online*, che spesso costituisce anch'esso un "ambiente di mercato" promotore di crescita, competitività e fattore di proiezione ad uno sviluppo in senso maggiormente concorrenziale degli assetti economici, con conseguente maggiore diffusione dei servizi digitali e relativi investimenti.

L'intervento normativo contribuisce quindi a limitare la frammentazione del mercato interno con specifico riferimento alle procedure amministrative e gli obblighi richiesti ai prestatori di servizi di *hosting*, con conseguente aumento della certezza del diritto per i prestatori di servizi e riduzione dei costi operativi.

Roma, 27 aprile 2023

 Il Capo dell'Ufficio Legislativo  
Antonio Mura

VISTO  
Roma,

Il Capo del Dipartimento per gli Affari Giuridici e Legislativi



