IL FENOMENO DEL *CYBERTERRORISMO* NELL'ORDINAMENTO ITALIANO

Introduzione

A partire dal tragico evento del 11 settembre 2001, proprio in ragione della gravità dell'attacco e della sua portata mediatica, il fenomeno terroristico è sempre stato sotto i riflettori degli ordinamenti statali dei diversi paesi, che hanno sviluppato e implementato al loro interno strategie di prevenzione e contrasto al terrorismo. Quello stesso evento ha dato il via a numerose ricerche in merito al rapporto del terrorismo con i mezzi di comunicazione di massa. L'utilizzo di internet, soprattutto nell'ultimo decennio, ha infatti cambiato radicalmente il modo di "fare" terrorismo, non solo dal punto di vista della rapidità di comunicazione tra le dislocate cellule terroristiche o per quanto riguarda la possibilità di diffondere celermente e globalmente messaggi e idee eversive, ma anche in termini di veri e propri attacchi cibernetici alle più importanti infrastrutture statali.

È chiaro allora che oggi ci troviamo a fronteggiare un'emergenza su scala globale: il terrorismo moderno, che è istantaneo ed imprevedibile, non si limita a colpire i suoi obiettivi, bensì sfrutta la tragedia per fare propaganda portando l'orrore nelle nostre case attraverso la rete.

Il *cyberterrorismo*

Il crescente sviluppo tecnologico e il contestuale maggior utilizzo dei sistemi informatici ha cambiato da ogni punto di vista il mondo della comunicazione. Essendo il mondo del web accessibile a tutti anche le stesse organizzazioni terroristiche si sono evolute, sfruttando il progresso tecnologico e l'informatizzazione per realizzare i loro obiettivi. Internet è di facile accesso da qualunque parte del mondo: un terrorista può raggiungere istantaneamente grandi platee oppure indirizzare i propri messaggi a specifici gruppi di individui; ha inoltre la possibilità di operare nel completo anonimato. Però, l'aspetto che rende Internet lo strumento ideale per i gruppi terroristici è il suo essere interattivo: è possibile infatti interagire in tempo reale con qualsiasi persona abbia una connessione Internet. Le organizzazioni terroristiche hanno, quindi, saputo sfruttare le potenzialità multimediali dell'era contemporanea; il web non solo permette di divulgare qualsiasi contenuto informativo in tutto il mondo, ma anche tutte quelle immagini che, per ragioni legate alla decenza, non possono andare in onda sugli schermi televisivi.
Già degli attentati dell'11 settembre tutte le organizzazioni terroristiche avevano il proprio sito, all'interno del quale generalmente fornivano informazioni utili per pianificare un attentato, mostravano la storia dell'organizzazione, la biografia dei leader, le mappe delle zone territoriali coinvolte, le attività e le basi sociali e ideologiche. In concomitanza con l'evoluzione tecnologia intercorsa dalla caduta delle torri gemelle ad oggi si è assistito

anche all'evoluzione della preesistente minaccia terroristica che, a differenza del passato, appare completamente destrutturata e assume connotati diversi, muovendosi attraverso diverse entità come i "lone wolf" (lupi solitari), i piccoli aggregati, le cellule costituite da soggetti che rivendicano di fatto entità di provenienza diversificate. Tutti questi diversi fenomeni hanno in comune un unico *background* culturale che è quello della cultura del terrorismo attraverso il web: il cd. "jihadismo globalizzato".

Oggi, per poter ben delineare l'utilizzo che i gruppi terroristici fanno della rete Internet e per meglio individuare le attività da questi svolte, è opportuno fare un'importante distinzione all'interno della nozione di *cyberterrorismo*, che è ormai entrata a far parte del linguaggio comune.

La prima tipologia, che è definita *Target Oriented*, o semplicemente *cyberterrorismo*, è ancora oggi motivo di numerose difficoltà legate alla mancanza di un unanime accordo sul significato da attribuirgli. Un'iniziale definizione del termine, che risale al 1980, fu fornita da un ricercatore dell'*Institute of Security and Intelligence* della California, il quale lo ha definito come «la convergenza dei termini cyberspazio e terrorismo»[1]. Un'altra definizione è stata formulata nel 1998 da parte di un agente speciale dell'FBI, Mark Pollit, che associò il termine *cyberterrorismo* ad «attacchi premeditati e con scopi politici portati alla informazioni o a sistemi informatici di gestione dell'informazione che possano determinare conseguenze violente contro obiettivi che non siano in stato di guerra»[2]. Nel medesimo anno, una studiosa di *Computer Science* presso la Georgetown University elaborò una definizione che includeva all'interno della categoria degli atti *cyberterroristici* anche «atti politicamente motivati che possano causare gravi perdite economiche, di elettricità o acqua»[3]. In sintesi, il controverso fenomeno del *cyberterrorismo* possiamo dire che oggi rappresenta una particolare minaccia derivante dallo spazio cibernetico e caratterizzata dal fatto di essere, almeno potenzialmente, idonea a causare danni ingenti a persone o cose o a scatenare il panico. Suddetta minaccia viene realizzata da organizzazioni terroristiche attraverso attacchi a infrastrutture critiche di un Paese, come possono essere gli aeroporti o le centrali elettriche e nucleari.
La seconda tipologia, la *Tool Oriented*, che possiamo anche definire radicalizzazione *online*, invece, si presta ad avere contenuto molto ampio, poiché in questo caso la rete è individuata come uno strumento di supporto all'attività terroristica: essa comprende sia le attività di comunicazione interna tra cellule terroristiche, sia il processo di propaganda e reclutamento effettuato tramite il web.

Fare propaganda e pubblicità è sicuramente il primo scopo che i terroristi possono raggiungere attraverso l'uso di Internet. La propaganda comporta la diffusione su internet di materiale multimediale il cui obiettivo primario è quello di fare pubblicità, diffondendo messaggi ideologici o promuovendo gli ideali e le attività terroristiche. Ancora l'obiettivo pubblicitario si esplica spesso nella volontà di "comunicare il terrore": con questa espressione si suole indicare la diffusione di materiali dai contenuti violenti o che minacciano l'uso della forza per incutere paura.

La più grande potenzialità, però, della propaganda *online* per le organizzazioni terroristiche rimane la possibilità di reclutamento, incitamento, radicalizzazione e infine guerra psicologica.

---

[1] B. Collin, *The future of cyberterrorism, Crime and Justice International*, Marzo 1997.
[2] M. M. Pollit, *Cyberterrorism – Fact or Fancy?*, in Computer Fraud & Security, febbraio 1998.
[3] P. Lorusso, *L'insicurezza nell'era digitale. Tra cybercrimes e nuove frontiere dell'investigazione*, 2011

Il reclutamento su Internet avviene, nella maggior parte dei casi, tramite l'utilizzo di siti protetti da password, forum o chat room dedicate nelle quali i terroristi individuano i potenziali sostenitori. Tali soggetti, spesso provenienti da realtà sociali particolarmente vulnerabili o emarginate, sono facilmente condizionabili facendo presa sul tema della religione o su sentimenti di ingiustizia, esclusione o umiliazione, promuovendo e glorificando atti di violenza e terrorismo come strumenti di riscatto e giustizia.
Reclutamento, incitamento e radicalizzazione possono essere visti come passaggi di uno stesso percorso che ha come obiettivo quello di condurre il soggetto radicalizzato a compiere atti di violenza basati su ideologie estremiste. Pertanto, questo processo differisce dalla propaganda vera e propria, poiché le attività che lo accompagnano, pragmaticamente parlando, mirano ad un preciso risultato: vengono infatti utilizzate le cosiddette "bolle informative" per le quali, attraverso l'uso di mezzi informatici, si crea una sfera sociale all'interno della quale il futuro o potenziale terrorista possa accorgersi di nuove informazioni e accettare nuove idee, che per quanto possano essere terrificanti, nel corso di questo processo diventano quasi normali e auspicabili.

Oltre agli scopi propagandistici e di reclutamento, per i gruppi terroristici l'utilizzo di Internet è fondamentale ai fini dell'addestramento dei soggetti radicalizzati e della pianificazione di attentati.
L'addestramento può avvenire così a distanza con diversi mezzi multimediali, il cui contenuto può essere il più vario: come costruire un esplosivo, come maneggiare armi o come pianificare ed eseguire al meglio un attacco terrorista.
Come già anticipato, la rete web offre ai terroristi un mezzo celere e economico di comunicazione, ma soprattutto immediato e anonimo: tutto ciò permette alle varie cellule terroristiche, diffuse in tutto il mondo, di mantenere stretti contatti e di condividere informazioni efficientemente.

Un ultimo, ma non meno importante, utilizzo del web è quello dei finanziamenti: questo può avvenire con diversi mezzi come il finanziamento diretto, l'e-commerce, gli strumenti di pagamento online e la raccolta di donazioni attraverso organizzazioni di carità.

Necessità di un bilanciamento tra libertà di espressione e Internet

L'art. 21 della Costituzione italiana sancisce il diritto "di manifestare liberamente il proprio pensiero con la parola, lo scritto e ogni altro mezzo di diffusione". A questo proposito sia dottrina che giurisprudenza sono concordi nel ritenere che tale norma costituzionale comprenda anche il diritto di informare, il quale garantisce la possibilità di rendere manifeste le proprie opinioni personali attraverso la condivisione con altri delle informazioni di cui si è in possesso. Inoltre, l'art. 21 assicura la possibilità di accedere ai dati e alle notizie disponibili senza alcuna restrizione: grazie a questa previsione l'individuo può raccogliere dati e informazioni e, analizzandoli, può elaborare le proprie opinioni personali.
Sotto questo aspetto è possibile individuare l'importanza di Internet e dei mezzi di comunicazione e di circolazione delle informazioni nel processo formativo del pensiero del singolo individuo.
Naturalmente il diritto enunciato dall'art. 21 Cost. non è illimitato: l'ordine pubblico tutelato dalla stessa Costituzione risulta essere un limite all'esercizio tale diritto.

Rapporti normativi tra *cybercrime* e *cyberterrorismo*

Il fenomeno del terrorismo cibernetico, ad oggi, non risulta essere una fattispecie legale tipizzata nel quadro del diritto penale sostanziale, pertanto è necessario verificare l'astratta applicabilità ad esso delle norme incriminatrici vigenti nel nostro ordinamento. Tale mancata tipizzazione potrebbe essere frutto della natura composita del fenomeno terroristico, all'interno del quale è, infatti, possibile rinvenire alcune componenti fenomeniche comuni sia alla criminalità informatica che al terrorismo tradizionale.
Con l'entrata in vigore del Trattato di Lisbona nel 2009, la criminalità informatica e il terrorismo sono stati classificati, per espressa previsione dell'articolo 83, primo paragrafo, del TFUE[4], fra i fenomeni criminosi di natura grave e transnazionale, sui quali l'Unione Europea possiede una competenza penale. In applicazione del citato articolo, sono state adottate la direttiva 2013/40/UE del 12 agosto 2013 relativa agli attacchi contro i sistemi di informazione e la direttiva 2017/541/UE del 15 marzo 2017 sulla lotta contro il terrorismo.
Quest'ultimo provvedimento del 2017 connota, almeno parzialmente, la stretta connessione che intercorre tra spazio cibernetico e terrorismo, riconoscendo così la modalità di azione *online*, che caratterizza le nuove organizzazioni terroristiche: l'articolo 21[5], infatti, rubricato "misure per contrastare i contenuti online riconducibili alla pubblica provocazione", pone a carico degli Stati l'obbligo di rimuovere alla fonte i contenuti *online* che costituiscono una pubblica provocazione per commettere un reato di terrorismo. Tale obbligo si sostanzia nell'adozione di misure necessarie alla rimozione tempestiva dei contenuti *online*, ospitati nel proprio territorio, attraverso i quali viene perpetrato il reato di pubblica provocazione ovvero, ove ciò non sia possibile, per bloccare l'accesso a tali contenuti agli utenti di Internet[6]. Inoltre, nella relazione di accompagnamento alla proposta di direttiva, nell'enunciare che per "fornitura di addestramento" si intende la condotta volta ad impartire istruzioni per la fabbricazione o l'uso di esplosivi e armi da fuoco o comunque ad impartire metodi specifici al fine di commettere o contribuire alla commissione di un reato di terrorismo, viene specificato che tale norma ha la funzione di "*contrastare la diffusione di istruzioni e manuali (online) ai fini dell'addestramento e della pianificazione di attentati e più specificatamente la diffusione (attraverso Internet) di informazioni sulle risorse e i metodi terroristici, che funge in tal modo da campo di addestramento virtuale*".
Quanto sopra detto riflette la multiformità del terrorismo, la quale rende potenzialmente applicabili a tale fenomeno le disposizioni penali in materia di reati informatici. Ad ulteriore riprova di ciò, nella Convenzione di Budapest sul *cybercrime* del 2001, che è stata ratificata in Italia con la l. 48/2008, è esplicitamente sottolineato che l'applicazione delle disposizioni previste non è rivolta solo ai reati elencati nella Convenzione, ma viene

---

[4] "*Il Parlamento europeo e il Consiglio, deliberando mediante direttive secondo la procedura legislativa ordinaria, possono stabilire norme minime relative alla definizione dei reati e delle sanzioni in sfere di criminalità particolarmente grave che presentano una dimensione transnazionale derivante dal carattere o dalle implicazioni di tali reati o da una particolare necessità di combatterli su basi comuni. Dette sfere di criminalità sono le seguenti: terrorismo, tratta degli esseri umani e sfruttamento sessuale delle donne e dei minori, traffico illecito di stupefacenti, traffico illecito di armi, riciclaggio di denaro, corruzione, contraffazione di mezzi di pagamento, criminalità informatica e criminalità organizzata.*
In funzione dell'evoluzione della criminalità, il Consiglio può adottare una decisione che individua altre sfere di criminalità che rispondono ai criteri di cui al presente paragrafo. Esso delibera all'unanimità previa approvazione del Parlamento europeo."
[5] Della direttiva (UE) 2017/541.
[6] Santini S., *L'Unione Europea compie un nuovo passo nel cammino della lotta al terrorismo: una prima lettura della Direttiva 2017/541/UE*, in *Diritto Penale Contemporaneo*, fasc. 7-8/2017.

anche estesa a tutti quei reati che presuppongono la necessaria raccolta della prova informatica[7].
In applicazione di quanto sopra, si può affermare, a titolo esemplificativo, che un attacco informatico diretto a deteriorare, cancellare, alterare o sopprimere informazioni, dati o programmi informatici utilizzati dallo Stato o da un altro ente pubblico può integrare il reato di cui all'art. 635-*ter* c.p., anche quando il reato sia stato commesso con fini terroristici.

Applicabilità della legislazione antiterrorismo al fenomeno di *cyberterrorismo*

La disciplina antiterrorismo in Italia è stata oggetto di importanti innovazioni negli anni 2015 e 2016 e grazie a queste è stato possibile applicare tale disciplina, pur con non poche difficoltà, a fatti riconducibili al *cyberterrorismo*.
L'articolo 270-*quinquies* c.p. qualifica come reato l'addestramento con finalità di terrorismo anche internazionale, il quale comprende l'attività di chi addestra o fornisce istruzioni su come preparare un attentato terroristico come anche quella di chi, essendosi addestrato autonomamente, pone in essere comportamenti univocamente finalizzati alla commissione di atti terroristici. L'articolo si conclude prevedendo un aumento di pena nel caso in cui l'addestramento o l'istruzione sia avvenuta per il tramite di strumenti informatici o telematici. La fattispecie risulta quindi applicabile sia a chi, con finalità di terrorismo, fornisce informazioni attraverso la rete, come nel caso di *tutorial* su come accedere al *dark web* per l'acquisto di armi, sia a colui che assume un certo *know-how* tramite l'utilizzo della rete su come, per esempio, costruire esplosivi autoprodotti.
L'ultima clausola del citato articolo ha fatto sorgere un dibattito dottrinale in merito alla punibilità di fatti diretti alla mera acquisizione di informazioni: è importante, però, ricordare che le informazioni acquisite devono essere funzionali al compimento di atti terroristici, pertanto si può concludere che la mera detenzione o acquisizione, anche continuata, di informazioni relative a preparazione di esplosivi, o simili, non assumono alcuna rilevanza penale.

Sentenza Corte di Cassazione, n. 47489/2015

Merita menzione una sentenza della Corte di Cassazione in materia di *cyberterrorismo*, nella quale essa ha affermato che l'utilizzo della rete ai fini di propaganda delle attività del cd. Stato Islamico integra il reato di apologia[8] finalizzato alla partecipazione ad un'organizzazione di stampo terroristico[9].
Nel caso di specie l'imputato, di origini marocchine, era accusato di apologia dello Stato Islamico a causa della diffusione in rete di un documento, in lingua italiana, dal titolo "Lo Stato Islamico, una realtà che ti vorrebbe comunicare". La Cassazione ha ritenuto che la diffusione di tale documento potesse configurarsi come propaganda terroristica, laddove rivolgeva un invito ad unirsi al Califfato islamico "accettandone la natura combattente". La Corte ha inoltre sottolineato che il contenuto "presentava personaggi ufficialmente classificati come terroristi nei documenti internazionali e conteneva diversi link a siti

[7] Art. 14 Convenzione di Budapest, 2001.
[8] ex art. 414 c.p.
[9] ex art. 270-*bis* c.p.

internet facenti capo all'organizzazione terroristica". A fronte di queste considerazioni, i giudici hanno respinto la tesi sostenuta dal ricorrente, secondo cui il documento incitava ad un'adesione solo di tipo ideologico allo Stato Islamico e ha aggiunto che ai fini dell'integrazione del reato di apologia "non basta l'esternazione di un giudizio positivo su un episodio criminoso, per quanto odioso e riprovevole esso possa apparire alla generalità delle persone dotate di una sensibilità umana, ma occorre che il comportamento dell'agente sia tale per il suo contenuto intrinseco, per la condizione personale dell'autore e per le circostanze di fatto in cui si esplica, da determinare il rischio, non teorico, ma effettivo, della consumazione di altri reati e, specificamente, di reati lesivi di interessi omologhi a quelli offesi da crimine esaltato". Infine, la Corte ha concluso che la natura pubblica dell'apologia, nel caso di specie, è stata perfettamente integrata dalle modalità di diffusione del documento.

Conclusioni

Il *cyberterrorismo* si identifica quindi come un fenomeno ibrido, al quale, nell'ordinamento italiano, sono applicabili sia la disciplina dei reati cibernetici che quella antiterrorismo. Quest'ultima tende a prevenire il reato, mediante un arretramento della soglia di rilevanza penale, sanzionando in questo modo condotte preparatorie al concreto atto terroristico. In questo contesto, potendo sorgere il rischio limitare in modo ingiustificato e sproporzionato le libertà individuali protette dalla Costituzione, ha un ruolo fondamentale il giudice nell'evitare che l'arretramento della soglia di punibilità sconfini nella repressione di forme di manifestazione del pensiero.

Margherita Del Deo
margherita.deldeo@gmail.com

BIBLIOGRAFIA

ANGELO A., *Istigazione a delinquere: fattispecie criminosa e condotte configurabili su Internet*, Diritto.it, 2017

BASTIANI D., *Terrorismo e media: la comunicazione del terrore*, Informazioni della Difesa, 2012

FLOR R., *Cyber-terrorismo e Diritto Penale in Italia,* in *Diritto Penale e Modernità. Le nuove sfide fra terrorismo, sviluppo tecnologico e garanzie fondamentali*

LAMBERTI C., *Gli strumenti di contrasto al terrorismo e al cyber-terrorismo nel contesto europeo,* Rivista di Criminologia, Vittimologia e Sicurezza – Vol VIII – N. 2 – Maggio – Agosto 2014

LORUSSO P.*, L'insicurezza nell'era digitale. Tra cybercrimes e nuove frontiere dell'investigazione,* 2001

PAGANINI P., *Il ruolo della componente tecnologica nel moderno terrorismo*, RISE, 2016

SACCHETTI V., *Il contrasto alla propaganda terroristica online nell'ambito dell'Unione europea: tutela attuale e prospettive future*, rivista Eurojus, 2019

SANTINI S., *L'Unione Europea compie un nuovo passo nel cammino della lotta l terrorismo: una prima lettura della Direttiva 2017/541/UE*, in Diritto Penale Contemporaneo, fasc. 7-8/2017

VIGNERI A. F., *Cyberterrorismo: realtà o finzione? Profili problematici di definizione e contrasto*, da Opinio Juris

ZICCARDI G., *Internet, sicurezza e libertà personali nell'epoca dell'emergenza terrorismo: alcune riflessioni.*