DIRITTO PENALE CONTEMPORANEO

DIRITTO PENALE CONTEMPORANEO

Fascicolo
4/2019

ISSN 2039-1676

Diritto Penale Contemporaneo è un periodico on line, ad accesso libero e senza fine di profitto, nato da un'iniziativa comune di Luca Santa Maria, che ha ideato e finanziato l'iniziativa, e di Francesco Viganò, che ne è stato sin dalle origini il direttore nell'ambito di una partnership che ha coinvolto i docenti, ricercatori e giovani cultori della Sezione di Scienze penalistiche del Dipartimento "C. Beccaria" dell'Università degli Studi di Milano. Attualmente la rivista è edita dall'Associazione "Diritto penale contemporaneo", il cui presidente è l'Avv. Santa Maria e il cui direttore scientifico è il Prof. Gian Luigi Gatta. La direzione, la redazione e il comitato scientifico della rivista coinvolgono oggi docenti e ricercatori di numerose altre università italiane e straniere, nonché autorevoli magistrati ed esponenti del foro.
Tutte le collaborazioni organizzative ed editoriali sono a titolo gratuito e agli autori non sono imposti costi di elaborazione e pubblicazione.

La rivista fa proprio il Code of Conduct and Best Practice Guidelines for Journal Editors elaborato dal COPE (Comittee on Publication Ethics).

***Peer review*.**
Salvo che sia diversamente indicato, tutti i contributi pubblicati nella sezione *papers* di questo fascicolo hanno superato una procedura di *peer review*, attuata secondo principi di trasparenza, autonomia e indiscusso prestigio scientifico dei revisori, individuati secondo criteri di competenza tematica e di rotazione all'interno dei membri del Comitato scientifico. Ciascun lavoro soggetto alla procedura viene esaminato in forma anonima da un revisore, il quale esprime il suo parere in forma parimenti anonima sulla conformità del lavoro agli standard qualitativi delle migliori riviste di settore. La pubblicazione del lavoro presuppone il parere favorevole del revisore. Di tutte le operazioni compiute nella procedura di *peer review* è conservata idonea documentazione presso la redazione.

Modalità di citazione.
Per la citazione dei contributi presenti nei fascicoli di *Diritto penale contemporaneo*, si consiglia di utilizzare la forma di seguito esemplificata: N. COGNOME, *Titolo del contributo*, in *Dir. pen. cont.*, fasc. 1/2017, p. 5 ss.

4/2019

CONTENUTI TERRORISTICI *ON LINE*: L'UNIONE EUROPEA LAVORA A NUOVE NORME PER PREVENIRNE LA DIFFUSIONE

di Raffaella Pezzuto

SOMMARIO: 1. Il quadro di riferimento: cenni alla normativa europea in materia di lotta al terrorismo e alla radicalizzazione violenta – 2. La proposta di Regolamento della Commissione europea sulla prevenzione della diffusione di contenuti terroristici *on line* (COM(2018)640 finale) alla luce dell'orientamento generale del Consiglio UE del 6 dicembre 2018 (ST15336/18): novità e finalità – 2.1. Ambito di applicazione soggettiva: il prestatore di servizi di *hosting* – 2.2. Ambito di applicazione oggettiva: la diffusione di contenuti terroristici *on line* – 2.3. Gli obblighi a carico del prestatore di servizi di *hosting* – 2.4. La tutela dei diritti fondamentali e i meccanismi di reclamo e di ricorso giudiziario – 2.5. La cooperazione tra gli Stati membri, gli organismi dell'Unione e i prestatori di servizi di *hosting* – 3. La normativa italiana in materia di rimozione dei contenuti terroristici dal *web*: prime riflessioni sulla compatibilità con il Regolamento in fase di adozione.

1. Il quadro di riferimento: cenni alla normativa europea in materia di lotta al terrorismo e alla radicalizzazione violenta.

Dopo gli sconvolgenti attentati dell'11 settembre 2001, l'Unione europea ha preso atto della necessità di promuovere misure di prevenzione e contrasto del terrorismo internazionale su due diversi fronti: l'uno di carattere repressivo, favorendo l'armonizzazione delle norme di diritto penale in tutti gli Stati membri e rafforzando i meccanismi di cooperazione giudiziaria e di scambio di informazioni; l'altro diretto alla realizzazione di politiche di sicurezza e socio-culturali idonee a disinnescare la potentissima arma della radicalizzazione violenta.

Sul primo fronte, furono immediatamente adottati una serie di strumenti cruciali per assicurare una risposta giudiziaria efficace al terrorismo e alla criminalità organizzata transnazionale, tra i quali si segnalano la Decisione quadro 2002/584/GAI sul mandato di arresto europeo, la Decisione 2002/187/GAI istitutiva di Eurojust[1] (successivamente modificata dalla Decisione 2009/426/GAI[2] e da ultimo sostituita dal

[1] Sull'istituzione di Eurojust v. L. SALAZAR, *Eurojust: una prima realizzazione della decisione del Consiglio europeo di Tampere*, in *Doc. giust.*, 2000, n. 6, c. 1339; G. DE AMICIS, *La costruzione di Eurojust nell'ambito del terzo pilastro dell'Unione europea*, in *Cass. pen.*, 2001; G. CASELLI – G. DE AMICIS, *La natura di Eurojust e la sua attuazione nell'ordinamento interno*, in *Dir. e giustizia*, 2003, 28, 94 ss.; G. SANTALUCIA, *Le misure di legislazione interna per l'Eurojust, in Diritto e formazione*, 2003, 1705 ss.; G. NICASTRO, *Eurojust*, in AA.VV., *Diritto penale europeo e ordinamento italiano*, Milano, 2006, 63 ss.

[2] Sulle modifiche introdotte dalla Decisione 2009/426/GAI, vedi C. FERRARA, *La decisione del Consiglio*

Regolamento 1727 del 14 novembre 2018 istitutivo dell'Agenzia dell'Unione europea per la cooperazione giudiziaria penale[3]), nonché la Decisione quadro del Consiglio 2002/475/GAI in materia di lotta al terrorismo (successivamente modificata dalla Decisione quadro 2008/919/GAI), nella quale venivano stabilite norme comuni di incriminazione delle condotte di terrorismo. Con quest'ultima, in particolare, veniva per la prima volta riconosciuta a livello europeo l'importanza di una strategia comune per il contrasto e la prevenzione del terrorismo di matrice jihadista. L'obiettivo era quello di rendere omogenea in tutti gli Stati Membri la definizione dei reati terroristici, compresa quella dei reati riconducibili ad organizzazioni terroristiche; di introdurre nuove fattispecie comuni di reato, volte ad anticipare la soglia di punibilità anche a condotte prodromiche all'atto terroristico; di prevedere pene e sanzioni commisurate alla gravità dei reati per le persone fisiche o giuridiche responsabili di tali reati. Si mirava, inoltre, a stabilire regole armonizzate di giurisdizione per garantire che i reati di terrorismo potessero essere perseguiti in modo efficace, nonché a prevedere specifiche misure per la protezione delle vittime[4]. L'impianto normativo della Decisione in parola si è talmente sedimentato nel diritto positivo degli Stati membri, divenendo un *acquis* europeo, che molte delle previsioni in essa contenute sono state riprese e potenziate dalla Direttiva del 15 marzo 2017 n. 541 sulla lotta al terrorismo, emanata al fine di aggiornare ed estendere il quadro europeo di tutela penale[5].

2002/187/GAI del 28 febbraio 2002 che istituisce Eurojust e successive modificazioni con particolare riferimento alle disposizioni inerenti i poteri del collegio e del membro nazionale, in AA.VV., *Il diritto penale e la procedura penale negli strumenti legislativi dell'Unione Europea*, Vol. I, in coll. *Diritto dell'Unione europea e diritti umani* a cura di Roberto Conti, Padova, 2011, 108 ss.; F. SPIEZIA, *I cambiamenti in corso nello Spazio europeo di libertà, sicurezza e giustizia: quale futuro per Eurojust?*, in questa *Rivista*, 19 marzo 2015. Il 1° dicembre 2009, a pochi mesi di distanza dalla pubblicazione nella Gazzetta ufficiale della Decisione 2009/426/GAI, entrò in vigore il Trattato di Lisbona, recante, all'art. 85 TFUE, il nuovo quadro giuridico per Eurojust, assegnandole il compito di sostegno e potenziamento alla cooperazione giudiziaria. In particolare il Trattato introdusse la possibilità, legiferando attraverso lo strumento del regolamento, di ricomprendere tra i compiti di Eurojust anche il potere di a) avviare indagini penali o proporne l'avvio alle autorità nazionali competenti; b) coordinare le indagini avviate o delle quali è stato proposto l'avvio; c) potenziare la cooperazione giudiziaria, anche attraverso la composizione dei conflitti di competenza tra le autorità giudiziarie degli Stati membri.

[3] Il 14 novembre 2018 è stato adottato il nuovo Regolamento (UE) 2018/1727 del Parlamento europeo e del Consiglio che istituisce l'Agenzia dell'Unione europea per la cooperazione giudiziaria penale (Eurojust) che sostituisce, abrogandola, la precedente decisione 2002/187/GAI. Pur essendo entrato in vigore l'11 dicembre 2018, il Regolamento si applicherà solo a decorrere dal 12 dicembre 2019, al fine di consentire agli Stati membri un congruo periodo di adattamento alle novità recate dallo stesso. Vedasi sulla genesi e sulle innovazioni dallo stesso introdotte, L. SALAZAR, *La riforma di Eurojust e i suoi riflessi sull'ordinamento italiano*, in questa *Rivista*, fasc. 1/2019, p. 43 ss.

[4] Vedasi al riguardo N. PIACENTE, *La decisione quadro del Consiglio 2002/475/GAI del 13 giugno 2002 sulla lotta contro il terrorismo e successive modifiche*, in AA.VV., *Il diritto penale e la procedura penale negli strumenti legislativi dell'Unione Europea*, *cit*., 70 ss.

[5] Con la Direttiva UE del 14 marzo 2017 n. 541, che ha sostituito la Decisione del Consiglio 2002/475/GAI abrogandola, il Parlamento europeo e il Consiglio hanno ravvisato soprattutto la necessità di dare una risposta efficace al fenomeno dei combattenti terroristi stranieri (*foreign terrorist fighters*), adempiendo agli obblighi internazionali derivanti sia dalla Risoluzione del Consiglio di Sicurezza delle Nazioni Unite 2178/2014, che dalla Convenzione di Varsavia del Consiglio d'Europa per la prevenzione del terrorismo (2005) e dal suo Protocollo addizionale fatto a Riga nel 2015. In particolare, la Direttiva ha introdotto come

A seguito degli attentati del marzo 2004 a Madrid e del luglio 2005 a Londra, veniva inoltre adottata la Decisione 2005/671/GAI concernente lo scambio di informazioni e la cooperazione in materia di reati terroristici, chiedendo a ciascuno Stato membro di trasmettere le relative informazioni ad Eurojust, Europol e agli altri Stati membri, nonché di designare un'autorità quale corrispondente nazionale di Eurojust per le questioni legate al terrorismo. Tale disciplina è stata rafforzata sia attraverso le integrazioni apportate all'articolo 2 dalla sopra menzionata Direttiva 2017/541, che dalla recente entrata in vigore del Regolamento del 14 novembre 2018 su Eurojust, il quale non ha previsto modifiche sostanziali dal punto di vista dei meccanismi reciproci di informazione, ma ha sicuramente conferito agli stessi maggiore incisività in virtù della natura regolamentare della fonte legislativa che ora li prevede, vincolando gli Stati membri in maniera diretta ed immediata anche per ciò che attiene ai loro obblighi di completa e tempestiva trasmissione ad Eurojust delle informazioni detenute dalle competenti autorità nazionali, trasmissione che non sembra avere soddisfatto, almeno sino ad oggi, le aspettative sottese agli strumenti dell'Unione[6].

---

nuove fattispecie di reato: a) i viaggi all'interno, all'esterno o verso l'UE per fini terroristici, ad esempio per aderire alle attività di un gruppo terroristico o al fine di commettere un attentato terroristico; b) l'organizzazione e l'agevolazione di tali viaggi, anche tramite sostegno logistico e materiale, come l'acquisto di biglietti o la pianificazione di itinerari; c) la partecipazione a e la realizzazione di un addestramento a fini terroristici, ad esempio per la fabbricazione o l'uso di esplosivi, armi da fuoco o sostanze nocive o pericolose, rispecchiando la disposizione esistente riguardo alla fornitura consapevole di tale addestramento; d) il fatto di fornire o raccogliere capitali, con l'intenzione o la consapevolezza che tali capitali saranno utilizzati per commettere reati di terrorismo e reati connessi a gruppi terroristici o ad attività terroristiche, adeguando così il quadro normativo dell'UE agli *standards* FAFT/GAFI sul finanziamento del terrorismo. La Direttiva integra, inoltre, la normativa vigente in materia di diritti delle vittime. Essa include un elenco di servizi volti a soddisfare le esigenze specifiche delle vittime del terrorismo, quali il diritto di ricevere immediato accesso a servizi di sostegno professionale che forniscano assistenza medica e psicosociale, o di ricevere consulenza giuridica o pratica, nonché assistenza nelle richieste di risarcimento. Sono inoltre rafforzati i meccanismi di risposta di emergenza immediatamente dopo un attentato. Il legislatore italiano ha recepito questa direttiva con la legge di delegazione europea 2016-2017 (L. 25 ottobre 2017, n. 163). Sulla direttiva in parola vedasi S. SANTINI, *L'Unione Europea compie un nuovo passo nel cammino della lotta al terrorismo: una prima lettura della direttiva 2017/541*, in questa *Rivista*, fasc. 7-8/2017, p. 13 ss.; S. DE LUCA, *La direttiva 2017/541/UE e il difficile bilanciamento tra esigenze di pubblica sicurezza e rispetto dei diritti umani*, in *Eurojus*, 3 luglio 2017; SERVIZIO STUDI DEL SENATO, Dossier "*Direttiva (UE) 2017/541 del Parlamento europeo e del Consiglio, del 15 marzo 2017, sulla lotta contro il terrorismo e che sostituisce la decisione quadro 2002/475/GAI del Consiglio e modifica la decisione 2005/671/GAI del Consiglio*", accessibile a questo *link*; L. MARINI, *Foreign terrorist fighters: verso la revisione della risoluzione 2178 (2014)*, in questa *Rivista*, 20 dicembre 2017.

[6] L'articolo 22 della Direttiva 2017/541 ha modificato l'articolo 2 della Decisione 2005/671/GAI, nell'ottica del rafforzamento della cooperazione tra Stati membri, ponendo tale disposizione in linea con quanto disposto dall'articolo 7 del Protocollo addizionale del 2015 alla Convenzione di Varsavia del Consiglio d'Europa sulla prevenzione del terrorismo del 2005, che già contemplava il rafforzamento della cooperazione tra gli Stati firmatari nell'ottica della prevenzione dei reati di terrorismo (cfr. sul punto S. SANTINI, *L'Unione europea compie un nuovo passo avanti nel cammino alla lotta al terrorismo*, cit., 40). Inoltre, l'articolo 21 del nuovo Regolamento su Eurojust (2018/1727 del 14 novembre 2018) ha disciplinato in maniera organica lo scambio di informazioni con gli Stati membri e tra membri nazionali, prevedendo al comma 9 che "il presente articolo fa salvi altri obblighi relativi alla trasmissione di informazioni a Eurojust, tra cui quelli derivanti dalla decisione 2005/671/GAI del Consiglio" (cfr. sul punto L. SALAZAR, *La riforma di Eurojust e i suoi riflessi sull'ordinamento italiano*, cit., 48).

Sul versante del contrasto alla radicalizzazione e all'estremismo violento, la Commissione europea, nella sua Comunicazione del 21 settembre 2005[7], formulava per la prima volta un espresso riferimento alla lotta alla radicalizzazione come parte di un approccio globale di prevenzione del terrorismo, offrendo una definizione della stessa quale "fenomeno che vede persone abbracciare opinioni, vedute e idee che potrebbero portare ad atti terroristici quali definiti all'articolo 1 della Decisione quadro del 2002 sulla lotta contro il terrorismo". In particolare, dopo gli attacchi terroristici di Madrid e Londra sopra menzionati, la Commissione riteneva necessario indirizzare le strategie di prevenzione e contrasto del terrorismo non solo attraverso strumenti di diritto penale, ma anche attraverso misure ispirate dalla dimensione storico-sociale, religiosa ed ideologica del fenomeno, volte a prevenire qualsiasi forma di radicalizzazione violenta – di ispirazione religiosa ma anche di tipo nazionalista, anarchico, separatista, di estrema sinistra o di estrema destra – mediante il sostegno agli Stati membri in settori strategici, quali lo sviluppo di efficaci politiche di contronarrativa attraverso il *web* ed i media, l'istruzione e la partecipazione dei giovani alla vita sociale, l'occupazione, le questioni relative all'inclusione e all'integrazione all'interno di una comunità, l'uguaglianza di opportunità, la non discriminazione e il dialogo interculturale.

Nella medesima direzione, venendo a tempi più recenti, con la Comunicazione del 15 gennaio 2014[8] la Commissione europea ha dato ai Paesi membri un vero e proprio elenco di priorità nella lotta alla radicalizzazione violenta di matrice jihadista che prevede, tra l'altro, lo sviluppo di strategie nazionali globali, la valorizzazione delle attività della Rete per la sensibilizzazione in materia di radicalizzazione (RAN)[9], la formazione degli operatori che lavorano con individui o gruppi a rischio e una sempre maggiore diffusione di messaggi alternativi, volti a destrutturare la propaganda estremista e rafforzare la capacità di reazione delle vittime.

La prevenzione del terrorismo e dell'estremismo violento è stata, inoltre, individuata nell'Agenda europea sulla sicurezza per il quinquennio 2015-2020 come la sfida più urgente insieme alla lotta alla criminalità organizzata e alla criminalità informatica[10]. Per rispondere a tali minacce, il Consiglio dell'Unione ha approvato, il 20 novembre 2015, delle conclusioni sul rafforzamento della risposta di giustizia penale alla radicalizzazione, invitando gli Stati membri a sviluppare indici di valutazione del rischio e strumenti che consentano l'individuazione di segni precoci di radicalizzazione

---

[7] Comunicazione della Commissione al Parlamento europeo e al Consiglio del 21.09.2005 (COM(2005) 313 definitivo) *"Reclutamento per attività terroristiche – Affrontare i fattori che contribuiscono alla radicalizzazione violenta"*.

[8] Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle Regioni del 15.01.2014 (COM(2013) 941 final) *"Prevenire la radicalizzazione che porta al terrorismo e all'estremismo violento: rafforzare la risposta dell'UE"*.

[9] Si tratta di un centro di eccellenza – il *Radicalisation Awareness Network* (RAN) – istituito nel 2011 e composto da 700 esperti provenienti da tutta Europa, che ha come finalità lo scambio di idee e progetti per un efficace contrasto dei fenomeni di radicalizzazione.

[10] Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale e al Comitato delle Regioni del 28.04.2015 (COM(2015) 185 final) *"Agenda europea sulla sicurezza"*.

attraverso un maggiore scambio di informazioni[11]; pochi giorni dopo, il 25 novembre 2015, anche il Parlamento europeo ha adottato una risoluzione sulla prevenzione della radicalizzazione e del reclutamento di cittadini europei da parte di organizzazioni terroristiche, aggiornando la definizione di radicalizzazione quale "fenomeno che vede persone abbracciare opinioni, pareri e idee intolleranti suscettibili di portare all'estremismo violento"[12]. Al fine di implementare le linee di azione tracciate dal Parlamento e dal Consiglio, il 20 aprile 2016 la Commissione europea ha presentato la Comunicazione dal titolo "Attuare l'Agenda europea sulla sicurezza per combattere il terrorismo e preparare il terreno per un'autentica ed efficace Unione della sicurezza"[13], in cui ha posto l'accento sulla necessità di adottare misure più efficaci per contrastare, in particolare, la minaccia terroristica dei combattenti stranieri di ritorno dai teatri di guerra, favorendo la circolazione delle informazioni su tutti i movimenti di questi ultimi – sia in uscita che in entrata – e agevolando l'inserimento dei soggetti già radicalizzati in programmi di riabilitazione e di sostegno al disimpegno dalla violenza. Inoltre, ha istituito nel 2017 un Gruppo di esperti di alto livello sulla radicalizzazione, che ha presentato il suo primo rapporto il 18 maggio 2018[14], contenente una serie di raccomandazioni strategiche e politiche da attuare a livello UE. Tale lavoro è stato accolto con particolare favore dalla Commissione, che nella sua Comunicazione del 13 giugno 2018[15] ha assunto l'impegno di dar seguito in tempi brevi alla raccomandazione che prevede l'instaurazione di un meccanismo di cooperazione europea per assicurare un coinvolgimento più profondo degli Stati membri nelle attività di contrasto dell'estremismo violento, i cui risultati verranno valutati entro la fine del 2019.

Con particolare riferimento alla lotta alla radicalizzazione ed al proselitismo che avvengano attraverso l'uso illegale di internet, la Direttiva 2017/541 sopra menzionata, il cui termine di recepimento è scaduto l'8 settembre 2018, ha per la prima volta introdotto l'obbligo per gli Stati membri di adottare misure finalizzate alla prevenzione della propaganda *on line* attraverso la rimozione tempestiva – ovvero il blocco dell'accesso, qualora la prima non fosse possibile – di contenuti *on line* che costituiscano una pubblica incitazione a commettere un reato di terrorismo, nella piena garanzia dei diritti fondamentali degli utenti ad informare e ad essere informati. È stato, altresì, proposto un piano a lungo termine che affianchi, agli strumenti repressivi di natura penale, politiche socio-culturali volte a favorire l'integrazione e il reinserimento all'interno di una comunità dei soggetti che manifestano una propensione

---

[11] Si fa riferimento alle *"Conclusioni del Consiglio dell'Unione europea e degli Stati membri riuniti in sede di Consiglio sul rafforzamento della risposta della giustizia penale alla radicalizzazione che conduce al terrorismo e all'estremismo violento"* del 20 novembre 2015 (2016/C 467/02) in Gazz. Uff. UE 15.12.2016 – C 467/3.

[12] Vedasi il considerando lett. B) della Risoluzione del Parlamento europeo del 25 novembre 2015 sulla prevenzione della radicalizzazione e del reclutamento di cittadini europei da parte di organizzazioni terroristiche (2015/2063(INI)) (2017/C 366/08), in Gazz. Uff. UE 27.10.2017 – C366/101.

[13] COM(2016)230 final.

[14] Accessibile a questo *link*.

[15] Comunicazione della Commissione al Parlamento europeo, al Consiglio europeo e al Consiglio del 13.06.2018 (COM(2018) 470 final) "*Quindicesima relazione sui progressi compiuti verso un'autentica ed efficace Unione della sicurezza*".

all'estremismo violento, anche attraverso efficaci programmi di deradicalizzazione; si è evidenziata, infine, la necessità di una condivisione tra gli Stati membri di informazioni ed esperienze, invitando ciascun Paese a coinvolgere la società civile e le comunità locali per promuovere politiche di formazione e sensibilizzazione che consentano un tempestivo riconoscimento e contrasto dei segnali di radicalizzazione[16].

Nella consapevolezza che l'attuazione di tali disposizioni da parte degli Stati membri non possa efficacemente avvenire se non attraverso una adeguata responsabilizzazione, a livello europeo, dei prestatori di servizi internet di *hosting* rispetto alla necessità di prevenire la diffusione in rete di contenuti terroristici, il 1º marzo 2018 la Commissione europea ha adottato una Raccomandazione sulle misure per contrastare i contenuti illegali *on line*, prendendo spunto dalla propria Comunicazione di settembre 2017, nonché dagli sforzi compiuti nell'ambito del Forum dell'UE su Internet[17]. Attraverso tale esercizio, si è avviata a livello UE una forma di dialogo e di cooperazione tra gli Stati membri ed i prestatori di servizi *on line* al fine sia di contenere il ricorso da parte dei terroristi a questo veicolo di comunicazione, sia di sviluppare

---

[16] Nella stessa direzione seguita dall'Unione, l'Assemblea generale delle Nazioni Unite, il 26 giugno 2018, ha adottato una risoluzione (A/RES/72/284) contenente la sesta revisione della Strategia globale anti-terrorismo dell'ONU (che dal 2006, anno della sua prima formulazione, viene aggiornata ogni due anni), ponendo l'accento sulla necessità di una sempre maggiore condivisione delle informazioni a livello internazionale e di un rafforzamento delle politiche di prevenzione della radicalizzazione violenta. In particolare, tra le priorità individuate dalle Nazioni Unite vi è quella di sviluppare strategie di riabilitazione e reintegrazione dei soggetti radicalizzati, tenendo conto dell'età e dell'ambiente di provenienza degli stessi, nonché quella di valorizzare un approccio multidimensionale al fenomeno che riconosca un ruolo anche alle società civili. Queste ultime, a detta dell'Assemblea generale, possono infatti offrire un importante contributo di mediazione con le comunità locali e dedicare una particolare attenzione ai bambini, che da sempre rappresentano la categoria più vulnerabile ed esposta al rischio radicalizzazione, promuovendo specifiche attività di supporto psicosociale, come le terapie post-trauma, e vigilando affinché sia sempre garantito il pieno rispetto della loro dignità e dei diritti riconosciuti dai trattati internazionali. Pertanto, gli Stati che hanno aderito alla strategia globale anti-terrorismo dell'ONU vengono invitati a migliorare i loro sforzi per mettere a punto programmi di deradicalizzazione e per condurre politiche reali di lotta alla povertà, di incentivi alla crescita economica ed allo sviluppo sostenibile dei paesi in difficoltà, in una prospettiva di prosperità globale, di buon governo, e di rispetto dei diritti umani per favorire un dialogo interculturale che assicuri pari dignità a tutte le religioni, alle tradizioni e alle diverse culture. Si segnala, inoltre, che il Parlamento europeo, nella sua Raccomandazione al Consiglio concernente la 73ª sessione dell'Assemblea generale delle Nazioni Unite tenutasi dal 18 al 27 settembre 2018, ha espresso la propria condanna del terrorismo e il pieno sostegno a favore di azioni volte a sconfiggere ed eradicare le organizzazioni terroristiche, in particolare Daesh/ISIS, ed ha invitato gli Stati membri a proseguire nelle iniziative poste in essere dai partner locali per "concepire, attuare e sviluppare approcci intesi a contrastare la radicalizzazione e il reclutamento a fini terroristici", in linea con il piano d'azione delle Nazioni Unite per prevenire l'estremismo violento (Raccomandazione del Parlamento europeo del 5 luglio 2018 al Consiglio concernente la 73ª sessione dell'Assemblea generale delle Nazioni Unite (2018/2040(INI)).

[17] Raccomandazione del 1° marzo 2018 sulle misure per contrastare efficacemente i contenuti illegali *on line* (C(2018)1177 final). Tale Raccomandazione, richiamando la citata Comunicazione della Commissione del 2017 (COM (2017) 555 final) sulla lotta ai contenuti illeciti *on line*, ha individuato una serie di misure atte ad arrestare efficacemente la pubblicazione e la diffusione di propaganda terroristica *on line*, tra cui il miglioramento del processo di segnalazione, un termine di un'ora per rispondere alle segnalazioni, misure proattive per individuare tali contenuti, la rimozione efficace e salvaguardie sufficienti per valutare accuratamente i contenuti terroristici.

un'adeguata contronarrativa. Gli oggettivi passi in avanti registratisi per effetto di questa iniziativa non sono stati tuttavia tali da contribuire a risolvere completamente il problema: tra le cause del successo parziale la Commissione ha individuato principalmente quella del carattere volontario di questa forma di cooperazione tra i settori pubblico e privato, da cui è disceso il numero complessivamente ridotto dei prestatori di servizi coinvolti nella collaborazione, nonché la lentezza e la parzialità del processo di rimozione dei contenuti illeciti in parola[18].

Alla luce di tali esiti non pienamente soddisfacenti e di una serie di attacchi terroristici in diverse città europee, il tema è stato portato all'attenzione del Consiglio europeo che, nelle sessione del 28 giugno 2018, ha da un lato invitato l'industria di settore a sviluppare nuove tecnologie e strumenti diretti a migliorare l'individuazione automatica e la conseguente rimozione dalla rete di tali contenuti illeciti; dall'altro, ha salutato con favore l'intenzione della Commissione di presentare una proposta legislativa intesa a migliorare l'individuazione e la rimozione dalla rete di contenuti che incitino all'odio ovvero a commettere atti di terrorismo[19].

Dando seguito a tale impulso del Consiglio europeo, il 12 settembre 2018 la Commissione europea ha presentato la proposta di Regolamento a cui è dedicato il presente studio (COM(2018)640 final)[20], che mira a contrastare l'utilizzo illecito di internet a fini di reclutamento, sostegno e celebrazione delle attività terroristiche, attraverso la riduzione della presenza di materiale propagandistico di carattere terroristico *on line*. Occorre segnalare che la scelta della Commissione è stata quella di limitare la proposta di misure normative di rimozione obbligatoria da parte dei *service*

---

[18] Oltre al Forum dell'UE su internet, si segnalano le iniziative della Commissione europea di sensibilizzazione delle piattaforme informatiche iniziate con la conclusione nel maggio del 2016 di un accordo ("*Code of conduct*") con Facebook, Microsoft, Google (YouTube) e Twitter per contrastare il diffondersi di contenuti d'odio *on line*, al fine di una più efficace applicazione della Decisione quadro 2008/913/GAI del 28 novembre 2008 sulla lotta contro talune forme ed espressioni di razzismo e xenofobia mediante il diritto penale. I risultati di tale accordo vengono costantemente monitorati dal 2016 ed hanno mostrato progressi crescenti nella volontaria attività dei prestatori di servizi di rimuovere i contenuti d'odio segnalati. All'esito del quarto monitoraggio presentato dalla Commissione europea il 4 febbraio 2019, si è registrato il positivo risultato di una tendenziale risposta entro 24 ore, da parte dei prestatori di servizi, alle segnalazioni ricevute, nonché della rimozione, nel 2018, del 72% dei contenuti segnalati, con un significativo miglioramento rispetto al 59% del 2017 ed al 28% nel 2016 (vedi al seguente *link*).

[19] Si ricorda che il Consiglio europeo, già nella sessione del 22-23 giugno 2017, aveva esortato le imprese a sviluppare "nuove tecnologie e nuovi strumenti al fine di migliorare l'individuazione automatica e la rimozione dei contenuti che incitano a compiere atti terroristici", sostenendo che "[s]e necessario si dovrebbero completare tali iniziative con le pertinenti misure legislative a livello dell'UE". Peraltro, già taluni Stati membri hanno nel frattempo legiferato in materia, costringendo così l'UE ad accelerare nell'adozione di misure normative comuni, al fine di evitare la frammentazione delle discipline nazionali. Ad esempio, la Germania ha approvato nel 2017 una legge per migliorare l'applicazione del diritto nei *social network* in base alla quale i *providers* sono obbligati a designare una persona abilitata a ricevere richieste di informazioni dalle autorità di contrasto e a rimuovere i contenuti illeciti (vedi a questo *link*). La legge prevede sanzioni fino a 500.000 euro in caso di mancata nomina del rappresentante legale o di mancata risposta a richieste di informazioni da parte della persona abilitata a riceverle.

[20] Proposta di regolamento del Parlamento europeo e del Consiglio relativo alla prevenzione della diffusione di contenuti terroristici *on line* del 12.09.2018 (COM(2018)640 final), accessibile a questo *link*.

providers ai soli contenuti terroristici *on line*, lasciando fuori dall'ambito di applicazione del nuovo Regolamento tutti gli altri contenuti che rientrano nella più ampia sfera dell'incitamento all'odio e alla discriminazione. La Commissione ha riferito sui progressi fatti in questa direzione nelle Comunicazioni del 10 ottobre e dell'11 dicembre 2018, in cui ha altresì invitato il Parlamento ed il Consiglio ad adottare la menzionata proposta legislativa prima della fine del mandato parlamentare di maggio 2019, ritenendola una misura essenziale di risposta al fenomeno della radicalizzazione violenta[21].

Da parte sua il Consiglio dell'Unione europea ha avviato l'esame della proposta di Regolamento a livello tecnico, in seno al *Terrorism Working Party*, il 25 settembre 2018, per giungere infine all'adozione dell'orientamento politico generale nella sessione ministeriale "Giustizia e Affari interni" del 6 dicembre 2018, proponendo una serie di modifiche all'articolato della Commissione europea di cui si terrà conto nel presente lavoro (ST15336/18; denominato, d'ora in avanti, "orientamento generale")[22].

Quanto al Parlamento europeo, nella Risoluzione adottata il 12 dicembre 2018 – accogliendo con favore la proposta legislativa della Commissione sulla prevenzione della diffusione di contenuti terroristici *on line* e invitando i co-legislatori a lavorare con urgenza sulla stessa – al punto 48 ha sottolineato "la necessità di conseguire l'individuazione automatica e l'eliminazione sistematica, rapida, permanente e completa dei contenuti terroristici *on line* in base a chiare disposizioni giuridiche, comprese salvaguardie, e al controllo umano", nonché "la necessità di evitare che il contenuto già rimosso venga ricaricato"[23].

Il negoziato della proposta di Regolamento è allo stato nella fase finale di trilogo tra la Commissione europea, il Consiglio UE e il Parlamento europeo, con l'auspicio che lo strumento possa essere definitivamente adottato prima delle elezioni parlamentari europee di maggio 2019.

Dal quadro sopra descritto emerge con chiarezza l'approccio integrato scelto dall'Unione nella lotta al terrorismo e alla radicalizzazione violenta, che si è qui voluto – sia pur brevemente – delineare al fine di individuare il contesto sistemico in cui è stata promossa la recente iniziativa normativa oggetto del presente studio, finalizzata a potenziare la prevenzione di tali fenomeni soprattutto in quel mondo virtuale che appare oggi porre le sfide più complesse ed insidiose: il *web*.

---

[21] Comunicazione della Commissione al Parlamento europeo, al Consiglio europeo e al Consiglio del 10.10.2018 (COM(2018) 690 final) *"Sedicesima relazione sui progressi compiuti verso un'autentica ed efficace Unione della sicurezza"*: vedi, in particolare, pagina 6. Comunicazione della Commissione al Parlamento europeo, al Consiglio europeo e al Consiglio dell'11.12.2018 (COM(2018) 845 final) *"Diciassettesima relazione sui progressi compiuti verso un'autentica ed efficace Unione della sicurezza"*: vedi in particolare pagine 4 e 5.

[22] Orientamento generale del Consiglio UE del 6.12.2018 sulla proposta di Regolamento del Parlamento europeo e del Consiglio relativo alla prevenzione della diffusione di contenuti terroristici *on line* (ST15336/18), accessibile a questo *link*.

[23] Risoluzione del Parlamento europeo del 12 dicembre 2018 sulle conclusioni e raccomandazioni della Commissione speciale sul terrorismo (2018/2044(INI)).

2. La proposta di Regolamento della Commissione europea sulla prevenzione della diffusione di contenuti terroristici on line (COM(2018)640 final) alla luce dell'orientamento generale del Consiglio UE del 6 dicembre 2018 (ST15336/18): novità e finalità.

Venendo alla lettura dell'articolato della proposta di Regolamento, la principale novità è l'introduzione nel diritto UE dello strumento dell'*ordine di rimozione* che obbliga i prestatori di servizi di *hosting* operanti sul territorio dell'Unione a rimuovere i contenuti terroristici *on line* o a disabilitarne l'accesso entro un'ora dalla ricezione dell'ordine, a pena di imposizione di sanzioni.

Viene così superato il regime di cooperazione volontaria tra gli Stati membri e l'industria digitale avviato dall'Unione nel 2015, rivelatosi – come sopra detto – non pienamente soddisfacente, per adottare invece misure più rigorose di prevenzione e contrasto fondate sull'imposizione di precisi obblighi giuridici a carico dei prestatori di servizi di *hosting*, che sono peraltro chiamati a collaborare tra loro e con le autorità competenti, compresa Europol, per mettere in atto più incisive misure proattive e migliori meccanismi di monitoraggio e risposta alle segnalazioni di contenuti illegali.

È bene fin d'ora evidenziare che l'impianto della proposta di Regolamento prevede non solo adempimenti a carico dei *providers*, ma anche l'attuazione di misure di varia natura da parte degli Stati membri, i quali sono tenuti a contribuire attivamente al raggiungimento degli obiettivi del nuovo Regolamento attraverso il potenziamento delle capacità delle autorità nazionali di rispondere efficacemente alle minacce poste da un utilizzo improprio della rete a fini terroristici.

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 providers* che offrano i propri servizi sul territorio dell'Unione, tutelando altresì la fiducia e la sicurezza dei cittadini.

La scelta dell'articolo 114 TFEU quale unica base giuridica della proposta di Regolamento desta, tuttavia, qualche perplessità, atteso che l'articolato normativo disciplina, in modo trasversale e comunque prevalente, ambiti e misure che attengono rispettivamente alla prevenzione e alla lotta al terrorismo, al coordinamento ed alla cooperazione tra forze di polizia e autorità giudiziarie, anche tramite Europol, che sono oggetto delle previsioni dettate dagli articoli 67, comma 3, 87 e 88 del medesimo TFEU.

2.1. Ambito di applicazione soggettiva: il prestatore di servizi di hosting.

La proposta di Regolamento si applica, ai sensi del secondo comma dell'articolo 1, ai prestatori di servizi di *hosting* che offrono i propri servizi nell'Unione,

indipendentemente dal luogo del loro stabilimento principale e dalla loro dimensione imprenditoriale.

La definizione di "prestatore di servizi di *hosting*" è contenuta nell'articolo 2 (1) e fa riferimento ai servizi digitali che memorizzano informazioni e materiali forniti da un destinatario del servizio su sua richiesta e li rendono disponibili a terzi, indipendentemente dalla natura meramente tecnica, automatica o passiva di tale attività. Il Consiglio UE, in sede di orientamento generale, ha modificato il considerando n. 10 della proposta della Commissione al fine di precisare meglio quali siano i prestatori di servizi destinatari della nuova normativa: vi rientrano, per esempio, le piattaforme dei *social media*, i servizi di *streaming video*, i servizi di condivisione di video, audio e immagini, i servizi di condivisione di file e altri servizi di *cloud* e di memorizzazione. Non vi rientrano, invece, i prestatori di servizi che effettuano il semplice trasporto dei dati ("*mere conduit*"), senza memorizzazione o con memorizzazione solo temporanea ("*caching*") dei contenuti, a cui si applicano gli articoli 12, 13 e 15 della Direttiva sul commercio elettronico 2000/31/CE, recepiti nel nostro ordinamento dagli articoli 14, 15 e 17 del Decreto legislativo 9 aprile 2003, n. 70, secondo cui "l'autorità giudiziaria o quella amministrativa avente funzioni di vigilanza può esigere anche in via d'urgenza, che il prestatore, nell'esercizio delle attività di cui al comma 2, impedisca o ponga fine alle violazioni commesse".

All'articolo 2(3) viene, altresì, definito il concetto di "offrire servizi nell'Unione": il Consiglio UE ha allineato tale definizione, in sede di orientamento generale, a quella contenuta nella proposta di Direttiva sulla nomina di rappresentanti legali da parte dei prestatori di servizi ai fini dell'acquisizione di prove nei procedimenti penali (COM(2018)226 final) e nella proposta di Regolamento relativo agli ordini europei di produzione e di conservazione delle prove elettroniche in materia penale (COM(2018)225 final), entrambe presentate dalla Commissione europea il 17 aprile 2018 ed attualmente in fase di negoziato[24]. La finalità è quella di assicurare l'applicabilità del Regolamento sulla prevenzione della diffusione dei contenuti terroristici *on line* anche ai *service providers* che siano stabiliti in Paesi terzi ma che operino nel mercato unico digitale europeo, purché il *provider* abbia un "collegamento sostanziale" con uno o più Stati membri, che sicuramente esiste quando ha uno stabilimento nel territorio dell'Unione. In mancanza di questo, tale requisito dovrebbe essere valutato sulla base di "specifici criteri fattuali" quali l'esistenza di un numero significativo di utenti in uno o più Stati membri, o la destinazione delle attività verso uno o più Stati membri deducibile, per esempio, dall'uso di una lingua o di una moneta generalmente utilizzata nello Stato membro in questione, ovvero la possibilità di ordinare prodotti o servizi. La semplice

[24] Si precisa che il Consiglio UE ha approvato in data 7 dicembre 2018 l'orientamento generale sulla proposta di Regolamento relativo agli ordini europei di produzione e di conservazione delle prove elettroniche in materia penale (ST15292/18) ed in data 8 marzo 2019 l'orientamento generale sulla proposta di Direttiva sulla nomina di rappresentanti legali da parte dei prestatori di servizi ai fini dell'acquisizione di prove nei procedimenti penali (ST6946/19). Vedasi, su tali proposte normative, R. PEZZUTO, *Accesso transnazionale alla prova elettronica nel procedimento penale: la nuova iniziativa legislativa della Commissione europea al vaglio del Consiglio dell'Unione*, in questa *Rivista*, fasc. 1/2019, p. 57 ss.

accessibilità del servizio, invece, non dovrebbe di per sé costituire condizione sufficiente per l'applicazione del Regolamento (vedasi considerando n. 10 e 11).

Il prestatore di servizi di *hosting* che non sia stabilito nell'Unione è tenuto, ai sensi dell'articolo 16 e dei considerando n. 35 e 36, a designare un proprio rappresentante legale nell'Unione, ovvero una persona fisica o giuridica che agisca in suo nome e per suo conto al fine di ricevere, trattare ed eseguire gli ordini di rimozione, le segnalazioni, le richieste e le decisioni emesse dalle autorità nazionali competenti.

In linea di principio, il *service provider* può decidere liberamente in quale Stato membro designare il proprio rappresentante legale purché sia uno Stato membro in cui fornisce servizi o ha la propria sede di stabilimento: ciò al fine di evitare che la scelta si diriga verso un Paese con cui il *provider* non ha nessuna connessione, magari solo per ragioni inerenti all'importo delle sanzioni di natura amministrativa o penale che – ai sensi dell'articolo 18 – potranno essere comminate a suo carico in caso di violazione degli obblighi e il cui importo potrà essere diverso a seconda degli Stati membri[25].

Ai sensi dell'articolo 15, l'obbligo di designazione del legale rappresentante e le eventuali sanzioni in caso di inadempimento devono essere imposti dallo Stato membro in cui il prestatore di servizi è stabilito. Ove, invece, il *provider* non sia stabilito nell'Unione, l'imposizione di questo obbligo spetta allo Stato membro in cui risiede o è stabilito il suo rappresentante legale. Laddove il prestatore di servizi di *hosting* ometta di designare un rappresentante legale, tutti gli Stati membri sono competenti, ma quello tra loro che decida di esercitare la propria competenza deve informarne gli altri. Questo perché i *service providers* non possono essere obbligati a designare nell'Unione più di un rappresentante legale, né un gruppo societario a designare molteplici rappresentanti (ovvero uno per ogni società facente parte del gruppo).

Affinché il sistema possa funzionare in modo efficiente, l'articolo 17 prevede la designazione anche da parte di ciascuno Stato membro di una o più autorità competenti ad emanare gli ordini di rimozione, individuare e segnalare contenuti terroristici ai *providers*, sorvegliare l'attuazione delle misure proattive da parte di questi ultimi e far loro rispettare gli obblighi previsti dal Regolamento, pena l'imposizione di sanzioni. Le autorità in questione possono essere amministrative, esecutive o giudiziarie, a seconda dell'assetto istituzionale ed ordinamentale di ciascuno Stato membro, e la loro designazione deve essere comunicata alla Commissione europea, che ne pubblica gli estremi nella Gazzetta Ufficiale dell'Unione, anche per facilitare i contatti e lo scambio di informazioni tra gli Stati membri (considerando n. 13). Tali autorità di fatto costituiscono l'interlocutore principale del *service provider* che in quello Stato membro

[25] L'articolo 18 della proposta di Regolamento prevede, infatti, che siano gli Stati membri a stabilire autonomamente le sanzioni da irrogare ai *providers* in caso di violazione degli obblighi previsti dal Regolamento stesso, senza fissare dunque sanzioni armonizzate a livello UE ma prevedendo solo che gli Stati membri le determinino in maniera tale che siano efficaci, proporzionate e dissuasive. Il considerando n. 38, modificato dal Consiglio UE in sede di orientamento generale, chiarisce la natura di tali sanzioni, che può essere amministrativa o penale, ed i criteri che gli Stati membri dovrebbero seguire nel determinarle. Nell'eventualità di sistematica inosservanza nel rimuovere i contenuti terroristici, un fornitore di servizi potrebbe dover pagare sanzioni fino al 4% del suo fatturato mondiale per l'ultimo esercizio finanziario.

abbia deciso di nominare il proprio rappresentante legale e devono renderne pubblica la designazione ai sensi dell'articolo 16.

L'articolo 14 stabilisce, altresì, che tutti i prestatori di servizi di *hosting*, indipendentemente dal loro luogo di stabilimento nell'UE o in un Paese terzo, devono istituire un punto di contatto incaricato di ricevere gli ordini di rimozione e le segnalazioni per via elettronica e di assicurarne il rapido trattamento, informandone il pubblico (ad esempio attraverso il proprio sito *web*), pena l'imposizione di sanzioni, e indicando altresì la lingua o le lingue in cui sarà possibile rivolgersi al punto di contatto (tra cui deve figurare necessariamente almeno una delle lingue ufficiali dello Stato membro in cui il *provider* ha la sua sede di stabilimento o il suo rappresentante). Contrariamente al rappresentante legale, il punto di contatto assolve compiti di natura operativa, non deve necessariamente essere situato sul territorio dell'Unione e – ove si tratti di prestatori di servizi di *hosting* "esposti a contenuti terroristici" (intendendosi per tali, come diremo in seguito, quelli che abbiano ricevuto ordini di rimozione) – dovrebbe essere accessibile 24 ore su 24 e 7 giorni su 7 (considerando n. 33).

Anche gli Stati membri sono tenuti ad istituire un punto di contatto per trattare le richieste di informazioni sugli ordini di rimozione e segnalazioni emesse dalle proprie autorità nazionali competenti, dandone notizia al pubblico (per esempio, anche attraverso il portale europeo della giustizia elettronica).

2.2. *Ambito di applicazione oggettiva: la diffusione di contenuti terroristici* on line.

La proposta di Regolamento in esame mira ad impedire l'uso improprio dei servizi di *hosting* ai fini della diffusione di contenuti terroristici *on line*, intendendosi per tali, ai sensi dell'articolo 2(5), i materiali che possono incitare, incoraggiare, appoggiare la commissione di reati terroristici o promuovere le attività di un gruppo terroristico anche attraverso l'arruolamento e l'addestramento. Nella definizione rientrano, pertanto, i contenuti che forniscono indicazioni per la fabbricazione o l'uso di esplosivi, armi o sostanze nocive, nonché su metodi o tecniche, compresa la localizzazione degli obiettivi, finalizzati alla perpetrazione di condotte terroristiche.

Il Consiglio UE ha modificato la formulazione della norma originariamente proposta dalla Commissione europea, per allinearla maggiormente alle previsioni della direttiva (UE) n. 541/2017 sulla lotta contro il terrorismo, il cui termine per il recepimento da parte degli Stati membri è scaduto l'8 settembre 2018. Ha altresì emendato il considerando n. 9, al fine di individuare criteri di valutazione della offensività del contenuto *on line,* da parte delle autorità nazionali competenti e dei *providers,* che siano rispettosi dei diritti fondamentali di informazione e di espressione dei cittadini, nonché delle norme di regolamentazione della stampa e del pluralismo dei media, garantendone il giusto bilanciamento con le esigenze di sicurezza pubblica e di contronarrativa: viene, a tal fine, evidenziata la necessità di tenere conto dell'idoneità di tali contenuti di portare a "conseguenze dannose, compromettendo la sicurezza e l'incolumità delle persone",

anche alla luce del fatto che si tratti di materiale prodotto o diffuso da un'organizzazione terroristica o da un soggetto "listato" come terrorista dall'Unione[26].

2.3. Gli obblighi a carico del prestatore di servizi di hosting.

L'articolo 3 prevede un *generale obbligo di diligenza dei providers* che operino all'interno dell'Unione europea, indipendentemente dal loro luogo di stabilimento principale o dimensione imprenditoriale, che consiste nell'adottare misure adeguate, ragionevoli e proporzionate, anche attraverso idonee condizioni contrattuali di utilizzo delle utenze, finalizzate a garantire la sicurezza dei propri servizi e l'individuazione e rimozione efficaci dei contenuti terroristici *on line*, nel pieno rispetto dei diritti fondamentali degli utilizzatori e tenendo in considerazione la fondamentale importanza che riveste la libertà di espressione e di informazione in una società aperta e democratica. Tale obbligo di diligenza non è, tuttavia, da considerare come un obbligo generale di sorveglianza, che finirebbe con l'essere eccessivamente gravoso per l'attività di impresa (considerando n. 12). La norma in esame si pone in linea di continuità rispetto all'articolo 15 della Direttiva 2000/31/CE sul commercio elettronico (attuato nel nostro ordinamento dall'articolo 17 del Decreto legislativo 9 aprile 2003, n. 70), secondo cui il prestatore di servizi di *hosting* non è assoggettato ad un obbligo generale di sorveglianza sulle informazioni che trasmette o memorizza, né ad un obbligo generale di ricercare attivamente fatti o circostanze che indichino la presenza di attività illecite. Al riguardo il considerando n. 19 della proposta di Regolamento precisa che la decisione delle autorità nazionali di imporre specifiche misure proattive e proporzionate non dovrebbe, in linea di principio, comportare l'imposizione di un obbligo generale di sorveglianza, come stabilito all'articolo 15, paragrafo 1, della direttiva 2000/31/CE, per gli Stati membri. Tuttavia, alla luce dei rischi particolarmente gravi associati alla diffusione dei contenuti terroristici, esse potranno, in via eccezionale, derogare al principio in parola, garantendo un giusto equilibrio tra le esigenze di sicurezza pubblica e gli interessi e i diritti fondamentali lesi, tra cui, in particolare, la libertà di espressione e di informazione, la libertà d'impresa, la protezione dei dati personali e della vita privata. Gli obblighi di diligenza per i prestatori di servizi di *hosting* dovrebbero in ogni caso riflettere e rispettare l'equilibrio menzionato nella Direttiva sul commercio elettronico.

La proposta di Regolamento passa poi a definire specifici obblighi a carico dei prestatori di servizi di *hosting*, in considerazione della loro particolare responsabilità nei confronti della società civile sotto il profilo della protezione dei servizi dall'uso illegale degli utilizzatori a fini terroristici, indicandone altresì le linee di interazione istituzionale con gli Stati membri e gli organi competenti dell'Unione.

Obbligo di rimozione: viene, in particolare, previsto dall'articolo 4 *l'obbligo per i providers di rimuovere i contenuti terroristici o di disabilitarne l'accesso entro un'ora*, ove

[26] Sul "*listing*" terroristico in ambito ONU ed UE, vedasi M. TEBALDI, *Le* black lists *nella lotta al terrorismo*, in questa *Rivista*, fasc. 7-8/2018, pp. 77 ss.

ricevano un ordine di rimozione dalla competente autorità giudiziaria o amministrativa di uno Stato membro. Spetta al *provider* decidere se rimuovere il contenuto ovvero disabilitarne l'accesso per gli utilizzatori nell'Unione (considerando n. 13), ma in ogni caso è giuridicamente tenuto ad adempiere entro il brevissimo termine di un'ora, in considerazione del fatto che la diffusione di contenuti propagandistici con finalità di terrorismo nel *web* è particolarmente dannosa e pericolosa proprio nelle prime ore del caricamento *on line* a causa della velocità di condivisione sulla rete.

La norma in parola definisce, altresì, gli elementi minimi di informazione che gli ordini di rimozione devono contenere, rinviando all'allegato I della proposta di Regolamento che contiene un modulo di richiesta immediatamente fruibile dalle autorità nazionali competenti. Il principio di fondo è che l'ordine di rimozione debba includere elementi esplicativi chiari ed inequivoci sull'identità dell'autorità nazionale emittente e sul contenuto *web* di cui si richiede la rimozione (anche attraverso l'indicazione dell'URL o la trasmissione di uno *screenshot*), nonché sulla qualificazione del contenuto come terroristico in base alla definizione prevista dal Regolamento stesso. Ove vi sia una richiesta del *provider* o dell'utilizzatore interessato ("fornitore di contenuti"), l'autorità competente deve trasmettere una motivazione supplementare delle ragioni che l'hanno indotta a considerare il contenuto come terroristico: nelle more, tuttavia, il prestatore di servizi è comunque tenuto ad adempiere all'ordine di rimozione. La motivazione in parola dovrebbe contenere chiarimenti sufficienti per garantire al *provider* e, in ultima analisi, all'utilizzatore, l'esercizio pieno del proprio diritto di ricorso giurisdizionale avverso l'ordine emesso dall'autorità nazionale, ma non dovrebbe in ogni caso includere informazioni sensibili che possano pregiudicare l'esito delle indagini in corso (considerando 13 *bis* introdotto dal Consiglio UE in sede di orientamento generale).

Riguardo alle procedure che regolano l'interazione tra il prestatore di servizi di *hosting* e l'autorità nazionale emittente, quest'ultima è tenuta ad indirizzare l'ordine di rimozione allo stabilimento principale del *provider* o al suo legale rappresentante e a trasmetterlo al suo punto di contatto, utilizzando mezzi elettronici che consentano la tracciabilità delle comunicazioni (considerando 14). Il prestatore di servizi di *hosting* dovrà a sua volta informare l'autorità nazionale emittente della data e dell'ora in cui il contenuto è stato rimosso o reso inaccessibile, utilizzando il modulo di cui all'allegato II della proposta di Regolamento. Ove, invece, il *provider* non possa adempiere per cause di forza maggiore o impossibilità a lui non imputabili, ovvero per vizi manifesti o informazioni insufficienti nell'ordine di rimozione, lo comunica all'autorità emittente utilizzando il modulo di cui all'allegato III della proposta di Regolamento e in tal caso il termine di rimozione entro un'ora rimane sospeso finché l'impossibilità non sia cessata o i chiarimenti non siano stati forniti dall'autorità emittente.

Viene, altresì, sancito l'obbligo dell'autorità emittente di informare della trasmissione dell'ordine – allorché sia divenuto definitivo – l'autorità nazionale competente a vigilare sulle misure proattive a carico del *provider* previste dall'articolo 6, di cui parleremo in seguito, affinché possa assicurare i dovuti seguiti.

Vale, infine, evidenziare una significativa novità introdotta dal Consiglio UE in sede di orientamento generale rispetto all'originaria proposta normativa della

Commissione europea, ovvero la "procedura di consultazione per gli ordini di rimozione" disciplinata dal nuovo articolo 4 *bis*. Si tratta di una procedura parallela rispetto alla notifica dell'ordine di rimozione al *provider*, che si applica solo quando il *provider* ha la propria sede di stabilimento in uno Stato membro diverso rispetto a quello dell'autorità di emissione dell'ordine: essa consiste sostanzialmente nella trasmissione di una copia dell'ordine di rimozione, da parte dell'autorità emittente, all'autorità di regola competente ad emettere ordini di rimozione per lo Stato membro in cui ha la propria sede di stabilimento il prestatore di servizi di *hosting*, al fine di consentire a quest'ultima di valutare la sussistenza di eventuali pregiudizi che il provvedimento in parola possa arrecare agli interessi fondamentali di tale Stato membro e di darne conseguente informazione all'autorità emittente, la quale è tenuta a prendere in conto le circostanze rappresentate e – se necessario – revocare od adeguare l'ordine di rimozione.

Pur nella diversità degli strumenti giuridici, questa procedura di consultazione sembra richiamare concettualmente il meccanismo di notifica dell'ordine europeo di produzione della prova elettronica da parte dell'autorità giudiziaria emittente, allo Stato membro tenuto ad eseguirlo, anch'essa introdotta dal Consiglio UE in sede di orientamento generale sulla proposta di Regolamento relativo agli ordini europei di produzione e di conservazione di prove elettroniche in materia penale (COM(2018)225 final).[27] La preoccupazione politica sembra essere quella di temperare gli effetti del principio di mutuo riconoscimento delle decisioni tra gli Stati membri, al fine di assicurare tutela agli interessi fondamentali dello stato di esecuzione della decisione stessa. Alla luce di questo, non è chiaro tuttavia perché il Consiglio UE abbia limitato l'ambito della procedura di consultazione di cui all'articolo 4 *bis* all'autorità competente dello Stato membro in cui il *provider* ha la propria sede di stabilimento, e non l'abbia invece estesa anche all'autorità competente dello Stato membro in cui si trovi il suo rappresentante legale, atteso che non tutti i *provider* hanno una sede di stabilimento sul territorio dell'Unione.

Obbligo di valutazione delle segnalazioni. I prestatori di servizi di *hosting* sono, altresì, tenuti, ai sensi dell'articolo 5, ad apprestare misure operative e tecniche per assicurare la rapida valutazione su base volontaria (e dunque in assenza di un ordine di rimozione), dei contenuti terroristici che le autorità nazionali competenti e gli organismi dell'Unione segnalino loro, attraverso precise indicazioni (ad esempio, l'URL) idonee a consentirne la pronta individuazione: tale valutazione verte sulla compatibilità dei contenuti segnalati con le proprie condizioni contrattuali di utenza e si conclude con l'autonoma decisione del prestatore di servizi di *hosting* di rimuovere o meno il contenuto segnalato, informandone "senza indebito ritardo" l'autorità segnalante (considerando n. 15).

Obbligo di adozione di misure proattive e di trasparenza. I prestatori di servizi di *hosting* sono, inoltre, chiamati a proteggere il servizio e gli utenti dagli abusi adottando autonomamente "misure proattive", quale per esempio impedire il ricaricamento di

---

[27] Vedasi nota 24 a piè di pagina e R. PEZZUTO, *Accesso transnazionale alla prova elettronica nel procedimento penale*, *cit.*, pp. 76-78.

contenuti rimossi, e ciò anche ricorrendo a strumenti di individuazione e rimozione automatica del contenuto illecito (articolo 6). Queste misure devono essere efficaci e proporzionate, da un lato, al rischio e al livello di esposizione delle piattaforme internet ai contenuti terroristici, dall'altro rispettose dei diritti fondamentali degli utilizzatori e della libertà di espressione ed informazione.

Il considerando n. 16 precisa, al riguardo, che l'esistenza di ordini di rimozione emessi nei confronti di un *provider* è indicativa dell'alto rischio che esso funga da piattaforma di diffusione di contenuti terroristici: da tale stato di "esposizione a contenuti terroristici", che tendenzialmente riguarda le imprese digitali di maggiori dimensioni commerciali, derivano – ai sensi della proposta di Regolamento – una serie di obblighi aggiuntivi a carico dei prestatori di servizi di *hosting* quale quello (sopra menzionato) di assicurare un punto di contatto operativo 24h su 24h e 7 giorni su 7 (considerando n. 33). Inoltre, i *service providers* che abbiano ricevuto un ordine di rimozione divenuto definitivo devono presentare, almeno una volta all'anno, una relazione all'autorità nazionale competente a sorvegliare l'attuazione delle misure proattive adottate (individuata ai sensi dell'articolo 17, comma 1, lett. c), anche per consentire alla stessa una valutazione del funzionamento degli strumenti automatizzati utilizzati, della sorveglianza umana e dei meccanismi di verifica applicati per evitare rimozioni errate (articoli 6 e 9; considerando n. 18 e 19).

I *service providers* devono altresì pubblicare, ai sensi dell'articolo 8 e del considerando n. 24, relazioni annuali sulla trasparenza in merito alle misure intraprese contro la diffusione di contenuti terroristici, che vengono utilizzate dagli Stati membri (ciascuno con riferimento ai *providers* che operano nella propria giurisdizione) per elaborare un resoconto annuale alla Commissione europea, a fini di monitoraggio dei risultati e dell'impatto delle nuove regole (articolo 21 e considerando n. 41). In particolare, la proposta di Regolamento prevede che la Commissione debba presentare un dettagliato programma di monitoraggio sulla base del quale – entro due anni dall'entrata in vigore del Regolamento – riferirà al Parlamento europeo ed al Consiglio sull'attuazione della nuova normativa, avvalendosi sia dei rapporti forniti dalle industrie di settore, sia delle informazioni fornite dagli Stati membri. Successivamente e non prima di tre anni dall'entrata in vigore del Regolamento, l'intero esercizio costituirà oggetto di un processo di valutazione da parte della Commissione, i cui risultati potranno eventualmente portare ad una proposta di modifica del Regolamento in questione.

Obbligo di conservazione dei contenuti. L'articolo 7 prevede l'obbligo dei prestatori di servizi di *hosting* di conservare i contenuti rimossi ed i relativi dati per finalità specifiche e per un tempo limitato. Tali dati dovrebbero essere solo quelli che andrebbero altrimenti perduti a seguito della rimozione del contenuto digitale: possono, ad esempio, includere quelli relativi agli abbonati (che consentono di identificare l'utilizzatore che ha caricato i contenuti), alle transazioni e agli accessi (che consentono di individuare data e ora della connessione e disconnessione dal servizio *web*).

In particolare, l'obbligo di conservazione dei contenuti ha due finalità principali: quella di garantire il diritto dell'utilizzatore al riesame amministrativo o giurisdizionale del provvedimento di rimozione o di disabilitazione dell'accesso, a tutela dei suoi diritti

fondamentali e dell'eventuale ripristino dei materiali sul *web* in caso di esito a lui favorevole del procedimento di riesame; quella di garantire l'attività di indagine da parte dell'autorità giudiziaria, in considerazione della potenziale utilità di tali materiali per prevenire o perseguire reati di terrorismo.

Il comma 2 dell'articolo 7 prevede che i contenuti rimossi debbano essere conservati per un periodo di sei mesi, salvo espressa richiesta dell'autorità amministrativa o giudiziaria competente di preservarli per un periodo più lungo; viene inoltre assicurato il prolungamento del termine in parola per tutto il tempo necessario a concludere il procedimento di riesame amministrativo o giudiziario del provvedimento di rimozione, a tutela dei diritti fondamentali del fornitore di contenuti. Vengono, infine, fatte salve le garanzie procedurali e le misure investigative relative all'accesso ai contenuti e ai relativi dati conservati a fini di indagine e azione penale per reati di terrorismo, previste dalle legislazioni nazionali degli Stati membri o dal diritto UE (considerando n. 22 e 23): il riferimento è da intendersi soprattutto alle nuove norme UE in fase di adozione in materia di ordini europei di produzione e conservazione della prova elettronica[28], che sembrano pertanto doversi considerare prevalenti sui limiti temporali di conservazione dei contenuti terroristici previsti dall'articolo 7.

2.4. La tutela dei diritti fondamentali ed i meccanismi di reclamo e di ricorso giudiziario.

Al fine di apprestare un rimedio ad eventuali ingiustificate rimozioni, la proposta di Regolamento prevede una serie di misure di salvaguardia intese a garantire il pieno rispetto dei diritti fondamentali quali la libertà di espressione e di informazione, tra cui l'obbligo di informare gli utenti quando il loro contenuto viene rimosso, a meno che non vi siano motivi di sicurezza pubblica per non farlo (articolo 11), e l'obbligo di predisporre efficaci meccanismi di reclamo e ricorso giudiziario per assicurare che gli utilizzatori possano sempre impugnare la rimozione dei contenuti, in osservanza dell'articolo 19 del Trattato sull'Unione europea e dell'articolo 47 della Carta dei diritti fondamentali dell'UE (articoli 4 e 10).

In particolare, l'articolo 10 prevede l'obbligo per il prestatore di servizi di *hosting* di predisporre efficaci meccanismi di reclamo attivabili da parte dell'utilizzatore il cui contenuto sia stato rimosso (o il cui accesso sia stato disabilitato) per violazione delle condizioni contrattuali che regolano il servizio internet, a seguito di una segnalazione ricevuta dal *provider* o dell'adozione di una misura proattiva da parte di quest'ultimo: il prestatore di servizi è tenuto ad esaminare tempestivamente ogni reclamo ed eventualmente a ripristinare il contenuto erroneamente rimosso senza indebito ritardo, informando in ogni caso l'autore del reclamo degli esiti delle proprie valutazioni (considerando n. 25).

---

[28] Proposta di Regolamento relativo agli ordini europei di produzione e di conservazione di prove elettroniche in materia penale (COM(2018)225 final): vedasi anche nota a piè di pagina n. 24.

Inoltre, all'utilizzatore deve essere sempre assicurato il diritto di proporre ricorso innanzi all'autorità giurisdizionale dello Stato membro che ha emesso l'ordine di rimozione, garantendogli ai fini dell'impugnazione la conoscenza dei motivi per cui il contenuto che ha caricato è stato rimosso o il relativo accesso disabilitato (articolo 11). Le autorità nazionali, nell'emettere l'ordine, possono tuttavia disporre che la motivazione non venga divulgata all'utilizzatore quando sussistano ragioni di sicurezza pubblica o di segretezza delle indagini. Un aspetto particolarmente delicato nel corso del negoziato della proposta di Regolamento a Bruxelles si è rivelato proprio quello del periodo massimo di secretazione delle informazioni da comunicare agli utilizzatori ai sensi dell'articolo 11, atteso che l'iniziale proposta della Commissione europea prevedeva un termine di quattro settimane, ritenuto del tutto inadeguato dagli Stati membri, in considerazione della necessità di preservare il buon esito delle indagini. La soluzione raggiunta nel testo di compromesso di orientamento generale adottato dal Consiglio UE a dicembre scorso prevede ora il termine di sei settimane, rinnovabile di altre sei settimane, ma ci sarebbe da chiedersi se si sia così effettivamente raggiunto un giusto bilanciamento tra la tutela dell'interesse dell'utilizzatore a ricorrere contro il provvedimento di rimozione da un lato, e le esigenze di giustizia e sicurezza pubblica dall'altro, atteso che non si tengono in alcun conto i diversi termini di durata delle indagini penali previsti dagli ordinamenti degli Stati membri.

2.5. La cooperazione tra gli Stati membri, gli organismi dell'Unione e i prestatori di servizi di hosting.

La sezione IV della proposta di Regolamento mira a stabilire un quadro chiaro di riferimento per rafforzare la cooperazione e il coordinamento tra i prestatori di servizi di *hosting*, gli Stati membri ed Europol. In particolare, l'articolo 13 prevede l'obbligo per i Paesi dell'Unione di collaborare tra loro e, se del caso, con Europol, al fine di evitare possibili duplicazioni derivanti dall'emissione di ordini di rimozione o segnalazioni relative ai medesimi contenuti, nonché interferenze in indagini portate avanti parallelamente da due o più Stati membri. La norma prevede, inoltre, di avvalersi di appositi strumenti, compresi quelli di Europol, per il trattamento degli ordini di rimozione e delle segnalazioni e di collaborare anche con riferimento alle misure proattive a carico dei *providers*.

Si segnala al riguardo che nell'adottare l'orientamento generale il Consiglio UE ha integrato il testo dei considerando n. 27 e 30 originariamente proposti dalla Commissione europea per assicurare che gli Stati membri mettano in atto il coordinamento in parola *prima* di emettere ordini di rimozione o segnalazioni (cosiddetta "prevenzione di conflittualità"), nonché per incentivare l'uso degli strumenti di Europol.

Viene, infine, sancito l'obbligo degli Stati membri di predisporre adeguati canali di comunicazione per garantire il tempestivo scambio di informazioni tra le autorità nazionali competenti, anche al fine di una proporzionata ed equa applicazione delle sanzioni (considerando n. 29), nonché l'obbligo per i prestatori di servizi di *hosting* di

informare immediatamente l'autorità investigativa dello Sato membro o degli Stati membri interessati, dell'esistenza di eventuali prove della perpetrazione di reati di terrorismo di cui i *providers* vengano a conoscenza. Tali informazioni potrebbero essere utilizzate dagli organi inquirenti per emettere misure investigative previste dalla legislazione nazionale od europea, ivi incluso l'ordine europeo di produzione e di conservazione della prova elettronica (considerando n. 31 e 32).

3. La normativa italiana in materia di rimozione dei contenuti terroristici dal web: prime riflessioni sulla compatibilità con il Regolamento in fase di adozione.

La legislazione italiana prevede già dal 2015 norme specifiche che consentono all'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*. Si tratta, in particolare, del decreto-legge 18 febbraio 2015, n. 7, convertito con modificazioni dalla legge 17 aprile 2015, n. 43, che ha adottato importanti misure di contrasto al terrorismo anche di matrice internazionale, introducendo nuove figure di reato destinate a punire chi organizza, finanzia e propaganda viaggi a scopi terroristici e chi si arruola o si addestra, anche autonomamente, per le medesime finalità, così recependo nel nostro ordinamento il dettato della storica risoluzione del Consiglio di Sicurezza delle Nazioni Unite n. 2178(2014). Proprio in ragione del diffuso utilizzo della rete e dei *social network* in questo tipo di attività criminali, è stata anche prevista un'aggravante per i delitti di addestramento, di istigazione e di apologia del terrorismo che consiste nel commettere tali condotte attraverso strumenti telematici o informatici[29].

Venendo all'articolo 2 del decreto-legge in parola, dedicato in particolare al tema che qui ci occupa, esso 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, quando il pubblico ministero procede per reati di terrorismo (e in particolare per quelli previsti dagli articoli 270 *bis*, 270 *ter*, 270 *quater* e 270 *quinquies* del codice penale) e vi sono concreti elementi che lo inducano a ritenere che le attività criminose vengono perpetrate per via telematica, ordina con decreto motivato ai *service providers* la rimozione dei contenuti. Nel caso di contenuti caricati dagli utilizzatori su piattaforme di *hosting*, deve essere disposta la rimozione dei soli specifici contenuti ritenuti illeciti, intervenendo così in

[29] Sul punto F. VIGANÒ, *Pubblicato sulla Gazzetta Ufficiale il nuovo decreto legge in materia di contrasto al terrorismo*, in questa *Rivista*, 23 febbraio 2015; S. LICCIARDELLO, *Nuove norme antiterrorismo in Italia*, sezione *Il mondo dell'intelligence* nel sito del Sistema di informazione per la sicurezza della Repubblica *www.sicurezzanazionale.gov.it*, 9 settembre 2016; A. CAVALIERE, *Considerazioni critiche intorno al d.l. Antiterrorismo, n. 7 del 18 febbraio 2015*, in *Dir. pen. cont. – Riv. trim.*, 2/2015, p. 232 ss.; R. KOSTORIS, F. VIGANÒ (a cura di), *Il nuovo 'pacchetto' antiterrorismo*, Torino, 2015; G. LEO, *Nuove norme in materia di terrorismo*, in questa *Rivista*, 18 dicembre 2015.

maniera selettiva ed evitando l'eliminazione "di massa" di testi, immagini, video e siti *web*, che violerebbe la libertà di espressione e di informazione degli utenti[30].

I *providers* destinatari dell'ordine di rimozione devono adempiere immediatamente e comunque non oltre quarantotto ore dal ricevimento della notifica. In caso di mancata ottemperanza, viene disposta dal giudice competente, su richiesta del pubblico ministero, l'interdizione dell'accesso al dominio internet 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[31].

Appare, altresì, rilevante richiamare il dettato dell'articolo 16 del Decreto legislativo 9 aprile 2003, n. 70, che ha recepito l'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.

Inoltre, l'articolo 17 del medesimo Decreto legislativo (che attua l'articolo 15 della Direttiva 2000/31/CE) precisa – come sopra già evidenziato – 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

---

[30] Nel corso dell'audizione presso le Commissioni parlamentari sul testo del decreto-legge, l'allora Garante della Privacy Antonello Soro ha evidenziato che l'inibizione, su ordine del pubblico ministero, dell'accesso a siti contenuti nella *black-list*, deve essere circoscritta ai soli contenuti accessibili al pubblico, escludendo espressamente ogni forma di monitoraggio delle comunicazioni private che violerebbe il diritto alla segretezza delle comunicazioni di cui dall'articolo 15 della Costituzione (A. SORO, *Disposizioni normative in tema di lotta al terrorismo – Audizione del Presidente Antonello Soro presso le Commissioni riunite Giustizia e Difesa* – Camera dei Deputati, 4 marzo 2015, accessibile al seguente *link*).

[31] Nel corso dell'audizioni parlamentare sul testo del decreto-legge, l'allora Capo della Polizia, Prefetto Alessandro Pansa, ha evidenziato i rischi connessi alla mancata rimozione di contenuti con finalità terroristica da un *social network*, nelle quarantotto ore successive alla richiesta del pubblico ministero: vedasi *Audizione del Prefetto Alessandro Pansa su C. 2893 Governo recante "Conversione in legge, con modificazioni, del decreto-legge 18 febbraio 2015, n. 7, 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"*. 395. XVII Legislatura – Bollettino delle giunte e delle commissioni parlamentari – Commissioni Riunite (II e IV), 25 febbraio 2015, p. 10 (accessibile a questo *link*).

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.

Il sopra delineato quadro normativo interno relativo alla responsabilità del *provider* induce, in primo luogo, ad interrogarsi sulla sua compatibilità con le diposizioni del nuovo Regolamento in fase di adozione. Quest'ultimo, nel considerando n. 5, fa riferimento al rapporto tra il proprio articolato e l'articolo 14 della Direttiva 2000/31/CE sul commercio elettronico sopra menzionato, precisando che "l'applicazione del presente regolamento non dovrebbe pregiudicare l'applicazione dell'articolo 14 della direttiva 2000/31/CE". In particolare, tutte le misure adottate dal prestatore di servizi di *hosting* ai sensi del nuovo Regolamento, comprese le eventuali misure proattive, non dovrebbero comportare automaticamente la perdita, per il *provider*, del beneficio dell'esenzione di responsabilità prevista in tale disposizione; inoltre, rimane impregiudicata la competenza delle autorità e degli organi giurisdizionali nazionali a stabilire la responsabilità dei prestatori di servizi di *hosting* nei casi (sopra menzionati) in cui – ai sensi dell'articolo 14 – non possano beneficiare di tale esenzione (ovvero in caso di conoscenza dell'illiceità dell'informazione o di inerzia nella rimozione).

Da ciò deriva a livello interpretativo che successivamente all'adozione della proposta di Regolamento di cui qui ci occupiamo, dovrebbe rimanere attuale quella giurisprudenza di legittimità che ha rinvenuto proprio nell'articolo 14 della Direttiva 2000/31/CE sul commercio elettronico (e conseguentemente nell'articolo 16 del Decreto legislativo n. 70/2003 che lo recepisce) la fonte dell'obbligo per il *provider* di impedire l'evento (*rectius*: il persistere dell'evento), legittimante un'imputazione di responsabilità dello stesso a titolo concorsuale (concorso per omissione) in caso di inadempimento dell'obbligo di rimozione del contenuto illecito. Questa responsabilità è stata affermata in particolare dalla Corte di cassazione in una sentenza del 27 dicembre 2016 (Cass. Pen., Sez. V, 27 dicembre 2016, n. 54946), in cui la Suprema Corte ha ritenuto la sussistenza della responsabilità dell'imputato a titolo di concorso (per omissione) nel reato di diffamazione, poiché il *provider*/imputato aveva consapevolmente mantenuto il contenuto diffamatorio sul proprio sito e consentito "che lo stesso esercitasse l'efficacia diffamatoria", anche se aveva avuto conoscenza dell'evento lesivo ancora prima dell'ordine di sequestro del sito, avendo la parte offesa inviato un'e-mail con cui richiedeva la rimozione del contenuto diffamatorio. In particolare, si riteneva la responsabilità del provider per "avere l'imputato mantenuto consapevolmente l'articolo sul sito"[32].

[32] Per la configurazione di una sorta di concorso omissivo del *provider* a seguito di richiesta di rimozione del contenuto illecito (e il criterio, attesa la sua *ratio*, si ritiene, che valga sia se la richiesta provenga dal PM che da qualsiasi altro interessato), vedasi anche Tribunale civile di Torino, 7 aprile 2017, n. 1928, in *Danno resp.*, 2018, 1, p. 87 ss.; Tribunale civile di Napoli Nord, 3 novembre 2016, in *Giur. it.*, 2017, 3, p. 629 ss.

Secondo alcuni critici, alla stregua di questa impostazione la responsabilità concorsuale si manifesterebbe in un momento successivo a quello della consumazione del reato che è diretto ad impedire, ciò in evidente contrasto con l'elaborazione giurisprudenziale e dottrinale sulla costruzione della fattispecie omissiva impropria risultante dal combinato disposto degli artt. 40 e 110 c.p, sul presupposto che il reato di diffamazione integra, infatti, un reato istantaneo. Si potrebbe, tuttavia, osservare al riguardo che tale ricostruzione poteva avere una sua *ratio* in tempi in cui non esisteva internet, quando la diffamazione a mezzo stampa era davvero un reato istantaneo perché con la pubblicazione dell'articolo in cartaceo si consumava la condotta di reato. Oggi, con internet, l'offesa al bene giuridico (in questo caso la reputazione, ma lo stesso vale per tutti gli altri beni protetti, inclusa la tutela della sicurezza pubblica di cui si occupa la proposta di Regolamento qui in esame) si rinnova continuamente: ogni giorno che la notizia rimane postata sul sito il reato si rinnova, anzi l'offesa si amplifica giorno per giorno per la velocità di diffusione sulla rete (invece di attutirsi come avveniva in passato, con i vecchi *media*) e progressivamente acquisisce connotati via via più gravi, raggiungendo sempre nuovi soggetti.

Vale, infine, rilevare che sarà opportuna una riflessione ad ampio spettro, in sede di attuazione a livello nazionale dell'articolo 18 della proposta di Regolamento (che impone agli Stati membri di adottare norme sulle sanzioni applicabili in caso di violazione da parte dei prestatori di servizi di *hosting* di determinati obblighi a loro carico), sulla tipologia delle sanzioni da imporre, atteso che il considerando n. 38 della proposta di Regolamento, così come modificato dal Consiglio UE in sede di orientamento generale, precisa che tali sanzioni potranno essere sia di natura amministrativa che penale e che occorrerà effettuare un bilanciamento affinché siano, da un lato, efficaci e dissuasive, e dall'altro proporzionate alla violazione ed alla limitazione delle libertà fondamentali. Con specifico riferimento all'inadempimento dell'obbligo di cui al primo comma, lett. b) dell'articolo 18 in parola ("attuazione degli ordini di rimozione e relativo feedback"), il nostro ordinamento prevede – sulla base delle disposizioni sopra indicate – solo una sanzionabilità penale e civile del *provider* a seguito dell'inadempimento dell'ordine dell'autorità giudiziaria, atteso che le sanzioni amministrative previste dall'articolo 21 del decreto legislativo n. 70/2003 non riguardano le condotte omissive del prestatore di servizi di *hosting* di cui all'articolo 16 del decreto legislativo stesso. Ciò porrà dei delicati aspetti interpretativi e di raccordo, anche per quanto attiene alle questioni inerenti alla giurisdizione, rispetto alla legislazione di altri Stati membri che potrebbero, invece, ricondurre le violazioni in parola alla mera sfera amministrativa, potendo peraltro ciascun Paese, ai sensi dell'articolo 17 della proposta di Regolamento, designare autorità competenti diverse (intendendo con questo anche di natura diversa, giudiziaria o amministrativa) per emanare gli ordini di rimozione (ai sensi del primo comma, lett. a) e per far rispettare gli obblighi al *provider* mediante sanzioni (ai sensi del primo comma, lett. d).