Informatica e diritto, XLIII annata, Vol. XXVI, 2017, n. 1-2, pp. 139-176

Il fenomeno del *cybercrime* nello spazio giuridico contemporaneo. Prevenzione e repressione degli illeciti penali connessi all'utilizzo di Internet per fini di terrorismo, tra esigenze di sicurezza e rispetto dei diritti fondamentali

Pietro Maria Sabella*

1. Il terrorismo internazionale di matrice religiosa e l'utilizzo del web. Fra esigenze repressive e tutela dei diritti fondamentali. Una premessa

È di grande evidenza come, a partire dalla fine del secolo scorso, il mondo abbia dovuto iniziare a confrontarsi con l'affermazione del fenomeno terroristico di matrice religiosa su scala globale[1] che, in pochi anni, si è imposto alla nostra attenzione come antagonista in grado di colpire in modo feroce in diversi punti del pianeta, sfruttando a proprio vantaggio sia le maglie lasciate

* L'A. è dottore di ricerca in Diritto e impresa presso l'Università LUISS "Guido Carli".

[1] Per un approfondimento specifico sul rapporto tra tale fenomeno e il diritto penale, anche in prospettiva comparata, si veda F. Fasani, *Terrorismo islamico e diritto penale*, Padova, Cedam, 2016.

 ISSN 0390-0975 ISBN 978-88-495-3707-9

aperte dai vari sistemi di sicurezza di molti Paesi sia i moderni mezzi di comunicazione digitale, particolarmente efficaci nel garantire un rapido flusso di informazioni.

È altresì vero, infatti, come gruppi terroristici fondamentalisti, quali Daesh o, già prima, Al Qaeda[2], abbiano sempre fatto impiego in modo specifico e massiccio dei vari strumenti di comunicazione e, in particolare, di Internet e dei social media, non solo per fini propagandistici ma, più recentemente, anche per controllare, manovrare, attivare e dirigere all'interno dello scacchiere globale i propri "lupi solitari" o le c.d. "cellule dormienti" o, ancora, per fornire guide e *vademecum* utili alla radicalizzazione e all'auto-addestramento dei c.d. foreign fighter.

La questione, peraltro, ha assunto particolare rilievo alla luce dei recenti tragici eventi che hanno investito il territorio europeo e non solo, e che sembrano portare alla luce la parziale fallacia delle misure adottate a livello nazionale e sovranazionale per il contrasto al terrorismo e la capacità di questi gruppi di incidere, proprio mediante questi strumenti di comunicazione, sulla stessa tenuta complessiva dell'ordine democratico di un Paese.

In questo contesto, lo strumento digitale diventa l'elemento nodale nella organizzazione di attacchi terroristici e nella predisposizione di attività quali il reclutamento, il finanziamento, la propaganda, la formazione, l'apologia e la diffusione di informazioni utili per determinare processi di radicalizzazione.

Tutto ciò impone l'esigenza di procedere a una più profonda riflessione sulla connessione tra la difesa della sicurezza pubblica e l'utilizzo della Rete, al fine di potere agire in chiave preventiva, indebolendo il forte legame che unisce attività terroristiche e i nuovi mezzi di comunicazione di massa.

Nella ricerca di un ragionevole equilibrio tra la necessità di salvaguardare l'ordine pubblico internazionale, la sicurezza nazionale e il web – che rischia di affermarsi quale mezzo funzionale alla propaganda (in via preliminare) e alla commissione (in via successiva) di reati a fini terroristici – è importante creare un meccanismo di mutuo dialogo tra istituzioni pubbliche e soggetti privati, in primo luogo gli ISP - *Internet Service Provider*, gli *hosting provider*[3]

[2] M. NORMALE, *Nuove prospettive della criminologia nell'ambito del computer crime*, in "Gnosis", 1997, n. 1.

[3] Cfr. Cass., sez. III pen., 3 febbraio 2014, n. 5107, con nota di S. CORBETTA, *Caso "Google": nessuna responsabilità dell'Host Provider per l'omesso impedimento di reati realizzati dagli utenti della rete*, in "Diritto penale e processo", 2014, n. 3, p. 277 ss., ove i giudici di legittimità escludono una responsabilità penale dell'*hosting provider* per omesso impedimento dell'evento lesivo, riconoscendone invece una di tipo commissivo per trattamento illecito dei

ISSN 0390-0975 ISBN 978-88-495-3707-9

e quindi i social network[4], fondato su un sistema normativo "integrato" e multilivello[5], idoneo a definire misure condivise per la prevenzione di quei reati informatici che alimentano ulteriormente i circuiti linfatici dei gruppi terroristici, la cui difficile perimetrazione *materiale* sembra trovare opportuno contrappeso nell'*immateriale* spazio digitale.

Di fronte a questo allarmante fenomeno si è assistito all'espansione del diritto penale contemporaneo[6], oltre che del diritto sanzionatorio amministrativo e, purtroppo, anche di una risposta in termini militari.

2. Esiste un ruolo del diritto penale nel cyberspazio?

Rispetto a queste nuove manifestazioni di criminalità terroristica bisogna chiedersi se il sistema penale nazionale e di derivazione europea stia iniziando a mostrare i propri limiti.

L'impossibilità di garantire un'efficace protezione dei beni individuali e collettivi attraverso il solo impiego dello strumento penalistico ha generato modelli di legislazione – come è possibile notare in via esemplificativa dall'impianto della direttiva antiterrorismo (UE) 2017/541 – che sembrano riproporre il rischio di un ritorno al *diritto penale del nemico*[7] e alle logiche

dati, dal momento in cui l'Autorità gli rende nota l'illiceità dei contenuti che ospita. Nel senso opposto, Cass., sez. V pen., 27 dicembre 2016, n. 54946, con commento di A. Ingrassia, *Responsabilità penale degli internet service provider: attualità e prospettive*, in "Diritto penale e processo", 2017, n. 12, p. 1621 ss., con la quale la Corte riscontra una responsabilità penale del manager di un sito internet per non avere eliminato gli effetti dannosi derivanti dal protrarsi di un contenuto diffamatorio presente nello stesso.

[4] E. Rosati, G. Sartor, *Social networks e responsabilità del provider*, www.medialaws.eu, 23 aprile 2012. Peraltro, i social network, rispetto agli *hosting provider*, possono essere posti in un rapporto di *genus* a *species*, cfr. L. Picotti, *I diritti fondamentali nell'uso ed abuso dei social network. Aspetti penali*, in "Giurisprudenza di merito", 2012, n. 12, p. 2522.

[5] V. Militello, *L'identità della scienza giuridica penale nell'ordinamento multilivello*, in "Rivista italiana di diritto e procedura penale", 2014, n. 1, p. 107 ss.

[6] Di questo avviso, V. Militello, *Terrorismo e sistema penale: realtà, prospettive, limiti*, presentazione del VII corso interdottorale di diritto e procedura penale "Giuliano Vassalli" (Noto, 11-13 novembre 2016), in "Diritto penale dell'economia", 2017, n. 1, p. 4.

[7] *Ex multis* in relazione all'elaborazione concettuale del diritto penale del nemico in materia di terrorismo, F. Fasani, *op. cit.*, p. 147 ss.; G. Marino, *Il sistema antiterrorismo alla luce della l.43/2015: un esempio di diritto penale del nemico?*, in "Rivista italiana di diritto e procedura penale", 2016, n. 3, pp. 1388-1426; S. Bonini, *Lotta alla criminalità organizzata e terroristica, garanzia dell'individuo, garanzia della collettività, riflessioni schematiche*, in "Cassazione penale", 2009, n. 5, p. 2216 ss.; R. Bartoli, *Lotta al terrorismo internazionale. Tra diritto penale del nemico, jus in bello del criminale e annientamento del nemico assoluto*, Torino, Giappichelli,

 ISSN 0390-0975 ISBN 978-88-495-3707-9

del diritto penale d'autore quale consigliato strumento di politica criminale nel contrasto al terrorismo islamico.

Infatti, in assenza di strumenti normativi extra-penali efficaci a regolare il fenomeno e a prevenirlo, il legislatore tende poi a ricorrere a fattispecie incriminatrici in cui la soglia di intervento penale risulta essere alquanto anticipata a fronte di condotte, invece, solo potenzialmente lesive di beni giuridici tangibili.

Oppure, come accaduto di recente proprio in relazione agli illeciti informatici, si assiste ad arresti della giurisprudenza di legittimità[8] con i quali si tenta di attribuire ai *service provider* una posizione di garanzia rispetto alle pubblicazioni di post effettuate dai singoli utenti in contrasto con la riserva di legge[9], al fine di offrire una forma di tutela simile a quella fornita in tema di pedo-pornografia in Internet[10].

2008; F. VIGANÒ, *Sul contrasto al terrorismo internazionale di matrice islamica tramite il sistema penale, tra diritto penale del "nemico" e legittimi bilanciamenti*, in "Studi urbinati", 2007, n. 4, p. 336 ss.; M. DONINI, *Il diritto penale di fronte al "nemico"*, in "Cassazione penale", 2006, n. 2, p. 737; F. PALAZZO, *Contrasto al terrorismo, diritto penale del nemico e principi fondamentali*, in "Questione giustizia", 2006, n. 4, p. 674 ss.; L. FERRAJOLI, *Il «diritto penale del nemico» e la dissoluzione del diritto penale*, in "Questione giustizia", 2006, n. 4, pp. 797-812.

[8] Si fa ancora riferimento alla recente sentenza Cass., sez. V pen., n. 54946/2016, cit. Tuttavia, è opportuno segnalare come questi nuovi orientamenti siano stati fatti propri anche dai giudici di Strasburgo; basta infatti ricordare il caso *Delfi As. c. Estonia*, del 16 giugno 2015, in cui la Grande Camera della Corte EDU si è pronunciata per la prima volta sulla delicata questione della compatibilità della responsabilità degli *Internet Service Provider* con la Convenzione stessa e, più in particolare, sull'eventualità che uno Stato membro possa incorrere nella violazione della libertà di espressione ai sensi dell'art. 10 CEDU qualora consideri un ISP – nel caso di specie si trattava di un portale di news on line – responsabile per avere pubblicato alcuni contenuti incitanti all'odio e alla violenza rispetto ai terzi. La Corte, in questo caso, si è espressa a favore della responsabilità dell'ISP e della mancata violazione dell'art. 10 CEDU da parte dell'Estonia seguendo però un *iter* logico giuridico alquanto discutibile.

[9] Sul tema A. INGRASSIA, *op. cit*, p. 1625; R. BARTOLI, *Brevi considerazioni sulla responsabilità penale dell'internet service provider*, in "Diritto penale e processo", 2013, n. 5, pp. 600-606; *funditus*, F. RUGGIERO, *Individuazione nel ciberspazio del soggetto penalmente responsabile e ruolo dell'Internet provider*, in "Giurisprudenza di merito", 2001, n. 2, p. 586 ss.; V. ZENO-ZENCOVICH, *I rapporti fra responsabilità civile e responsabilità penale nelle comunicazioni su internet (riflessioni preliminari)*, in "Il Diritto dell'informazione e dell'informatica", 1999, n. 6, p. 1049 ss.; S. SEMINARA, *La responsabilità penale degli operatori su internet*, in "Il Diritto dell'informazione e dell'informatica", 1998, n. 4-5, p. 745 ss.

[10] D. DE NATALE, *Responsabilità penale dell'internet service provider per omesso impedimento e per concorso nel reato di pedopornografia*, in G. Grasso, L. Picotti, R. Sicurella (a cura di), "L'evoluzione del diritto penale nei settori d'interesse europeo alla luce del Trattato di Lisbona", Milano, Giuffrè, 2011, p. 295 ss.; A. MANNA, *Considerazioni sulla responsabilità penale*

ISSN 0390-0975 ISBN 978-88-495-3707-9

Ed ecco che, come già accaduto in passato nel nostro Paese, in relazione alla lotta al crimine organizzato e, in particolare, a "Cosa nostra"[11], sembra riemergere la necessità di ribadire come imprescindibile un equilibrio tra diverse esigenze di tutela in contrapposizione, ovvero fra salvaguardia della sicurezza pubblica da un lato, e protezione dei diritti fondamentali dei singoli individui, dall'altro.

Questo bilanciamento è oggi fondamentale, onde scongiurare la prima reale disfatta contro il terrorismo internazionale, consistente nella rinuncia o nell'indebolimento delle garanzie e dei diritti costituzionali dei cittadini per scopi repressivi. Ciò significa che in una società ove il mondo reale e quello virtuale risultano essere sempre più integrati, il diritto e il processo penale non dovranno liberarsi dei propri tratti costitutivi tipici, in particolare dei principi di riserva di legge, offensività e del giusto processo, *ex* artt. 25, co. 2 e 111 Cost. e artt. 6 e 7 CEDU, ma dovranno modularsi con altre discipline scientifiche per decifrare e interpretare il linguaggio delle nuove tecnologie ed il loro impatto sulle categorie tradizionali del diritto[12] e del processo.

Nel contesto attuale, in cui si interviene con la sanzione penale per reprimere e prevenire comportamenti che hanno luogo anche in uno spazio virtuale e privo di una chiara regolamentazione *multilivello*, il rischio appare proprio quello di risultare o scarsamente efficaci o eccessivamente repressivi.

In particolare, l'accento va qui posto sull'efficacia dell'attuale disciplina penale in materia di contrasto al terrorismo circa la capacità di inserirsi in maniera adeguata nel delicato rapporto tra esigenze di garanzia di libertà costituzionali e repressione di comportamenti potenzialmente delittuosi e offensivi per l'intera collettività, ovvero fra libera manifestazione del pensiero, tutela della privacy e ordine pubblico.

Non è innegabile che risulterà molto complesso trovare un efficace equilibrio, soprattutto in relazione ai casi in cui il fenomeno criminale prenda origine all'interno del web, mediante un rapido scambio di informazioni finalizzate al compimento di fatti particolarmente lesivi e veicolate attraverso messaggi ispirati a convinzioni religiose, morali o etiche che sembrano – solo in apparenza – qualificare il tipo di autore del reato distinguendolo dal resto dei consociati.

dell'internet provider in tema di pedofilia, in "Il Diritto dell'informazione e dell'informatica", 2001, n. 2, pp. 145-151.

[11] Sul punto G. FIANDACA, C. VISCONTI, *Scenari di mafia. Orizzonte criminologico e innovazioni normative*, Torino, Giappichelli, 2010, p. 534.

[12] M. HILDEBRANDT, *Smart Technologies at the Ends of Law*, Northampton, USA, 2015.

 ISSN 0390-0975 ISBN 978-88-495-3707-9

È qui allora che un'esasperata rincorsa alla sconfitta del nemico potrebbe portare ad appiattire la risposta sanzionatoria sull'autore più che sul fatto[13] e su alcune manifestazioni di pensiero o di religione, solo potenzialmente in grado di esprimersi al di là dei confini del lecito, oltre che non lasciare comprendere quali siano le reali dinamiche che interessano la commistione dell'*agere* criminoso e dell'uso del web.

Questo rischio, in definitiva, appare dunque ancora più verosimile proprio in ragione del fatto che il diritto penale è chiamato a rispondere al fenomeno terroristico internazionale all'interno di una nuova dimensione immateriale, priva di un sostrato giuridico composito in grado di regolarne – sotto una pluralità di aspetti – il funzionamento e di individuarne i limiti esplicativi.

In questo frangente storico, peraltro, la *cyber law*, intesa quale complesso normativo che regola il rapporto tra gli utenti all'interno del mondo virtuale per proteggere interessi di fondamentale importanza fra cui, *in primis*, la personalità individuale, la riservatezza o il diritto d'autore[14], appare ancora in una fase di evoluzione embrionale, almeno nel contesto nazionale, per potere supportare il legislatore penale nel corretto inquadramento di alcuni comportamenti di forte impatto sociale, regolati tuttavia ancora secondo una concezione del diritto che nel cyberspazio risulta inefficace.

Del resto, il cyberspazio[15] rappresenta un non luogo in cui miliardi di informazioni possono essere trasferite raggiungendo simultaneamente un elevatissimo numero di persone, consentendo così un salto di qualità rispetto ai metodi di comunicazione precedentemente disponibili.

Anche per questo motivo, il cyberspazio si configura, oramai, come spazio privilegiato di formazione delle intelligenze individuali, ma soprattutto

[13] Nel recente passato un simile dibattito si è sviluppato con l'introduzione del delitto di detenzione di materiale pedo-pornografico, sul punto, G.L. GATTA, *Protezione dei minori contro lo sfruttamento e l'abuso sessuale: ratificata la Convenzione di Lanzarote del 2007 (e attuata una mini-riforma nell'ambito dei delitti contro la persona)*, in "penalecontemporaneo.it", 20 settembre 2012; rispetto al reato di immigrazione clandestina vedi C. RUGGIERO, *La depenalizzazione del reato di "immigrazione clandestina": un'occasione mancata per il sistema penale italiano*, in "penalecontemporaneo.it", 22 febbraio 2017.

[14] G. ZICCARDI, *Cyber law in Italy*, Milano, Kluwer Law International, 2013; L. EDWARDS, C. WAELDE, *Law and Internet*, Oxford, Hart, 2000; D.R. JOHNSON, D. POST, *The Rise of Law in Cyberspace*, in "Stanford Law Review", 1996, p. 1367.

[15] Il termine sembra essere stato coniato nel 1982, nella sua forma inglese *cyberspace*, all'interno di un racconto fantascientifico dal titolo *Burning Chrome* di William Gibson. Tuttavia esso è stato più ampiamente utilizzato, trovando quindi maggiore diffusione sempre con lo stesso autore nel più noto romanzo *Neuromancer*, 1984 (trad. it. 1986).

ISSN 0390-0975 ISBN 978-88-495-3707-9

collettive, tanto che in esso trovano una propria dimora identità multiple e condivise, comunità virtuali e forme cooperative di intesa che, intorno alla promozione o condivisione di istanze locali o globali di ogni genere, costituiscono veri e propri gruppi di attivismo.

Inoltre, la possibilità di accedervi con relativa facilità e con costi sufficientemente bassi ha determinato, in questi ultimi anni, anche un netto cambiamento della consapevolezza del *sapere* e della sua gestione; il cyberspazio, infatti, non è solo una via d'accesso al flusso ininterrotto di informazioni ma è esso stesso uno strumento di creazione e manipolazione delle informazioni.

Lo sviluppo e la capillarizzazione delle reti informatiche e degli strumenti di comunicazione digitali in tutto il pianeta ha accentuato in modo evidente anche il processo di distribuzione del potere verso nuovi centri di comando e di influenza i quali, sempre meno, sono rappresentati dal tradizionale Stato-nazione[16]; come è noto, esso, in alcuni contesti, diventa invero lo stesso soggetto passivo dell'uso delittuoso della Rete.

Si sono già registrati casi del genere, come per l'attacco informatico subito nel 2007 dall'Estonia che, per diverse ore, è rimasta priva del funzionamento dei servizi essenziali, dall'erogazione dell'acqua, della corrente elettrica, fino alle transazioni bancarie; e ancora quello subito l'anno successivo dalla Georgia, in concomitanza della crisi bellica scoppiata con la Federazione Russa.

Da questi esempi si desume come il cyberspazio sia il nuovo campo di battaglia e di competizione geopolitica, tanto da essere definito come il *quinto dominio* della difesa militare[17], all'interno del quale, inevitabilmente, il comportamento dell'essere umano potrà connotarsi anche di un disvalore penale, che si estrinsecherà in un illecito informatico o nel c.d. *cybercrime*[18].

Il cyberspazio diventa così un mezzo criminogeno estremamente potente ed efficace, in quanto il criminale informatico, a fronte della possibilità di conservare l'anonimato, potrà essere in grado di realizzare una pluralità di illeciti diversi, minando non solo l'integrità di beni giuridici individuali ma anche collettivi, come quello della sicurezza e dell'ordine pubblico.

[16] Per approfondire il tema, E. MAURO, Z. BAUMAN, *Babel*, Roma-Bari, Laterza, 2015.

[17] R. AZZARONE, *Cyber vademecum*, Parte II, in "Gnosis", 2014, n. 3, pp. 36-47, il quale afferma che il cyberspazio rappresenta proprio il quinto elemento del controllo militare dopo terra, acqua, cielo e spazio.

[18] A. ROSSETTI, R. CASIRAGHI, G. VACIAGO, S. RICCI, *Prevention and Fight Against Cyber-crime: The ILLbuster Project*, in "Ciberspazio e diritto", 2015, n. 1, p. 155 ss.; M.C. DE VIVO, G. RICCI, *Diritto, crimini, tecnologie*, in questa *Rivista*, 2012, n. 2, p. 27 ss. Si veda anche T. KRONE, *High Tech Crime Brief*, Canberra, Australian Institute of Criminology, 2005.

 ISSN 0390-0975 ISBN 978-88-495-3707-9

L'uso e la stessa dipendenza dallo spazio digitale hanno portato, in effetti, alla drammatica crescita esponenziale di minacce e attacchi di ogni tipo che hanno reso vulnerabile, praticamente, ogni dispositivo elettronico in dotazione ad un individuo.

Basti pensare che le statistiche pubblicate dal *World Economic Forum* nel 2015 hanno stimato il costo globale e complessivo della criminalità informatica in circa 445 miliardi di dollari l'anno e che, in mancanza di idonei strumenti normativi e tecnici di difesa e prevenzione, per l'anno 2020, le perdite economiche potrebbero giungere a toccare la vetta di 3.000 miliardi di dollari[19].

Oltre che strumento criminogeno, come già anticipato, il cyberspazio è, in realtà, un vero e proprio campo di battaglia, all'interno del quale, oltre ai classici sistemi informatici interconnessi, sono presenti dispositivi sia hardware che software, capaci di violare la sicurezza di infrastrutture tecniche e virtuali di ogni genere e, dunque, in grado di danneggiare in modo trasversale sia il know-how di aziende strategiche per l'economia di un Paese o, perfino, di impossessarsene, sia di colpire i centri nevralgici della sicurezza di una nazione, oltre che i singoli individui.

Ecco che in questo nuovo contesto sociale, culturale e tecnologico, il contrasto al terrorismo internazionale di matrice religiosa non potrà essere innovato e reso maggiormente efficiente in assenza di una strategia che veda al centro anche il ruolo degli *Internet Service Provider* e, dunque, dei social network nell'identificazione delle minacce e nella prevenzione della diffusione di messaggi e informazioni in grado di rafforzare il vincolo terroristico, inducendo alla preparazione e alla realizzazione di nuovi attacchi.

Tuttavia, come verrà meglio evidenziato nel prosieguo, occorrerà evitare di costruire dei modelli normativi di prevenzione e repressione fondati su una funzione di "censura" esercitata dagli ISP e dai social network posti, così, in una posizione di garanzia rispetto alle attività dell'utente o, in assenza di un controllo "forte" da parte di questi soggetti privati, lasciare, come accaduto negli USA con il *Cyber Security Information Sharing Act* del 2015[20], che istituzioni pubbliche o governative possano entrare in possesso di una vastissima quan-

[19] Sono dati del Consorzio Interuniversitario per l'Informatica inseriti in *Il futuro della Cybersecurity in Italia*, 2015, p. 2; cfr. P. SEVERINO, *Le frontiere della sicurezza informatica e prevenzione del cybercrime*, in "Luiss Open", 8 settembre 2017, p. 8 ss.

[20] Già sul *Patriot Act* e la contrapposizione fra diverse esigenze di tutela, vedi A. DE PETRIS, *Il Patriot Act e le nuove libertà digitali*, in "Il Diritto dell'informazione e dell'informatica", 2007, n. 3, p. 599 ss.

ISSN 0390-0975 ISBN 978-88-495-3707-9

tità di informazioni trasmesse proprio dagli ISP per prevenire attività illecite, determinando, indirettamente, una violazione della privacy degli utenti.

Del resto, un controllo preventivo su tutte le informazioni in entrata, incentrato sulla valutazione della loro liceità, richiederebbe maggior tempo e, di riflesso, una parziale compromissione della velocità istantanea del processo di scambio di informazioni tipica di Internet[21].

In ogni caso, il tema della prevenzione e repressione dei delitti con finalità di terrorismo all'interno di Internet pone ulteriori sfide che, come accennato, dovranno essere affrontate con l'ausilio di categorie scientifiche ulteriori rispetto a quelle classiche del diritto penale, proprio per evitare di strutturare fattispecie che, infine, non potranno che risultare inefficaci o derogatorie di alcuni principi fondamentali.

In questa sfida, comunque, bisognerà avere il coraggio di non lamentare, eventualmente, solo "torsioni" o "tensioni" delle categorie classiche del diritto penale di parte generale o speciale, ma affrontare con coraggio il tema della commistione del mondo reale con quello virtuale. Si tratta piuttosto di pensare a una *cyber criminal law* che rechi con sé inevitabilmente la necessità di giungere a una nuova identificazione delle tipologie e modalità di condotta, talvolta totalmente automatizzate[22], dei soggetti attivi coinvolti, degli eventuali concorrenti, nonché di nuovi beni giuridici da tutelare[23], da aggiungere a quello del mantenimento dell'ordine e della sicurezza pubblica, come potrebbe essere, ad esempio, per il concetto di sicuro e adeguato accesso al web e ai suoi contenuti e a una libera espressione del proprio pensiero all'interno dello stesso[24].

[21] A. CHEUNG, R.H. WEBER, *Internet Governance and the Responsibility of Internet Services Providers*, in "Wisconsin International Law Journal", vol. 26, 2008, n. 2, p. 403 ss.; M. KONKEL, *Internet Indecency, International Censorship, and Service Providers Liability*, in "New York Law School Journal on International and Comparative Law", vol. 19, 1999-2000, p. 453 ss. In Italia, L. PICOTTI, *La nozione di "criminalità informatica" e la sua rilevanza per le competenze europee*, in "Rivista trimestrale di diritto penale dell'economia", 2011, n. 4, p. 827 ss.

[22] Solleva il problema sulla rilevanza penale delle condotte automatizzate, R. BARTOLI, *Brevi considerazioni sulla responsabilità penale dell'internet service provider*, cit., p. 604.

[23] In relazione all'individuazione del bene giuridico tutelato, cfr. A. MANNA, *Società dell'informazione e diritto penale: problemi e prospettive*, in "Archivio penale", 2014, n. 1, p. 340 ss.

[24] Ci si vuole collegare alla proposta di Stefano Rodotà, formulata in occasione dell'*Internet Governance Forum* del 2010, per la quale si intendeva modificare il testo costituzionale con la previsione di una disposizione che garantisse l'eguale diritto di accesso alla rete Internet, in condizioni di parità, trasfusa nel d.l. costituzionale A.S. 2485, XVI leg., nonché alla *Convenzione sul Cybercrime* adottata nel 2001 dal Consiglio d'Europa e alla *Carta dei Diritti Globali di Internet*, predisposta a Vilnius dall'*Internet Governance Forum* del 2010, con le

 ISSN 0390-0975 ISBN 978-88-495-3707-9

Infine, bisognerà decidere se lo sviluppo della tematica relativa alla società della comunicazione digitale e del diritto penale dovrà seguire, ancora una volta, il *modello* dei sotto-sistemi penali o dovrà integrarsi con il sistema penale tradizionale codicistico[25].

2.1. Il cybercrime *e il cyberterrorismo*

Giunti a questo punto, prima di analizzare in maniera più approfondita le criticità che l'attuale ordinamento penale esprime in materia di contrasto al terrorismo internazionale di matrice religiosa e utilizzo delittuoso di Internet e dei social media, per esigenze di completezza è necessario distinguere fra le varie tipologie di *cybercrime* fino ad oggi identificate, al fine di evidenziare le caratteristiche essenziali del terrorismo informatico ma, soprattutto, la sua stretta dipendenza dai mezzi di comunicazione[26].

Il *cybercrime* può essere definito come un comportamento delittuoso posto in essere mediante l'uso distorto o abusivo dei sistemi hardware e software, comprendenti genericamente l'accesso illegale, la manipolazione e l'intercettazione di dati, l'interferenza con il corretto funzionamento di strumenti informatici e l'uso improprio di dispositivi[27], contraddistinto tendenzialmente dalla coesistenza di alcuni elementi quali: a) l'anonimato del soggetto attivo o la sua difficoltosa reperibilità; b) l'automatizzazione parziale o totale della condotta; c) la significativa intensità del momento *volitivo* del dolo; d) l'indebolimento delle coordinate spazio-temporali per una corretta identificazione del *tempus* e del *locus commissi delicti*.

Date queste premesse[28], possiamo poi procedere a elencare le principali categorie di crimini informatici esistenti.

quali si intende incentivare uno sviluppo delle reti informatiche nel rispetto dei principi fondamentali, fra cui spiccano la libertà di manifestazione del pensiero e la privacy. Per un approfondimento sulla rilevanza costituzionale di Internet si rimanda a G. AZZARITI, *Costituzione e Internet*, in "Diritto e Internet", 2011, n. 2, p. 7 ss.

[25] Sul tema si veda G. FIANDACA, *In tema di rapporti tra codice e legislazione penale complementare*, in "Diritto penale e processo", 2001, n. 2, p. 137 ss.

[26] Per un'ampia analisi del vasto panorama dei crimini informatici, si veda A.A. GILLESPIE, *Cybercrime, Key Issues and Debates*, Oxon-New York, Routledge, 2016.

[27] Ricostruisce e definisce similmente il crimine informatico la Convenzione del Consiglio d'Europa sulla criminalità informatica di Budapest, del 23 novembre 2001.

[28] L. PICOTTI, *La nozione di "criminalità informatica" e la sua rilevanza per le competenze penali europee*, cit., p. 827 ss., ove l'A. distingue anche fra reati informatici "in senso stretto", ovvero fra quei reati che già a livello di tipizzazione legislativa richiedono necessariamente fra

ISSN 0390-0975 ISBN 978-88-495-3707-9

Cybercrime comune, che comprende le minacce informatiche poste in essere da singoli individui o da organizzazioni criminali nazionali e transazionali, che sfruttano indebitamente il cyberspazio per la commissione di alcuni reati come, ad esempio, la truffa, l'estorsione, la molestia o lo stalking, ma anche il furto di identità, la sottrazione indebita di informazioni o la creazione di falsi marchi e brevetti.

Cyber hactivism, che si identifica per il fatto che l'attacco informatico è prodotto da singoli, gruppi o comunità di hacker, i quali, per ragioni ideologiche, politiche, di semplice protesta, per rivalsa nei confronti di alcuni individui o di gruppi economici, aggirano i dispositivi di sicurezza dei congegni elettronici oggetto dell'attacco per cagionare un danno al sistema o per ottenere alcune specifiche informazioni, raccoglierle, riutilizzarle altrove o divulgarle al pubblico. I fatti connessi al caso Wikileaks sono la corretta testimonianza della raccolta di informazioni a danno di alcuni soggetti e istituzioni pubbliche, per favorirne la conoscenza da parte del pubblico.

Cyber espionage, che può essere qualificato come quel tipo di attività finalizzata a sfruttare le potenzialità e le dinamiche di Internet per sottrarre segreti industriali per fini di concorrenza sleale o per venire a conoscenza di progetti e documenti militari segreti di enti o istituzioni straniere e ottenere così una superiorità strategica.

Cyber war, realizzata da istituzioni pubbliche, da enti privati, dagli eserciti e dall'intelligence, anche in periodi di conflitto bellico, attraverso minacce informatiche che hanno come destinatari nazioni, enti pubblici, territori e le loro infrastrutture strategiche e le loro risorse; si tratta di un vero e proprio conflitto fra nazioni, ove all'interno dello scenario virtuale, le forze in campo si combattono attraverso una regolare demolizione delle barriere di protezione critica della sicurezza dell'avversario o mediante un'integrazione di queste attività con quelle tipiche di ogni guerra[29].

Cyber terrorism, che si configura nell'ipotesi in cui l'utilizzo della Rete avvenga da parte di organizzazioni terroristiche anche internazionali, per propaganda, addestramento, affiliazione, coordinamento di operazioni belliche o contro la sicurezza collettiva e individuale, per scopi di finanziamento,

gli elementi costitutivi l'utilizzo delle tecnologie e dei prodotti informatici, o la produzione di effetti tipici su di essi; e i reati informatici "in senso ampio", i quali, invece, si caratterizzano per trovare nel cyberspazio una peculiare modalità di realizzazione e di aggressione.

[29] Così, R. PINO, *Il "cyberterrorismo": un'introduzione*, in "Ciberspazio e diritto", 2013, n. 3, p. 429.

 ISSN 0390-0975 ISBN 978-88-495-3707-9

per danneggiare infrastrutture pubbliche o per sabotare processi informatici funzionali alla sicurezza nazionale[30].

Il cyberterrorismo, dunque, in base alla definizione data sopra, è il frutto dell'incrocio fra attività terroristica ispirata a ideologie sovversive o antidemocratiche e informatica.

Più in generale, l'intreccio fra terrorismo internazionale e comunicazione è ormai tale da avere generato un rapporto di simbiosi e di interdipendenza reciproca[31] tanto da potere affermare che, in mancanza di una trasmissione via Internet o televisiva degli effetti degli attacchi terroristici e, quindi, di una propagazione mediatica della potenza intimidatrice, lo stesso gruppo terroristico potrebbe essere definito come inesistente sulla scena globale.

Il terrorismo internazionale, per esempio quello di matrice islamica, infatti, fin dal momento di programmazione e predisposizione di ogni singolo attacco, si prefigge lo scopo di ottenere la massima risonanza possibile delle conseguenze delle proprie gesta. I singoli attentati, del resto, sono realizzati non solo per destabilizzare l'ordine democratico e la sicurezza pubblica interna, ma per ottenere un "effetto moltiplicatore" della propaganda dell'ideologia jihadista; la stessa ragione dell'esistenza del terrorismo islamico internazionale sembra risiedere nella necessità di fare conoscere la propria esistenza e di imporre la propria visibilità alle masse e alle istituzioni. Esso si impone sul proscenio internazionale come un vero e proprio progetto politico e sociale che, più che testimoniare una realtà, tenta di essere mera rappresentazione globale di sé.

E tale intreccio era così vivido nel pensiero di alcuni sociologi, che, già negli anni Sessanta del secolo scorso, Marshall McLuhan ebbe ad affermare che «il terrorismo è un modo di comunicare. Senza comunicazione non vi sarebbe terrorismo»[32]. Ciò che si è accentuato rispetto al passato è la spettacolarizzazione del terrorismo, il singolo gesto, sempre più cruento e disumano, diventa strumento simbolico per alimentare la trasmissione delle notizie, ottenere consenso e determinare la paura nella mente degli spettatori.

Solo in quanto spettatore il cittadino è testimone dell'efferatezza del terrorismo contemporaneo. L'individuo, quindi, sempre meno elemento attivo di

[30] D. COHEN, *L'evoluzione del terrorismo contemporaneo nel cyber-spazio*, in "Gnosis", 2016, n. 2, p. 118 ss.; R. PINO, *op. cit.*, p. 430.

[31] In materia di comunicazione e terrorismo già, G. WARDLAW, *Political Terrorism: Theory, Tactics, and Counter-measures*, Cambridge, Cambridge University Press, 1989.

[32] M. MCLUHAN, *Gli strumenti del comunicare*, trad. it., Milano, Il Saggiatore, 1967.

ISSN 0390-0975 ISBN 978-88-495-3707-9

una società, diventa ora consumatore, ora spettatore, dunque, utente passivo dello strumento di comunicazione che crea fatti e non più li riporta.

In definitiva, il *cyber terrorism* può essere identificato in una nuova modalità d'azione dei gruppi terroristici, i quali, non solo agiscono adoperando la Rete come arma per porre in essere attacchi contro altri sistemi informatici per destabilizzare, alterare, danneggiare o distruggere strutture o impianti strategici, ma soprattutto mira alla guerra di informazione.

Ecco che l'essere riusciti a identificare la fenomenologia del *cyber terrorism*, attribuendogli proprie autonomia e identità rispetto all'insieme dei fatti illeciti realizzabili in Rete, significa che è oramai chiaro come il terrorismo internazionale, anche di matrice religiosa, riesca ad orientare le proprie attenzioni su attività di destabilizzazione e allarme sociale poste in essere anche attraverso l'impiego di strumenti informatici.

Per tale motivo, dunque, il potenziale militare e offensivo di una struttura terroristica si può misurare anche rispetto al coefficiente di abilità di navigazione nella Rete, di utilizzo indebito dei sistemi informatici e di capacità di trasmettere messaggi e informazioni propagandistiche, che, in sé, ormai rappresentano la vera forza di queste organizzazioni.

Altro elemento rilevante del terrorismo 2.0 è rappresentato dal concreto utilizzo da parte di queste organizzazioni di appositi siti internet, anche presenti nel c.d. *dark web* per comunicare con efficacia immediata a livello internazionale, ma anche per affiliare, finanziarsi, promuovere attività criminose insieme ad altre organizzazioni criminali, eludendo in tal modo gli ordinari strumenti di investigazione delle forze dell'ordine di tutto il mondo.

Peraltro, il processo di finanziarizzazione che connota tutte le organizzazioni criminali contemporanee, le quali operano secondo i canoni tipici dell'impresa, suggerisce come gli strumenti informatici risultino essere il canale attraverso il quale terrorismo e criminalità organizzata nazionale e internazionale hanno avviato processi di comunicazione e di collaborazione illecita[33].

Operazioni di riciclaggio, traffico di stupefacenti, tratta di esseri umani per le coste dei tre continenti che si affacciano sul Mediterraneo[34] sono preordinate, condotte e controllate attraverso la Rete e l'utilizzo di supporti informatici.

[33] A. LAUDATI, *Terrorismo internazionale, criminalità organizzata e money transfer*, in "Gnosis", n. 24, 2002.

[34] In materia, V. MILITELLO, A. SPENA, *Il traffico di migranti, diritti, tutele, criminalizzazione*, Torino, Giappichelli, 2015.

 ISSN 0390-0975 ISBN 978-88-495-3707-9

3. Il terrorismo internazionale di matrice religiosa nel cyberspazio

Come già largamente anticipato, l'utilizzo di Internet da parte delle organizzazioni terroristiche di matrice religiosa e, in particolare, di quelle che si fanno promotrici del jihad[35], ha determinato un mutamento complessivo dell'intero fenomeno del terrorismo di tipo islamico, sollevando nuove problematiche che hanno aumentato la complessità del fenomeno[36].

Le organizzazioni terroristiche fondamentaliste e internazionali, quali Daesh, Boko Haram o prima ancora Al Qaeda, mostrano di essere pienamente consapevoli della potenza che le moderne tecnologie dell'informazione e della comunicazione garantiscono in termini di efficacia nella realizzazione dei propri scopi.

Del resto, la stessa Al Qaeda si è imposta nel panorama globale quale network del terrore, in grado di potersi avvalere di piccoli nuclei operativi o anche di semplici "lupi solitari" presenti in tutto il mondo, capaci di agire sia su sollecitazione diretta che in maniera spontanea.

Il network di Al Qaeda si configura come una galassia di realtà autonome che operano in condizioni isolate rispetto alla "cellula madre", pur condividendone gli stessi obbiettivi e alcuni mezzi. Questo sistema fa sì che eliminando una "cellula" non si mina la sicurezza delle altre, dal momento che non esiste alcun legame gerarchico tra le stesse, apparendo quindi la struttura come una "rete" e non più come la classica piramide.

Nel tempo, poi, il web è stato ancor di più impiegato per esigenze di reclutamento, addestramento, raccolta fondi, pianificazione operativa delle attività terroristiche e condivisione delle informazioni. In poche parole, mediante Internet e, in particolar modo, attraverso alcuni social network le organizzazioni terroristiche internazionali di matrice religiosa sono state in grado di formare un proprio esercito operativo, i cui individui possono anche agire in modo del tutto spontaneo, in osservanza di precetti religiosi

[35] F. Fasani, *op. cit.*, p. 4.

[36] M. Donini, *Il terrorista-straniero come nemico e le contraddizioni di una giurisdizione penale di lotta*, in "Quaderni fiorentini per la storia del pensiero giuridico moderno", 2009, n. 38, pp. 1699-1724; A. Spataro, *Le forme attuali di manifestazione del terrorismo nell'esperienza giudiziaria: implicazioni etniche, religiose e tutela dei diritti umani*, in C. De Maglie, S. Seminara (a cura di), "Terrorismo internazionale e diritto penale", Padova, Cedam, 2007, p. 172 ss.; F. Viganò, *Terrorismo, guerra e sistema penale*, in "Rivista italiana di diritto e procedura penale", 2006, n. 2, p. 648 ss.

ISSN 0390-0975 ISBN 978-88-495-3707-9

o etici distorti che determinano l'azione delittuosa in modo inaspettato e imprevedibile.

L'interconnettività garantita da un costante utilizzo degli strumenti digitali consente oggi potenzialmente a chiunque di entrare in contatto con le organizzazioni terroristiche fondamentaliste e di acquisire una grande quantità di informazioni propagandistiche di matrice religiosa con scopi sovversivi e di intraprendere così un percorso di radicalizzazione potenzialmente idoneo a manifestarsi anche con attività delittuose.

In questo contesto, la Rete rimane sempre il principale strumento attraverso il quale le organizzazioni terroristiche che inneggiano al jihad riescono, con la spettacolarizzazione della violenza, ad ottenere il principale e più semplice risultato, ovvero la diffusione della paura e la sensazione di costante assenza di sicurezza.

Peraltro e in modo particolare Daesh, sfruttando le esperienze già maturate nel tempo da Al Qaeda, ha potuto avvalersi di una significativa competenza tecnologica che ha dato luogo alla nascita di un nuovo *warfare*[37] che combina gli attacchi terroristici realizzati in luoghi fisici secondo i classici schemi bellici o pseudo-bellici con quelli cibernetici, aventi un'efficacia trasversale e del tutto asimmetrica.

Mediante la combinazione di queste due metodologie di azione, Daesh, costituitasi nell'IS, è riuscita a creare un'illusione di potenza globale del tutto superiore a quella reale, ovvero a quella tangibile nelle aree del Medio Oriente sottoposte al suo controllo. Infine, questo gruppo terroristico, differentemente da quanto fatto anche da Al Qaeda, ha fatto sistematicamente ricorso a un impiego strategico dei social network senza precedenti, in particolar modo di Twitter e Facebook per fini di propaganda e di reclutamento dei foreign fighter.

Sui social vengono, infatti, prodotte e condivise informazioni di ogni tipo, aventi ad oggetto sia elementi di propaganda, utili per affiliazione e reclutamento, quali manuali con contenuto religioso e video di formazione per l'utilizzo di armi o di tecniche di combattimento corpo a corpo, che schemi di azione militare, mappe ferroviarie, reti idriche, orari di volo, non solo in lingua araba.

Tuttavia, fortunatamente, in questo ultimo periodo si è accentuata la scissione fra l'impiego di questa congiunta modalità di azione, dislocata fra realtà e mondo virtuale.

[37] R. Azzarone, *"Cyber vademecum". Cenni di diritto internazionale* (Parte VII), in "Gnosis", 2016, n. 2, pp. 144-151.

 ISSN 0390-0975 ISBN 978-88-495-3707-9

Infatti, se da un lato, la propaganda con scopi di reclutamento ha registrato particolari successi, soprattutto in Europa[38], dall'altro il sedicente stato islamico non ha intaccato in maniera profonda la *homeland security* di nessun Paese occidentale.

In pratica, questo fenomeno impone una profonda analisi circa il rapporto tra la libertà di ogni singolo utente e la capacità delle legislazioni dei Paesi occidentali, ispirati ad un modello liberal-democratico, di garantire la sicurezza individuale e collettiva senza distorcere e indebolire il web quale strumento di autentica libertà[39].

4. Il quadro giuridico europeo in materia di cybersecurity e cyberterrorismo e attività dei social media. Brevi cenni

Data questa premessa, fondamentale per comprendere il fenomeno del *cybercrime* terroristico, occorre adesso volgere lo sguardo all'ordinamento giuridico europeo e domestico, per capire, appunto, quale sia lo stato dell'arte in materia di contrasto al terrorismo internazionale, se esso appaia coerente con i principi fondamentali del sistema penale e costituzionale e in grado di riflettere un adeguato equilibrio fra esigenze repressive e tutela dei diritti individuali e collettivi.

Sul punto, è necessario peraltro sottolineare anticipatamente come ancora non vi sia una totale integrazione fra la normativa europea in materia di prevenzione del *cybercrime* e, dunque, di cybersecurity, e diritto penale in materia di contrasto al terrorismo internazionale, in quanto i due sistemi di regolazione si sviluppano su assi direttrici parzialmente paralleli e con finalità differenti.

In primo luogo, infatti, le misure di prevenzione europee agli attacchi cibernetici appaiono maggiormente attente alla tutela degli interessi economici e finanziari dell'Unione, più che alla salvaguardia dell'assetto democratico dei Paesi membri e dell'ordine pubblico. La normativa europea di settore, espressa già con la direttiva 2008/114/CE[40] e più recentemente con la direttiva

[38] Le stime dell'Europol riflettono una cifra significativa: dal 2014 al 2016, il numero dei reclutati via Internet è aumentato dai 18 del dicembre 2014 ai 6.506 del settembre 2016.

[39] Sul punto, S. Rodotà, *Una costituzione per internet*, in "Politica del diritto", 2010, n. 3, p. 339 ss.

[40] Si tratta della direttiva sull'identificazione e designazione delle infrastrutture critiche europee e sulla verifica della necessità di migliorare la loro protezione per l'attuazione del programma EPCIP (Programma Europeo di protezione delle infrastrutture critiche) avente ad oggetto non solo il terrorismo ma anche le attività criminali organizzate e le catastrofi naturali. Con essa si mira ad adottare procedure e strumenti specifici per ottenere un'analisi dei rischi, una valuta-

ISSN 0390-0975 ISBN 978-88-495-3707-9

2016/1148/UE[41] è focalizzata sulla prevenzione di attacchi informatici nei confronti di centri nevralgici o strategici per il funzionamento e la sopravvivenza delle stesse infrastrutture, mediante la predisposizione di funzionali ed efficaci apparati amministrativi pubblici e privati in grado di gestire minacce, crisi e un flusso di informazioni fra enti e Paesi membri utile per debellare l'effetto catastrofico delle stesse.

La disciplina europea in materia di contrasto al terrorismo internazionale, invece, innovata con la direttiva (UE) 2017/541[42], mira a eliminare alla fonte la circolazione di informazioni finalizzate al finanziamento, alla propaganda e al reclutamento da parte di organizzazioni terroristiche, *ex* art. 21, limitandosi però doverosamente a sollecitare gli Stati membri alla «rimozione alla fonte dei contenuti online che costituiscono una pubblica provocazione per commettere un reato di terrorismo».

In tal modo, gli Stati membri dovrebbero approntare un meccanismo efficace per contrastare il terrorismo sul web che si sostanzierebbe nella previsione di misure necessarie per assicurare la «tempestiva rimozione dei contenuti online» presenti sugli ISP e sui siti internet del proprio territorio, mediante i quali viene posta in essere una pubblica provocazione. Ove ciò non sia possibile, bisognerebbe intervenire «bloccando l'accesso a tali contenuti».

La rilevanza assegnata dalla direttiva alla tempestiva rimozione di questi contenuti emerge al punto che viene demandato agli Stati, quando i contenuti illeciti sono ospitati fuori dal proprio territorio, di cooperare con i Paesi terzi per la loro rimozione.

Infine, evidenziata l'interferenza che le suddette misure potrebbero avere con alcune libertà fondamentali, *in primis*, quella attinente alla manifestazione

zione dell'impatto, l'eventuale effetto domino, le misure finanziarie a sostegno degli Stati membri e l'individuazione delle infrastrutture critiche europee, nonché lo scambio di informazioni fra i Paesi membri; la direttiva è stata recepita in Italia con il d.lgs. 11 aprile 2011, n. 61.

[41] È la c.d. direttiva NIS, mediante la quale, desiderando proseguire i lavori di armonizzazione e di implementazione delle normative europee in materia di prevenzione al *cybercrime*, si è individuato un termine di 21 mesi, entro il quale i Paesi membri devono anche aumentare il livello di cooperazione internazionale in materia di protezione e salvaguardia dei sistemi informatici strategici anche in caso di attacco imminente o in corso.

[42] L'intervento tende a colmare le lacune presenti nella decisione quadro 2002/475/GAI in materia di lotta contro il terrorismo così come aggiornata dalla decisione quadro 2008/919/GAI, alla luce della risoluzione 2178(2014) del Consiglio di Sicurezza delle Nazioni Unite e del Protocollo addizionale alla convenzione del Consiglio d'Europa per la prevenzione del terrorismo, firmato a Riga il 22 maggio 2015, con l'introduzione di quattro nuovi obblighi di incriminazione: la ricezione di addestramento, i viaggi, l'organizzazione o agevolazione di viaggi a fini terroristici e, infine, il finanziamento del terrorismo.

 ISSN 0390-0975 ISBN 978-88-495-3707-9

del pensiero, consacrata in Costituzione e nei trattati internazionali, esse dovranno rispettare alcuni requisiti.

In primo luogo, dovranno essere garantite procedure trasparenti e proporzionate atte a fornire agli utenti un adeguato livello di «certezza e prevedibilità del diritto»; in secondo luogo, tutti gli utenti dovranno avere la possibilità di ricorrere in giudizio per conoscere i motivi della rimozione o del blocco subito.

Infine, precisa il ventitreesimo considerando della direttiva, queste misure non «dovrebbero»[43] porre a carico dei fornitori dei servizi di hosting alcun generale obbligo di sorveglianza sulle informazioni che trasmettono o memorizzano, né tantomeno costoro dovrebbero essere considerati responsabili, salve le ipotesi in cui «siano effettivamente a conoscenza dell'illiceità dell'attività o dell'informazione».

Ciò che sembra ancora aperto al confronto e al dibattito futuro è, dunque, il tema dell'individuazione del ruolo e di eventuali responsabilità penali, oltre che civili[44], a carico degli *hosting provider*, dal momento che, rispetto al cyberterrorismo dell'informazione, della propaganda e del reclutamento, sembrerebbero proprio questi gli unici soggetti in grado di intervenire concretamente ostacolando la perpetrazione di questi delitti con finalità di terrorismo.

Tuttavia, se da un lato è necessario coinvolgere in maniera progressiva gli ISP nella definizione di strategie di prevenzione e di controllo delle attività illecite in Rete, in quanto essi stanno sempre più assumendo un ruolo incisivo nell'evoluzione socio-tecnologica contemporanea, dall'altro, è opportuno

[43] Questo è il testo del considerando: «La rimozione di contenuti online che costituiscono una pubblica provocazione per commettere un reato di terrorismo o, ove non sia possibile, il blocco dell'accesso a tali contenuti a norma della presente direttiva, non dovrebbe pregiudicare le disposizioni della direttiva 2000/31/CE del Parlamento europeo e del Consiglio. In particolare, non dovrebbe essere imposto ai fornitori di servizi alcun obbligo generale di sorveglianza sulle informazioni che trasmettono o memorizzano né di ricercare attivamente fatti o circostanze che indichino la presenza di attività illecite. Inoltre, i fornitori di servizi di hosting non dovrebbero essere considerati responsabili a condizione che non siano effettivamente a conoscenza del fatto che l'attività o l'informazione è illecita e non siano al corrente di fatti o di circostanze che rendono manifesta l'illegalità dell'attività o dell'informazione».

[44] In materia, per quanto riguarda l'ordinamento italiano, si rimanda al d.lgs. 9 aprile 2003, n. 70, ove, in particolare l'art. 17 esclude l'obbligo per il provider di vigilare sul materiale che si limita a trasmettere e memorizzare, nonché l'onere di ricercare fatti o circostanze sintomatici di attività illecite; l'art. 16, poi, distingue fra responsabilità civile e penale: l'ISP non sarà responsabile ove non appaia effettivamente a conoscenza del fatto che l'informazione o l'attività memorizzate siano illecite; cfr. A. INGRASSIA, *op. cit.*, p. 1625; A. MACRILLÒ, *Caso Google - Vivi "down": negato in appello il concorso omissivo nel delitto ex art. 167 D.L.vo n. 196/03*, in "Rivista penale", 2013, n. 7-8, pp. 825-831.

ISSN 0390-0975 ISBN 978-88-495-3707-9

intervenire in maniera equilibrata e ponderata, onde evitare di criminalizzare un intero settore, l'Internet, connotato dalla massima libertà di espressione e di movimento virtuale, pregiudicando l'esercizio di diritti fondamentali garantiti sia dalla Costituzione (art. 21 Cost.) che dalla Carta di Nizza (art. 11) e dalla CEDU (artt. 8 e 9).

Utili potrebbero risultare anche le argomentazioni della Corte di giustizia Ue, la quale, in diverse sentenze[45], ha sottolineato due aspetti principali: il primo, relativo ad una generica irresponsabilità del provider, sempre che esso mantenga una posizione effettivamente neutrale rispetto ai comportamenti degli utenti; e il secondo, relativo all'assenza di obblighi di sorveglianza preventiva in capo agli ISP. Tuttavia, la Corte precisa che la neutralità dell'ISP non possa essere invocata quando il prestatore di servizio non si limiti al trattamento dei dati in modo automatico, ma svolga un ruolo attivo atto a consentirgli la conoscenza o un controllo di questi ultimi, attraverso attività di riorganizzazione o sistematizzazione dei dati. Riguardo al secondo aspetto, la Corte cerca sempre di affermare che obbligare il provider a predisporre un sistema di filtraggio preventivo dei contenuti caricati dagli utenti, oltre a costituire un sistema complesso, costoso e permanente, causerebbe una grave violazione della libertà di impresa del prestatore di servizi di hosting, oltre che una lesione dei diritti fondamentali degli utenti, quali il diritto alla tutela dei dati personali e la loro libertà di ricevere o di comunicare informazioni.

Rispetto al ruolo dei social network, oggi comunque è innegabile che essi non si limitino solamente a essere il luogo aperto e libero dello scambio di informazioni e di idee, in quanto essi stessi, mediante l'impiego di algoritmi che concentrano il flusso di alcune specifiche informazioni verso determinati profili, creano indirettamente il tipo di informazione al quale ogni individuo sarà facilitato ad accedere. Questo meccanismo, che segue evidentemente logiche commerciali, può, però, consentire ad alcune tipologie di utenti, già inclini al culto dell'odio o della violenza, di giungere facilmente e rapidamente a informazioni aventi un contenuto sensibile e foriero di condotte penalmente rilevanti aventi finalità di terrorismo.

Ecco che dunque servirebbe una maggiore attenzione sui profili di responsabilità degli ISP, anche e preferibilmente di matrice extra-penale, sia per

[45] *Ex multis*, CGUE, sez. III, 16 marzo 2016, causa C-484/14; CGUE, sez. III, 16 febbraio 2012, causa C-360/10, *Sabam c. Netlog*, con ampio commento di R. PETRUSO, *Responsabilità degli intermediari e di internet e nuovi obblighi di conformazione: robo-takedown, policy of termination, notice and take steps*, in "Europa e diritto privato", 2017, n. 2, p. 451 ss.

 ISSN 0390-0975 ISBN 978-88-495-3707-9

evitare che lo *jus terribile* debba intervenire reprimendo anche generici «atti intenzionali»[46] posti in essere in Internet solo attraverso opinabili manifestazioni del pensiero, sia per evitare che, a causa della lacuna, il legislatore, come fatto negli USA con lo *Sharing Act*, intervenga per disporre e controllare indirettamente le informazioni in circolazione sui social.

5. Gli strumenti di tutela penale nel contrasto al terrorismo internazionale informatico: la "perenne emergenza" fra eccessi di tutela e conflittualità con i diritti fondamentali

Passando adesso all'esame dell'assetto delle più recenti riforme penali in materia di terrorismo internazionale, possiamo evidenziare come le evoluzioni normative in materia di contrasto al terrorismo internazionale, da ultimo completate con la direttiva (UE) 2017/541[47], non appaiano, come anticipato, del tutto rispettose dei principi fondanti il diritto penale liberale, in quanto esse sono caratterizzate da una progressiva anticipazione della tutela anche rispetto ai meri atti preparatori che, in alcuni casi, sembrano persino riconoscere un disvalore penale a forme di *tentativo di attentato*.

Particolari dubbi sollevano le recenti fattispecie di auto-addestramento, di cui all'art. 270-*quinquies* c.p., come riformato nel 2015, e le condotte di apologia, le quali, in sé, sono difficilmente inquadrabili al di fuori dell'ottica del diritto penale d'autore.

Queste recenti opzioni legislative sono fortemente condizionate da scelte politico-criminali internazionali e, in particolare, europee e sembrano discostarsi fortemente dall'osservanza di alcuni principi cardine, quali quelli di offensività e di determinatezza[48].

Si tratta, infatti, di forme di tipizzazione frutto di un'eccessiva espansione dell'ambito di applicazione del diritto penale ottenuta, come detto, anche con

[46] Si fa riferimento all'art. 3 della direttiva (UE) 2017/541 che richiede l'incriminazione di atti intenzionali.

[47] Sul punto, S. Santini, *L'Unione Europea compie un nuovo passo nel cammino della lotta al terrorismo: una prima lettura della direttiva 2017/541*, in "Diritto penale contemporaneo", 2017, n. 7-8, p. 13 ss.

[48] Ne discutono approfonditamente A. Cavaliere, *Il contrasto del terrorismo tra esigenze di tutela e garanzie individuali*, in "Diritto penale e processo", 2017, n. 8, pp. 1089-1100; L. Picotti, *Terrorismo e sistema penale: realtà, prospettive, limiti*, in "Diritto penale contemporaneo", 2017, n. 1, p. 249 ss.

ISSN 0390-0975 ISBN 978-88-495-3707-9

l'anticipazione della soglia di intervento penale attraverso la configurazione di reati di pericolo concreti e astratti.

Siamo praticamente innanzi ad un nuovo processo di pan-penalizzazione del contrasto al terrorismo che rischia, come già accaduto in passato in materia di reati tributari con la l. 7 agosto 1982, n. 516, definita con l'epiteto "Manette agli evasori"[49], di rimanere del tutto inefficace e di sterilizzare ogni aspettativa general-preventiva connessa all'uso della pena.

In fondo, l'affastellarsi di interventi legislativi in tale settore ha condotto alla costruzione di un vero e proprio sotto-sistema penale in materia di lotta al terrorismo che, potrebbe, però, in realtà, rivelare un'inadeguatezza generale nel produrre un programma politico-criminale multilivello ma realmente integrato, soddisfacente e coerente con il rispetto dei principi individuali e collettivi.

I reati contro il terrorismo sembrano, dunque, richiamare la tecnica legislativa tipica della "perenne emergenza"[50], che dà luogo a una legislazione che, diventando strumento di "lotta", punta a fornire un senso di certezza, di sicurezza o di appagamento all'interno della collettività, facendo uso, però, di strumenti punitivi e preventivi extra-ordinari e di dubbia compatibilità costituzionale[51].

Un tipico esempio che ha posto problemi di lettura di queste fattispecie si registra, ancora oggi, rispetto all'incerto rapporto tra l'art. 270 c.p. (*Associazioni sovversive*) e la fattispecie gemella di cui all'art. 270-*bis* c.p. (*Associazioni con finalità di terrorismo anche internazionale o di eversione dell'ordine democratico*). La praticamente quasi totale omogeneità fra i due fatti tipici solleva ancora dubbi circa il loro effettivo coordinamento, inducendo a ritenere, appunto, che quest'ultima sia stata introdotta con lo *scopo simbolico*[52] di attuare un inasprimento sanzionatorio. Complessivamente, il sotto-sistema in materia di contrasto al terrorismo di cui agli artt. 270-*bis* c.p., come modificato nel

[49] E. MUSCO, *La riforma del diritto penale tributario*, in "Rivista della Guardia di Finanza", 1999, p. 2463; E. LO MONTE, *L'illecito penale tributario tra tecniche di tutela ed esigenza di riforme*, Padova, Cedam, 1996, p. 215 ss.; T. PADOVANI, *Problemi generali e analisi delle fattispecie previste dai nn. 1, 2, 3, 4, 5, 6 dell'art. 4, legge n. 516/1982*, in C.F. Grosso (a cura di), "Responsabilità e processo penale nei reati tributari", Milano, Giuffrè, 1982, p. 199 ss.

[50] S. MOCCIA, *La perenne emergenza. Tendenze autoritarie nel sistema penale*, Napoli, ESI, 2000.

[51] Vedi sul punto, A. PAGLIARO, *Sulla tutela penale dell'ordine pubblico nella legislazione dell'emergenza*, in "Studi in onore di G. Delitala", Milano, Giuffrè, 1984, p. 1031 ss.

[52] S. RODOTÀ, *Alla ricerca della libertà*, Bologna, Il Mulino, 1978, p. 116.

 ISSN 0390-0975 ISBN 978-88-495-3707-9

2015[53] su impulso della direttiva 2015/849/UE e come verrà nuovamente in parte modificato per via della direttiva del 2017, volendo perseguire lo scopo di rendere inoperativi i "lupi solitari" e le singole cellule, anche per mancanza di finanziamenti economici, si presenta come un modello legislativo in cui le fattispecie incentrano il disvalore penale del fatto tipico più sulla persona e sulle sue caratteristiche soggettive che sulla condotta vera e propria.

Inoltre, la volontà legislativa finalizzata alla repressione delle associazioni terroristiche anche nella loro fase genetica si è tradotta in una inevitabile ma eccessiva anticipazione della tutela penale, con la conseguenza che le fattispecie qui richiamate sembrano volere colpire, in primo luogo, il *tipo* di autore e solo successivamente il fatto concreto, proprio perché contraddistinte da una logica emergenziale e di «allarme sociale»[54] che, mediante esse, si cerca di combattere.

Un esempio attuale può essere ricavato dall'introduzione da parte della direttiva del 2017 di quattro nuovi obblighi di incriminazione a carico degli Stati membri, non previsti né dalla decisione quadro 2002/475/GAI, né dalla decisione 2008/919/GAI, che riguardano condotte solo teleologicamente finalizzate alla realizzazione di atti terroristici, tuttavia ancora risultanti ad uno stato preparatorio o di mera organizzazione: ricezione di addestramento a fini terroristici, i viaggi a fini terroristici, l'organizzazione o l'agevolazione di viaggi a fini terroristici, e il finanziamento del terrorismo.

Queste disposizioni, attuative degli artt. 3, 4, 5 e 6, del Protocollo addizionale del Consiglio d'Europa per la prevenzione del terrorismo, secondo l'art. 13 della direttiva, operando come disposizione *orizzontale*[55], conferiscono la possibilità di sanzionare penalmente queste quattro condotte anche in assenza dell'effettiva commissione di un reato di terrorismo o di stabilire un collegamento con uno specifico reato previsto dalla direttiva.

Il vero timore, dunque, è che, nell'ansia di apprestare almeno formalmente adeguate soluzioni al dramma del terrorismo internazionale jihadista, il legislatore prosegua una rincorsa al fenomeno aumentando la produzione legislativa e incriminatrice, smarrendo, però, il vero scopo del diritto penale che, dovendo essere sempre l'*extrema ratio*, non può assumersi il compito attribuito ad altri rami dell'ordinamento e ad altre istituzioni[56].

[53] A. CAVALIERE, *Considerazioni critiche intorno al d.l. antiterrorismo, n. 7 del 18 febbraio 2015*, in "Diritto penale contemporaneo", 2015, n. 2, p. 230 ss.

[54] A. PAGLIARO, *op. cit*, p. 1032.

[55] S. SANTINI, *op. cit.*, p. 15 ss.

[56] F. VON LISTZ, *La teoria dello scopo nel diritto penale*, trad. it., Milano, Giuffrè, 1962.

ISSN 0390-0975 ISBN 978-88-495-3707-9

Del resto, non è possibile pensare di arginare il proselitismo digitale, la propaganda e, in generale, la diffusione di informazioni favorevoli alla causa del terrorismo jihadista con l'esclusivo impiego della sanzione penale.

Non si può combattere un fenomeno nuovo che si sviluppa e cresce nello spazio cibernetico con gli stessi strumenti normativi adottati in passato contro il terrorismo interno e le criminalità organizzate. Il rischio e l'effetto conseguente non possono che essere la contrazione dei diritti costituzionalmente garantiti, l'inasprimento della sanzione e la rinuncia alle libertà a favore di una inafferrabile sicurezza.

5.1. (Segue) Il bene giuridico tutelato dalle fattispecie di contrasto al terrorismo internazionale e tecniche legislative di tutela

Ecco che occorrerebbe anche ripensare a quali possano o debbano essere i beni giuridici tutelati dalle fattispecie incriminatrici di terrorismo e di cyberterrorismo nelle sue varie espressioni.

Secondo alcuni[57], insieme alla consueta salvaguardia di beni giuridici collettivi, come la sicurezza e l'ordine pubblico, andrebbero concretamente garantite la vita e l'incolumità degli individui, in considerazione del fatto che i più recenti attacchi terroristici scatenati dai "lupi solitari", più che compromettere la sicurezza e l'ordine, hanno *semplicemente* comportato la distruzione del bene vita di centinaia di persone.

Tuttavia, ricalibrare la condotta sulla lesività del bene vita più che su quello dell'ordine pubblico, avrebbe come effetto quello di non consentire un'eccessiva anticipazione della tutela a vantaggio, invece, della configurazione di questi delitti come reati di danno[58].

Neanche una rivalutazione del concetto stesso di ordine pubblico potrebbe condurre a soluzioni efficaci, poiché il rischio sarebbe sempre quello di ampliare oltremodo il contenuto del concetto, tornando a reprimere la c.d. "tranquillità sociale" come accadeva in periodi storici decisamente connotati da un clima poco democratico[59].

[57] A. CAVALIERE, *Il contrasto del terrorismo tra esigenze di tutela e garanzie individuali*, cit., p. 1090.

[58] Si rimanda per questi aspetti a G. FIANDACA, E. MUSCO, *Diritto penale - parte generale*, Torino, Zanichelli, 2014, p. 173.

[59] R. CANOSA, *La legislazione eccezionale sull'ordine pubblico in Italia, tra storia e cronaca (1861-1973)*, in Aa.Vv., "Ordine pubblico e criminalità", Milano, Mazzotta, 1975, p. 15 ss.; G. NEPPI MODONA, *Sciopero, potere politico e magistratura, 1870-1922*, Bari, Laterza, 1969.

 ISSN 0390-0975 ISBN 978-88-495-3707-9

Una soluzione reale potrebbe essere quella di ripensare la tecnica di costruzione legislativa delle fattispecie secondo schemi differenti: ovvero realizzare un efficace contrasto alla fortificazione dei gruppi terroristici solamente implementando le misure patrimoniali finalizzate a impedire il finanziamento e l'arricchimento degli associati, dei gruppi e dei singoli individui legati ideologicamente al terrorismo internazionale, secondo quanto già fatto nel nostro ordinamento contro le criminalità organizzate di tipo mafioso[60], nonché ottimizzare gli strumenti di indagine informatica utilizzabili dalle forze dell'ordine e di intelligence in fase investigativa[61].

Sebbene, anche questa opzione possa far emergere ulteriori dubbi in tema di compatibilità con i principi costituzionali a tutela del diritto di difesa, di proprietà privata, nonché di riservatezza e libertà di manifestazione del pensiero, oltreché di uguaglianza, bisogna sempre ricordare che, innanzi a fenomeni di così grande impatto sociale, qualunque soluzione rischia di sacrificare ora le esigenze repressive, ora i diritti fondamentali.

Bisognerebbe, in realtà, considerare che le attività di propaganda, apologia e reclutamento da parte dei gruppi terroristici poste in essere in Internet, più che porre in pericolo beni quale l'ordine o la sicurezza pubblica, mettono in pericolo, in prima battuta, la sicurezza di Internet e il suo libero accesso. Tuttavia, tale scommessa va affrontata cercando di ottenere il massimo risultato con la minima torsione dei diritti fondamentali e nella consapevolezza del cambiamento che Internet ha determinato sia nella configurazione delle condotte che delle modalità di estrinsecazione della libertà di pensiero e di espressione.

La Costituzione italiana, ormai inserita nel contesto europeo di tutele dei diritti dell'Uomo e del Cittadino, sicuramente domanda al legislatore nazionale di rispettare in modo indefettibile alcuni specifici principi, quali

[60] Si pensi alla disciplina della confisca quale sanzione e misura di sicurezza *ex* art. 12-*sexies*, d.l. 8 giugno 1992, n. 306, sul punto A.M. MAUGERI, *Le sanzioni patrimoniali come moderno strumento di lotta contro il crimine: reciproco riconoscimento e prospettive di armonizzazione*, Milano, Giuffrè, 2008; D. FONDAROLI, *Le ipotesi speciali di confisca nel sistema penale. Ablazione patrimoniale, criminalità economica, responsabilità delle persone fisiche e giuridiche*, Bologna, Bononia University Press, 2007.

[61] M. DANIELE, *Contrasto al terrorismo e captatori informatici*, in "Rivista di diritto processuale", 2017, n. 2, p. 393 ss., ove l'A. analizza alcuni nuovi strumenti investigativi, finalizzati a intercettare le comunicazioni dei terroristi in qualsiasi luogo il dispositivo in loro detenzione si trovi, dunque, indipendentemente dai limiti spaziali che, come noto, nel tempo, hanno sollevato vari dibattiti circa la legittimità dello strumento dell'intercettazione; vedi anche A. GAITO, S. FURFARO, *Le nuove intercettazioni «ambulanti»: tra diritto dei cittadini alla riservatezza ed esigenze di sicurezza per la collettività*, in "Archivio penale", 2016, n. 2, p. 16 ss.

ISSN 0390-0975 ISBN 978-88-495-3707-9

quello di responsabilità penale personale, *ex* art. 27, co. 1 Cost., di divieto di trattamenti disumani o comunque contrari ad un percorso di rieducazione del reo e di offensività del reato[62].

Questi suindicati principi devono rappresentare l'ago della bilancia nella ricerca di un equilibrio coerente per un sistema penale moderno e democratico e non possono essere oggetto di rinuncia neanche a fronte dell'esasperato perseguimento di esigenze general-preventive connesse alla tutela dell'ordine e della sicurezza pubblica.

Tuttavia, come già anticipato, anche se si cerca di rifiutare le logiche del *diritto penale del nemico* che pongono una netta scissione fra il cittadino e l'*estraneo*, ormai il nostro ordinamento si è dotato di alcune particolari fattispecie costruite sulla punibilità del mero accordo o di atti preparatori o di forme estreme di radicalizzazione; in questo contesto, vengono particolarmente in rilievo il c.d. auto-addestramento di cui all'art. 270-*quinquies* c.p. o alcuni delitti contro l'ordine pubblico, quali l'istigazione o l'apologia del delitto.

5.2. L'eccessiva anticipazione della tutela: l'esempio dell'apologia e dell'istigazione ai delitti di terrorismo con mezzo informatico

Volendo proprio partire dall'analisi di quest'ultima ipotesi, si può segnalare come recentemente la Corte di cassazione sia intervenuta in materia, rispetto ad alcuni casi di apologia dell'IS attraverso Internet[63].

Come noto, intanto, le caratteristiche della fattispecie richiedono che la condotta di istigazione consista nell'impegno a fare sorgere o a rafforzare l'altrui proposito criminoso, mentre l'apologia consiste nell'esaltazione di un fatto delittuoso finalizzato a spronare altri all'emulazione o all'imitazione.

Queste condotte devono poi essere accompagnate dalla *pubblicità* che determina sia la nota modale della condotta sia gli stessi destinatari del messaggio. I comportamenti in questione devono avere, altresì, ad oggetto, rispettivamente, la commissione di uno o più reati e uno o più delitti, fra i quali rientrano anche quelli associativi. In tal senso, peraltro, si è espressa la Corte di cassazione con la sentenza 15 maggio 2017, n. 24103[64]. In entrambi i casi è

[62] A. CAVALIERE, *Il contrasto del terrorismo tra esigenze di tutela e garanzie individuali*, cit., p. 1091.

[63] Cass., sez. I pen., 6 ottobre 2015, n. 47489, con nota di C. ROSSI, *L'elemento oggettivo del reato di cui all'art. 414, comma 4, c.p.*, in "Cassazione penale", 2016, n. 6, p. 2470 ss.

[64] Cass., sez. I pen., 15 maggio 2017, n. 24103, ove si afferma che «il reato è configurabile nel caso della diffusione di un messaggio o documento apologetico attraverso il suo inserimento su

 ISSN 0390-0975 ISBN 978-88-495-3707-9

poi necessaria la concretezza del pericolo, consistente nell'effettiva idoneità della condotta istigatrice o apologetica a provocare la commissione di delitti e, quindi, conseguentemente, a turbare l'ordine pubblico[65].

L'idoneità concreta del pericolo viene a dipendere sia dal contenuto intrinseco del messaggio veicolato dal contesto e dall'ambito spaziale in cui esso è proclamato sia dalle condizioni personali dell'autore che, ovviamente, distorce la ricostruzione in chiave oggettiva del fatto. Entrambi i delitti, poi, si configurano con il dolo generico.

Va ricordato inoltre che alla fattispecie base sono state affiancate due circostanze aggravanti ad effetto speciale legate proprio alla finalità terroristica.

La prima è stata introdotta con la l. 31 luglio 2005, n. 155 e prevede un innalzamento della pena della metà quando l'istigazione o l'apologia riguardi «delitti di terrorismo o crimini contro l'umanità». In pratica, questa circostanza aggravante potrà essere applicata, ad esempio, per l'ipotesi in cui un imam sproni alcuni adepti o fedeli a recarsi sui luoghi in conflitto in Medio Oriente per intraprendere il jihad o quando inneggi e accolga favorevolmente gli atti di terrorismo realizzati in un qualche punto nel pianeta.

La seconda aggravante, invece, prevista con l'art. 2, co. 1, l. 17 aprile 2015, n. 43, prevede l'aumento di pena fino a due terzi se il fatto di apologia o di istigazione sia commesso mediante l'uso di «strumenti informatici o telematici». La circostanza trova operatività tutte le volte in cui l'autore utilizzi strumenti informatici di diverso tipo, compresi pertanto i social network e che consentano la comunicazione fra più soggetti attraverso l'elaborazione di dati e lo scambio di informazioni.

In questo modo, il legislatore ha inteso colpire specificamente i fatti caratterizzati da una potenzialità diffusiva ampia e praticamente incontrollabile, ovvero quei soggetti che dimostrano una pericolosità intrinseca maggiore di coloro che "si limitano" a fare uso dei classici strumenti di informazione che non raggiungono idealmente lo stesso numero di persone[66].

un sito internet privo di vincoli di accesso, in quanto tale modalità ha una potenzialità diffusiva indefinita» (fattispecie in cui il reato è stato escluso relativamente a comunicazioni telematiche meramente private, mentre lo si è ritenuto quale possibile integrazione relativamente a videoregistrazioni di contenuto apologetico dell'ISIS e del terrorismo di matrice islamica diffuse tramite Facebook).

[65] Rispetto al presupposto dell'idoneità, si veda S. ZIRULIA, *"La TAV va sabotata": Erri De Luca assolto dall'accusa di istigazione a delinquere*, in "penalecontemporaneo.it", 8 febbraio 2016.

[66] Ne parla diffusamente A. CAVALIERE, *Considerazioni critiche intorno al d.l. antiterrorismo, n. 7 del 18 febbraio 2015*, cit., p. 234.

ISSN 0390-0975 ISBN 978-88-495-3707-9

L'utilizzo dello strumento di Internet e dei social network per diffondere con fini di propaganda il messaggio del jihad del Califfato è stato, come anticipato, recentemente sottoposto al vaglio della Corte di cassazione, la quale non ha esitato a confermare una misura cautelare per istigazione e apologia connessi ai delitti di terrorismo sulla Rete.

In questo caso di specie, i giudici della Suprema Corte hanno confermato come la condotta posta in essere fosse pienamente ascrivibile all'ipotesi delittuosa di cui all'art. 414, co. 3 c.p., poiché pienamente idonea a mettere in pericolo il bene giuridico dell'ordine pubblico.

Infatti, il messaggio diffuso in Rete e sui social non aveva soltanto un contenuto squisitamente ideologico, di narrazione del fenomeno terroristico, ma risultava essere intrinsecamente finalizzato a esaltare la diffusione e l'espansione dell'IS, con l'uso delle armi, in un contesto di contrapposizione tra mondo islamico e mondo infedele da epurare.

Ancora più di recente, la Corte di cassazione[67] ha nuovamente confermato la configurabilità del delitto di istigazione e di apologia di terrorismo con mezzi informatici e, in particolare, mediante Facebook, rispetto al fatto posto in essere da una giovane donna, la quale all'interno del social aveva dimostrato di condividere la «causa del terrore». Secondo la Corte «era ragionevole il convincimento che la stessa fosse pronta a superare gli attuali confini di condotte contenute nel reato di opinione per misurarsi e sperimentare pratiche concrete di aiuto verso soggetti in transito in Italia». I giudici, in particolare, sostenevano l'esistenza dei motivi alla base dell'irrogazione della misura cautelare in forza del fatto che l'indagata «avesse manifestato la volontà di assumere un ruolo positivo di sostegno alla causa del terrorismo religioso» non riconoscendo, peraltro, autorità ad altra struttura ordinamentale.

Infine, sempre la Corte di cassazione[68] è giunta ad affermare il perfezionamento del delitto di apologia del terrorismo per la mera condivisione di un video di propaganda dell'ISIS su Facebook in quanto la propaganda risulta rafforzata utilizzando l'opzione "mi piace" prevista dal social.

In pratica, la Corte riconosce esplicitamente la notevole influenza che il social network riesce a svolgere nel condizionamento delle coscienze in materia di terrorismo islamico attestando che il riferimento continuo al conflitto sia in grado di svolgere una funzione apologetica nei confronti degli utenti di Facebook.

[67] Cass., sez. I pen., 20 luglio 2016, n. 31249.

[68] Cass., sez. V pen., 25 settembre 2017, n. 55148.

 ISSN 0390-0975 ISBN 978-88-495-3707-9

Questi casi giurisprudenziali riflettono essenzialmente il conflitto in corso fra le esigenze di tutela dell'ordine pubblico e della sicurezza collettiva e il riconoscimento di un'ampia libertà di manifestazione del pensiero.

Infatti, in queste ipotesi, la Corte di cassazione ha riconosciuto una particolare pericolosità dei comportamenti posti in essere proprio in ragione del fatto che il contesto in cui si è sviluppata la pubblicizzazione del messaggio sia stata la Rete e, in modo specifico, Facebook.

L'Internet, anche per la giurisprudenza italiana, rappresenta dunque un mezzo molto efficace per gli scopi propagandistici dei gruppi terroristi di matrice religiosa in quanto *ex se* idoneo a determinare concreti rischi di radicalizzazione diffusa di quei soggetti che, per la loro condizione personale, nonché per condizione culturale, economica e religiosa, potrebbero lasciarsi facilmente influenzare dal messaggio che invita a prendere parte al jihad[69].

Tuttavia, le decisioni dimostrano come la tutela apprestata dal giudice penale sia particolarmente anticipata, in quanto non solo viene data applicazione di un reato di pericolo in assenza di un comportamento materiale, ma di un reato di pericolo già, di per sé, foriero di dubbi di compatibilità con il principio di offensività e tassatività per l'intrinseca estrema anticipazione della tutela.

Sembra così avere avuto diffusione l'argomentazione politico-criminale volta a legittimare una così ampia anticipazione della tutela.

Essa fa leva sulla funzione special-preventiva del diritto penale, la quale dovrebbe incitare a un intervento della sanzione prima della realizzazione di un danno. Tuttavia, però, il dato in base al quale la pena debba tendere alla prevenzione generale e speciale non significa affatto che questa debba intervenire prima che sia posta in essere una condotta in grado di porre in pericolo concretamente il bene o i beni giuridici tutelati[70].

Soprattutto il caso della mera adesione al progetto islamico attraverso un "mi piace", seppur manifestazione di un comportamento inquietante, non può attestarsi quale pietra miliare nella giurisprudenza penale italiana, poiché ciò significherebbe attribuire una responsabilità penale a chiunque possa inconsciamente o istintivamente aderire a un pensiero o compiacersi di un comportamento; in pratica, non solo il principio di offensività ap-

[69] Ne parla F. FASANI, *op. cit.*, p. 61 ss.

[70] S. MOCCIA, *Il diritto penale tra essere e valore. Funzione della pena e sistematica teleologica*, Napoli, ESI, 1992, p. 80 ss.; F. PULITANÒ, *La formulazione delle fattispecie di reato: oggetti e tecniche*, in Aa.Vv., "Beni e tecniche della tutela penale. Materiali per la riforma del codice", Milano, Franco Angeli, 1987, p. 35 ss.

ISSN 0390-0975 ISBN 978-88-495-3707-9

parirebbe leso, ma anche la stessa *materialità* che governa il diritto penale liberal-democratico.

5.3. Gli accordi e gli atti preparatori fuori e dentro l'Internet

Il dibattito intorno alla punibilità dei fatti collegati al terrorismo si vivacizza in particolare poi con riferimento alla punibilità degli atti preparatori, oltre che della sola condivisione di un'ideologia violenta. Rispetto a questi comportamenti che, come noto, non consistono ancora in un'azione diretta, in modo non equivoco, a cagionare un fatto di reato (sulla falsariga del tentativo, *ex* art. 56 c.p.), il principio di offensività dovrebbe essere il necessario riferimento teleologico e interpretativo nell'opera di configurazione dei fatti di reato e di loro successiva applicazione da parte della magistratura[71].

In questo senso, dunque, non dovrebbe essere sufficiente la sola "materializzazione" della condotta, ma risulterebbe come necessaria la capacità della stessa di porre in pericolo un bene giuridico. La mera dichiarazione criminosa, pertanto, non sarebbe – in ogni caso – nulla in più di una semplice manifestazione di pensiero, priva di connotati tipicamente offensivi. Anche l'accordo criminoso, in sé, è solo una manifestazione esteriore di un pensiero criminoso che, seppur per certi aspetti possa apparire soddisfare il requisito di materialità, risulterebbe ancora lontano alla soglia del tentativo offensivo.

La criminalizzazione di meri atti preparatori (o degli "atti intenzionali" *ex* art. 3, direttiva 2017) o solo astrattamente pericolosi, come nei casi qui analizzati, porta con sé l'effetto di una eccessiva soggettivizzazione della fattispecie.

In questo modo, il disvalore del fatto potrebbe imperniarsi sull'atteggiamento interiore o sullo stile di vita del soggetto agente, aumentando conseguentemente la discrezionalità del giudice, il quale potrebbe orientarsi così su pre-comprensioni fondate sul diritto d'autore[72].

Come risultato finale dell'introduzione di fattispecie non orientate al principio di offensività e costruite come reati di pericolo astratto, simili ad un tentativo di attentato, come nel caso del 270-*quinquies* c.p., si ha la penalizzazione in concreto di comportamenti, forse, fin troppo indeterminati, per i quali è anche complesso ricostruire il nesso di causalità.

[71] S. MOCCIA, *L'odierna funzione di "controllo" e "orientamento" della dottrina*, in "Criminalia", 2013, p. 409 ss.

[72] Così A. CAVALIERE, *Il contrasto del terrorismo tra esigenze di tutela e garanzie individuali*, cit., p. 1095.

 ISSN 0390-0975 ISBN 978-88-495-3707-9

Ecco che appare percepibile come i diritti dell'individuo vengano, almeno in parte, sacrificati sull'altare dell'ordine pubblico, secondo un'accezione idealizzata, ma è anche vero che molto difficilmente finanche la Corte EDU si spingerebbe a riconoscere la violazione dei principi alla base del giusto processo, art. 6, o di legalità, art. 7 CEDU in ipotesi di tale genere, strettamente connessi al terrorismo jihadista.

In conclusione, ciò che continua in ogni caso a emergere è che il confronto tra terrorismo e tutela dell'ordine pubblico si è trasferito proprio sul "campo di battaglia" del cyberspazio, in cui i social network possono anche assumere la veste di alfieri di un'idea o di un'ideologia[73]; e se è vero che un punto di forza del terrorismo jihadista del Daesh è rappresentato proprio dalla capacità di valorizzare la libertà di espressione delle società occidentali che combattono per trasmettere messaggi di propaganda, è altresì vero che è proprio mediante la promozione di una cultura della corretta informazione che probabilmente sarà possibile arginare la diffusione di messaggi falsi o, come in questo caso, apologetici e istigatori al terrorismo islamico.

5.4. Il delitto di istruzione e di auto-addestramento. Internet e i social media al centro delle spinte repressive del diritto penale

Altro caso paradigmatico dell'interconnessione evidente fra terrorismo internazionale di matrice religiosa e utilizzo di Internet e dei social media, si ha con riferimento al già più volte citato delitto di istruzione o di "auto-addestramento" di cui all'art. 270-*quinquies* c.p.[74]

Questa fattispecie si rivolge, in particolar modo, alla repressione dei comportamenti delittuosi potenzialmente realizzabili dai c.d. "lupi solitari"[75], dagli "zombie" e dai foreign fighter.

[73] A. TETI, *Isis e social network. Da Twitter a Facebook passando per Whatsapp e Youtube*, in "Gnosis", 2015, n. 4, p. 75 ss.

[74] R. BARTOLI, *L'autoistruzione è più pericolosa dell'addestramento e dell'istruzione: verso un sovvertimento dei principi?*, in "Diritto penale e processo", 2017, n. 5, p. 626; F. FASANI, *op. cit.*, p. 358 ss.; R. WENIN, *Disposizioni sull'addestramento nell'uso di armi: un sintomo della degenerazione delle coerenza sistemica*, in "Rivista italiana di diritto e procedura penale", 2015, n. 4, p. 1893.

[75] F. VIGANÒ, *Minaccia dei lupi solitari e risposta dell'ordinamento: alla ricerca di un delicato equilibrio tra diritto penale, misure di prevenzione e tutela dei diritti fondamentali della persona*, in R.E. Kostoris, F. Viganò (a cura di), "Il nuovo pacchetto antiterrorismo", Torino, Giappichelli, 2016, p. 71 ss.

ISSN 0390-0975 ISBN 978-88-495-3707-9

Le difficoltà che stanno ormai incontrando i livelli posti all'apice del network terroristico internazionale, almeno rispetto all'avanzata degli eserciti kurdo e siriano nei territori conquistati dall'IS, e la sempre maggiore attenzione investigativa riservata al radicalismo islamico da parte delle forze dell'ordine e di intelligence dei Paesi europei e occidentali, hanno comportato una trasformazione della fisionomia stessa della cellula e del gruppo terroristico collegato al nucleo centrale operativo.

È possibile infatti sottolineare, su una certa base empirica, anche rispetto alle recenti recrudescenze del fenomeno stesso, come si stia delineando una maggiore autonomia dei singoli gruppi radicalizzati presenti in occidente, a volte persino sconnessi da qualunque logica di terrore globale.

A fronte dell'indebolimento di Daesh nel controllo del territorio in Medio Oriente, si assiste, invece, a una diffusione dell'educazione radicalizzata, su Internet e sui social, religiosa e militare. I mezzi di comunicazione digitale stanno sempre più acquisendo un'importanza strategica per il terrorismo internazionale nello svolgimento di alcune fondamentali attività precedentemente realizzate in modo massiccio all'interno dei campi di addestramento collocati in Africa e in Medio Oriente.

Dunque, dal momento che indottrinamento, addestramento e reclutamento sono ostacolati in modo più efficace dai militari e dall'intelligence – almeno nella vita reale – Internet ha finito per acquisire una spiccata centralità.

L'implementazione dell'utilizzo di Internet e dei social da parte del terrorismo islamico ha condotto, da un lato, all'ottimizzazione delle performance rispetto al raggiungimento di un numero sempre più cospicuo di individui in tutto il globo, ma, dall'altro, a un indebolimento delle ideologie originali del Daesh a causa delle forti trasformazioni che le informazioni presenti nel cyberspazio hanno subito nel tempo.

Infatti la costante rielaborazione e condivisione delle informazioni ha sostanzialmente modificato il contenuto di alcuni elementi caratterizzanti l'ideologia terroristica legata all'ISIS, così come, del resto, in questi ultimi anni, ha comportato la vistosa manipolazione del significato proprio di alcuni versi del Corano.

La diffusione indiscriminata di messaggi islamisti ha così condotto ad una sorta di "terrorismo fai da te"[76] per cui singoli individui presenti all'interno

[76] L. VIDINO, *Il jihadismo autoctono in Italia: nascita, sviluppo e dinamiche di radicalizzazione*, Milano, ISPI, 2014.

 ISSN 0390-0975 ISBN 978-88-495-3707-9

dei territori dei Paesi occidentali, dopo avere acquisito autonomamente informazioni di matrice jihadista, si attivano per la realizzazione di atti di tipo terroristico.

Questo comportamento contraddistingue la figura del c.d. "lupo solitario", il quale, appunto, agisce in modo indipendente, in maniera del tutto scollegata dalle direttive e dalle iniziative provenienti dalla "cellula" principale sita nei territori occupati in Medio Oriente.

In certi altri casi, l'auto-addestramento mediante Internet e i social network può essere funzionale a determinare la scelta di alcuni individui di recarsi all'estero per combattere a favore della causa jihadista; si tratta, fondamentalmente, della figura del foreign fighter, il quale dopo avere assimilato questa ideologia, viene condotto in alcuni specifici territori in Medio Oriente o nel Nord Africa per essere addestrato o, comunque, instradato al terrorismo attivo.

Infine, è stata individuata[77] una nuova figura rappresentata da quei terroristi islamici, definiti "zombie"[78], che, essendo pronti a dare la propria vita, già competenti adeguatamente nell'uso delle armi e degli esplosivi o con alcune esperienze in Medio Oriente, si muovono all'interno di reti poco strutturate, basate su legami culturali o affettivi, agendo anch'essi in modo indipendente e imprevedibile, commettendo delitti di diversa specie con finalità terroristica.

Il diritto penale nazionale, su sollecitazione della direttiva europea del 2015, ha così provveduto, mediante l'introduzione dell'art. 270-*quinquies* c.p., a reprimere i comportamenti delittuosi di chi riesca a istruirsi o ad "auto-addestrarsi" autonomamente per poi compiere atti finalizzati, in modo inequivoco alla commissione delle condotte di cui all'art. 270-*sexies* c.p. Questo fatto tipico si inserisce già in un quadro normativo che, fin dal 2005, incriminava le condotte dell'addestratore e dell'istruttore, mentre considerava penalmente irrilevanti i comportamenti di chi si auto-istruiva o auto-addestrava.

Anche questa fattispecie, come già parzialmente anticipato, ha creato non pochi dubbi di compatibilità con i principi fondamentali del diritto penale contemporaneo e, in primo luogo, con i principi di offensività e di determinatezza.

Infatti, il comportamento tipizzato si pone al confine con il mero esercizio di un diritto[79], in quanto non si caratterizza né per la realizzazione di atti

[77] F. FASANI, *op. cit.*, p. 96 ss.

[78] M. LOMBARDI, *Nuove forme di terrorismo: zombie*, www.ispionline.it/it/pubblicazione/nuove-forme-di-terrorismo-zombie-11994, 2015.

[79] M. PELISSERO, *Contrasto al terrorismo internazionale e il diritto penale al limite*, in "Gli speciali di questione giustizia. Terrorismo internazionale, politiche di sicurezza, diritti fondamentali", 2016, p. 99 ss.

ISSN 0390-0975 ISBN 978-88-495-3707-9

preparatori, né per l'appartenenza o la partecipazione del soggetto agente a un'associazione terroristica. La norma, dunque, cerca essenzialmente di prevenire o reprimere i fatti potenzialmente realizzabili dai c.d. "lupi solitari" o dai foreign fighter, anticipando la tutela penale in un momento ancora precedente alla realizzazione di atti preparatori.

Sebbene la fattispecie tenda a punire quei comportamenti che si materializzano nella realizzazione di "comportamenti univocamente diretti" ad una delle condotte di cui all'art. 270-*sexies* c.p., è tuttavia esplicito come, in realtà, la consumazione venga individuata nello stesso momento in cui si utilizzano informazioni dirette ad un potenziale auto-addestramento aggressivo.

La tutela penale sembra così tanto anticipata da finire per sanzionare la libertà di manifestazione del pensiero, diventando così del tutto inefficace, poiché in concreto pienamente contrastante con i diritti costituzionali e della Carta EDU. Appare dunque indispensabile un'attività ermeneutica della giurisprudenza in grado di salvaguardare il rispetto dell'esercizio delle libertà e dei diritti del cittadino.

La Corte di cassazione, invece, con una recente pronuncia[80], proprio analizzando il fatto di chi aveva scaricato da Internet video e documenti aventi un valore didattico circa l'uso di armi e di esplosivi da utilizzare per il compimento di atti terroristici di matrice jihadista, ha ritenuto che questo stesso comportamento risultasse già, *ex se*, idoneo a configurarsi come comportamento univocamente diretto a realizzare un fatto collocabile nell'alveo di cui all'art. 270-*sexies* c.p. e, dunque, penalmente rilevante ai sensi dell'art. 270-*quinquies* c.p., come riformato nel 2015.

Fondamentalmente, la Corte ha appiattito sull'elemento soggettivo l'intera condotta, non valutandola oggettivamente e in coerenza con il principio di offensività. Finanche il dolo specifico non è apparso concretamente ricostruito secondo i comuni criteri ermeneutici che richiedono che il fine sia realmente idoneo a concretizzarsi in atti preparatori.

Occorrerebbe, in realtà, in fase applicativa della fattispecie, assicurarsi che il soggetto agente abbia concretamente utilizzato informazioni, video e materiali idonei non solo a esplicare un'efficacia auto-didattica, ma idonee a condurre realmente a un'azione, oggettivamente tangibile e, in particolare, univocamente dirette a realizzare una delle condotte di cui all'art. 270-*sexies* c.p.[81]

[80] Cass., sez. V pen., 19 luglio 2016, n. 6061.

[81] M. PELISSERO, *op. cit.*, pp. 110-112.

 ISSN 0390-0975 ISBN 978-88-495-3707-9

In conclusione, dunque, il diritto penale sembra ora inefficace, ora contrastante con alcuni canoni e principi fondamentali di matrice costituzionale, almeno tutte le volte in cui, svilendo i principi di materialità e di offensività, cerca di sanzionare il traffico di informazioni connotate da una dimensione religiosa, politica o ideologica violenta e sovversiva ma, di per sé sola, inidonea a ledere o mettere in pericolo il bene giuridico dell'ordine pubblico.

6. Quale ruolo degli Internet Service Provider nella prevenzione degli illeciti con finalità di terrorismo internazionale. Osservazioni conclusive

A conclusione di questa trattazione è possibile evidenziare, in prima battuta, come sia palese la necessità di affrontare le problematiche connesse al terrorismo internazionale e all'abuso di Internet e dei mezzi informatici avvalendosi di una normativa sovranazionale, realmente integrata e multilivello[82] che sia, altresì, il frutto concreto di una collaborazione fra gli Stati anche in termini di sviluppo e di condivisione di una cultura della cybersecurity.

L'esigenza di giungere a un equilibrio fra tutela dell'ordine, sicurezza pubblica e libertà fondamentali in Internet rappresenta un obiettivo al quale non è possibile continuare a rinunciare, proprio perché è su questo campo che si accerterà la robustezza delle moderne democrazie occidentali.

Se infatti verrà demandato solo al diritto penale di derivazione europea il compito di contrastare il nuovo terrorismo contemporaneo, continueremo ad assistere a un approccio al fenomeno rispondente a una strategia bellica di vera e propria *war on terrorism*[83], che arricchirà progressivamente l'ordinamento nazionale di norme eccezionali decisamente derogatorie dei principi tradizionali del diritto penale.

Del resto, abbiamo visto come le fattispecie sulle quali ci si è soffermati, oltre a sollevare evidenti problemi al confronto con i principi di garanzia del diritto penale, incidono sull'esercizio di taluni diritti e libertà costituzionali, *in primis*, sulla libertà di manifestazione del pensiero – come esemplificativamente accade per i delitti di istigazione o apologia – sulla libertà di circolazione e, in generale, sulla libertà personale.

[82] V. Militello, *Terrorismo e sistema penale: realtà, prospettive, limiti*, cit., p. 6, il quale sottolinea l'importanza di una strategia condivisa e integrata in materia di contrasto ai delitti con finalità di terrorismo da parte dei Paesi Ue.

[83] A. Cavaliere, *Il contrasto del terrorismo tra esigenze di tutela e garanzie individuali*, cit., p. 1095.

ISSN 0390-0975 ISBN 978-88-495-3707-9

Tale processo, inoltre, determinerebbe l'ampliamento di un conflitto giuridico fra la normativa nazionale, che dovrebbe rimanere coerente con i principi costituzionali e che non consentirebbe un'anticipazione così forte della tutela, e la normativa Ue che, invece, sollecita gli Stati ad assicurare ciecamente la repressione del fenomeno terroristico. In pratica, si tratta di saggiare la tenuta dello Stato di diritto innanzi ad esigenze di tutela apparentemente in contrasto.

In definitiva, però, non si tratta di rinunciare all'impiego di fattispecie incriminatrici in materia di terrorismo internazionale, dato che alcune di esse esplicano realmente una funzione preventiva solo mediante l'incriminazione di atti preparatori[84], ma di accertare, in primo luogo, l'esistenza di un reale equilibrio, ovvero di una proporzionalità, fra la restrizione della libertà fondamentale oggetto di compressione, il bene giuridico tutelato prescelto e la pena adottata[85].

Nell'esaminare poi l'efficacia lesiva delle condotte prodromiche di preparazione di atti con finalità di terrorismo dovrebbe essere necessario accertare, escludendo seppur *utili* presunzioni, la concreta idoneità delle stesse a determinare il raggiungimento degli scopi coperti dal dolo specifico, per comprendere se, anche nel caso – ad esempio – della mera adesione psicologica alla propaganda dell'ISIS, manifestata con un semplice "mi piace", vi sia una minima ma reale componente di offensività.

Peraltro, se il terrorismo internazionale continua a mantenere una propria vitalità proprio attraverso le attività di propaganda e apologia, di addestramento e di reclutamento su Internet, occorre comprendere come sia di fondamentale importanza l'approfondimento del ruolo da affidare agli *Internet Service Provider* nella prevenzione di tali fenomeni.

Tale indagine[86], come già accaduto in materia di delitti contro la privacy e la riservatezza informatica, la proprietà intellettuale[87] o di pedo-pornografia e

[84] F. VIGANÒ, *Incriminazione di atti preparatori e principi costituzionali di garanzia nella vigente legislazione antiterrorismo*, in "Ius17@unibo.it", 2009, n. 1, pp. 171-190.

[85] F. PALAZZO, *Contrasto al terrorismo, diritto penale del nemico e principi fondamentali*, cit., p. 675.

[86] A. INGRASSIA, *op. cit.*, p. 1621; A. MANNA, *Società dell'informazione e diritto penale: problemi e prospettive*, cit., p. 342; L. BARTOLI, *Brevi considerazioni sulla responsabilità penale dell'Internet service provider*, cit., p. 602; L. PICOTTI, *I diritti fondamentali nell'uso ed abuso dei social network. Aspetti penali*, cit., p. 2527.

[87] R. FLOR, *Tutela penale e autotutela tecnologica dei diritti d'autore nell'epoca di internet*, Padova, Cedam, 2010.

 ISSN 0390-0975 ISBN 978-88-495-3707-9

abuso sessuale a danno dei minori[88], ha sollecitato sia la giurisprudenza[89] sia la dottrina a ragionare su eventuali profili di responsabilità penale da rinvenire in capo agli *hosting provider* e *Internet Service Provider* in relazione sia a condotte attive, di tipo concorsuale, tenute consapevolmente e in accordo con uno o più utenti, sia soprattutto a eventuali condotte omissive, in grado di configurare persino un reato omissivo improprio per non avere impedito l'evento, *ex* art. 40 c.p., cagionato dalle attività poste in essere dall'utente su una piattaforma on line.

Lo stesso dibattito potrebbe sollevarsi anche nel campo della prevenzione e repressione dei delitti con finalità di terrorismo, dato che alcuni di essi, apologia, propaganda, reclutamento e finanziamento, hanno luogo, come visto, proprio per il tramite della diffusione di una vasta quantità di informazioni sensibili attraverso Internet.

Data questa premessa, occorrerebbe dunque comprendere se le condotte caratterizzate da automatismi tecnologici possano determinare ipotesi di responsabilità per reati omissivi impropri in capo all'Internet provider anche in questi casi e in relazione ad un settore che, in sé, oltre a non essere pericoloso, è caratterizzato dalla massima libertà di accesso ad ogni tipo di utente in tutto il mondo.

Ad oggi, anche in considerazione del fatto che non si possa superficialmente procedere ad una equiparazione fra ISP, social media e ordinario editore, il quale tendenzialmente è in grado di controllare i contenuti delle comunicazioni e le informazioni in via preliminare prima della pubblicazione, non esiste un fondamento normativo che imponga agli ISP un obbligo giuridico di impedire l'evento lesivo da parte dell'utente[90].

Per di più, il legislatore ha finanche escluso un obbligo generale di mera sorveglianza (art. 17, co. 1, d.lgs. 70/2003), né tantomeno sembra che un obbligo di impedimento possa essere ricavato dagli obblighi di rimozione

[88] D. De Natale, *op. cit.*, p. 297; L. Picotti, *La legge contro lo sfruttamento sessuale dei minori e la pedopornografia in internet (l. 6 febbraio 2006, n. 38) (Parte seconda)*, in "Studium iuris", 2007, n. 11, p. 1196 ss.; A. Manna, *Considerazioni sulla responsabilità penale dell'internet provider in tema di pedofilia*, in "Il Diritto dell'informazione e dell'informatica", 2001, n. 2, p. 145 ss.

[89] Si veda fra tutti, il caso *Google v. Vividown*, già citato, Cass., sez. III pen., 3 febbraio 2014, n. 5107 o più recentemente presso la CEDU *Delfi c. Estonia* del 2015 o *Pihl c. Svezia* del 2017.

[90] R. Flor, *op. cit.*, p. 451; in generale si veda C.E. Paliero, *La causalità dell'omissione: formule concettuali e paradigmi prasseologici*, in "Rivista italiana di medicina legale", 1992, n. 4, p. 821 ss.

ISSN 0390-0975 ISBN 978-88-495-3707-9

degli effetti derivanti da reati già consumati dagli utenti o dagli obblighi di segnalazione degli illeciti (*ex* art. 17, co. 2, d.lgs. 70/2003).

Peraltro, l'eventuale assunzione di una posizione di protezione, che ha ad oggetto la necessità di fare fronte alla vulnerabilità di determinati beni, dovrebbe comportare anche una specifica tutela penale nei confronti del bene meta-giuridico dell'*Internet sicuro*, rispetto al quale i provider dovrebbero garantire la salvaguardia rispetto ad ogni forma di pericolo. Tutt'al più, potrebbero profilarsi ipotesi di responsabilità omissive solo quando l'ISP decida di non attivarsi per rimuovere il contenuto illecito dopo avere ricevuto l'ordine da parte dell'Autorità, poiché, in questo caso, potendo esercitare poteri effettivi contribuirebbe ad aggravare il pericolo presente nella Rete.

Continua tuttavia ad emergere la necessità di scandagliare più a fondo, anche per individuare eventuali profili di responsabilità, quei comportamenti posti in essere da *hosting* e *service provider* caratterizzati dal mantenere e diffondere le informazioni introdotte sulla Rete da singoli utenti in base a meccanismi di indicizzazione, selezione e riorganizzazione dei contenuti per scopi commerciali.

In questi casi, qualora questo meccanismo non dipendesse da un processo totalmente automatizzato impostato dal singolo utente, ma da uno customizzato appositamente dall'ente e solo parzialmente automatizzato per agevolare, per fini di lucro, lo stesso nella propria ricerca, potrebbero emergere condotte rispetto alle quali rivelerebbe un potere di controllo da parte dell'ISP.

In ogni caso, attribuire a questi soggetti la funzione o l'onere di selezionare preliminarmente i contenuti da proporre nella Rete significherebbe demandare ad essi il compito di disegnare la stessa fisionomia di Internet attraverso l'esercizio di un'attività censoria per conto dello Stato. In questo senso, si approntererebbe un sistema probabilmente più efficace nella prevenzione dei delitti di terrorismo perpetrati in Internet con il rischio di destabilizzarne fortemente l'autonomia e l'autodichia parziale. Le stesse libertà fondamentali potrebbero risultare limitate e, dunque, indirettamente controllate da un soggetto privato, costituzionalmente e culturalmente inadatto a tale ruolo.

Il risultato, in termini di garanzia di un corretto equilibrio fra privacy, libertà fondamentali e sicurezza e ordine pubblico, non sarebbe quello sperato.

Ecco che, ad oggi, una maggiore e adeguata prevenzione dei delitti con finalità di terrorismo perpetrati via Internet, rispettosa della corretta salvaguardia degli interessi qui sopra citati, potrebbe essere ottenuta mediante l'implementazione del meccanismo del *notice and takedown*, previsto dal d.lgs.

 ISSN 0390-0975 ISBN 978-88-495-3707-9

70/2003 in relazione alla disciplina sul commercio e adoperato anche rispetto ai delitti di pedo-pornografia.

In base a tale sistema, l'ISP, facendo impiego di specifici algoritmi in grado di identificare la minaccia, consistente in un contenuto potenzialmente illecito, deve obbligatoriamente informare dell'esistenza di questi dati di cui sia dubita la liceità l'Autorità, la quale, dopo avere svolto le proprie valutazioni, potrà impartire un ordine di rimozione o di inibizione dell'accesso al contenuto stesso e di oscuramento dell'account dell'utente.

Tale modello di controllo successivo delle condotte illecite realizzate dagli utenti, se supportato anche dallo sviluppo di una cultura della cybersecurity in grado di agevolare e rafforzare la cooperazione tra istituzioni pubbliche e enti privati, potrebbe consentire di ampliare controlli ramificati in tutta la Rete senza incidere sulle libertà fondamentali, almeno finché esse non sfocino in apologie o istigazioni concretamente offensive.

In questo contesto, dunque, particolare attenzione dovrebbe essere prestata al lavoro condotto dal Coordinatore antiterrorismo, istituito dal Consiglio europeo nel 2004, il quale sta concentrando in maniera rilevante risorse e capitali per sollecitare le istituzioni europee e nazionali ad adottare strumenti legislativi e tecnici e attuare una politica di prevenzione che parta proprio dal web, e che integri la cultura della cybersecurity con la repressione dei reati di terrorismo transnazionale.

Il pericolo reale e attuale che sembra tuttavia ancora permanere è quello inerente alla tenuta del nostro sistema democratico innanzi a un'eccessiva enfatizzazione delle paure determinate dalle logiche del terrore. L'insieme delle ricostruzioni e riflessioni qui svolte dovrebbe suggerire come i legislatori nazionale ed europeo non possano affatto rinunciare alla ricerca di un accettabile equilibrio tra esigenze di tutela dei principi fondamentali di sicurezza e ordine pubblico e libertà dei cittadini, entrambi indefettibili in uno Stato liberale e democratico.

E in tale ricerca, il diritto penale non può che continuare a rappresentare sempre l'*extrema ratio*, anche rispetto alla lotta al terrorismo contemporaneo in Internet.

ISSN 0390-0975 ISBN 978-88-495-3707-9