



Corso di laurea in Giurisprudenza

Cattedra di Diritto Internazionale

La criminalità organizzata transnazionale nell'era
del digitale: la teoria della responsabilità
internazionale degli Stati per le attività illecite
delle mafie tradizionali e digitali.

Prof. Pietro Pustorino

RELATORE

Prof. Roberto Virzo

CORRELATORE

Silvia Petruzzi Matr. 177553

CANDIDATO

Anno Accademico 2024/2025

INDICE

INTRODUZIONE.....	7
Capitolo 1	10
La criminalità organizzata transnazionale e la sua evoluzione nell'era del dominio digitale.....	10
1.1 La criminalità organizzata transnazionale.....	10
1.1.1 Definizione e caratteristiche principali della criminalità organizzata transnazionale.....	11
1.1.2 Dalle caratteristiche principali della criminalità organizzata a quelle di più recente evoluzione: come la globalizzazione ha inciso nello sviluppo del fenomeno.....	15
1.1.3 Le principali organizzazioni criminali transnazionali.....	18
1.2 La criminalità organizzata transnazionale: uno studio sul mondo digitale del <i>Deep web</i> e <i>Dark web</i>	21
1.2.1 Introduzione al <i>Deep web</i> e al <i>Dark web</i>	21
1.2.2 Traffici illeciti e mercato nero.....	23
1.2.3 Dal <i>Dark web</i> alle criptovalute: come le monete virtuali siano il principale strumento virtuale per gestire i traffici mafiosi nel <i>Dark web</i>	26
1.3 L'IA al servizio della criminalità organizzata transnazionale.....	27
1.3.1 L'ottimizzazione delle attività illecite.....	28
1.3.2 Il <i>Dark web</i> è ancora l'unico strumento virtuale per delinquere? Come le nuove organizzazioni criminali transnazionali prediligano gli strumenti di IA per la realizzazione del crimine.....	30
1.4 Conclusioni.....	31
Capitolo 2	33
La responsabilità degli Stati alla luce delle azioni della criminalità organizzata transnazionale tradizionale e moderna.....	33

2.1 Il concetto di responsabilità nel diritto internazionale.	36
2.1.1 Il ruolo del Progetto ARSIWA nella codificazione della responsabilità internazionale degli Stati.	41
2.1.2 La responsabilità dello Stato nel diritto internazionale.	44
2.1.3 Il criterio di attribuzione della condotta illecita dei privati allo Stato: l'articolo 8 del Progetto ARSIWA.	47
2.2 Il principio di <i>Due Diligence</i> nel Diritto Internazionale: origini, ruolo e importanza del principio.	52
2.2.1 Responsabilità internazionale per omessa <i>due diligence</i> : presupposti e conseguenze giuridiche dell'inadempimento.	57
2.2.2 La violazione dell'obbligo di <i>due diligence</i> in caso di condotta illecita di privati: i profili di responsabilità internazionale dello Stato.	61
2.2.3 I limiti della <i>due diligence</i> : un dibattito dottrinale.	63
2.3 Organizzazioni criminali e attività illecite nel cyberspace: i profili di responsabilità internazionale degli Stati.	65
2.3.1 Il principio di <i>due diligence</i> nel <i>cyberspace</i> : il ruolo dell'attribuzione e le difficoltà nello spazio cibernetico.	69
2.3.2 Il fenomeno dei <i>cyber</i> attacchi delle mafie e la responsabilità degli Stati per omessa <i>due diligence</i>	72
2.3.3 Il caso degli attacchi hacker da parte della mafia russa: in che modo la Russia ha affrontato tale fenomeno.	76
2.4 Conclusioni.	82
Capitolo 3	85
I nuovi strumenti di repressione e di contrasto alla criminalità organizzata transnazionale.	85
3.1 Critica all'obsoleta Convenzione di Palermo rispetto alle nuove forme di mafie nel mondo <i>cyber</i>	85

3.1.1 Le criticità della Convenzione di Palermo rispetto all'evoluzione criminale nell'era digitale.....	86
3.1.2 La necessità per la Convenzione di essere aggiornata sulla criminalità informatica e sui nuovi crimini organizzati del web: il <i>phishing</i> e la tratta illecite nel <i>dark web</i>	89
3.1.3 La mancanza di prospettive future nella Convenzione di Palermo.	93
3.1.4 I possibili scenari futuri.....	95
3.2 La Convenzione di Budapest tra aspetti positivi e criticità.	96
3.2.1 La convenzione di Budapest e i primi apporti offerti al contrasto dell'entità criminale informatica.	97
3.2.2 Le criticità della Convenzione di Budapest alla luce dell'evoluzione digitale del crimine organizzato informatico.	100
3.3 La nuova frontiera offerta dalle Nazioni Unite per il futuro del contrasto del cyber crime: le possibili soluzioni tra il trattato globale dell'ONU e l'uso dell'IA.	103
3.3.1 Come il trattato globale sulla criminalità informatica potrebbe sostituire la Convenzione di Budapest.....	104
3.3.2 L'IA come possibile alleato nella lotta al <i>cybercrime</i> e alla criminalità informatica organizzata.	109
3.4 Conclusioni	110
CONCLUSIONI.....	113
BIBLIOGRAFIA.....	117
SITOGRAFIA	123

INTRODUZIONE.

La criminalità organizzata transnazionale è uno dei fenomeni che più mina la stabilità e la sicurezza globale. Nel mondo l'avvento della globalizzazione e dell'innovazione tecnologica ha portato conseguenze anche nelle attività illecite commesse dai gruppi criminali che rispetto al passato, non parrebbero più essere radicate solo nel territorio, ma anche implementate in strumenti virtuali e informatici che danno modo alle organizzazioni criminali di rendere il crimine più dinamico ed occulto.

Nell'analisi della nascita e dell'evoluzione delle organizzazioni criminali nel mondo, la posizione più rilevante a livello internazionale la ricoprono gli Stati, i soggetti internazionali protagonisti del contrasto al fenomeno criminale e sottoposti al rispetto di obblighi di prevenzione e repressione delle conseguenze dannose che da tali crimini possano derivare.

Pertanto, il primo capitolo verterà sull'analisi del fenomeno del crimine organizzato, esaminando in via generica le radici dell'entità delle organizzazioni e la loro evoluzione, sia tradizionale che digitale. Sebbene l'elaborato offra un'ampia panoramica storico evolutiva dell'entità criminale presa in esame, il nucleo dell'analisi si incentra sulla figura dello Stato, nei confronti del quale sarà condotto un esame della posizione giuridica che questo ricopre rispetto alle attività criminali. Più precisamente, inquadrando le organizzazioni criminali nella categoria degli attori non statali, l'elaborato verterà sull'esame dei profili di responsabilità internazionale che il diritto configura quando gli illeciti internazionali sono realizzati da privati, analizzando la logica dell'istituto della responsabilità internazionale e i criteri di attribuzione relativi all'imputabilità di questa allo Stato. Dopo aver analizzato i profili generali dell'istituto, partendo dall'esame del concetto di responsabilità nel diritto internazionale e della sua evoluzione storico concettuale, sarà dedicata un'ampia trattazione all'opera di codificazione più importante nell'ambito dell'istituto della responsabilità internazionale, il Progetto di articoli sulla responsabilità degli Stati per atti internazionalmente illeciti, presentato dalla CDI nel 2001 e adottato dall'Assemblea Generale delle Nazioni Unite. Alla luce dell'analisi della struttura del Progetto e degli elementi che questo prevede ai fini della configurabilità della responsabilità internazionale, sarà richiamata l'attenzione sulla fattispecie dell'articolo 8 ARSIWA in quanto, trattando della responsabilità per fatti di privati, intercetterebbe a

pieno l'ambito giuridico preso in esame dall'elaborato, ossia la responsabilità internazionale dello Stato per le attività criminali delle mafie, tradizionali e cibernetiche. Attraverso l'analisi dei criteri di attribuzione ex art. 8 ARSIWA sarà delineata la possibilità o meno di attribuire responsabilità internazionale allo Stato per le attività illecite di privati, come nel caso delle mafie, ponendo in evidenza le difficoltà dell'imputabilità dei crimini allo Stato in vista del rigido standard probatorio imposto dagli ARSIWA per l'attribuzione, parametro che diviene particolarmente oneroso nello spazio virtuale in cui odiernamente le mafie operano. La finalità del presente lavoro, proponendosi di esaminare se e in che misura lo Stato si possa configurare come responsabile delle attività criminali e dopo aver osservato l'inoperabilità dell'art. 8, orienterà tale indagine giuridica verso uno dei principi più rilevanti in tema di responsabilità internazionale dello Stato: il principio della *due diligence*. Alla luce di tale concetto e della sua portata giuridica, sarà condotta un'analisi generica della responsabilità configurabile nel caso in cui, in presenza di obblighi di prevenzione, uno stato manchi di rispettare il principio della *due diligence*. Coerentemente con l'oggetto dell'elaborato, legato alla nuova entità mafiosa operativa nello spazio virtuale, si analizzerà come la *due diligence*, declinata all'ambito informatico, imponga l'adozione di misure e condotte diligenti e coerenti rispetto alle facoltà statale, in assenza delle quali verrebbe a configurarsi responsabilità internazionale dello Stato che, seppur non ha diretto o controllato effettivamente i crimini, potrebbe violare o omettere la *due diligence* in materia, favorendo la proliferazione di conseguenze dannose. Sarà osservato come la dovuta diligenza imponga degli standard probatori concretamente meno rigidi rispetto al disposto ex art. 8 ARSIWA. Al fine di osservare lo standard di *due diligence* dovuto nell'ambito dello spazio virtuale, sarà preso in esame il caso della mafia russa e di come lo Stato della Russia abbia effettivamente rispettato l'obbligo di *due diligence* in relazione ai numerosi attacchi informatici mafiosi sofferti, con lo scopo di valutare se il criterio applicato dalla Russia sia stato considerato soddisfacente dello standard diligente dovuto o meno, sulla scorta della dottrina e della giurisprudenza internazionale in materia.

A conclusione della trattazione, l'ultimo capitolo lascerà spazio ad una riflessione critica degli strumenti convenzionali attualmente esistenti posti a repressione dell'entità mafiosa tradizionale e cibernetica, e ad un'osservazione prospettica intenta a definire nuove

misure di contrasto che possano colmare l'obsolescenza delle Convenzioni di Palermo e di Budapest e che possano dirsi attuali e funzionali per gli Stati rispetto al *cybercrime* mafioso contemporaneo.

Capitolo 1

La criminalità organizzata transnazionale e la sua evoluzione nell'era del dominio digitale.

1.1 La criminalità organizzata transnazionale.

Il fenomeno della criminalità organizzata transnazionale è un male da cui l'intera comunità internazionale è afflitta. L'entità delle organizzazioni criminali e delle varie forme di gruppi a struttura associativa viene concepita come entità criminale organizzata agli inizi del ventesimo secolo, periodo in cui gli atteggiamenti delinquenti dei gruppi saranno effettivamente riconosciuti come caratteristici dei gruppi criminali organizzati.¹ Lo sviluppo delle organizzazioni criminali più imponenti, divenute transnazionali attraverso il processo di globalizzazione, hanno portato nel tempo gli Stati ad affrontare una sfida complessa che può essere compresa a partire dall'analisi del fenomeno in quanto tale, e del suo funzionamento. Difatti, la proliferazione dei mercati globali e della liberalizzazione delle merci in grado di circolare da uno Stato all'altro hanno accelerato ed intensificato il potere criminale che ha sfruttato l'assenza di tali ostacoli per tessere una rete di scambi illeciti sempre più diffusa.²

Alla luce del processo di globalizzazione, sarà opportuno proporre una panoramica storico evolutiva dell'entità criminale organizzata transnazionale e di come questa abbia implementato la propria operatività grazie all'evoluzione globale generale, pertanto saranno oggetto di analisi le caratteristiche che attualmente compongono la struttura dei gruppi criminali e delle dimensioni che il crimine organizzato ha assunto nel corso dell'evoluzione globale. Lo studio del funzionamento della macchina criminosa e

¹ Centonze, Alessandro. *Criminalità organizzata e reati transnazionali*. Osservatorio permanente Criminalità organizzata, vol. 10 di Osservatorio permanente sulla criminalità organizzata, Giuffrè Editore, 2008, pp. 120, 123.

² Centonze, Alessandro. *Criminalità organizzata e reati transnazionali*. Osservatorio permanente Criminalità organizzata, vol. 10 di Osservatorio permanente sulla criminalità organizzata, Giuffrè Editore, 2008, p. 4.

dell'evoluzione delle organizzazioni criminali transnazionali, dato soprattutto dalla globalizzazione, porterà ad interrogarsi sulla posizione giuridica degli Stati nei confronti delle attività illecite delle organizzazioni criminali del mondo, e in particolare, sulla forma di responsabilità internazionale che si configura in relazione a tale fattispecie.

1.1.1 Definizione e caratteristiche principali della criminalità organizzata transnazionale.

La criminalità organizzata transnazionale costituisce uno dei fenomeni che più minano la sicurezza globale, rappresentando una sfida sempre più complessa per il diritto internazionale. Le organizzazioni criminali, soprattutto quelle a stampo mafioso, hanno assunto aspetti nettamente transnazionali nell'arco degli ultimi due decenni, in quanto sempre più intensamente hanno incentrato i loro interessi alla ricerca di mercati e coalizioni che prescindessero dai confini nazionali e che dessero loro la possibilità di realizzare attività illecite in più Stati, puntando soprattutto a quelli più deboli e privi di adeguate politiche criminali e di contrasto.³

Per comprendere a pieno le caratteristiche che determinano il fenomeno è fondamentale rammentare la definizione di criminalità organizzata transnazionale che viene fornita nella Convenzione delle Nazioni Unite contro la criminalità organizzata, comunemente conosciuta come Convenzione di Palermo, secondo cui: *“per gruppo criminale organizzato si intende un gruppo strutturato di tre o più persone, esistente per un periodo di tempo e che agisce di comune accordo allo scopo di commettere uno o più reati gravi o illeciti stabiliti conformemente alla presente Convenzione, al fine di ottenere, direttamente o indirettamente, un vantaggio finanziario o altro vantaggio materiale.”*⁴

La Convenzione delle Nazioni Unite successivamente definisce all'articolo 3 il reato transnazionale e i suoi caratteri principali attestando che: *“un reato è di natura transnazionale se: (a) è commesso in più di uno Stato; (b) è commesso in uno Stato, ma*

³ Ponti, Christian. “Il diritto internazionale e la criminalità organizzata”. *Rivista Di Studi E Ricerche sulla criminalità organizzata*, Università degli Studi di Milano, vol. 1, n. 1, 2015, pp. 23, 24.

⁴ Nazioni Unite. *Convenzione delle Nazioni Unite contro la criminalità organizzata transnazionale*. New York, 2000, art. 2, lett. a, p. 5.

una parte sostanziale della sua preparazione, pianificazione direzione o controllo avviene in un altro Stato; (c) è commesso in uno Stato, ma coinvolge un gruppo criminale organizzato impegnato in attività criminali in più di uno Stato; oppure (d) è commesso in uno Stato, ma ha effetti sostanziali in un altro Stato.”⁵

La Convenzione delle Nazioni Unite contro la criminalità organizzata transnazionale e i suoi tre protocolli addizionali, inerenti alla tratta di esseri umani, al traffico di armi da fuoco e alla tratta di migranti, rappresentano l’attuale regime internazionale esistente al riguardo, intento a dotare gli Stati della capacità di conoscere come prevenire e reprimere il crimine organizzato transnazionale.⁶

L’organizzazione criminale transnazionale è contrassegnata da caratteristiche generali e specifiche che si riferiscono sia alla composizione dell’associazione in quanto tale, che parrebbe essere particolarmente articolata, sia alla natura del singolo atto criminale che distingue le varie attività illecite delle organizzazioni.⁷

Per tanto, partendo dall’analisi degli elementi distintivi dell’azione criminosa dei gruppi, questa presenterebbe due aspetti focali: il primo è quello di riuscire a ledere uno o più Stati su più livelli in quanto il crimine, insinuandosi nel tessuto economico e sociale dello Stato vittima, è in grado di arrecare una serie di lesioni ai diritti fondamentali e alle libertà individuali, riuscendo a minare la solidità dello Stato e l’affidabilità del sistema finanziario; tutto ciò spiegherebbe la logica adottata dal Consiglio d’Europa nel testo del Libro Bianco, secondo la quale il danno arrecato dall’azione criminosa di tali gruppi è molto più grave di quello che si configurerebbe in altri tipi di reato, soprattutto per la caratteristica transnazionale di tale fattispecie criminosa, la cui pianificazione,

⁵ Nazioni Unite. *Convenzione delle Nazioni Unite contro la criminalità organizzata transnazionale*. New York, 2000, art. 3, para. 2, p. 6.

⁶ Ponti, Christian. “Il diritto internazionale e la criminalità organizzata”. *Rivista Di Studi E Ricerche sulla criminalità organizzata*, Università degli Studi di Milano, vol. 1, n.1, 2015, p. 25.

⁷ Consiglio D’Europa. *Libro bianco sulla criminalità organizzata transnazionale*. Strasburgo: tipografia del Consiglio d’Europa, 2014, p. 17.

programmazione ed esecuzione avvengono nei confronti di più Stati, sfruttando alleanze e appoggi all'estero.⁸

Il secondo aspetto caratterizzante l'azione criminosa risiede nella bi-dimensione del crimine organizzato transnazionale che appare essere sia locale che transfrontaliera.⁹

La duplicità dimensionale dei crimini è data sia dal *modus operandi* attraverso cui questi vengono attuati, sia dalla tipologia di attività e dagli esiti che ne conseguono; le azioni criminose sono contraddistinte dall'essere implementate in programmi criminali estremamente flessibili in grado di adattarsi alle esigenze contingenti.¹⁰

In merito alle caratteristiche del gruppo che compone l'organizzazione criminale, queste si riferiscono alla dimensione organizzativa dell'associazione che presenta diverse peculiarità. L'organizzazione deve essere composta da più individui che svolgano un ruolo specifico e diverso l'uno dall'altro al fine ultimo di raggiungere lo scopo illecito.¹¹

La dimensione dell'organizzazione appare estremamente stabile e strutturata, alle volte presentando dei caratteri nettamente rudimentali o altre volte altrettanto complessi.¹²

Lo scheletro organizzativo, basato su di un programma che esula dalla commissione di semplici reati isolati, deve risultare evidentemente funzionale al raggiungimento di benefit per l'organizzazione nel suo insieme.¹³

Nell'analisi degli aspetti cardini della criminalità organizzata transnazionale una delle risorse più considerevoli è il complesso di rapporti redatti dall'*Europol*.

⁸ Consiglio d'Europa. *Libro bianco sulla criminalità organizzata transnazionale*. Strasburgo: tipografia del Consiglio d'Europa, 2014, pp. 13, 17.

⁹ Consiglio d'Europa. *Libro Bianco sulla criminalità organizzata transnazionale*. Strasburgo: tipografia del Consiglio d'Europa, 2014, p. 17.

¹⁰ Consiglio d'Europa. *Libro bianco sulla criminalità organizzata transnazionale*. Strasburgo: tipografia del Consiglio d'Europa, 2014, p. 16.

¹¹ Consiglio d'Europa. *Libro bianco sulla criminalità organizzata transnazionale*. Strasburgo: tipografia del Consiglio d'Europa, 2014, p. 16.

¹² Consiglio d'Europa. *Libro bianco sulla criminalità organizzata transnazionale*. Strasburgo: tipografia del Consiglio d'Europa, 2014, p. 16.

¹³ Consiglio d'Europa. *Libro bianco sulla criminalità organizzata transnazionale*. Strasburgo: tipografia del Consiglio d'Europa, 2014, p. 16.

L'*EUROPOL* (*European Union Agency for law enforcement cooperation*) è un'agenzia dell'Unione Europea con sede all'Aia, divenuta operativa in data 01/07/1999. Si fonda sulla volontà dell'Unione di istituire tra le forze di polizia di tutti gli Stati membri un organo in grado di garantirne la cooperazione nella prevenzione e nella lotta contro ogni forma di criminalità organizzata transnazionale. Nel 2013, attraverso uno dei suoi rapporti denominati *SOCTA*¹⁴, l'*Europol*¹⁵ si impegnava a spiegare i settori principali in cui le organizzazioni criminali operavano: immigrazione clandestina (fonte di rilevanti guadagni), traffico illegale di stupefacenti sintetici e frodi intracomunitarie¹⁶. Infine, qualche anno più tardi, l'*Europol* tramite un altro *SOCTA*, è tornata ad analizzare il fenomeno della criminalità organizzata transnazionale in Europa, sottolineando come questa soffra molto della copiosa presenza delle mafie sul territorio, gruppi che costituiscono fonte primaria dei danni riportati al tessuto socio-economico europeo¹⁷. Tuttavia, è opportuno ricordare che l'*Europol* rimane un'agenzia che presta un supporto in materia di contrasto alla criminalità organizzata per gli Stati. Pertanto, non detenendo alcun potere vincolante su di essi, la competenza a disciplinare e dirigere l'operato delle proprie forze di polizia rimane dello Stato, insieme alla capacità di decidere se partecipare alle azioni di indagine e polizia dell'*EUROPOL*, oppure astenersi dal farlo.

¹⁴ Il rapporto *SOCTA* è il classico strumento di rapporto attraverso il quale l'*Europol* analizza gli aspetti cardini della criminalità organizzata di natura transnazionale presente sul territorio europeo, approfondendo e aggiornando gli stati delle attività illecite che i gruppi realizzano.

¹⁵ *EUROPOL*: è una istituzione europea che si occupa di contrastare il fenomeno della criminalità organizzata transnazionale e del terrorismo, favorendo lo scambio di analisi e informazioni tra i Paesi Membri. (Morelli E. "Europol: cos'è e come funziona". *Forze Italiane*, 2019, consultabile sul sito <https://www.forzeitaliane.it/europol-cos-e-e-come-funziona>).

¹⁶ Consiglio d'Europa. *Libro bianco sulla criminalità organizzata transnazionale*. Strasburgo: tipografia del Consiglio d'Europa, 2014, p. 16.

¹⁷ Venezia, Lorenzo. "Il *SOCTA* 2017 dell'*Europol*: un'analisi sulla criminalità". *Diritto Consenso*, 2018, consultabile sul sito <https://www.dirittoconsenso.it/2018/03/26/socta-2017-europol-analisi-sulla-criminalita/>

La necessità di ricercare una cooperazione funzionale tra gli Stati origina dal fatto che le mafie che oggi gli Stati si trovano a reprimere appaiono estremamente sofisticate nella loro operatività, divenuta particolarmente problematica in seguito al processo di globalizzazione che ha permesso alle organizzazioni criminali di espandere la gestione delle proprie attività illecite, sfruttando negativamente gli effetti della interconnessione globale. Alla luce di quanto esposto, seguirà l'analisi del processo che ha portato all'integrazione globale e di come questa abbia concretamente rappresentato l'opportunità per le mafie di espandersi all'avanguardia.

1.1.2 Dalle caratteristiche principali della criminalità organizzata a quelle di più recente evoluzione: come la globalizzazione ha inciso nello sviluppo del fenomeno.

La globalizzazione è inevitabilmente una realtà attuale che ha effetti su ogni aspetto della vita sociale: economico, culturale, religioso. È doveroso riconoscere alla globalizzazione di aver evoluto e innalzato ad universale l'informazione e la comunicazione e di aver globalizzato l'accesso a beni e servizi. ¹⁸

Quando però la globalizzazione diviene l'opportunità più grande per la realizzazione del crimine organizzato allora rappresenta un problema imponente. ¹⁹

Le organizzazioni criminali transnazionali devono la loro più estesa evoluzione al fenomeno della globalizzazione sociale ed economica degli Stati del mondo, un fenomeno che ha permesso loro di passare dall'essere gruppi che operano localmente, a divenire i protagonisti delle attività illecite transnazionali più minatorie nei confronti della sicurezza governativa degli Stati.

I riscontri della globalizzazione da una parte hanno potenziato l'economia nello scenario internazionale, facendo crescere le imprese, le industrie e le società, dall'altra parte però

¹⁸ Pavone, Gianmichele. "Criminalità transfrontaliera e meccanismi di contrasto dell'ordinamento internazionale". *Altalex*, 2008, consultabile sul sito <https://www.altalex.com/documents/news/2014/03/08/criminalita-transfrontaliera-e-meccanismi-internazionali-di-contrasto>

¹⁹ Musci, Aldo. *Tutte le mafie del mondo. Una mappa della criminalità organizzata nell'epoca della globalizzazione*. Stampa Alternativa/Nuovi equilibri, Viterbo, 2011, p. 8.

hanno offerto un'ampissima opportunità per le organizzazioni criminali di sfruttare i traffici transnazionali.²⁰ Tutto il fenomeno della globalizzazione “inversa” (espressione utilizzata dallo scrittore Musci nel suo scritto intitolato “Tutte le mafie del mondo. Una mappa della criminalità organizzata nell'epoca della globalizzazione” per indicare la parte oscura e controproducente della globalizzazione) è dominato dalle mafie transnazionali che risultano possedere l'abilità di condurre, tramite tipologie associative integrate, dei veri e propri processi delinquenziali.²¹

Le organizzazioni criminali transnazionali sfruttano tale fenomeno soprattutto in ambito finanziario per poter investire i proventi dei loro illeciti in facciate legali.²²

Ad oggi le mafie globali detengono affari di ampissima portata in quanto la globalizzazione ha concesso alle vecchie e alle nuove mafie di poter porre in essere attività illecite in mercati internazionali in cui il controllo di queste risulterebbe estremamente difficile a causa della disorganicità legislativa attuata in differenti paesi.²³ La globalizzazione porta il peso di aver dotato le mafie transnazionali di una nuova posizione nei mercati globali: queste sono passate dall'essere entità intromesse ad essere entità totalmente integrate nell'economia legale.²⁴

²⁰ Savona, Ugo Ernesto, Lasco Federico, Di Nicola Andrea. “Processi di globalizzazione e criminalità organizzata transnazionale”. Università degli Studi di Trento, *Eprint*, 1998. eprints.biblio.unitn.it/197/1/Globalizzazione_e_criminalit%C3%A0.pdf

²¹ Musci, Aldo. *Tutte le mafie del mondo. Una mappa della criminalità organizzata nell'epoca della globalizzazione*. Stampa Alterativa/Nuovi equilibri, Viterbo, 2011, p. 12.

²² Consiglio D'Europa. *Libro bianco sulla Criminalità organizzata transnazionale*. Strasburgo: tipografia del Consiglio d'Europa, 2014, p. 38.

²³ Musacchio, Vincenzo. “Criminalità organizzata transnazionale, globalizzazione e ruolo della cooperazione internazionale”. *Articolo21*, 2018, consultabile su <https://www.articolo21.org/2018/04/criminalita-organizzata-transnazionale-globalizzazione-e-ruolo-della-cooperazione-internazionale/>

²⁴ Oddo, Giuseppe. “La mafia: da soggetto infiltrato a soggetto integrato nell'economia legale”. *Stati Generali della lotta alla criminalità organizzata: Mafie e globalizzazione*,

Rispetto al passato, il campo maggiormente potenziato dalla globalizzazione e poi sfruttato dalle organizzazioni criminali è quello del traffico di stupefacenti in cui queste adoperano le regole classiche di domanda e offerta..²⁵

L'entità della mafia globale ha un volto estremamente più moderno ed evoluto nel campo dei narcotraffici in quanto la globalizzazione permette di sfruttare reti integrate di criminali appartenenti alla più disparate aree del mondo potenziandone i traffici e raffinandone le modalità esecutive grazie al sistema della telefonia e dell'informatica..²⁶

Infine, la faccia oscura della globalizzazione, fino a questo punto analizzata, ha portato diverse organizzazioni criminali a conseguire guadagni nettamente superiori rispetto a quelli di determinate imprese o società multinazionali..²⁷

Relazione finale, a cura di Ernesto Savona, Tavolo Telematico n.1, *Transcrime*, 2023.
www.transcrime.it/wp-content/uploads/2023/02/Mafie-e-Globalizzazione_Final-report.pdf

²⁵ Oddo, Giuseppe. “La mafia: da soggetto infiltrato a soggetto integrato nell’economia legale”. *Stati Generali della lotta alla criminalità organizzata: Mafie e globalizzazione*, *Relazione finale*, a cura di Ernesto Savona, Tavolo Telematico n.1, *Transcrime*, 2023.
www.transcrime.it/wp-content/uploads/2023/02/Mafie-e-Globalizzazione_Final-report.pdf

²⁶ Marino, Giuseppe Carlo. *Globalmafia. Manifesto per un’internazionale antimafia*. Milano: Bompiani, Studio G. Due s.r.l., 2011, p. 102.

²⁷ Oddo, Giuseppe. “La mafia: da soggetto infiltrato a soggetto integrato nell’economia legale”. *Stati Generali della lotta alla criminalità organizzata: Mafie e globalizzazione*, *Relazione finale*, a cura di Ernesto Savona, Tavolo Telematico n.1, *Transcrime*, 2023.
www.transcrime.it/wp-content/uploads/2023/02/Mafie-e-Globalizzazione_Final-report.pdf

1.1.3 Le principali organizzazioni criminali transnazionali.

Le organizzazioni criminali transnazionali si espandono per il globo e spesso sono accomunate da principi ed evoluzioni apparentemente diversi ma comunque rivolti allo scopo unico di ottenere ricchezza e dominio sulle spalle della comunità globale.²⁸

La criminalità organizzata transnazionale, soprattutto a stampo mafioso, denota oggi una serie di clan, gruppi e organizzazioni strutturate ed interconnesse nel mondo economico e politico; è indubbio quindi che il mondo fa i conti tutti i giorni con differenti tipologie di mafie che vengono indicate con il nome del territorio dove sono principalmente nate e poi sviluppate: parliamo quindi di criminalità organizzata russa, cinese, italiana, messicana, albanese eccetera. ²⁹

L'attenzione più viva è quella che riescono ad attirare particolari mafie transnazionali, *in primis* per le abilità criminose incomparabili che presentano; il Giappone, per esempio, è il Paese nativo di una delle organizzazioni criminali transnazionali più note al mondo: la *Yakuza*.³⁰

L'organizzazione criminale *Yakuza* ha origini antichissime e nasce per curarsi soprattutto dei dimenticati dallo Stato, costruita sulla base di una struttura organizzativa che si discosta totalmente dall'adozione della democrazia, prediligendo il totalitarismo e la violenza; ciononostante la *Yakuza* nel tempo ha sviluppato un forte potere seduttivo grazie alle garanzie che era in grado di offrire ai suoi componenti: grazia, protezione e potere.³¹

²⁸ Colonna Vilasi, Antonella. *Mafie. Origini e sviluppo del fenomeno mafioso*. Dissensi, 2012, p. 7.

²⁹ Colonna Vilasi, Antonella. *Mafie. Origini e sviluppo del fenomeno mafioso*. Dissensi, 2012, p. 43.

³⁰ Musci, Aldo. *Tutte le mafie del mondo. Una mappa della criminalità organizzata nell'epoca della globalizzazione*. Stampa Alterativa/Nuovi equilibri, Viterbo, 2011, p 20.

³¹ Musci, Aldo. *Tutte le mafie del mondo. Una mappa della criminalità organizzata nell'epoca della globalizzazione*. Stampa alterativa/Nuovi equilibri, Viterbo, 2011, pagine 21, 22.

La *Yakuza* diviene una delle organizzazioni criminali più potenti grazie ai differenti settori in cui penetra e domina, come quello dei traffici illeciti di prostituzione, di estorsioni, di riciclaggio, di stupefacenti e di contrabbando di organi umani.³²

La *Yakuza* è promotrice soprattutto delle attività illecite legate all'industria della pornografia, che coinvolge la maggior parte delle organizzazioni criminali asiatiche come la Cina e le Filippine, dove i guadagni principali sono quelli provenienti dalla commercializzazione di film pornografici.³³

La prosecuzione dell'analisi delle mafie del mondo porterebbe poi a focalizzare l'attenzione anche sul territorio est europeo, in quanto luogo segnato dal passaggio di imponenti e pericolose organizzazioni criminali transnazionali che vale la pena analizzare se si vuole effettivamente capire come funge la macchina del crimine organizzato. Contrariamente a ciò che comunemente si ipotizza, il fenomeno dei gruppi criminali in Russia non nasce con lo scioglimento dell'*Urss*, bensì molto prima; i predecessori della criminalità organizzata russa sembrerebbero risalire ai cosiddetti Ladri nella legge, individui criminali che si attenevano ad una organizzazione strutturata sulla base di regole severe che configurava un'autentica setta segreta nata da una ideologia contrastante l'abolizione della proprietà privata imposta dal sistema del ³⁴PCUS.³⁵

Attualmente l'organizzazione dei Ladri nella legge sarebbe ancora esistente, costituita da un paio di centinaia di seguaci e perfettamente integrata nei meccanismi dell'economia russa.³⁶

³² Musci, Aldo. *Tutte le mafie del mondo. Una mappa della criminalità organizzata nell'epoca della globalizzazione*. Stampa alternativa/Nuovi equilibri, Viterbo, 2011, p. 35.

³³ Musci, Aldo. *Tutte le mafie del mondo. Una mappa della criminalità organizzata nell'epoca della globalizzazione*. Stampa alternativa/Nuovi equilibri, Viterbo, 2011, p. 36.

³⁴ PCUS: partito comunista dell'Unione Sovietica (PCUS) di stampo marxista e leninista, costituito nel 1925 guidò l'Urss fino al 1991, anno del suo scioglimento.

³⁵ Musci, Aldo. *Tutte le mafie del mondo. Una mappa della criminalità organizzata nell'epoca della globalizzazione*. Stampa Alternativa/Nuovi equilibri, Viterbo, 2011, p. 84.

³⁶ Musci, Aldo. *Tutte le mafie del mondo. Una mappa della criminalità organizzata nell'epoca della globalizzazione*. Stampa Alternativa/Nuovi equilibri, Viterbo, 2011, p. 85.

Proseguendo nella trattazione del fenomeno delle mafie nel mondo, non può che non essere citata e analizzata un'altra organizzazione criminale dai tratti spiccatamente transnazionali che appartiene al quadrante dell'America Settentrionale: la mafia messicana, cui protagonista principale è il Cartello.

Il Cartello nasce come un'organizzazione di scarso rilievo e di ristretta entità che incomincia ad occuparsi prevalentemente di contrabbando di tabacco negli U.S.A e cresce al punto tale da divenire l'organizzazione criminale transnazionale *leader* dei più grandi narcotraffici nel mondo, in grado di far circolare anche solo nel Messico il 70% e il 50% rispettivamente di cocaina e *marijuana*.

La mafia messicana rimane una delle entità criminali più complesse e studiate al livello internazionale per la struttura che presenta: estremamente decentrata, popolata da svariati sottogruppi chiamati "*cosche*" a cui si aggiungono clan minori come quello di *Tijuana*, *Sonora*, *Juarez*, *Sinaloa* eccetera.³⁷

Infine, è da considerare che una trattazione attenta a portare alla luce quelle che sono le principali organizzazioni criminali transnazionali del mondo non può che doverne analizzare un'ultima: la mafia italiana. La penisola è il territorio nativo delle più grandi e antiche organizzazioni criminali transnazionali che hanno dominato, controllato e potenziato i più imponenti traffici di attività illecite nel mondo, associazioni criminali come Cosa Nostra in Sicilia, la 'ndrangheta in Calabria e la Camorra in Campania.

Tali organizzazioni sono riuscite a colonizzare mezzo globo diffondendo e sfruttando il loro *modus operandi* del crimine organizzato basato sulla struttura familiare solida, saldata sull'onore e sull'omertà.³⁸ Attraversare la nascita e l'operato di queste organizzazioni porterebbe ad un'analisi storica e culturale estremamente vasta per essere qui trattata, per tanto, è opportuno segnalare la particolarità più importante e dannosa in grado di racchiudere le potenzialità di tali gruppi, ovvero quella inerente alla capacità di

³⁷ Musci, Aldo. *Tutte le mafie del mondo. Una mappa della criminalità organizzata nell'epoca della globalizzazione*. Stampa Alterativa/Nuovi equilibri, Viterbo, 2011, pp. 213, 214, 215.

³⁸ Musci Aldo. *Tutte le mafie del mondo. Una mappa della criminalità organizzata nell'epoca della globalizzazione*. Stampa Alterativa/Nuovi equilibri, Viterbo, 2011, pp. 233, 234.

Cosa Nostra, o della 'ndrangheta, o della Camorra, di essere perennemente interconnesse con tutte le altre mafie globali, fattore che ha permesso loro di espandersi nei mercati neri mondiali, cui è destinata l'infinita corrente di traffici che il nostro Paese è costretto a contrastare ogni giorno, spesso con scarsi risultati.³⁹

1.2 La criminalità organizzata transnazionale: uno studio sul mondo digitale del *Deep web* e *Dark web*.

Il percorso fino a qui tracciato ha rappresentato una introduzione alla tematica del crimine organizzato transnazionale, gettando le basi per la comprensione del funzionamento delle organizzazioni criminali. Alla luce di quanto esaminato, è opportuno affrontare quello che vuole essere un paragrafo dedicato a come, già da tempo, il crimine organizzato si è evoluto rispetto al passato, allertando gli Stati a dover elaborare e attuare misure coerenti e funzionali rispetto alla nuova minaccia criminosa. Attualmente, rispetto alla territorialità che legava i traffici agli Stati dove venivano attuati, il crimine organizzato viene pensato e realizzato sulle reti oscure dell'universo del *Web*. Nel contesto odierno, il concetto di *Dark web* e *Deep web* è assimilabile alle attività più oscure condotte dalle organizzazioni criminali transnazionali. È estremamente necessario trattare un'analisi consapevole degli strumenti invisibili che oggi le mafie prediligono per la realizzazione del crimine organizzato e di come questi strumenti non solo rappresentino un'opportunità per i gruppi criminali, ma anche di come costituiscano settori difficilmente accessibili e comprensibili soprattutto per le autorità di polizia internazionale, il che ne rende il contrasto un problema tutt'ora irrisolto.

1.2.1 Introduzione al *Deep web* e al *Dark web*.

La rete internet è il fulcro delle comunicazioni, dell'informazione e anche di tutte le attività socioeconomiche attuali nel mondo. Apparentemente si presenta come una unità,

³⁹ Musci Aldo. *Tutte le mafie del mondo. Una mappa della criminalità organizzata nell'epoca della globalizzazione*. Stampa Alternativa/Nuovi equilibri, Viterbo, 2011, p. 233.

facendo pensare ai suoi visitatori che tutto ciò che di *Internet* c'è da sapere sia palese ai loro occhi, eppure non è così.⁴⁰ *Internet* è un universo composto da tre sostanziali strati che vengono indicati come: *Surface web*, *Deep Web* e *Dark web*.

Il *Deep* e il *Dark web* costituiscono i due mondi più insidiosi e oscuri dell'universo virtuale per come lo conosciamo, ma prima di scoprirne il motivo è essenziale chiarire cosa sono e come funzionano. Il *Deep* e *Dark web* costituiscono entrambe le aree sommerse di *internet*, non accessibili a chiunque.

La definizione di *Deep web* è riconducibile a quella sezione della rete che a differenza del *Surface web* non risulta indicizzata nei motori di ricerca *standard*, pertanto si configura come inaccessibile, eccetto per i pochissimi utenti che ne conoscono l'esistenza.⁴¹



Immagine consultabile su www.unionepolizialeitaliana.it/2021-15/ ⁴²

⁴⁰ Costante, Massimo. *Deep web e dark web: Cos'è e come funziona la rete nascosta del deep web e il fenomeno criminale dei black market nel Dark web*. Independently published, 2021, p. 3.

⁴¹ Crapanzano, Laura. "I rischi oscuri del dark web". *Unione polizia locale italiana*, 2021, www.unionepolizialeitaliana.it/2021-15/

⁴² www.unionepolizialeitaliana.it/2021-15/

Erroneamente oggi il termine *Deep web* viene usato per indicare il *Dark net*, tuttavia questi fenomeni sono distinti e costituiscono una parte specifica del *web*. Il *Dark net* è un termine rappresentativo di un qualsiasi gruppo ristretto e chiuso di individui interconnessi che comunicano tra loro programmando attività illecite.⁴³

L'altro insidioso mondo di internet è il cosiddetto *Dark web*, un complesso di dati e contenuti modificati e resi appositamente anonimi, dunque impersonali. A differenza del *Deep web*, il *Dark web* è lo strato della rete più occulta, dove effettivamente il crimine si consuma: nel *Dark web* è presente uno smisurato traffico nero in cui avviene la compravendita di droga, materiale pornografico, armi e organi umani, rappresentando le più grandi operazioni di cui le organizzazioni criminali transnazionali si servono in totale anonimata.⁴⁴ Il carattere transnazionale degli odierni gruppi criminali è evidentemente enfatizzato dall'incidenza sempre più concreta del dominio virtuale del *Dark web*, dove l'illegalità regna indisturbata e in cui qualsiasi bene può essere oggetto di mercificazione. Il *Dark web* è il luogo ideale dove impiantare gli affari illegali dei grandi gruppi criminali in quanto è garante di un anonimato totale, grazie al quale la possibilità di risalire all'indirizzo di chi è connesso risulta nulla, così come è inattuabile la possibilità di tracciare le transazioni grazie all'utilizzo delle criptovalute o dei *bitcoin*, ossia valute anonime e ancora poco approfondite.

1.2.2 Traffici illeciti e mercato nero.

Il *Dark Net* rappresenta la casa degli odierni traffici illeciti e dell'intero mercato nero, in cui si consente di avere un rapporto diretto e anonimo con i più grandi spacciatori, trafficanti di armi o trafficanti di organi senza aver più bisogno di un soggetto che agisca

⁴³ Costante, Massimo. *Deep web e dark web: Cos'è e come funziona la rete nascosta del deep web e il fenomeno criminale dei black market nel Dark web*. Independently published, 2021, pp. 3, 10.

⁴⁴ Perego, Giorgio. "Dark web: come si entra e che succede se accedo." 2023, consultabile su www.insic.it/privacy-e-sicurezza/information-security/dark-web-come-si-entra-e-che-succede-se-accedo/#Cosa_succede_nel_Dark_Web

da tramite. Il mercato nero digitale si fonda su di un sistema all'avanguardia, perfettamente strutturato e particolarmente attento sia alla qualità delle merci che all'affidabilità dei venditori, seppure questo appaia paradossale. I traffici illegali sul mercato nero del *Dark web* attestano un guadagno che si aggira tra i trecentomila e i cinquecentomila dollari al giorno, confermando la totale inarrestabilità dei flussi.⁴⁵

Il mercato nero virtuale più importante è il *Silk Road*, un *dark-marketplace* nato nel 2011 come servizio omezzo sulla rete *Tor*⁴⁶ in cui le organizzazioni criminali transnazionali più grandi si occupano di commerciare sostanze illegali, armi e guadagnare dalla vendita di numerosi altri beni illegali; ad oggi gli oggetti protagonisti di questi traffici risulterebbero essere soprattutto i dati degli utenti, per i quali *hacker* e criminali informatici pagano elevatissimi prezzi.

Sebbene i gestori del sito furono arrestati pochi anni dopo l'apertura della piattaforma, il mercato nero online riaprì poco dopo con un nome aggiornato, ossia *Silk Road 2.0*, ideato da altri individui che hanno accresciuto sempre di più la *security* della piattaforma con misure molto più stringenti, ma comunque non sufficienti ad evitare un'ultima chiusura del mercato nel novembre del 2014.

Ad oggi entità come *Europol*, *FBI* e *NCA* sono sempre più occupate a coordinarsi a livello internazionale per svelare i traffici illeciti che esistono su diversi altri mercati neri del

⁴⁵ Forte, Monica. "Profondo nero web: la necessità di informare (e formare) giovani e adulti." *Stampoantimafioso*, 2020, consultabile sul sito www.stampoantimafioso.it/profondo-nero-web-la-necessita-di-informare-e-formare-giovani-e-adulti/

⁴⁶ Il termine *Tor* si riferisce a "The Onion Router", ossia una tipologia di browser attraverso il quale si accede al *Dark web*. È una rete creata nel 1998 tramite una tecnologia *onion routing* in grado di garantire l'anonimato nel corso della navigazione virtuale. (Sbaraglia, Giorgio. "Tor: cos'è e come usare il browser e la darknet in sicurezza per navigare nel Dark Web." *Cybersecurity*, 2022, consultabile sul sito www.cybersecurity360.it/soluzioni-aziendali/tor-cose-e-come-usarlo-in-sicurezza-per-navigare-nel-dark-web/).

Dark web, intento reso estremamente difficile dal fatto che per ogni *marketplace* illegale che viene chiuso, altri cinque nuovi ne nascono.⁴⁷

Il mercato nero è il movente dell'evoluzione della mafia: le nuove criminalità organizzate, soprattutto quelle Messicane, Cinesi, Russe e Italiane sono le protagoniste dello sfruttamento del mercato nero virtuale per espandere le loro attività di narco traffico, assodando gli *hacker* più esperti al mondo per operare su piattaforme del genere.⁴⁸

Le risorse e le potenzialità delle nuove mafie digitali, nate o evolute nel *Dark net*, rappresentano un pericolo da non sottovalutare e che nessun paese dovrebbe trascurare.⁴⁹. Nel prosieguo dell'analisi verrà osservato che il *Dark web* e il *Deep web* non sono più gli unici strumenti utilizzati per la realizzazione del *cybercrimine*, in quanto lo sviluppo digitale degli ultimi anni ha offerto alle organizzazioni criminali transnazionali degli strumenti in grado di garantire loro una quasi totale elusione del controllo da parte delle autorità di polizia internazionali, come le criptovalute, fattore che diminuirebbe le possibilità per gli Stati di arrestare il fenomeno.

⁴⁷ Hattemer, C. "Che cos'è esattamente il mercato nero del Dark Web Silk Road?" *Avira.com*, 2024, consultabile sul sito [www.avira.com/it/blog/mercato-nero-del-dark-web-silk-](http://www.avira.com/it/blog/mercato-nero-del-dark-web-silk-road?srsId=AfmBOoopZ2t7zCZGHcc1GlE354eF1saaEKubXCLPTLq4j5sbRZky0fn4)

[road?srsId=AfmBOoopZ2t7zCZGHcc1GlE354eF1saaEKubXCLPTLq4j5sbRZky0fn4](http://www.avira.com/it/blog/mercato-nero-del-dark-web-silk-road?srsId=AfmBOoopZ2t7zCZGHcc1GlE354eF1saaEKubXCLPTLq4j5sbRZky0fn4)

⁴⁸ Arena, Joska. "L'evoluzione della mafia nel cyberspazio: dal pizzo al dark web, dallo spaccio all'intelligenza artificiale". *Il Sicilia*, 2024, consultabile sul sito www.ilsicilia.it/evoluzione-della-mafia-nel-cyberspazio-dal-pizzo-al-dark-web-dallo-spaccio-allintelligenza-artificiale/

⁴⁹ Arena, Joska. "L'evoluzione della mafia nel cyberspazio: dal pizzo al dark web, dallo spaccio all'intelligenza artificiale". *Il Sicilia*, 2024, consultabile sul sito www.ilsicilia.it/evoluzione-della-mafia-nel-cyberspazio-dal-pizzo-al-dark-web-dallo-spaccio-allintelligenza-artificiale/

1.2.3 Dal *Dark web* alle criptovalute: come le monete virtuali siano il principale strumento virtuale per gestire i traffici mafiosi nel *Dark web*.

Il cambiamento e l'evoluzione negli strumenti informatici di cui le organizzazioni criminali transnazionali sono riuscite a dotarsi, ha mutato anche la denominazione odierna di tali gruppi, i quali possono essere indicati come organizzazioni criminali cibernetiche.

In particolar modo, di mafia cibernetica se ne parla principalmente quando viene trattato l'utilizzo che tali organizzazioni fanno di monete virtuali realizzate tramite un sistema di codici: le criptovalute.⁵⁰

L'utilizzo delle criptovalute nasceva con l'intento di fornire un sistema di pagamento rivoluzionario nelle transazioni online, indipendente da qualsivoglia supervisione o ingerenza governativa. La tipologia di criptovaluta più conosciuta e analizzata è il *bitcoin*, reputata come la prima criptovaluta decentralizzata e controllata tramite la *blockchain*. La *blockchain* è un sistema di crittazione che permette lo scambio di dati evitando che un determinato *file* o dato possa venire contraffatto; la caratteristica principale delle criptovalute risiede nel fatto che queste offrono l'opportunità di avere totale gestione dei propri *asset*.⁵¹

I clan mafiosi si avvalgono di *bitcoin* per realizzare il pagamento di beni, attività e sostanze che rappresentano l'oggetto principale dei traffici transnazionali sostenuti nel mercato nero del *Dark web*; in particolar modo i *bitcoin* vengono utilizzati per pagare il commercio di armi e soprattutto di umani e dei loro organi. In Italia la 'ndrangheta e Cosa Nostra sono i clan mafiosi più all'avanguardia dei nostri tempi, in quanto si servono di

⁵⁰ Le criptovalute sono delle monete virtuali decentralizzate, rappresentano il metodo di pagamento virtuale utilizzato odiernamente. (Cervi, C. "Criptovalute: cosa sono e come funzionano?". *Money.it*, 2022, consultabile su www.money.it/Criptovalute-cosa-sono-come-funzionano#google_vignette).

⁵¹ Polimeni, Francesca. "Criptovalute e cybericiclaggio: l'arma segreta della criminalità organizzata." *Giuridicamente.com*, 2022, consultabile sul sito www.giuridicamente.com/1/cryptovalute-e-cyber-riciclaggio-larma-segreta-della-criminalita-organizzata/

broker in grado di coordinare gli scambi tra trafficanti ed avventori, eludendo il sistema della *blockchain*, con la finalità ultima di esportare, in modo particolare in Sudamerica, grandi carichi di cocaina..⁵²

Infine, può affermarsi come la diretta conseguenza del vivere in un'era che offre l'utilizzo di tali strumenti configuri nuove forme di crimini posti in essere *in primis* dalle mafie cibernetiche che affinano ed evolvono sempre di più reati come il riciclaggio di proventi illeciti, finendo per reinserirli nel circuito legale. Una moltitudine di associazioni criminali, operanti a livello transnazionale, riesce ad eludere le operazioni investigative delle autorità utilizzando monete virtuali e distribuendole in portafogli del tutto ignoti. Alla luce di questa breve analisi inerente a come il crimine organizzato venga attualmente posto in essere, nel paragrafo che seguirà verrà introdotto l'ultimo strumento tecnologico caduto nelle mani delle organizzazioni criminali transnazionali: l'intelligenza artificiale.

1.3 L'IA al servizio della criminalità organizzata transnazionale.

Tutti gli strumenti virtuali fino ad ora analizzati, inglobati nel nuovo *modus operandi* utilizzato dalle organizzazioni criminali transnazionali per compiere azioni criminose, cedono il passo a quella che oggi è la forma di tecnologia esistente più avanzata: l'IA..⁵³ L'intelligenza artificiale costituisce l'ennesimo strumento di cui le organizzazioni criminali si avvalgono per la realizzazione dei traffici illeciti in quanto rappresenta l'opportunità di potenziare ed ottimizzare la resa delle attività criminose. Per tanto, sarà opportuno esaminare come le più variegate tipologie di traffici gestiti dai gruppi criminali si siano evoluti nel tempo e siano riusciti ad implementare la loro resa grazie all'utilizzo della tecnologia dell'Intelligenza Artificiale, strumento di cui le mafie riconoscono le potenzialità investendo in individui altamente formati per sfruttare al meglio le risorse dell'innovazione informatica.

⁵² Silvis, Piernicola. "Mafie e criptovalute: contro l'evoluzione tecnologica, le armi investigative sono spuntate." *Ilfattoquotidiano.it*, 2022, consultabile sul sito <https://www.ilfattoquotidiano.it/2022/07/23/mafie-e-criptovalute-contro-levoluzione-tecnologica-le-armi-investigative-sono-spuntate-3/6617135/>

⁵³ IA: formula abbreviata per indicare l'Intelligenza artificiale.

1.3.1 L'ottimizzazione delle attività illecite

Nel contesto attuale il mondo si presenta come un luogo dominato dalle interconnessioni, in cui il concetto di distanza è nullo, e in cui emerge una nuova dimensione virtuale e parallela denominata spazio cibernetico, in cui anche la criminalità organizzata si è adattata e continua a adattarsi.⁵⁴

Il *cyberspazio*⁵⁵ è il luogo nativo della mafia cibernetica, la nuova forma di criminalità organizzata transnazionale affascinata sempre più da questo spazio digitale in cui non esistono confini geografici e l'anonimato è garantito.⁵⁶

Le attività criminali delle mafie sono oggi ottimizzate non solo per l'esistenza del *cyberspazio* e di mercati neri virtuali, ma soprattutto per l'apporto dell'IA che agevola il crimine informatico di cui i soggetti principalmente coinvolti rimangono le mafie.⁵⁷

Quando vengono analizzate le attività illecite e il loro attuale potenziamento, si fa riferimento ad aspetti del crimine evoluti grazie al digitale; ad oggi il *cybercrime* legato al traffico di droga, armi o organi consta di tempistiche di pianificazione ed esecuzione estremamente ridotte grazie ad innovativi *server* che dimezzano i tempi di comunicazione

⁵⁴ Gratteri Nicola, Nicaso Antonio. *Il grifone. Come la tecnologia sta cambiando il volto della 'ndrangheta*. Milano, Mondadori, 2023, p. 2.

⁵⁵ il cyberspazio è un termine utilizzato per indicare l'insieme dei luoghi virtuali nei quali gli individui utenti sono tra loro connessi tramite una rete telematica in cui potersi muovere e interagire. (Treccani. [cyberspazio]. In Vocabolario Online. Istituto della Enciclopedia Italiana Fondata da Giovanni Treccani S.p.a. [<https://www.treccani.it/vocabolario/cyberspazio/>])

⁵⁶ Mele, Pierluigi. "Lotta alla cyber-mafia. La nuova frontiera della criminalità organizzata". *Rainews.it*, 2023, consultabile su www.rainews.it/articoli/2023/04/lotta-alla-cyber-mafia-la-nuova-frontiera-della-criminalit-organizzata-4b56f11c-4f83-4a55-8433-d4fc7c19ecd9.html

⁵⁷ Rijitano, Rosita. "Cybercrime, l'allarme dell'Interpol: "Con l'intelligenza artificiale sarà a portata di tutti". *Lavialibera.it*, 2024, consultabile sul sito www.lavialibera.it/it-schede-1781-cybercrime_interpol_intelligenza_artificiale

con i venditori e anonimizzano gli scambi realizzati tramite innovativi strumenti di trasferimento virtuale. Le organizzazioni criminali transnazionali più strutturate come la mafia nigeriana e la mafia cinese oramai sono le principali detentrici di interi capitali digitali attraverso cui attuano crimini informatici, come le frodi *fintech*, furto di *file* e dati, attacchi *ransomware* e addirittura contrabbando di esseri umani nel *dark web*, il tutto ottimizzato dall'intelligenza artificiale.⁵⁸

Le innovazioni riscontrate nel *cybercrime* destano sempre più preoccupazione per la complessa struttura degli attacchi in grado di apportare un'estrema difficoltà al controllo e all'investigazione delle autorità internazionali.⁵⁹

Alla luce delle più recenti attività investigative e di indagine nel nostro paese, soprattutto l'organizzazione criminale calabrese della 'ndrangheta risulterebbe essere la più preparata rispetto all'utilizzo di piattaforme virtuali clandestine di *trading*, per sfruttare e manipolare le aziende più potenti, con lo scopo ultimo di convincerle a vendere ai clan i crediti che vantano nei confronti della Pubblica amministrazione italiana.⁶⁰

L'ipotetica soluzione di contrasto al *cyber crime* e all'odierno utilizzo illecito dell'IA si baserebbe sull'azione di contrasto e vigilanza da parte delle autorità di controllo, attuata tramite avanzati strumenti interconnessi e dotati di una tecnologia all'avanguardia in grado di penetrare nelle reti virtuali dei traffici e distruggerli alla radice, o quanto meno complicarne l'attuazione.⁶¹

⁵⁸ Iezzi, Pierguido. “La mafia cavalca l'onda dell'innovazione digitale”. *Panorama.it*, 2023, consultabile sul sito www.panorama.it/tecnologia/cyber-security/mafia-innovazione-digitale-computer-affari

⁵⁹ Iezzi, Pierguido. “La mafia cavalca l'onda dell'innovazione digitale.” *Panorama.it*, 2023, consultabile sul sito <https://www.panorama.it/tecnologia/cyber-security/mafia-innovazione-digitale-computer-affari>

⁶⁰ Gratteri Nicola, Nicaso Antonio. *Il grifone. Come la tecnologia sta cambiando il volto della 'ndrangheta*. Mondadori, 2023, pp. 4, 5.

⁶¹ Iezzi, Pierguido. “La mafia cavalca l'onda dell'innovazione digitale”. *Panorama.it*, 2023, consultabile sul sito www.panorama.it/tecnologia/cyber-security/mafia-innovazione-digitale-computer-affari

1.3.2 Il *Dark web* è ancora l'unico strumento virtuale per delinquere? Come le nuove organizzazioni criminali transnazionali prediligano gli strumenti di IA per la realizzazione del crimine.

Il termine intelligenza artificiale è riassuntivo di numerose tecnologie che ne costituiscono la base fondante e rimanda alla complessità delle macchine coinvolte, alcune articolate al punto tale da disorientare i loro stessi inventori.⁶²

Il metaverso, per esempio, è il nuovo scenario di appoggio attraverso cui i gruppi criminosi organizzati ottengono le conquiste più grandi nel campo del crimine, un luogo in grado di permettere ai clan criminali l'accesso a qualsivoglia ambiente ideale per delinquere, soprattutto perché anonimo.⁶³ Le organizzazioni criminali moderne attuano l'attività di riciclaggio di denaro illecito grazie all'utilizzo dell'IA, esponendo una preferenza nell'utilizzare quest'ultima piuttosto che il tradizionale *Dark web*.⁶⁴

Lo scenario di passaggio dal *Dark web* all'IA da parte delle organizzazioni criminali transnazionali è oggi appurato anche dal Procuratore generale Nicola Gratteri, sempre più interessato a mettere in luce come il *Dark web*, seppur affermato come pilastro del *cyber crime*, stia cedendo il posto all'IA per la realizzazione delle attività criminose.⁶⁵

⁶² Floridi Luciano, Cabitza Federico. *Intelligenza artificiale. L'uso delle nuove macchine*. Firenze, Milano, Giunti Editore S.p.a. / Bompiani, 2021, p. 29.

⁶³ Mele, Pierluigi. "I nuovi strumenti nelle mani delle mafie del terzo millennio-Intervista a Vincenzo Musacchio." *Rainews.it*, 2024, consultabile sul sito www.rainews.it/articoli/2024/04/bitcoin-dark-web-nanotecnologie-droni-e-intelligenza-artificiale-nuovi-strumenti-nelle-mani-delle-mafie-del-terzo-millennio---intervista-a-vincenzo-musacchio-82e70793-a08d-47dd-961d-fe0e83c0a41f.html

⁶⁴ Admin-PSF. "Intelligenza Artificiale e Criminalità Organizzata." *Progettosanfrancesco.it*, 2023, consultabile sul sito www.progettosanfrancesco.it/2023/05/11/39969/

⁶⁵ Messina, Piero. "Cybercrime, il rischio cresce. Ecco delle piccole regole per difendersi dagli hacker." *Innovationisland.it*, 2024, consultabile su <https://innovationisland.it/cybercrime-italia-regole-difendersi-attacchi-hacker/> .

Le autorità internazionali di polizia più importanti, come l'Interpol, hanno evidenziato come l'utilizzo dell'IA si sia concretizzata per estendere le attività illegali di uno dei cartelli della droga più critici del Messico: il *Jalisco New Generation Cartel* che attualmente sta usufruendo dell'intelligenza artificiale non solo per potenziare i traffici di stupefacenti ma anche per attuare frodi finanziarie che stanno crescendo a ritmi allarmanti.⁶⁶

Attualmente il traffico di esseri umani, di organi umani e di stupefacenti si basano su rotte modificate dall'utilizzo dell'intelligenza artificiale che promette di moltiplicarne i proventi e reimpiegarli nel mercato per massificarne la portata. Infine, è opportuno sottolineare come a livello internazionale, gli Stati si pongano in prima linea nell'ideazione di un sistema di allerta e prevenzione riguardante tutti gli aspetti analizzati finora; a riprova di quanto osservato è rilevante ricordare che recentemente, nel 2024 tale tematica ha occupato una posizione apicale nell'agenda di discussioni del G7 dei ministri degli Esteri, tenutosi a Capri.⁶⁷

1.4 Conclusioni.

Il capitolo ha voluto offrire una panoramica introduttiva del fenomeno della criminalità organizzata transnazionale, ripercorrendo l'evoluzione storica che ha portato alla formazione delle organizzazioni criminali e analizzando le caratteristiche principali che definiscono l'entità criminale organizzata. Dopo aver evidenziato che le caratteristiche dei gruppi criminali transnazionali sono numerose e che determinano specifiche conseguenze in diversi settori sociali, può essere osservato come la realtà della

⁶⁶ GuruHiTech. "L'intelligenza artificiale sta aiutando il Cartello Messicano." *Gurutech.com*, 2024, consultabile sul sito www.guruhitech.com/lintelligenza-artificiale-sta-aiutando-il-cartello-messicano/

⁶⁷ Mele, Pierluigi. "I nuovi strumenti nelle mani delle mafie del terzo millennio-Intervista a Vincenzo Musacchio." *Rainews.it*, 2024, consultabile sul sito www.rainews.it/articoli/2024/04/bitcoin-dark-web-nanotecnologie-droni-e-intelligenza-artificiale-nuovi-strumenti-nelle-mani-delle-mafie-del-terzo-millennio---intervista-a-vincenzo-musacchio-82e70793-a08d-47dd-961d-fe0e83c0a41f.html

criminalità organizzata transnazionale non sia solo riconducibile ad un gruppo strutturato di individui che si prefigge la realizzazione di attività criminali in più Stati, bensì possa configurare un fenomeno più articolato.

Oggi le organizzazioni criminali si potenziano ancor di più implementando i loro affari con le opportunità date dall'evoluzione digitale che ha orientato le mafie a sviluppare nuove forme del crimine organizzato transfrontaliero, utilizzando le sezioni oscure del *web* e delle tecnologie moderne, come l'IA.

Nel diritto internazionale il soggetto che riveste un ruolo esclusivo in relazione al fenomeno mafioso è lo Stato, in quanto è questo il soggetto internazionale che detiene la titolarità degli obblighi di prevenzione e repressione della criminalità organizzata transnazionale. Pertanto, alla luce della centralità dello Stato rispetto a tale entità criminale, la questione rilevante che costituirà il nucleo del capitolo ruota attorno alla figura dello Stato. In particolare, nel corso della trattazione l'elaborato si concentrerà sulla responsabilità internazionale dello Stato in materia di contrasto e prevenzione delle attività criminali delle mafie, soprattutto a fronte del loro attuale potenziamento informatico. Quanto detto introdurrebbe alla tematica centrale del secondo capitolo: un'analisi giuridica inerente all'istituto della responsabilità internazionale degli Stati per crimini commessi da gruppi privati come le mafie, analisi che delineerebbe la possibilità o meno di imputare allo Stato la responsabilità internazionale per le attività illecite portate avanti e potenziate dalle organizzazioni criminali, soprattutto nell'era più proficua per la realizzazione del crimine: l'era digitale.

Capitolo 2

La responsabilità degli Stati alla luce delle azioni della criminalità organizzata transnazionale tradizionale e moderna.

Il diritto internazionale è il complesso di norme che nasce e si sviluppa sull'esigenza di regolare i rapporti fra Stati che si impegnano a loro volta a rispettare quanto imposto dall'ordinamento giuridico internazionale tramite proprie norme.⁶⁸

Nel diritto internazionale, essendo lo Stato il destinatario delle norme atte ad orientarne la condotta,⁶⁹ la disciplina inerente alla responsabilità internazionale dello Stato rappresenta un istituto cardine dell'ordinamento giuridico internazionale in quanto attraverso di esso viene garantita l'efficacia delle norme e la tutela degli interessi principali della comunità internazionale, come la sicurezza, la pace e il rispetto dei diritti umani.⁷⁰ Esso si fonda sulla volontà di assicurare alla comunità internazionale che la responsabilità per fatti internazionalmente illeciti venga imputata agli Stati nei casi in cui tali violazioni siano ad essi giuridicamente attribuibili. La responsabilità internazionale degli Stati rappresenta la disciplina che l'elaborato intende esaminare al fine di comprendere se e in che modo, in relazione alle attività illecite delle organizzazioni criminali transnazionali, lo Stato possa essere chiamato a rispondere.

Il capitolo che seguirà intende in primo luogo analizzare il concetto di responsabilità nel diritto internazionale, e successivamente di osservare l'istituto della responsabilità internazionale dello Stato per fatti di privati, esaminando i criteri di attribuzione previsti

⁶⁸ Conforti, Iovane. *Diritto Internazionale*. Editoriale Scientifica, Napoli, XII Edizione, 2021, p. 3.

⁶⁹ Conforti, Iovane. *Diritto Internazionale*. Editoriale Scientifica, Napoli, VI Edizione, 1997, p. 4.

⁷⁰ Conforti, Iovane. *Diritto Internazionale*. Editoriale Scientifico, Napoli, XII Edizione, 2021, p. 14.

per tale forma di responsabilità. Alla luce di ciò, sarà primariamente trattata la fonte non vincolante che ha codificato il diritto consuetudinario in materia di responsabilità internazionale: il Progetto di articoli sulla responsabilità degli Stati per atti internazionalmente illeciti, redatto dalla Commissione di diritto internazionale nel 2001 e successivamente adottato dall'Assemblea Generale delle Nazioni Unite.⁷¹ Il Progetto rientra nelle fonti non vincolanti del diritto internazionale in quanto non costituendo un trattato non impone obblighi giuridici agli Stati. Tuttavia, esso rappresenta un'opera di codificazione della responsabilità internazionale, ossia un'opera atta a recepire e sistematizzare il diritto internazionale consuetudinario in materia di responsabilità dello Stato; nell'elaborazione di tale opera di codificazione l'Assemblea Generale delle Nazioni Unite ha istituito la Commissione di diritto internazionale come organo tecnico avente lo scopo di promuovere la codificazione delle regole inerenti alla responsabilità dello Stato. Difatti, nel corso dell'elaborazione del Progetto la Commissione ha promosso la codificazione attraverso l'adozione progressiva dei rapporti elaborati dai membri della Commissione denominati *Special Rapporteur*, in particolare viene ricordato l'apporto di Roberto Ago a cui veniva affidato il compito di determinare la struttura e l'orientamento del Progetto.⁷²

Saranno osservati gli elementi giuridici che il Progetto prevede ai fini della configurazione della responsabilità internazionale degli Stati, sia sul piano generale, che sul piano specifico inerente alle attività illecite commesse da soggetti privati (come i gruppi criminali mafiosi transnazionali), e di come lo Stato possa esserne o meno considerato responsabile.

In tale prospettiva, verrà svolta sia l'analisi degli elementi costitutivi del fatto internazionalmente illecito, attraverso l'esame dei primi articoli del Progetto, sia l'analisi dei criteri di attribuzione della responsabilità allo Stato, nello specifico riferendosi all'articolo 8 ARSIWA, intento a sancire la *conditio sine qua non* della responsabilità internazionale degli Stati per fatti illeciti commessi dai privati, fattispecie questa che

⁷¹ International Law Commission. *Draft Articles on Responsibility of States for Internationally Wrongful Acts, with Commentaries*. United Nations, 2001.

⁷² International Law Commission. *Draft Articles on Responsibility of States for Internationally Wrongful Acts, with Commentaries*. United Nations, 2001, p. 31.

regolerebbe anche l'attribuzione della responsabilità internazionale allo Stato per i crimini commessi dai gruppi mafiosi, oggetto dell'elaborato.

In relazione a tale trattazione, fondata sulla comprensione di come lo Stato possa o meno rispondere delle attività illecite delle organizzazioni criminali tradizionali e moderne, verrà introdotto l'esame del principio internazionale della *due diligence*. Il principio di diligenza dovuta stabilisce l'obbligo per lo Stato di prevenire e reprimere attività illecite attraverso l'adozione di condotte diligenti e di misure di prevenzione e contrasto, costituendo un criterio in grado determinare l'attribuzione della responsabilità internazionale allo Stato che avesse mancato di rispettare tale obbligo. Tale meccanismo di attribuzione della responsabilità internazionale è nettamente separato da quello offerto dall'art. 8 ARSIWA che consiste invece nello stabilire l'attribuzione della condotta illecita dei privati direttamente allo Stato nel caso in cui esso dirigesse o controllasse comportamenti idonei a violare obblighi internazionali. L'analisi di tale principio sarà funzionale a comprendere in che misura lo Stato, seppur non direttamente responsabile per illeciti di privati ai sensi degli ARSIWA, possa essere ritenuto responsabile sulla base del diverso meccanismo della *due diligence*, qualora lo Stato omettesse di adempiere all'obbligo di diligenza dovuta atto ad imporre misure di prevenzione e contrasto degli illeciti internazionali attuati dai privati.⁷³

Dopo un'analisi generale del concetto e della portata della *due diligence* nel diritto internazionale, particolare attenzione sarà dedicata agli scenari giuridici internazionali che si configurano nei casi in cui uno Stato manchi di rispettare la *due diligence* necessaria, in particolar modo riferendosi la trattazione all'ipotesi di omessa *due diligence* per fatti illeciti commessi da privati, nello specifico dalle organizzazioni criminali transnazionali a stampo mafioso.

Trattando l'elaborato anche dell'evoluzione cibernetica dei crimini organizzati, e volendo proseguire nell'esame atto a stabilire in che modo il diritto internazionale attribuisca o meno responsabilità internazionale dello Stato rispetto ai crimini tradizionali e moderni delle organizzazioni criminali, il principio internazionale della *due diligence* continuerà ad essere preso in considerazione anche al fine di valutare se il diritto internazionale

⁷³ Akingbade, Adedayo. "Due Diligence in International Law: Cause for Optimism?". *Irish Yearbook of International Law*, vol. 15, 2020, p 48.

configuri o meno l'attribuzione della responsabilità internazionale allo Stato in relazione alle conseguenze dannose che derivano dalla realizzazione dei *cybercrimes* delle organizzazioni criminali nello spazio virtuale, che lo Stato è chiamato a prevenire e reprimere.

Alla luce di ciò, verrà esaminato in che modo il concetto della *due diligence* è applicato anche al dominio cibernetico; in particolare verrà osservato come il mancato adempimento della *due diligence* informatica rappresenti un criterio idoneo a configurare responsabilità internazionale dello Stato che ha omesso di agire con la diligenza dovuta nel contrasto alle condotte illecite realizzate dalle organizzazioni criminali in particolare dalle mafie, non più sulla base dell'attribuzione del crimine allo Stato, bensì sull'ascrizione delle conseguenze negative che dall'illecito cibernetico possono derivare nel caso in cui lo Stato manchi di attuare la diligenza dovuta nello spazio virtuale.

Di conseguenza, il presente elaborato vuole prima porre in evidenza il grado di *due diligence* richiesto agli Stati chiamati a garantire l'attuazione della diligenza dovuta nelle proprie azioni di contrasto alle attività illecite cibernetiche potenzialmente ascrivibili alle organizzazioni mafiose attuali, e successivamente dimostrare se nel diritto internazionale possa dirsi possibile che uno Stato risponda dei *cybercrimes* delle organizzazioni criminali per omessa *due diligence* nelle azioni di contrasto e repressione condotte dallo Stato nello spazio cibernetico.

A supporto di tale analisi, il capitolo prenderà in esame il caso degli attacchi cibernetici attribuiti alla criminalità organizzata Russa, con l'intento di valutare ed analizzare nel concreto il comportamento dello Stato russo e, in particolare modo, di provare se lo standard di *due diligence* adottato da parte della Russia possa o meno aver portato alla configurazione di responsabilità internazionale dello Stato in materia.

2.1 Il concetto di responsabilità nel diritto internazionale.

Il concetto della responsabilità nel diritto internazionale nasce a partire dagli inizi del '900. La disciplina della responsabilità internazionale sorge dall'impossibilità del diritto interno dei singoli ordinamenti di imporre obblighi o di stabilire le conseguenze di violazioni internazionali agli Stati e conseguentemente di riuscire a determinare la

responsabilità degli Stati in caso di condotte o attività che configurano una violazione del diritto internazionale.⁷⁴

Le origini dell'istituto della responsabilità internazionale degli Stati risalgono a numerosi contributi di indagine, ricerca e codificazione da parte degli studiosi internazionali Anzilotti e Ago, che hanno apportato una svolta incisiva nella codificazione dell'istituto, ufficialmente presentato nel 2001 con l'approvazione del Progetto di articoli sulla responsabilità internazionale degli Stati da parte della CDI (Commissione di Diritto Internazionale).⁷⁵ Un apporto significativo per la codificazione del Progetto è rappresentato dalla teoria sulla responsabilità internazionale di Anzilotti che già nel 1902 si concentrava ad analizzare e teorizzare la duplice dimensione dell'istituto della responsabilità internazionale; difatti Anzilotti sviluppa la sua concezione nello scritto "Teoria generale della responsabilità dello Stato nel diritto internazionale." (Anzilotti 1902).⁷⁶, in cui ha sostenuto come la responsabilità dello stato si configurasse tanto per le azioni illecite commissive, quanto per le omissioni o le negligenze.⁷⁷

È opportuno osservare come nel diritto internazionale il Progetto rappresenti una fonte di *soft law* che ha codificato il diritto consuetudinario in tema di responsabilità internazionale. Nonostante la natura non vincolante del Progetto, tale opera di codificazione ha assunto un ruolo incisivo nell'orientare la prassi degli Stati e l'operato dei tribunali arbitrali internazionali che hanno semplificato la determinazione della

⁷⁴ Conforti, Iovane. *Diritto Internazionale*. Edizione Scientifica, Napoli, XII Edizione, 2021, pp. 418, 419.

⁷⁵ Conforti, Iovane. *Diritto Internazionale*. Edizione Scientifica, Napoli, XII Edizione, 2021, pp. 418, 419.

⁷⁶ Anzilotti, Dionisio. *Teoria generale della responsabilità dello Stato nel diritto internazionale (General theory of state responsibility in international law)*. Firenze, Lumachi editore, 1902.

⁷⁷ Nolte, Georg. "From Dionisio Anzilotti to Roberto Ago: The Classical International Law of State Responsibility and the Traditional Primacy of a Bilateral Conception of Inter-state Relations." *European Journal of International Law*, Volume 13, 2002, pp. 1083, 1084.

responsabilità internazionale e l'attribuzione dei fatti illeciti attraverso l'utilizzo dei principi codificati negli ARSIWA.⁷⁸

Il regime normativo della responsabilità internazionale degli Stati assume però connotazioni differenti a seconda del contesto in cui viene analizzata la tematica, in quanto dopo la codificazione del Progetto del 2001 si è reso palese che alcune parti di questo non codificassero pienamente il diritto consuetudinario, per esempio laddove il Progetto prevedeva regole più gravose per lo Stato responsabile in tema di contromisure, rispetto a quanto previsto dal diritto generale.⁷⁹

Nel quadro dell'ordinamento giuridico internazionale in generale, il tema della responsabilità internazionale detiene una rilevanza cardine in quanto lo Stato, sebbene non sia l'unico, rimane il principale destinatario della maggior parte degli obblighi internazionali di maggiore entità, come ripreso dalla Corte internazionale di Giustizia nel 1970, con la sentenza relativa al caso *Barcelona Traction*⁸⁰, in cui affermando come la responsabilità costituisca la necessaria conseguenza del diritto, la Corte si riferisce al fatto che è principalmente lo Stato a rispondere degli illeciti internazionali e che la conseguenza automatica della violazione di una norma internazionale sia la responsabilità statale.⁸¹

Proseguendo con l'analisi della disciplina della responsabilità internazionale degli Stati, viene osservato come questa sia contraddistinta da una natura autonoma.⁸²

Tale autonomia assume due forme: interna ed esterna. L'autonomia interna si riferisce al fatto che la disciplina sia autonoma rispetto ad altre appartenenti all'ordinamento

⁷⁸ Vengono ricordati i casi *Yokos v. Russia* (PCA, 2014) in cui il tribunale ha accertato la responsabilità del governo russo per esproprio e violazioni del diritto internazionale, ed il caso *Biwater Gauff v. Tanzania* (ICSID, 2008) in cui il tribunale ha accertato la responsabilità della Tanzania per danni causati dall'omissione di obblighi internazionali ai danni degli investitori.

⁷⁹ Pustorino, Pietro. *La responsabilità degli Stati*. Annali, VII, 2014, p. 909

⁸⁰ International Court of Justice. *Barcelona Traction, Light and Power Company, Limited Second Phase*, Judgment, I.C.J., Reports, 1970, para 36, p. 3.

⁸¹ Pustorino, Pietro. *La Responsabilità degli Stati*. Annali, VII, 2014, p. 910.

⁸² Pustorino, Pietro. *La Responsabilità degli Stati*. Annali, VII, 2014, p. 910.

internazionale, mentre l'autonomia esterna si riferisce al fatto che la disciplina della responsabilità internazionale sia indipendente e distaccata dai sistemi giuridici nazionali; di conseguenza ciò che rileva come comportamento lecito o illecito nel diritto interno potrebbe non rilevare nella disciplina della responsabilità internazionale ai fini della sua configurabilità.⁸³

Essendo l'elaborato intento a provare se uno Stato possa o meno essere chiamato a rispondere delle attività realizzate da gruppi criminali, l'aspetto dell'autonomia dell'istituto appena osservato appare estremamente rilevante, poiché permette di affermare come la responsabilità dello Stato possa configurarsi indipendentemente da quella degli autori dell'illecito, il che consente di valutare la condotta statale sulla base della violazione di obblighi internazionali propri, come quelli di prevenzione, la cui inosservanza potrebbe condurre all'imputazione della responsabilità in capo allo Stato, nonostante i crimini siano commessi da soggetti privati, come quelli mafiosi.

Il carattere dell'autonomia della responsabilità internazionale fu principalmente teorizzato da Roberto Ago⁸⁴, il quale dimostrò come la responsabilità internazionale dello

⁸³ Pustorino, Pietro. *La Responsabilità degli Stati*. Annali, VII, 2014, pp. 910-911.

⁸⁴ Roberto Ago, nato nel 1907 è considerato uno tra i più celebri giuristi internazionali del XX secolo. Ad oggi viene ricordato non solo per la sua carriera all'interno della Commissione di diritto Internazionale e della ICJ, di cui fu rispettivamente presidente e giudice, ma soprattutto come una tra le figure più importanti per il suo grande contributo di codificazione moderna del diritto internazionale.

Stato fosse una disciplina autonoma del diritto internazionale⁸⁵, non riconducibile alle altre discipline di diritto privato inerenti alla responsabilità civile.⁸⁶

Nonostante l'evoluzione che la responsabilità internazionale ha subito nel tempo con le concezioni appena menzionate, ciò che parrebbe non essere mutata fin dalla sua codificazione è la nozione di responsabilità internazionale, attualmente contenuta all'art. 1 del Progetto.⁸⁷

Tale impostazione riflette l'importanza di mantenere la nozione di responsabilità internazionale fondata sulla violazione di un obbligo internazionale e sulla volontà degli Stati di assumere tali obblighi, espressione della loro sovranità.⁸⁸

⁸⁵ L'apporto di Ago sull'autonomia della responsabilità internazionale è stato seguito dal processo di oggettivizzazione, un processo che ha portato la responsabilità internazionale a configurarsi sulla base della violazione di un obbligo internazionale, anche in assenza di danno concreto. Si parla di danno in quanto questo prima dell'oggettivizzazione del concetto di responsabilità internazionale, era un criterio centrale per l'accertamento della responsabilità, sia che si trattasse di responsabilità per atti internazionalmente illeciti, sia che si trattasse di atti non vietati dal diritto internazionale. Il danno continuava a costituire il punto cardine sia della responsabilità internazionale che della *liability*, ossia della responsabilità oggettiva. Il processo di oggettivizzazione portò all'eliminazione dell'elemento del danno come *conditio sine qua non* della responsabilità dello Stato per atti internazionalmente illeciti. (Crawford James, Pellet Alain, Olleson Simon, Parlett Kate. *The law of International Responsibility*. Oxford Commentaries on International Law, Oxford, Oxford University Press, 2010, pp. 10, 11, 12).

⁸⁶ Crawford James, Pellet Alain, Olleson Simon, Parlett Kate. *The law of International Responsibility*. Oxford Commentaries on International Law, Oxford, Oxford University Press, 2010, pp. 7, 8, 9, 11.

⁸⁷ Crawford James, Pellet Alain, Olleson Simon, Parlett Kate. *The law of International Responsibility*. Oxford Commentaries on International Law, Oxford, Oxford University Press, 2010, p. 199.

⁸⁸ Crawford James, Pellet Alain, Olleson Simon, Parlett Kate. *The law of International Responsibility*. Oxford Commentaries on International Law, Oxford, Oxford University Press, 2010, p. 200.

2.1.1 Il ruolo del Progetto ARSIWA nella codificazione della responsabilità internazionale degli Stati.

L'esame dell'evoluzione dottrinale del concetto di responsabilità nel diritto internazionale, di cui sopra, verrà qui fatta seguire da un'analisi del Progetto ARSIWA e del ruolo che questo ha rivestito nell'evoluzione concettuale dell'istituto della responsabilità internazionale. Il Progetto ARSIWA costituisce una fonte non vincolante del diritto internazionale in quanto non è idonea a creare obblighi giuridici direttamente vincolanti per gli Stati, difatti il Progetto rientra tra le fonti di *soft law* del diritto internazionale.

L'opera di codificazione del Progetto della Commissione di Diritto Internazionale, che al tempo ricopriva il ruolo di organo tecnico nei lavori di elaborazione del Progetto, sebbene costituisca una fonte di *soft law* rappresenta ad oggi il riferimento principale con riguardo alla materia della responsabilità statale, ed è l'esito di decenni di lavori atti al suo perfezionamento.⁸⁹

L'intero Progetto, infatti, è stato il risultato di complessi lavori di elaborazione, revisione e controllo, il che suggerisce come il tema della responsabilità internazionale possa essere stata fonte di grandi difficoltà nel processo di codificazione.⁹⁰

Sebbene nel 1956 l'iter di codificazione incominci con l'analisi della tematica della responsabilità dello Stato per i danni arrecati alle persone e alle proprietà dello straniero, successivamente il focus dei lavori, sottoposti alla guida dello *Special Rapporteur Ago*, si muove verso la necessità primaria di trovare una definizione alle regole generali poste a fondamento della responsabilità dello Stato, portando a non considerare più l'elemento del danno come pilastro fondante l'istituto della responsabilità internazionale, sulla scia

⁸⁹ Kinnear, Meg. "ARSIWA, ISDS, and the Process of Developing an Investor-State Jurisprudence". *ICSID Reports* 20, Cambridge University Press, 2022, p. 3, Web.

⁹⁰ Esposito Carlos, Parlett Kate. *The Cambridge Companion to the International Court of justice*. Cambridge Companions to Law, Cambridge University Press, 2023, p. 417.

delle idee sviluppate dall'Anzilotti già nel 1929.⁹¹ Il lavoro delle restanti parti del Progetto continuò sulla scia di ulteriori *Special Rapporteur*, come Arangio Ruiz che operò sulla parte seconda e terza del Progetto.⁹² I lavori terminarono con l'adozione della prima stesura dei *Draft Articles* da parte della Commissione. ⁹³

Nel 2001, dopo più di quaranta anni di lavoro, il Progetto viene presentato dalla Commissione di Diritto Internazionale e approvato, insieme ad un corpus di commenti inerenti ai singoli articoli, con la risoluzione 56/83.⁹⁴ del 2002 da parte dell'Assemblea Generale delle Nazioni Unite.⁹⁵

Nel diritto internazionale gli ARSIWA (*Articles on Responsibility of State for Internationally Wrongful Acts*) rivestono un ruolo giuridico preciso: quello di norme secondarie, in quanto non impongono agli Stati obblighi sostanziali, bensì descrivono gli elementi che configurano l'attribuzione e le conseguenze giuridiche che derivano dalla violazione di norme primarie. Nel diritto internazionale rileva la distinzione tra norme primarie e norme secondarie. Le norme primarie impongono degli obblighi agli Stati, statuendo inoltre cosa costituisca una violazione del diritto. Le norme secondarie invece

⁹¹ Sabino, Marta. *Il Regime di responsabilità degli Stati nella prassi degli organi di controllo delle convenzioni a carattere regionale sui diritti umani. Tra frammentazione e sviluppo progressivo del diritto internazionale*. Tesi di dottorato, Università degli Studi di Roma "La Sapienza", 2025, pp. 69, 70.

⁹² Sabino, Marta. *Il Regime di responsabilità degli Stati nella prassi degli organi di controllo delle convenzioni a carattere regionale sui diritti umani. Tra frammentazione e sviluppo progressivo del diritto internazionale*. Tesi di dottorato, Università degli Studi di Roma "La Sapienza", 2025, pp. 69, 70.

⁹³ Sabino, Marta. *Il Regime di responsabilità degli Stati nella prassi degli organi di controllo delle convenzioni a carattere regionale sui diritti umani. Tra frammentazione e sviluppo progressivo del diritto internazionale*. Tesi di dottorato, Università degli Studi di Roma "La Sapienza", 2025, p. 70.

⁹⁴ United Nations General Assembly. *Responsibility of States for Internationally wrongful acts*. A/res/56/83, United Nations, 28 January 2002.

⁹⁵ Kinnear, Meg. "ARSIWA, ISDS, and the Process of Developing an Investor–State Jurisprudence". *ICSID Reports* 20, Cambridge University Press, 2022, p. 3, Web

configurerebbero tutte quelle regole che si limitano a stabilire le conseguenze giuridiche che discendono dalla violazione di una norma primaria, ossia dall'inosservanza di un obbligo internazionale.

Difatti, gli articoli del Progetto identificano gli elementi atti alla configurazione dell'illecito internazionale, stabiliscono le condizioni necessarie affinché un determinato illecito possa essere attribuito allo Stato e infine prevedono le conseguenze giuridiche che discendono dalla violazione internazionale posta a fondamento della responsabilità configurata.⁹⁶ Per concludere, è opportuno osservare che proprio la natura delle norme secondarie del Progetto è un tema molto dibattuto in dottrina in quanto questa tende a separarsi tra il pensiero di Anzilotti e Ago, e quello della dottrina più recente.

Le norme secondarie contenute negli ARSIWA vengono configurate come neutrali e indipendenti dalle norme primarie, ovvero come norme che, seppure derivanti dalla violazione di obblighi primari, stabiliscano conseguenze giuridiche autonome, nonostante queste originino dalla violazione di obblighi primari.

Tale impostazione ha subito diverse critiche da parte della dottrina moderna, come nel caso del giurista indiano B.S. Chimni che ha osservato come: *"The assumption that secondary rules are completely decoupled from the primary rules of state responsibility is a fundamental flaw of ARSIWA."*⁹⁷

La dottrina moderna, come quella di Chimni, criticerebbe l'impostazione originaria in quanto fittizia, ribadendo che la separazione tra le norme primarie e secondarie non possa essere possibile alla luce della stretta connessione delle seconde rispetto alle prime.

Per concludere, viene osservato che la concezione delle norme secondarie del Progetto come indipendenti e neutrali è rimasta inalterata, e tale opera di codificazione si è confermata come il riferimento principale per la disciplina della responsabilità internazionale.

⁹⁶ Kinnear, Meg. "ARSIWA, ISDS, and the Process of Developing an Investor–State Jurisprudence". *ICSID Reports* 20, Cambridge University Press, 2022, p. 3, Web.

⁹⁷ Chimni, B. S. "The Articles on State responsibility and the Guiding Principles of Shared Responsibility: A TWAIL Perspective". *The European Journal of International Law*, Vol. 31, no. 4, Oxford University Press, 2020, p. 1213.

2.1.2 La responsabilità dello Stato nel diritto internazionale.

Avendo osservato i profili generali sia dell'evoluzione concettuale della responsabilità internazionale, sia del contributo del Progetto di articoli della CDI, l'attenzione sarà ora rivolta all'analisi della figura dello Stato in ambito di responsabilità internazionale, in particolare individuando i soggetti le cui condotte illecite possano essere attribuite allo Stato. Nel diritto internazionale le regole che sono state codificate in tema di responsabilità si fondano sulla figura dello Stato considerato il principale destinatario del regime di responsabilità internazionale; quanto osservato viene ribadito anche dalla dottrina di Conforti e Iovane che osservano come: *“quanto si dirà sulla responsabilità degli Stati vale anche, mutatis mutandis, per gli altri soggetti internazionali ad esclusione degli individui la cui responsabilità, sostanzandosi nella loro punizione nel caso di crimini internazionali, è regolata da norme che attengono al campo del diritto (internazionale) penale.”*⁹⁸ Quanto osservato da Conforti e Iovane pone in evidenza la centralità dello Stato in tema di responsabilità, sottolineando come il regime di responsabilità sia stato concepito principalmente sulla figura dello Stato, per poi essere applicato *mutatis mutandis* sugli altri soggetti internazionali, ad eccezione degli individui per i quali la responsabilità in questione è regolata dal diritto internazionale penale.

Difatti, anche per altri soggetti del diritto, come per le organizzazioni internazionali, è stata premura della Commissione di diritto internazionale riservare nel 2011, sulla scia del Progetto del 2001, una serie di articoli (ARIO)⁹⁹ circa la responsabilità delle organizzazioni internazionali che in larga parte si conformano alle già codificate regole in tema di responsabilità internazionale degli Stati.¹⁰⁰

⁹⁸ Conforti, Iovane. *Diritto Internazionale*. Edizione Scientifica, Napoli, XII Edizione, 2021, p. 420.

⁹⁹ D'Aspremont, Jean. “The Articles on the Responsibility of International Organizations: Magnifying the Fissures in the Law of International Responsibility”. *International Organizations Law Review*, vol. 9, no. 1, 2012, p. 15.

¹⁰⁰ Conforti, Iovane. *Diritto Internazionale*. Edizione Scientifica, Napoli, XII Edizione, 2021, p. 420.

L'istituto della responsabilità internazionale degli Stati si fonda su due elementi principali che rappresentano le condizioni necessarie per la configurazione della responsabilità internazionale: l'elemento oggettivo e l'elemento soggettivo.¹⁰¹

L'elemento oggettivo si riferisce all'atto internazionalmente illecito, che si configurerebbe quando, tramite una condotta commissiva o omissiva, viene violato un obbligo internazionale dello Stato, come statuito dall'articolo 2 lett. b del Progetto.¹⁰²

L'elemento soggettivo invece, si sostanzia nel criterio di imputabilità dell'illecito allo Stato, quindi nella riconducibilità della responsabilità internazionale a questo.

Alla luce del fatto che la trattazione vuole analizzare quali siano i soggetti di cui lo Stato assume la responsabilità nel caso di illeciti, l'analisi si concentra sull'elemento soggettivo dell'illecito. Tale profilo genera una complessità maggiore rispetto a quello oggettivo, in ragione della coincidenza che intercorre tra Stato e le articolazioni di questo; per esempio, vi è un confine sottile che intercorre tra Stato inteso come soggetto di diritto internazionale e Stato organizzazione inteso come apparato organizzativo.¹⁰³

Tale coincidenza si fonda sull'assunto che lo Stato, identificandosi attraverso gli organi che lo compongono, risponde delle azioni illecite degli stessi.¹⁰⁴

Alla luce di tale aspetto rileva la distinzione tra organo *de iure*, ossia quello che viene istituito legittimamente sulla base delle leggi interne statali, e l'organo *de facto* che seppur non legittimamente istituito dal diritto interno, assume funzioni pubbliche. Sebbene gli organi *de facto* non siano organi ufficiali dello Stato, al fine di garantire che in caso di illeciti compiuti da questi lo Stato non si sottragga alla responsabilità internazionale in

¹⁰¹ United Nations. *State Responsibility. Yearbook of the International Law Commission*, Volume 2, 1976, p. 75.

¹⁰² United Nations, International Law Commission. *Project of articles on International Responsibility of States for Internationally Wrongful Acts. With commentaries*. In *Yearbook of International Law Commission*, 2001, vol. II, chapter I, article 2, lett. b., p. 2.

¹⁰³ Conforti, Iovane. *Diritto internazionale*. Edizione Scientifica, Napoli, XII Edizione, 2021, pp. 421, 422.

¹⁰⁴ Conforti, Iovane. *Diritto internazionale*. Edizione Scientifica, Napoli, XII Edizione, 2021, p. 422.

virtù dell'aspetto non ufficiale di tali organi, la disciplina della responsabilità internazionale prevede che anche gli illeciti compiuti dagli organi *de facto* siano imputabili allo Stato. Per quanto concerne gli organi *de jure* l'articolo 4 ARSIWA sancisce l'attribuibilità allo Stato delle condotte di organi che esercitino funzioni legislative, giudiziarie, esecutive o altre: “*whatever position it holds in the organization of the State.*”¹⁰⁵

Per gli organi *de facto* invece la disciplina è contenuta all'articolo 5 ARSIWA che statuisce come: “*The conduct of a person or entity which is not an organ of the State under the articles 4 but which is empowered by that State to exercise elements of the governmental authority shall be considered an act of the State under international law, provided the person or entity is acting in that capacity in the particular instance.*”¹⁰⁶

L'impostazione degli articoli 4 e 5 ARSIWA riflette l'attribuzione piena della responsabilità nei confronti dello Stato, espandendo l'ambito dell'elemento soggettivo di attribuzione in quanto viene previsto che qualsiasi organo agisca in modo illecito, che sia un apparato *de iure* o un apparato *de facto* dello Stato sarà lo Stato a rispondere sul piano internazionale.

Viene poi specificato all'articolo 7 ARSIWA¹⁰⁷ come lo Stato sia responsabile anche nel caso in cui l'illecito sia compiuto dall'organo *de facto* o *de iure* che ha deciso di porre in essere atti *ultra vires*¹⁰⁸ o abbia violato il diritto interno, questo poiché ai fini

¹⁰⁵ International Law Commission. *Responsibility of States for Internationally Wrongful Acts*. United Nations, 2001, chapter II, art. 4, p. 2.

¹⁰⁶ United Nations, International Law Commission. *Project of articles on International Responsibility of States for Internationally Wrongful Acts. With commentaries*. In Yearbook of International Law Commission, 2001, vol. II, chapter II, art. 5, p.3.

¹⁰⁷ United Nations, International Law Commission. *Project of articles on International Responsibility of States for Internationally Wrongful Acts. With commentaries*. In Yearbook of International Law Commission, vol. II, chapter II, art. 7, p.3.

¹⁰⁸ Gli atti *ultra vires* costituiscono tutte quelle azioni che gli organi statali compiono in rappresentanza dello Stato che tuttavia vengono attuati eccedendo le proprie competenze.

dell'attribuzione la violazione del diritto interno rileva comunque come atto dello Stato a livello internazionale.¹⁰⁹

Tale impostazione ex articolo 7 del Progetto riflette quanto deciso dalla Corte Internazionale di Giustizia nel caso *Congo v Uganda* del 19 dicembre 2005.¹¹⁰ In riferimento all'attribuzione delle condotte illecite degli organi allo Stato, tale caso ha confermato l'attribuzione della responsabilità internazionale ai sensi dell'art. 4 nei confronti dell'Uganda per le azioni illecite commesse dai suoi organi di polizia nei confronti del Congo, e inoltre, ha chiarito che all'Uganda venivano imputati anche gli atti *ultra vires* compiuti da tali organi.¹¹¹

Le forme di attribuzione fin qui osservate non si arrestano all'ascrizione allo Stato degli illeciti realizzati dai propri organi, bensì comprendono una ulteriore fattispecie attributiva inerente all'imputazione allo Stato della responsabilità per illeciti commessi da figure private, ossia da attori non statali.

Tale fattispecie sarà esaminata nello specifico al punto 2.1.3, poiché risulta centrale nell'analisi principale dell'elaborato volto ad analizzare la possibilità di ricondurre o meno le azioni dei gruppi criminali privati transnazionali alla responsabilità dello Stato, analizzando tutti i criteri di attribuzione previsti dal diritto internazionale.

2.1.3 Il criterio di attribuzione della condotta illecita dei privati allo Stato: l'articolo 8 del Progetto ARSIWA.

L'analisi precedentemente condotta ha voluto introdurre l'istituto della responsabilità internazionale degli Stati, andando ad esaminare gli elementi necessari che il diritto internazionale richiede per la configurazione della responsabilità internazionale. In

¹⁰⁹ Conforti, Iovane. *Diritto internazionale*. Edizione Scientifica, Napoli, XII Edizione, 2021, pp 424, 425.

¹¹⁰ International Court of Justice. *Armed Activities on The Territory of the Congo (Democratic Republic of the Congo v. Uganda)*. International Courts of Justice, Judgement of 19 December 2005, I.C.J. Reports 2005.

¹¹¹ Conforti, Iovane. *Diritto internazionale*. Edizione Scientifica, Napoli, XII Edizione, 2021, p. 425.

particolare, l'analisi dell'elemento soggettivo della responsabilità statale che ha portato ad esaminare i vari soggetti i cui illeciti possono essere ricondotti allo Stato, conduce ora ad osservare la fattispecie che riguarda l'attribuzione delle condotte illecite dei privati allo Stato, regolata dall'articolo 8 ARSIWA.

Alla luce del fatto che l'elaborato è incentrato sull'analisi della possibilità di imputare allo Stato responsabilità internazionale per illeciti delle organizzazioni criminali, l'articolo 8 ARSIWA risulta direttamente pertinente alla fattispecie centrale dell'elaborato, in quanto rappresenta la norma atta a regolare l'imputazione allo Stato delle condotte dei privati, una categoria che comprenderebbe al suo interno anche gruppi di individui che d'accordo realizzano illeciti, come le mafie.

L'articolo 8 ARSIWA, disciplinando la: "*Conduct directed or controlled by a State.*"¹¹², statuisce come: "*The conduct of a person or group of persons shall be considered an act of a State under international law if the person or group of persons is in fact acting on the instructions of, or under the direction or control of, that State in carrying out the conduct.*"¹¹³

Il diritto internazionale, come principio generale, non tende ad attribuire allo Stato le condotte dei privati o di entità non statali in virtù del fatto che la responsabilità si fonda solo su azioni che siano espressione della volontà sovrana, in quanto solo gli illeciti commessi da organi dello Stato o da organi da esso controllati possono portare alla configurazione della responsabilità internazionale.¹¹⁴ Tuttavia, attraverso l'introduzione dell'articolo 8 ARSIWA il diritto internazionale ha previsto che a determinate condizioni, le condotte illecite di soggetti privati possano essere imputate allo Stato, costituendo

¹¹² United Nations, International Law Commission. *Project of articles on International Responsibility of States for Internationally Wrongful Acts*. In Yearbook of International Law Commission, 2001, vol. II, chapter II, article 8, p. 3.

¹¹³ United Nations, International Law Commission. *Project of articles on International Responsibility of States for Internationally Wrongful Acts*. In Yearbook of International Law Commission, 2001, vol. II, chapter II, article 8, p. 3.

¹¹⁴ Conforti, Iovane. *Diritto internazionale*. Edizione Scientifica, Napoli, XII Edizione, 2021, p. 422.

un'eccezione alla regola secondo cui la responsabilità internazionale viene attribuita allo Stato sulla base della volontà sovrana.¹¹⁵

Più precisamente la fattispecie dell'articolo 8 è stata l'unica in grado di ampliare l'ambito di imputazione non più solo agli organi statali in senso stretto, ma anche a tutti quei gruppi o soggetti che, seppur privati, operano in modo tale da configurare lo Stato come responsabile internazionalmente al verificarsi di determinate condizioni.

Invero, le due condizioni poste a fondamento della possibile imputabilità statale sono la direzione e il controllo esercitati dallo Stato stesso sulle condotte illecite dei privati, entrambe debbono risultare effettive affinché dei crimini realizzati da questi possa risponderne lo Stato, altrimenti la norma finirebbe per addossargli la responsabilità in via occulta e ingiustificata.¹¹⁶

In particolar modo, il criterio del controllo è quello che richiede un livello di effettività concreto, come confermato dalla giurisprudenza internazionale nel caso *Nicaragua vs. Stati Uniti*.¹¹⁷ (CIG, 1986), in cui la Corte ha elaborato il preciso criterio del: “*effective control*”¹¹⁸ per poter attribuire la responsabilità internazionale degli illeciti di gruppi privati allo Stato americano. Quanto detto si fonda sull'assunto che l'influenza che lo Stato deve esercitare deve apparire elemento concreto dell'atto illecito contestato.¹¹⁹

Le condizioni di attribuibilità previste dall'articolo 8 quali l'istruzione il controllo effettivo e la direzione si configurano come disgiuntivi, pertanto per integrare quanto statuito dall'articolo basterà che si manifesti anche solo una condizione tra queste e non

¹¹⁵ United Nations. *Draft Articles on Responsibility of States for Internationally Wrongful Acts, With Commentaries*. United Nations, 2008, p.47.

¹¹⁶ United Nations. *Draft Articles on Responsibility of States for Internationally Wrongful Acts, With Commentaries*. United Nations, 2008, p.47. (1, 2).

¹¹⁷ Corte Internazionale di Giustizia. *Attività militari e paramilitari in e contro il Nicaragua (Nicaragua c. Stati Uniti D'America)*. I.C.J. Reports, 1986.

¹¹⁸ Corte internazionale di Giustizia. *Attività militari e paramilitari in e contro il Nicaragua (Nicaragua c. Stati Uniti D'America)*. I.C.J. Reports, 1986, p. 14, para. 115.

¹¹⁹ United Nations. *Draft Articles on Responsibility of States for Internationally Wrongful Acts, With Commentaries*. United Nations, 2008, p.47, para. 115 (1, 2).

necessariamente tutte e tre.¹²⁰ Inoltre, va sottolineato che la direzione, il controllo o l'istruzione debbono sempre riferirsi alla condotta illecita posta in essere, in quanto sarebbe questa a configurare l'atto internazionalmente illecito.¹²¹ Come accennato precedentemente, il profilo che qui rileva dell'articolo 8 è quello inerente alla sfera soggettiva dei destinatari della norma. Il fatto che la norma si riferisca a soggetti quali le persone o i gruppi di persone è sintomo della volontà del legislatore internazionale di ricomprendere le aggregazioni di individui prive di un riconoscimento giuridico formale ma che agiscono *de facto* in modo coordinato e continuativo.¹²² Pertanto, è giuridicamente lecito porre in relazione la categoria delle persone o gruppi di queste ex art. 8, con l'entità collettiva delle organizzazioni criminali transnazionali di cui l'elaborato tratta. Le mafie, infatti, possono essere, ai sensi dell'art. 8, configurate come possibili destinatari della norma in quanto gruppo di persone, dotato di una struttura stabile e di una capacità collettiva effettiva, qualora la loro attività risulti concretamente diretta o controllata dall'apparato statale.

Se da una parte, in linea teorica, le organizzazioni mafiose integrano la sfera dei destinatari dell'articolo 8, dall'altra il criterio dell'imputabilità delle loro attività allo Stato è questione notevolmente più complessa. Come precedentemente accennato, la giurisprudenza della Corte Internazionale di Giustizia ha chiarito nel celebre caso *Military and Paramilitary Activities in and Against Nicaragua* (1986) ¹²³, che il criterio dell' "*effective control*" ¹²⁴ è quello in grado di attribuire la responsabilità internazionale

¹²⁰ United Nations. *Draft Articles on Responsibility of States for Internationally Wrongful Acts, With Commentaries*. United Nations, 2008, p. 48. (7).

¹²¹ United Nations. *Draft Articles on Responsibility of States for Internationally Wrongful Acts, With Commentaries*. United Nations, 2008, p. 48. (7).

¹²² United Nations. *Draft Articles on Responsibility of States for Internationally Wrongful Acts, With Commentaries*. United Nations, 2008, p. 49, (9).

¹²³ Corte internazionale di Giustizia. *Attività militari e paramilitari in e contro il Nicaragua (Nicaragua c. Stati Uniti D'America.)*. I.C. J. Reports, 1986, p. 14.

¹²⁴ Corte internazionale di Giustizia. *Attività militari e paramilitari in e contro il Nicaragua (Nicaragua c. Stati Uniti D'America.)*. I.C.J. Reports, 1986, p. 14, par. 115.

degli illeciti di gruppi privati allo Stato di riferimento, nel caso concreto allo stato americano.

Sebbene il caso Nicaragua tratti di un ambito completamente differente da quello delle mafie, quanto sancito dalla giurisprudenza della Corte è adattabile anche a fattispecie caratterizzate dalla presenza di organizzazioni criminali a stampo mafioso, in quanto, tanto come nel contesto militare, anche in quello mafioso il criterio stabilito dalla Corte Internazionale di Giustizia per valutare quando lo Stato sia responsabile o meno per le attività dei privati, e in particolare delle mafie, rimane quello della prova concreta di un controllo o di una direzione effettiva da parte di questo, elemento che parrebbe difficile da stabilire nel caso delle mafie, o meglio, che attualmente non trova evidenze in quanto non si rinvencono casi della CIG di responsabilità internazionale ai sensi dell'articolo 8, in relazione alle organizzazioni criminali.

L'analisi fin qui condotta dell'articolo 8 del Progetto, ha voluto mettere in evidenza come, in linea teorica, gruppi di persone come le organizzazioni criminali a stampo mafioso possano rientrare nella categoria dei soggetti a cui la norma si riferisce, mettendo in luce le relazioni che intercorrono tra tali gruppi e lo Stato. Tuttavia, se nel corso dell'analisi si è potuto evidenziare tale possibile inclusione, si è anche osservato come nella pratica il collegamento delle attività mafiose ad una responsabilità statale, oltre ad essere complessa per la rigidità dello standard probatorio richiesto, appare ancora priva di concretezza pratica nella giurisprudenza internazionale. Tale ipotesi di responsabilità internazionale ai sensi dell'articolo 8 ARSIWA potrà verificarsi solo nel caso in cui si riuscisse a provare che una delle attività illecite perpetrate da un gruppo criminale organizzato sia diretto, controllato o impartito da un organo statale o dall'apparato statale stesso; in particolare tale circostanza deve essere analizzata attraverso il test del controllo effettivo che è stato configurato dalla Corte Internazionale di Giustizia non solo nell'ambito del caso Nicaragua c. Stati Uniti osservato precedentemente, bensì anche nell'ambito di casi ulteriori della Corte. Per esempio, nel caso Bosnia Erzegovina c. Serbia e Montenegro¹²⁵ la Corte ha nuovamente utilizzato il criterio del controllo

¹²⁵ International Court of Justice. *Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro)*. I.C.J. 2007.

effettivo per valutare se la Serbia potesse essere responsabile delle condotte delle proprie forze armate sulla base di un ipotetico controllo effettuato dallo Stato su queste, infine concludendo che avendo la Serbia mancato di dimostrare un controllo effettivo sulle condotte illecite delle forze serbe non rispondeva di responsabilità internazionale ai sensi dell'articolo 8 ARSIWA.

Tuttavia, a fronte di tale limitazione pratica, nel paragrafo che seguirà verrà introdotta l'analisi del principio internazionale della *due diligence*, un criterio atto all'attribuzione della responsabilità internazionale, distinto da quello previsto ai sensi dell'art. 8 ARSIWA. Difatti, la *due diligence* rappresenta uno dei doveri internazionali di prevenzione e repressione più rilevanti in quanto la sua inosservanza è idonea a determinare l'insorgenza della responsabilità internazionale dello Stato, non in termini di controllo o direzione, come per l'articolo 8 ARSIWA, bensì sulla base del criterio di diligenza richiesta dal diritto internazionale che sarà analizzato prima in via generale e poi in particolare nel contesto delle mafie e delle attività criminali attualmente digitalizzate, oggetto del presente elaborato.

2.2 Il principio di *Due Diligence* nel Diritto Internazionale: origini, ruolo e importanza del principio.

In diritto internazionale il principio della *due diligence* orienta gli Stati verso un modello di comportamento diligente e ragionevole che questi debbono rispettare nell'attuazione di condotte di controllo e prevenzione. Il principio della *due diligence* rappresenta un criterio di attribuzione della responsabilità internazionale dello Stato ogni volta si realizzi una violazione del diritto internazionale che origina da una azione o da una omissione caratterizzata da comportamenti negligenti.¹²⁶

In continuità con quanto analizzato, pur non potendo osservare una giurisprudenza internazionale che abbia mai configurato responsabilità dello Stato ai sensi dell'articolo 8 ARSIWA in tema di attività mafiose da parte di uno Stato per assenza di rapporto di

¹²⁶ Kulesza, Joanna. *Due Diligence in International Law*. Leiden, Boston, Vol. 26, Queen Mary Studies In International Law, BRILL NIJHOFF, 2016, p. 2.

direzione o di controllo tra illeciti mafiosi e volontà statale, verrà analizzato quanto previsto per il diverso piano della *due diligence*, un principio internazionale che impone agli Stati l'obbligo positivo di attuare condotte preventive e repressive atte ad evitare che dagli illeciti possano derivare conseguenze dannose che avverrebbero sul proprio territorio o sotto la propria giurisdizione: tale principio diviene particolarmente complesso e rilevante in tema di attività criminali, soprattutto attualmente in materia di *cybercrimes* mafiosi, come verrà osservato più avanti.

Prima di analizzare il modo in cui il principio della *due diligence* possa declinarsi in base a quanto appena detto, sarà opportuno condurre un esame preliminare delle origini di tale principio, dell'evoluzione del suo contenuto e del ruolo giuridico che riveste attualmente nel diritto internazionale.

Il principio della *due diligence* è uno dei concetti più complessi e articolati del diritto internazionale in virtù della sua natura dinamica in grado di adattarsi a più di un contesto (come quello dei diritti umani, della salvaguardia ambientale, del settore industriale ecc..) e di evolvere il proprio adattamento parallelamente all'evoluzione delle sfide globali che gli Stati affrontano, come il crimine organizzato.¹²⁷

Strettamente legato alla disciplina della responsabilità internazionale degli Stati, il concetto della *due diligence* non trae la propria origine da una norma precisa o da un trattato internazionale specifico, bensì è il risultato di un complesso di fonti normative e giurisprudenziali.

Il concetto di *due diligence* è contenuto nel diritto romano che già prevedeva un modello di condotta del *diligens paterfamilias*, un comportamento diligente che richiamasse quello del buon padre di famiglia, e prevedeva un regime di responsabilità imputabile al soggetto che, non attuando la diligenza del *bonus paterfamilias*, arrecava danno a terzi.¹²⁸ Tale modello di condotta oggettivo, nonché di conseguente responsabilità, già esistente nel diritto romano, ha fortemente influenzato lo sviluppo e l'evoluzione del principio

¹²⁷ Kulesza, Joanna. *Due Diligence in International Law*. Leiden, Boston, Vol. 26, Queen Mary Studies In International Law, BRILL NIJHOFF, 2016, p. 1.

¹²⁸ Bonnitcha Jonathan, McCorquodale Robert. "The Concept of 'Due Diligence' in the UN Guiding Principles on Business and Human Rights". *European Journal of International Law*, Volume 28, Issue 3, August 2017, p. 902.

della *due diligence* nel diritto internazionale, destinato a divenire uno standard anch'esso di condotta, atto a definire e delimitare i confini della responsabilità internazionale degli Stati quando questi, nell'attuazione di certe condotte o attività, debbano porre in essere comportamenti ragionevoli, configurati come dovuti.¹²⁹ Nel diritto internazionale non si individua una regola generale che da una definizione univoca del concetto della *due diligence*, in quanto questo si è sviluppato nel tempo adattandosi caso per caso a regole specifiche.¹³⁰

A fondamento di quanto appena affermato viene richiamata una vasta giurisprudenza della Corte Internazionale di Giustizia che nel tempo ha dimostrato come la *due diligence* sia un principio autonomo del diritto internazionale, in grado di adattarsi ad una moltitudine di ambiti.¹³¹ Uno dei casi più rilevanti attraverso cui la Corte Internazionale di Giustizia ha chiarito la natura degli obblighi da cui origina l'attuazione del principio della *due diligence* è stato il *Corfù Channel case*.¹³² (Regno Unito c. Albania), in cui la Corte ha supportato l'idea della *due diligence* come principio che origina dall'esistenza di un obbligo primario che rende l'attuazione del principio della *due diligence* rilevante.¹³³ Nella prospettiva del presente elaborato tale visione della *due diligence* porrebbe le basi per affermare che uno Stato, sebbene non possa dirsi responsabile ai sensi dell'art. 8 del Progetto, possa comunque non andare esente da una eventuale imputazione laddove

¹²⁹ Bonniticha Jonathan, McCorquodale Robert. "The Concept of 'Due Diligence' in the UN Guiding Principles on Business and Human Rights." *European Journal of International Law*, Volume 28, Issue 3, August 2017, p. 903.

¹³⁰ McDonald, Neil. *The Role of Due Diligence in International Law*. Cambridge University Press, British Institute of International and Comparative Law, 2019, p. 1044.

¹³¹ McDonald, Neil. *The Role of Due Diligence in International Law*. Cambridge University Press, British Institute of International and Comparative Law, 2019, p. 1044.

¹³² Corte Internazionale di Giustizia. *Corfù Channel Case (Regno Unito c. Albania)*, Sentenza del 25 marzo 1948, p. 4.

¹³³ McDonald, Neil. *The Role of Due Diligence in International Law*. Cambridge University Press, British Institute of International and Comparative Law, 2019, p. 1044, 1045.

mancasce di rispettare il principio della *due diligence*, in quanto concetto riconosciuto dalla giurisprudenza internazionale della Corte.¹³⁴

La Corte Internazionale di Giustizia ha ribadito tale concezione in ulteriori sentenze, come in quella legata al caso *Pulp Mills* ¹³⁵ in cui viene riconosciuto ancora una volta che la fonte da cui gli obblighi legati alla *due diligence* derivano è una norma primaria di diritto internazionale, un'impostazione che ha permesso nel tempo di stabilire come la natura della *due diligence* fosse propriamente quella di principio e non di obbligo vero e proprio, in ragione del fatto che mentre un obbligo rappresenta la norma concreta da non dover violare, un principio configura la logica su cui tale norma si fonda e si orienta.¹³⁶ Successivamente al caso *Corfù Channel* (1949), il principio della *due diligence* ha costituito oggetto di trattazione anche nell'ambito della redazione degli ARSIWA, nel corso nel quale la CDI esaminò il concetto di *due diligence*, al fine di poterlo considerare come: “*parte delle norme secondarie del diritto internazionale*” ¹³⁷ come affermato da Mackenzie-Gray Scott nel suo scritto.¹³⁸ Nonostante ciò, concentrandosi il Progetto sui criteri di attribuzione delle condotte e non sui principi generali, la Commissione non inserì in via definitiva alcuna disposizione circa la *due diligence* nel Progetto.¹³⁹

Alla luce di quanto osservato circa il principio della *due diligence* nella giurisprudenza della Corte Internazionale di Giustizia, è opportuno esaminare il contenuto e gli elementi

¹³⁴ McDonald, Neil. *The Role of Due Diligence in International Law*. Cambridge University Press, British Institute of International and Comparative Law, 2019, p. 1044, 1045.

¹³⁵ International Court of Justice. *Pulp Mills on the River Uruguay (Argentina v. Uruguay)*, Reports of Judgements, Advisory Opinions and Orders, 20 April 2010. p. 14.

¹³⁶ McDonald, Neil. *The Role of Due Diligence in International Law*. Cambridge University Press, *British Institute of International and Comparative Law*, 2019, p. 1046.

¹³⁷ Mackenzie-Gray Scott, Richard. “Due Diligence as a secondary rule of General International Law.” *Leiden Journal of international law*, 34.2, 2021, p. 343.

¹³⁸ Mackenzie-Gray Scott, Richard. “Due Diligence as a secondary rule of General International Law.” *Leiden Journal of international law*, 34.2, 2021, p. 343.

¹³⁹ Mackenzie-Gray Scott, Richard. “Due Diligence as a secondary rule of General International Law.” *Leiden Journal of international law*, 34.2, 2021, p. 343.

che caratterizzano la *due diligence* nel diritto internazionale. Oltre ad osservare come il principio della *due diligence* si fondi su di un modello di condotta dovuta in quanto ragionevole, il contenuto di tale principio rimanda in via generica all'attività concreta di analisi e accertamento dei fatti, in grado di condurre gli Stati verso decisioni idonee e responsabili.¹⁴⁰ Muovendo dall'obbligo giuridico di attuazione della condotta diligente, gli Stati orientano e adattano tutte le misure da porre in essere, di modo che queste possano dirsi funzionali affinché determinati scenari negativi non vengano a concretizzarsi.¹⁴¹

Gli Stati percepiscono il principio di *due diligence* tanto come una guida nell'attuazione della condotta ragionevole da seguire nel rispetto di un obbligo giuridico, quanto come strumento funzionale ad evitare che lo Stato stesso, attuando la dovuta diligenza, eviti di incorrere in violazioni di diritto internazionale, e inoltre, di subire esiti spiacevoli dagli illeciti compiuti sul proprio territorio; lo strumento della *due diligence* infatti, è uno strumento rilevante sia per il diritto internazionale, sia per la politica internazionale, poiché: “*There may be various motivations other than a sense of legal obligation for a State to establish procedures to conduct what might be characterized as due diligence: political expediency, efficient use of resources, ensuring that the State makes decisions effectively and then acts effectively; and controlling costs.*”¹⁴². Tale concezione suggerisce che gli Stati nella *due diligence* non riscontrano solo un obbligo di prevenzione, bensì un incentivo pratico per migliorare l'efficienza Statale in svariati campi, come quello economico, sociale e politico, al fine ultimo di ridurre i rischi attraverso l'attuazione delle misure di prevenzione e repressione a cui la *due diligence* si riferisce.¹⁴³

¹⁴⁰ McDonald, Neil. *The Role of Due Diligence in International Law*. Cambridge University Press, British Institute of International and Comparative Law, 2019, p. 1049.

¹⁴¹ McDonald, Neil. *The Role of Due Diligence in International Law*. Cambridge University Press, British Institute of International and Comparative Law, 2019, p. 1049.

¹⁴² McDonald, Neil. *The Role of Due Diligence in International Law*. Cambridge University Press, British Institute of International and Comparative Law, 2019, p. 1049.

¹⁴³ McDonald, Neil. *The Role of Due Diligence in International Law*. Cambridge University Press, British Institute of International and Comparative Law, 2019, p. 1049.

Alla luce di ciò, il principio della *due diligence* non configura solo un obbligo positivo che gli Stati debbono rispettare, bensì rappresenta anche un supporto atto ad orientare correttamente l'adozione di misure preventive e repressive degli illeciti da parte dello Stato, affinché questo possa evitare il susseguirsi di conseguenze dannose derivanti dalle attività criminose.

Sebbene, come già osservato, nel diritto internazionale gli Stati genericamente non rispondano delle condotte illecite di attori non statali (se non quando si provi la direzione o il controllo statale su queste), il principio della *due diligence* fa sì che lo Stato sia comunque chiamato a prevenire e reprimere la condotta illecita dei privati e minimizzare le conseguenze negative che derivano dalle condotte criminali di tali soggetti.¹⁴⁴

Lo scenario giuridico che si apre con il mancato rispetto dello standard di *due diligence* da parte dello Stato, nei casi in cui questo si configuri come obbligo giuridico, costituirà l'oggetto di trattazione del paragrafo che segue, incentrato sull'analisi delle conseguenze che derivano dalla violazione e dalla omissione della *due diligence* nei casi in cui gli Stati abbiano l'obbligo giuridico di esercitarla.

2.2.1 Responsabilità internazionale per omessa *due diligence*: presupposti e conseguenze giuridiche dell'inadempimento.

Nel diritto internazionale una delle fonti da cui la responsabilità internazionale degli Stati può originare trova fondamento anche nel concetto della *due diligence*, appena esaminato. Quanto affermato configura il presupposto per cui uno Stato possa rispondere di responsabilità internazionale non solo sulla scorta di azioni positive internazionalmente vietate, bensì sulla scorta di omissioni di obblighi intenti a prevenire e reprimere la violazione di norme internazionali; per esempio rispetto al contesto centrale del presente elaborato inerente alle organizzazioni criminali, la Convenzione delle Nazioni Unite del 2000 contro la criminalità organizzata transnazionale impone all'art. 31 un obbligo di prevenzione atto a imporre agli Stati di: “sviluppare e valutare i progetti nazionali e di

¹⁴⁴ Bonnitcha Jonathan, McCorquodale Robert. “The Concept of ‘Due Diligence’ in the UN Guiding Principles on Business and Human Rights.” *European Journal of International Law*, Volume 28, Issue 3, August 2017, p. 904.

*stabilire e promuovere le migliori prassi e politiche finalizzate alla prevenzione della criminalità organizzata transnazionale.”*¹⁴⁵

Il fenomeno del mancato rispetto del principio della *due diligence* si concretizza principalmente nell’omissione da parte dello Stato di una condotta diligente posta a prevenzione e repressione di atti internazionalmente vietati.

L’esame della responsabilità internazionale per omessa *due diligence* si direbbe un’operazione complessa, in quanto generalmente condizionata all’analisi dell’elemento della ragionevolezza. Può osservarsi come, in termini generali, la possibilità di imputare ad uno Stato responsabilità internazionale per omessa *due diligence* non opera in via automatica in quanto non si imputa in via esclusiva sulla base dell’incapacità dello Stato di prevenire o reprimere condotte o eventi illeciti, bensì si ascrive dopo aver preso in esame la ragionevolezza dell’evento, delle circostanze che insistevano al momento della sua verifica e della effettiva capacità preventiva e repressiva di cui lo Stato è in possesso.¹⁴⁶

In giurisprudenza, tale processo identificativo circa le condizioni vigenti al momento della commissione dell’illecito e delle facoltà di contrasto di cui lo Stato è in possesso, è stato utilizzato come filtro per delineare una concreta violazione o omissione della *due diligence* dalla Corte Suprema del Regno Unito con la sentenza relativa al caso Smith¹⁴⁷ (2010)¹⁴⁸; la Corte ha fatto intendere come nell’identificare l’ipotesi di omessa *due diligence* debba essere preso in considerazione l’elemento della ragionevolezza che

¹⁴⁵ Assemblea Generale delle Nazioni Unite. *Convenzione delle Nazioni Unite contro la criminalità organizzata transnazionale*. Nazioni Unite, Palermo, 2000, art.31, n. 1, p. 20.

¹⁴⁶ Mackenzie-Gray Scott, Richard. “Due Diligence as a secondary rule of General International Law.” *Leiden Journal of international law* 34.2, 2021, p 362.

¹⁴⁷ Supreme Court of U.K. *R (Smith) v. Secretary of State for Defence*. U.K., 2010.

¹⁴⁸ Il caso Smith v. Secretary of State for Defence ha ad oggetto la responsabilità internazionale del Regno Unito nell’ambito di operazioni militari che ha condotto un soldato britannico alla morte. In tale circostanza la Corte Suprema del Regno Unito non ha condannato lo Stato di responsabilità internazionale per violazione del dovere di *due diligence* statale, in quanto la morte di un unico soldato non basterebbe a desumerne una sua violazione.

permetterebbe di valutare la *due diligence* dello Stato in base sia alle misure che *de facto* erano possibilmente adottabili, sia al tipo di condotta posta in essere dagli attori non statali.¹⁴⁹

Quanto generalmente osservato porterebbe a considerare ancora una volta la logica del principio della *due diligence*; difatti, l'imputazione di una violazione o omissione di tale dovere nei confronti degli Stati non parrebbe limitarsi all'analisi della loro capacità preventiva e repressiva dell'evento dannoso, bensì si estenderebbe a considerare la ragionevolezza come elemento in grado di evitare conclusioni automatiche, in quanto idoneo ad analizzare effettivamente le misure congrue e attuabili che lo Stato avrebbe potuto adottare ma che ha omissso.

Dopo aver osservato il fenomeno del mancato rispetto dell'obbligo di *due diligence* e di come questa venga esaminata non solo alla stregua della mancata prevenzione del danno ma anche sulla scia dell'elemento della ragionevolezza, sarà opportuno completare la trattazione con l'analisi delle possibili conseguenze giuridiche che discendono dal mancato rispetto della *due diligence*, alla luce di quanto statuito, seppur implicitamente, dal Progetto ARSIWA.

Sebbene la giurisprudenza della Corte Internazionale di Giustizia non sia mai arrivata a definire in modo puntuale le conseguenze specifiche che possano derivare dalla violazione della *due diligence*, potrebbe essere opportuno, rispetto alle violazioni dell'obbligo di *due diligence*, richiamare l'art.30 ARSIWA, ai sensi del quale: “*The State responsible for the internationally wrongful act is under an obligation: (a) to cease that act, if it is continuing; (b) to offer appropriate assurances and guarantees of non-repetition, if circumstances so require.*”¹⁵⁰

L'analisi dell'articolo 30 rispetto alle conseguenze derivanti dalla violazione della *due diligence* si fonda sul carattere inclusivo dell'articolo che si riferisce genericamente agli atti internazionalmente illeciti.

¹⁴⁹ Mackenzie-Gray Scott, Richard. “Due Diligence as a secondary rule of General International Law.” *Leiden Journal of international law* 34.2, 2021, p 362.

¹⁵⁰ United Nations, International Law Commission. *Project of articles on International Responsibility of States for Internationally Wrongful Acts. With commentaries*. In Yearbook of International Law Commission, 2001, vol. II, article 30.

Riguardo le conseguenze che da tali violazioni discendono, l'articolo prevede da una parte l'obbligo per lo Stato di cessare la condotta internazionalmente illecita, dove per condotta verrebbero compresi sia gli atti positivi che omissivi; dall'altra parte, nel secondo paragrafo l'articolo 30 imporrebbe allo Stato responsabile di predisporre delle misure adeguate a garanzia della non ripetizione futura.¹⁵¹

Pertanto, generalmente in linea con quanto l'articolo prevede, viene osservato che laddove uno Stato ometta l'attuazione della *due diligence* (previsto nell'articolo come atto internazionalmente illecito), questo potrebbe essere chiamato a rispondere ai sensi dell'articolo 30 del progetto ARSIWA, in quanto tale disposto non si limiterebbe a configurare responsabilità internazionale per azioni dirette, bensì la configurerebbe anche per le omissioni, anch'esse atti internazionalmente illeciti. In particolare, vengono messe qui in evidenza le omissioni di misure poste a prevenzione di eventuali eventi dannosi, qualora da tale condotta omissiva derivino dei danni riconducibili anche allo Stato.¹⁵²

Per tanto, lo Stato potrebbe essere tenuto, ai sensi dell'articolo 30 ARSIWA a cessare la condotta illecita laddove necessario, ed eventualmente a garantire, tramite l'attuazione di misure ragionevoli, che nel futuro possa essere assicurata una "*non-repetition*".¹⁵³

Per concludere, viene poi specificato che vi potrebbero essere dei casi specifici in cui lo Stato vittima della violazione potrebbe richiedere l'attuazione di misure specifiche orientate alla eliminazione di possibili ripetizioni future, difatti la norma potrebbe ritenersi connessa al principio della *due diligence* per la caratteristica preventiva e proattiva che assume, così come lo stesso principio viene concepito nel diritto internazionale.¹⁵⁴ Di seguito, l'oggetto dell'analisi si sposterà nuovamente sulla

¹⁵¹ United Nations. *Draft Articles on Responsibility of States for Internationally Wrongful Acts, With Commentaries*. United Nations, 2008, pp. 89, 90.

¹⁵² United Nations. *Draft Articles on Responsibility of States for Internationally Wrongful Acts, With Commentaries*. United Nations, 2008, pp. 88, 89.

¹⁵³ United Nations. *Draft Articles on Responsibility of States for Internationally Wrongful Acts, With Commentaries*. United Nations, 2008, pp. 90, 91.

¹⁵⁴ United Nations. *Draft Articles on Responsibility of States for Internationally Wrongful Acts, With Commentaries*. United Nations, 2008, pp. 88, 90.

tematica del mancato rispetto della *due diligence*, tuttavia in relazione al caso specifico in cui l'atto illecito è commesso da attori non statali.

2.2.2 La violazione dell'obbligo di *due diligence* in caso di condotta illecita di privati: i profili di responsabilità internazionale dello Stato.

In relazione all'oggetto del presente elaborato, inerente alle attività illecite delle organizzazioni criminali transnazionali e di come lo Stato possa o meno considerarsi responsabile, l'analisi verrà di seguito orientata verso la responsabilità internazionale degli Stati per omissione, laddove gli Stati non abbiano attuato la *due diligence* nella prevenzione e repressione di atti internazionalmente illeciti posti in essere da privati.

Precedentemente è stato osservato come, genericamente, la responsabilità internazionale non viene attribuita di per sé allo Stato laddove sia un attore non statale, o un soggetto privato a commettere un illecito, a meno che vi sia stata prova della direzione o del controllo da parte dello Stato su tali attività. Pertanto, in assenza di tali presupposti non può dirsi possibile l'imputazione delle condotte degli attori non statali allo Stato sul piano della responsabilità per azione.

Sebbene l'articolo 8 ARSIWA non risulti applicabile, la possibilità di imputare responsabilità internazionale allo Stato per atti di privati non si esaurisce qui; difatti, tale responsabilità diversa e complementare rispetto a quella configurabile ai sensi dell'art. 8 ARSIWA, trova giustificazione nel principio della *due diligence* alla luce degli obblighi primari di prevenzione, analizzando l'eventualità per cui lo Stato abbia o meno effettivamente posto in essere tutte le misure e le condotte necessarie per prevenire o reprimere un dato illecito. Il ruolo della *due diligence* diviene cruciale nella determinazione del nesso di omissione colpevole che intercorre tra lo Stato e le condotte illecite compiute da attori non statali, con riguardo anche alla gravità di tali condotte.¹⁵⁵ Come accennato, l'istituto della responsabilità basata sulla violazione della *due diligence* è nettamente diverso rispetto a quello della responsabilità ex art. 8 ARSIWA in virtù del fatto che, se da una parte l'articolo 8 ARSIWA determina le condizioni di imputabilità

¹⁵⁵ Mackenzie-Gray Scott, Richard. "Due Diligence as a secondary rule of General International Law." *Leiden Journal of International Law*, 34.2, 2021, p. 362.

della condotta allo Stato, dall'altra parte la *due diligence* attiene alla violazione dell'obbligo primario di prevenzione e vigilanza.¹⁵⁶

Nella valutazione della responsabilità internazionale per le condotte dei privati, la *due diligence*, oltre a soffermarsi sulle possibilità ragionevoli di cui dispone lo Stato al momento della commissione dell'illecito da parte dei privati, si concentra sul grado di influenza che questo avrebbe attuato nei confronti dell'esito della condotta posta in essere dai privati.¹⁵⁷ L'elemento dell'influenza e della condizionalità della condotta da parte dello Stato nei confronti dei privati è stato già affrontato in giurisprudenza dalla Corte Internazionale di Giustizia con riguardo al caso Bosnia c. Serbia, in cui la Corte da una parte ha sottolineato l'esclusione della sussistenza dei requisiti per l'attribuzione diretta delle condotte illecite dei privati (responsabili del genocidio), dall'altra ha riconosciuto la responsabilità della Serbia per aver mancato di ottemperare allo standard di diligenza dovuta nel corso della commissione del crimine; pertanto ha ribadito come la responsabilità non si possa imputare esclusivamente sulla base del mancato risultato raggiunto, bensì anche sulla concretezza dell'omissione di tutte le misure ragionevoli e possibili che lo Stato avrebbe dovuto attuare e che ha mancato di fare.¹⁵⁸

Ulteriore elemento caratterizzante tale possibile responsabilità ai sensi dello standard della *due diligence* è il criterio della prevedibilità delle circostanze, elemento che parrebbe comprendere l'eventualità in cui una determinata condotta, assieme alle conseguenze di questa, possano ragionevolmente dare luogo ad esiti prevedibilmente negativi. ¹⁵⁹

Alla luce di quanto analizzato, in conclusione viene osservato come la *due diligence* detenga un ruolo essenziale quando, nell'impossibilità di ricondurre responsabilità internazionale allo Stato ai sensi dell'art. 8 ARSIWA, debba valutarsi se lo Stato possa

¹⁵⁶ Mackenzie-Gray Scott, Richard. "Due Diligence as a secondary rule of General International Law." *Leiden Journal of International Law*, 34.2, 2021, p. 362.

¹⁵⁷ Mackenzie-Gray Scott, Richard. "Due Diligence as a secondary rule of General International Law." *Leiden Journal of International Law*, 34.2, 2021, p. 363.

¹⁵⁸ Mackenzie-Gray Scott, Richard. "Due Diligence as a secondary rule of General International Law." *Leiden Journal of International Law*, 34.2, 2021, p. 363.

¹⁵⁹ Mackenzie-Gray Scott, Richard. "Due Diligence as a secondary rule of General International Law." *Leiden Journal of International Law*, 34.2, 2021, p. 364.

essere imputato sulla base del diverso piano della violazione degli obblighi di prevenzione, valutata alla luce dello standard della *due diligence* che consente di accertare se uno Stato, pur non avendo guidato le condotte e le azioni di attori non statali, possa essere responsabile internazionalmente per la violazione degli obblighi di prevenzione.

2.2.3 I limiti della *due diligence*: un dibattito dottrinale.

Stando a quanto sin qui esaminato, è emerso come nel diritto internazionale il principio della *due diligence* ricopra un ruolo rilevante nella valutazione del comportamento atteso dagli Stati rispetto a quello realmente posto in essere. Dopo aver esaminato il percorso evolutivo del principio di *due diligence*, assieme ai suoi elementi compositivi e alla fattispecie di violazione, con particolare riguardo a quella omissiva, seguirà l'analisi dell'ambito di efficacia della *due diligence* dibattuto in dottrina e di come piuttosto che essere assoluto e privo di limiti operativi, il principio della *due diligence* siano contornato da circostanze e confini delimitati entro i quali opera.

Nel tempo si sono dibattute diverse posizioni teoriche che hanno messo in discussione la natura della *due diligence*, alle volte inquadrandola come soggettiva, altre volte come oggettiva.¹⁶⁰ La dottrina più recente ma soprattutto la prassi internazionale ha sostenuto la natura oggettiva della *due diligence* intesa come modello neutrale di condotta che gli Stati sono chiamati ad attuare. Tale osservazione ha portato ad affermare che la negligenza non costituisce un requisito necessario da dover dimostrare per la configurazione della responsabilità internazionale in quanto la responsabilità di uno Stato può configurarsi anche in presenza di una violazione oggettiva del principio di *due diligence*, ovvero quando lo Stato indipendentemente dalla sua volontà ometta di adempiere agli obblighi di prevenzione e controllo previsti dal diritto internazionale. ¹⁶¹

¹⁶⁰ Pisillo Mazzeschi, Riccardo. "The Due Diligence Rule and The Nature of the International Responsibility of States". *German Yearbook of International Law*, 1992, p. 42.

¹⁶¹ Pisillo Mazzeschi, Riccardo. "The Due Diligence Rule and The Nature of the International Responsibility of States". *German Yearbook of International Law*, 1992, p. 42.

La dottrina ha tenuto ad osservare come: “*However, although the concept of diligence is objective, it has undoubtedly an elastic and relative nature.*”¹⁶², tale impostazione dottrinale di R. Pisillo Mazzeschi parrebbe riflettere come il criterio della *due diligence* offra agli Stati dei margini di condotta da attuare che si adattino alle circostanze del caso specifico, il che renderebbe lo standard di *due diligence* adattabile e mai statico.¹⁶³ Quanto osservato in dottrina troverebbe fondamento nel fatto che l’ambito di efficacia della *due diligence* si adatta ad una vasta gamma di aree del diritto internazionale differenti tra loro, come l’ambito dei diritti umani, dello sviluppo ambientale, delle attività industriali, tutti contesti in cui si afferma uno standard di *due diligence* che possa essere più o meno rigido a seconda delle circostanze e delle conseguenze negative che si verificherebbero in assenza di questo. ¹⁶⁴

La dottrina, oltre a discutere l’ambito di efficacia della *due diligence*, ha dibattuto sulla tematica dei limiti che vengono attribuiti al principio di *due diligence*.

La prima delimitazione operativa di cui la dottrina ha discusso riguarda il fatto che il principio non deve essere inteso come illimitato, in quanto la sua applicazione è vincolata al caso concreto, in particolare dalle circostanze che rendono l’attuazione delle misure preventive possibile, escludendo invece la configurazione della responsabilità nel caso in cui l’adempimento di tali misure sia impossibile per lo Stato. ¹⁶⁵

¹⁶² Pisillo Mazzeschi, Riccardo. “The Due Diligence Rule and The Nature of the International Responsibility of States”. *German Yearbook of International Law*, 1992, p. 44.

¹⁶³ Pisillo Mazzeschi, Riccardo. “The Due Diligence Rule and The Nature of the International Responsibility of States”. *German Yearbook of International Law*, 1992, p. 44.

¹⁶⁴ Pisillo Mazzeschi, Riccardo. “The Due Diligence Rule and The Nature of the International Responsibility of States”. *German Yearbook of International Law*, 1992, p. 45.

¹⁶⁵ Pisillo Mazzeschi, Riccardo. “The Due Diligence Rule and The Nature of the International Responsibility of States” *German Yearbook of International Law*, 1992, p. 46.

Quanto detto suggerisce che, da una parte la responsabilità statale non possa essere configurata laddove l'evento dannoso sia la diretta conseguenza di un evento fortuito o straordinario; dall'altra parte che la *due diligence* che si richiede agli Stati non impone a questi di soddisfare obblighi inattuabili, piuttosto di operare in base ai propri mezzi e nel pieno delle proprie possibilità. ¹⁶⁶

Il principio di *due diligence* si estende a diverse aree internazionali in cui lo standard di condotta richiesto agli Stati possa divenire più o meno rigido a seconda della complessità dell'ambito in cui viene attuato e soprattutto sulla base delle conseguenze dannose che possano derivarvi.

Alla luce di quanto detto, nell'ultimo paragrafo del presente elaborato sarà preso in analisi l'ambito dinamico e complesso del *cyberspace*, un'area in cui la necessità di estendere l'applicazione del criterio della *due diligence* diviene sempre più rilevante ai fini dell'identificazione dei responsabili di condotte dannose, spesso perpetrate da organizzazioni criminali evolute, che pone gli Stati dinnanzi a nuove sfide.

Pertanto, verrà osservato come le nuove forme di crimine organizzato virtuale possano mettere in difficoltà il diritto internazionale nell'identificazione delle responsabilità e di come il principio della *due diligence* si declini e si applichi a tale ambito.

2.3 Organizzazioni criminali e attività illecite nel cyberspace: i profili di responsabilità internazionale degli Stati.

Nel primo capitolo del presente elaborato il tema delle organizzazioni criminali transnazionali e delle loro attività illecite perpetrate nel *cyberspace* è stato affrontato ampiamente, a partire dall'analisi della nascita e dell'evoluzione delle mafie divenute oggi attive nello spazio dinamico ed elusivo dello spazio cibernetico.

Nel quadro del diritto internazionale, i crimini cibernetici maggiormente complessi vengono prevalentemente ascritti alle organizzazioni criminali come le mafie, entità riconducibili alla categoria dei privati, come osservato in precedenza. Seppure gli Stati

¹⁶⁶ Pisillo Mazzeschi, Riccardo. "The Due Diligence Rule and The Nature of the International Responsibility of States", *German Yearbook of International Law*, 1992, p. 47.

continuino ad affidarsi al diritto internazionale per la regolamentazione del *cyberspace*, l'applicazione dell'istituto della responsabilità internazionale al dominio virtuale è limitato in relazione alla difficoltà riscontrata nell'identificare le condizioni di imputabilità delle condotte illecite virtuali allo Stato. ¹⁶⁷

Ai fini dell'attribuzione dei crimini informatici allo Stato, le *conditio* della direzione e del controllo concreto parrebbero estremamente complesse da provare in un ambiente come quello dello spazio virtuale, in cui le organizzazioni criminali, gli individui e gli stessi Stati potrebbero agire, controllare o dirigere crimini cibernetici mantenendo un profilo occulto. ¹⁶⁸

Alla luce della fattispecie appena osservata, viene esaminato ora il caso specifico in cui i privati, come le organizzazioni criminali, delinquono nello spazio cibernetico. Saranno analizzati i profili di responsabilità internazionale per gli illeciti commessi nel *cyberspace*, esaminando nuovamente l'articolo 8 ARSIWA, stavolta in relazione al modo in cui tale disposizione debba essere interpretata alla luce delle operazioni illecite che i gruppi criminali attuano nello spazio cibernetico. ¹⁶⁹

In dottrina l'utilizzo dell'articolo 8 ARSIWA per la configurazione della responsabilità statale crea un divario tra chi sostiene che lo standard probatorio della norma per l'imputazione dei crimini cibernetici di privati allo Stato sia eccessivamente rigida per essere provata con efficacia nel *cyberspace*, e chi invece sostiene che, nonostante tale

¹⁶⁷ Buchan Russell, Nicholas Tsagourias. "Special Issue: Non- State Actors and Responsibility in Cyberspace: State Responsibility, Individual Criminal Responsibility and Issues of Evidence." *Journal of Conflict and Security Law*, Oxford University Press, vol. 21, no. 3, 2016, p. 377.

¹⁶⁸ Buchan Russell, Nicholas Tsagourias. "Special Issue: Non- State Actors and Responsibility in Cyberspace: State Responsibility, Individual Criminal Responsibility and Issues of Evidence." *Journal of Conflict and Security Law*, Oxford University Press, vol. 21, no. 3, 2016, p. 378.

¹⁶⁹ Buchan Russell, Nicholas Tsagourias. "Special Issue: Non- State Actors and Responsibility in Cyberspace: State Responsibility, Individual Criminal Responsibility and Issues of Evidence." *Journal of Conflict and Security Law*, Oxford University Press, vol. 21, no. 3, 2016, pp. 378, 379.

difficoltà probatoria, il problema possa essere superato attraverso l'analisi degli obblighi di prevenzione da cui il principio della *due diligence* origina. ¹⁷⁰ La prima concezione osservata parrebbe sostenuta in dottrina dal giurista Kubo Macak ¹⁷¹ che sostiene come i tre standard probatori della responsabilità statale per le condotte illecite dei privati, quali la direzione, l'istruzione e il controllo sarebbero estremamente complesse da provare nello spazio cibernetico per i *cybercrimes*, in quanto la dinamicità e l'anonimato che offrono gli spazi virtuali (come il *dark web* e il *deep web* analizzati nel capitolo primo) renderebbero difficile provare concretamente se una determinata organizzazione criminale possa aver agito illecitamente nel *cyberspace* sotto la direzione o il controllo di uno Stato, impedendo di configurare responsabilità internazionale ai sensi dell'articolo 8 ARSIWA. ¹⁷² La complessità dell'attribuzione è dettata dalle caratteristiche dello spazio cibernetico; difatti è opportuno sottolineare come il problema più rilevante derivi comunque dall'impostazione dell'art. 8 ARSIWA, poiché analizzando il dettato normativo, il criterio del controllo, della direzione e dell'istruzione condividono alla base il rapporto di subordinazione tra lo Stato e gli attori non statali. Quanto osservato pone in evidenza come, seppure possa essere provata una forma orizzontale di complicità in cui lo Stato non dirige l'azione criminale ma tacitamente la consente, tale forma di coadiuvazione non si configura come soddisfattiva degli standard di attribuzione della

¹⁷⁰ Buchan Russell, Nicholas Tsagourias. "Special Issue: Non- State Actors and Responsibility in Cyberspace: State Responsibility, Individual Criminal Responsibility and Issues of Evidence." *Journal of Conflict and Security Law*, Oxford University Press, vol. 21, no. 3, 2016, pp. 378, 379.

¹⁷¹ Kubo Macak, professore di diritto internazionale alla *University of Exeter* del Regno Unito, ha lavorato tra il 2019 e il 2023 come consigliere legale presso l'*International Committee of Red Cross*. Particolarmente interessato al tema dei *cybercrimes* internazionali, è autore di diversi scritti inerenti a diritto internazionale umanitario e operazioni cibernetiche.

¹⁷² Buchan Russell, Nicholas Tsagourias. "Special Issue: Non- State Actors and Responsibility in Cyberspace: State Responsibility, Individual Criminal Responsibility and Issues of Evidence." *Journal of Conflict and Security Law*, Oxford University Press, vol. 21, no. 3, 2016, pp. 378, 379.

condotta illecita ex art. 8 ARSIWA, in quanto tali standard richiedono che vi sia la prova di un'attività di direzione e controllo da parte dello Stato sui crimini. ¹⁷³

La seconda visione dottrinale invece, è sostenuta da Russell Buchan¹⁷⁴, il quale riconosce inevitabilmente come l'impossibilità di configurare la responsabilità internazionale sia frutto dell'impostazione ex art. 8 ARSIWA, ma che tale *gap* normativo possa essere risolto in via generale dalla previsione degli obblighi di prevenzione previsti dal diritto internazionale in tema di tutela, come quello della *due diligence*, atto a imporre agli Stati di prevedere un piano cibernetico di prevenzione e repressione delle minacce virtuali.¹⁷⁵

Per concludere, proprio il piano degli obblighi di prevenzione configurati attraverso la *due diligence*, su cui si è ampiamente trattato in via introduttiva, saranno oggetto di analisi nella trattazione che seguirà, per valutare come tale principio di diritto internazionale venga declinato allo spazio cibernetico e di come questo possa o meno risolvere il problema dell'attribuzione degli illeciti virtuali dei gruppi criminali privati allo Stato, non tanto sulla base dell'attribuzione del crimine cibernetico in sé allo Stato, quanto perché si propenda ad ascrivergli le conseguenze dannose che da tale illecito derivano.¹⁷⁶

¹⁷³ Macak, Kubo. "Decoding Article 8 of the International Law Commission's Articles on State Responsibility: Attribution of Cyber Operations by Non-State Actors." *Journal of Conflict and Security Law*, Oxford University Press, 2016, p. 426, 427.

¹⁷⁴ Russell Buchan è un professore di diritto internazionale presso l'University of Reading del Regno Unito, ricomprendo anche il ruolo di *Senior Lecturer* in diritto internazionale presso l'*University of Sheffield*.

¹⁷⁵ Buchan Russell, Nicholas Tsagourias. "Special Issue: Non- State Actors and Responsibility in Cyberspace: State Responsibility, Individual Criminal Responsibility and Issues of Evidence." *Journal of Conflict and Security Law*, Oxford University Press, vol. 21, no. 3, 2016, p. 379.

¹⁷⁶ Macak, Kubo. "Decoding Article 8 of the International Law Commission's Articles on State Responsibility: Attribution of Cyber Operations by Non-State Actors." *Journal of Conflict and Security Law*, Oxford University Press, 2016, p. 428.

2.3.1 Il principio di *due diligence* nel *cyberspace*: il ruolo dell'attribuzione e le difficoltà nello spazio cibernetico.

L'evoluzione digitale globale è una delle cause primordiali del complesso problema che gli Stati si trovano oggi ad affrontare: i *cybercrimes* nello spazio virtuale. Tale area, oramai luogo principale in grado di permettere ad enti privati di delinquere, ha riscosso particolare interesse nella dottrina internazionale che non ha mancato di interrogarsi sui problemi di attribuzione della responsabilità internazionale in caso di illeciti commessi da privati nello spazio occulto del web. Come osservato al paragrafo di cui sopra, i problemi di imputabilità che non possono dirsi risolvibili a causa dell'impostazione normativa dell'articolo 8 ARSIWA rispetto alle caratteristiche dello spazio informatico, hanno portato gran parte della dottrina ad interrogarsi su ulteriori alternative, ponendo al centro della tematica le modalità con cui il principio della *due diligence* possa configurarsi nell'ambito del *cyberspace* e fungere da rimedio giuridico. Al fine ultimo di capire se e in che modo, a differenza della responsabilità internazionale dello Stato per fatto di privati ex art. 8 ARSIWA, la *due diligence* possa configurare una responsabilità internazionale dello Stato fondata sull'omissione della condotta diligente degli illeciti informatici delle organizzazioni criminali transnazionali, sarà opportuno prendere in analisi la modalità attraverso cui il concetto di diligenza dovuta si adatti al *cyberspace* e che caratteristiche assuma.¹⁷⁷

È bene ricordare che l'applicazione che si opera della *due diligence* nel dominio cibernetico è il risultato di un'analisi che origina dalla prassi e dalla dottrina internazionale atta a stabilire l'applicabilità della *due diligence* al mondo virtuale, in quanto nel diritto internazionale non è stato ancora riscontrato alcun riferimento giuridico

¹⁷⁷ Kavaliauskas, Aurimas. "Can the Concept of Due Diligence Contribute to Solving the Problem of Attribution with Respect to Cyber-Attacks Conducted by Non-State Actors which Are Used as Proxies by States?". *Teises Apzvalga Law Review*, 26, 2022, p. 8.

vincolante che statuisca obblighi di *due diligence* per gli Stati nell'ambito dello spazio cibernetico.¹⁷⁸

L'applicabilità della dovuta diligenza all'ambito cibernetico trova principale fondamento nel Tallinn Manual 2.0¹⁷⁹, l'opera accademica più rilevante circa l'adattabilità del diritto internazionale al mondo virtuale; in particolar modo il Tallinn Manual 2.0, seppure rappresenti una fonte di *soft law*¹⁸⁰, afferma alla regola numero 6 come: “*A State must exercise due diligence in not allowig its territory, or territory or cyber infrastructure under its governmental control, to be used for cyber operations that affect the rights of, and produce serious adverse consequences for, other States.*”¹⁸¹

Alla luce della regola numero 6 e dell'assoggettamento delle tecnologie dirompenti al diritto internazionale preesistente, si concluderebbe che il principio della *due diligence* vada ad applicarsi anch'esso alla dimensione cibernetica e alle operazioni informatiche, presentando caratteristiche specifiche per tale ambito. ¹⁸²

Dopo aver osservato che il principio della *due diligence* parrebbe senz'altro applicarsi allo spazio informatico, è opportuno esaminare come tale standard di condotta venga a declinarsi in tale contesto. Il concetto della *due diligence* anche nello spazio virtuale viene alla luce non come obbligo di mezzi, bensì come obbligo di risultato incentrato a

¹⁷⁸ Kavaliauskas, Aurimas. “Can the Concept of Due Diligence Contribute to Solving the Problem of Attribution with Respect to Cyber-Attacks Conducted by Non-State Actors which Are Used as Proxies by States?”. *Teises Apzvalga Law Review*, 26, 2022, p. 9.

¹⁷⁹ Schmitt, Michael N. *Tallin Manual 2.0 on the international Law Applicable to Cyber Operations*. Cambridge University Press, 2017.

¹⁸⁰ Il Tallin Manual 2.0 rappresenta una fonte non vincolante del diritto internazionale pubblico. In particolare, appartenendo alle fonti di *soft law*, il Tallin Manual 2.0 non detiene alcuna forza giuridica vincolante sugli Stati; pertanto, tale opera può solo orientare la prassi influenzando i comportamenti degli Stati in materia.

¹⁸¹ Schmitt, Michael, N. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge University Press, 2017, rule 6, p. 30.

¹⁸² Schmitt, Michael N. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge University Press, 2017, rule 6, p. 31.

realizzare la prevenzione e la repressione degli attacchi informatici o dei *cyber* crimini attuati dai privati.¹⁸³

Un ultimo profilo su cui occorre soffermarsi è quello relativo alla possibilità di configurare la *due diligence* come base giuridica della responsabilità statale per illeciti informatici commessi dai privati, ponendo rimedio al problema di attribuzione precedentemente affrontato. In linea generale ha già formato oggetto di riflessione da parte della CIG (nel caso Bosnia c. Serbia¹⁸⁴) il fatto che l'applicazione della *due diligence* possa essere contemplata come via secondaria per l'attribuzione della responsabilità internazionale quando tutte le ulteriori possibilità di attribuzione falliscano, questo può dirsi quindi funzionale nel caso dei crimini informatici da parte dei privati, in quanto se da una parte il meccanismo di attribuzione dell'articolo 8 ARSIWA non permetterebbe facilmente di imputare tali crimini allo Stato, dall'altra parte la *due diligence* potrebbe configurarsi come forma idonea all'ascrizione delle attività cibernetiche criminali allo Stato sulla base del fatto che lo Stato abbia omissso l'attuazione delle condotte diligenti imposte dal principio della *due diligence*, causando conseguenze estremamente dannose o pericolose.¹⁸⁵

Difatti, mentre la responsabilità internazionale dello Stato ex art. 8 ARSIWA prevede standard probatori, come la direzione e il controllo effettivo, eccessivamente rigidi per essere provati nello spazio occulto del *cyberspace*, la responsabilità internazionale fondata sulla violazione dell'obbligo di *due diligence* nello spazio cibernetico parrebbe basata su di un approccio più flessibile, in quanto ciò che rilevarebbe ai fini della configurazione della responsabilità non è la riconduzione dell'illecito informatico allo

¹⁸³ Schmitt, Michael N. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge University Press, 2017, rule 6, p. 31, 32.

¹⁸⁴ International Court of Justice. *Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro)*. I.C.J. 2007.

¹⁸⁵ Kavaliauskas, Aurimas. "Can the Concept of Due Diligence Contribute to Solving the Problem of Attribution with Respect to Cyber-Attacks Conducted by Non-State Actors which Are Used as Proxies by States?". *Teises Apzvalga Law Review*, 26, 2022, pp. 16, 17.

Stato, quanto piuttosto la violazione della garanzia di aver agito nel rispetto della *due diligence* cibernetica.¹⁸⁶

La responsabilità internazionale appena esposta si riferirebbe essenzialmente alla fattispecie omissiva del principio di *due diligence*. In ultimo quindi, nella trattazione successiva verrà presa in esame la responsabilità internazionale degli Stati nell'ambito di attività illecite degli attori non statali, come le organizzazioni criminali, commesse nello spazio virtuale e fondate sull'omissione degli standard di diligenza inerenti allo spazio virtuale.

2.3.2 Il fenomeno dei *cyber* attacchi delle mafie e la responsabilità degli Stati per omessa *due diligence*.

Nella realtà socio tecnologica odierna lo scenario offerto dall'operatività dello spazio virtuale è intriso tanto di aspetti positivi che la modernizzazione apporta alla comunità internazionale (come nel caso dell'evoluzione tecnologica delle comunicazioni tra Stati), quanto di criticità che non possono essere trascurate. Il nodo problematico più interessante preso in esame dal presente elaborato è quello inerente all'utilizzo del *cyberspace* da parte degli attori non statali come strumento tramite cui attuare crimini informatici o portare avanti traffici illeciti, grazie all'anonimato, all'assenza di barriere d'ingresso e ai costi d'operazione dimezzati offerti dal dominio cibernetico.¹⁸⁷

Per attori non statali, come già osservato, potrebbero essere intese una serie di entità quali gruppi che non appartengono alla struttura statale, individui singoli o corporazioni; tuttavia, nel tempo l'entità più rilevante che ha impiegato il *cyberspace* come luogo

¹⁸⁶ Kavaliauskas, Aurimas. "Can the Concept of Due Diligence Contribute to Solving the Problem of Attribution with Respect to Cyber-Attacks Conducted by Non-State Actors which Are Used as Proxies by States?". *Teises Apzvalga Law Review*, 26, 2022, pp. 23, 24.

¹⁸⁷ Buchan Russell, Nicholas Tsagourias. "Special Issue: Non- State Actors and Responsibility in Cyberspace: State Responsibility, Individual Criminal Responsibility and Issues of Evidence." *Journal of Conflict and Security Law*, Oxford University Press, vol. 21, no. 3, 2016, p. 377.

deputato alla gestione ed espansione delle attività criminali è la criminalità organizzata transnazionale. ¹⁸⁸

Sulla scia delle attività illecite delle mafie cibernetiche odierne viene ripresa l'analisi della responsabilità Statale fondata sulla fattispecie omissiva del principio di *due diligence* nel dominio virtuale.

La fattispecie particolare che viene osservata è quella dell'attribuzione della responsabilità allo Stato per omessa *due diligence* nei confronti delle attività illecite che le organizzazioni criminali attuano nel dominio informatico.

In primo luogo è opportuno individuare il presupposto giuridico sulla base del quale inquadrare una fattispecie omissiva della diligenza dovuta nello spazio virtuale; tale presupposto parrebbe fondarsi sull'assunto per cui le norme di diritto internazionale si adattino e si applichino anche alla dimensione virtuale del *cyberspace*, difatti viene osservato in dottrina come: “*Two key rules deriving from the principle of sovereignty and applying generally in international law are precisely the Corfù Channel and the no-harm principles. Thus, the presumption we ought to proceed from is that they apply to ICTs, in the absence of *leges speciales* to the contrary.*”¹⁸⁹ Per tanto, come appena esaminato, alla luce dell'applicazione del diritto internazionale al dominio virtuale, venendo a configurarsi il principio di *due diligence*, gli Stati saranno chiamati a rispondere di eventuali omissioni del principio anche nello spazio informatico.

Nell'ambito cibernetico la fattispecie omissiva in cui gli Stati potrebbero incorrere, non riguarderebbe in via esclusiva la mancata attuazione delle misure poste a prevenzione e repressione dei crimini informatici dei gruppi, bensì parrebbe riferirsi anche all'adozione di misure risultate disfunzionali rispetto alla possibilità di adottarne altrettante

¹⁸⁸ Buchan Russell, Nicholas Tsagourias. “Special Issue: Non- State Actors and Responsibility in Cyberspace: State Responsibility, Individual Criminal Responsibility and Issues of Evidence.” *Journal of Conflict and Security Law*, Oxford University Press, vol. 21, no. 3, 2016, p. 377.

¹⁸⁹ Coco Antonio, de Souza Dias Talita. “Cyber Due Diligence”. Patchwork of Protective Obligations in International Law, *European Journal of International Law*, Oxford University Press, volume 32, issue 3, 2021, p. 780.

ragionevolmente idonee e disponibili per lo Stato stesso.¹⁹⁰ Il concetto di *due diligence* cibernetica, contenuta sempre in obblighi primari da cui far discendere la responsabilità internazionale, nello spazio cibernetico può dare luogo ad una serie di modalità omissive della condotta dovuta, in ragione del fatto che il *cyberspace* è intriso di rischi informatici che gli Stati debbono analizzare e mitigare. ¹⁹¹

Sebbene la dottrina tratti debolmente l'attribuzione per omissione della responsabilità internazionale allo Stato per crimini commessi da gruppi privati nel *cyberspace*, la fattispecie omissiva parrebbe ad ogni modo lo strumento più flessibile in grado di permettere l'attribuzione di responsabilità internazionale allo Stato, non sulla base di prove che attestino il controllo o la complicità dello Stato con i gruppi criminali virtuali (estremamente difficili da provare), bensì sulla base dell'omissione generica delle condotte ragionevoli presumibili dal dovere di *due diligence*, ritenute collegate al crimine posto in essere e alle sue conseguenze dannose. ¹⁹²

L'attribuzione concreta di operazioni informatiche illecite rimane un ambito estremamente complesso da provare per essere posto a fondamento della responsabilità internazionale, in particolar modo quando si debba attestare la relazione tra lo Stato e i gruppi criminali nella realizzazione dell'illecito cibernetico, in quanto lo standard probatorio su cui dovrebbe basarsi l'esame rimane quello ex art. 8 ARSIWA, un test

¹⁹⁰ Schmid Evelyne, Erceis Ayse Ozge. "The Attribution of Omissions: Due Diligence in Cyberspace and State Responsibility." *Swiss Review of International and European Law*, vol 33, no. 4, 2023, p. 580.

¹⁹¹ Schmid Evelyne, Erceis Ayse Ozge. "The Attribution of Omissions: Due Diligence in Cyberspace and State Responsibility." *Swiss Review of International and European Law*, vol 33, no. 4, 2023, p. 580.

¹⁹² Schmid Evelyne, Erceis Ayse Ozge. "The Attribution of Omissions: Due Diligence in Cyberspace and State Responsibility." *Swiss Review of International and European Law*, vol 33, no. 4, 2023, p. 582.

eccessivamente complesso vista la difficile reperibilità di elementi di prova nel *cyberspace*.¹⁹³

Pertanto, in tale ambito si è orientata l'attribuzione della responsabilità internazionale verso la fattispecie omissiva della *due diligence* cibernetica da parte dello Stato, il quale nello spazio virtuale sfruttato dalle organizzazioni criminali moderne, potrebbe aver mancato di attuare una condotta preventiva e ragionevole richiesta, omettendo per esempio: “*to prevent its territory from being used for malicious cyber operations.*”¹⁹⁴

La visione dottrinale che maggiormente sostiene tale criterio di attribuzione è quella offerta dagli autori Evelyne Schmid e Ayse Ozge nella loro opera sulla responsabilità dello Stato per omessa *due diligence* nel *cyberspace*¹⁹⁵, i quali condividono a pieno l'attribuzione della responsabilità internazionale allo Stato quando questo ometta l'attuazione di condotte ragionevoli nel dominio informatico.

Per concludere, alla luce di quanto esaminato sulla *due diligence* informatica e sulla responsabilità internazionale che potrebbe configurarsi dall'omissione di questa per atti cibernetici dei gruppi criminali, nella trattazione che segue verrà preso in considerazione un caso pratico legato al fenomeno problematico delle operazioni cibernetiche illecite ascritte alla mafia russa e sarà osservato in che misura lo Stato della Russia avrebbe rispettato lo standard della *due diligence* cibernetica finora esaminata.

¹⁹³ Schmid Evelyne, Erceis Ayse Ozge . “The Attribution of Omissions: Due Diligence in Cyberspace and State Responsibility.” *Swiss Review of International and European Law*, vol 33, no. 4, 2023, p. 582, 583.

¹⁹⁴ Schmid Evelyne, Erceis Ayse Ozge . “The Attribution of Omissions: Due Diligence in Cyberspace and State Responsibility.” *Swiss Review of International and European Law*, vol 33, no. 4, 2023, p. 583.

¹⁹⁵ Schmid Evelyne, Erceis Ayse Ozge . “The Attribution of Omissions: Due Diligence in Cyberspace and State Responsibility.” *Swiss Review of International and European Law*, vol 33, no. 4, 2023, p. 583.

2.3.3 Il caso degli attacchi hacker da parte della mafia russa: in che modo la Russia ha affrontato tale fenomeno.

Il caso che verrà osservato nell'ultima parte del capitolo II vuole offrire un esempio concreto di organizzazione criminale mafiosa che, nel corso del tempo, più si è avvalsa dello spazio virtuale e del mondo *hacker* per colpire gli Stati ed espandere le loro attività cibernetiche illecite: la mafia russa.

In particolare, verrà offerta una panoramica generale del fenomeno criminale per arrivare alla questione principale inerente a come lo Stato della Russia, territorio in cui le organizzazioni sono radicate e dal quale operano, venga considerato responsabile o meno alla stregua dello standard di *due diligence* richiesto e dallo Stato concretamente applicato. Alla luce dell'ampia trattazione fin qui esposta circa l'ambito di operatività della responsabilità internazionale per atti privati e della *due diligence*, sebbene nella giurisprudenza internazionale della CIG la responsabilità della Russia per le attività cibernetiche della mafia non sia mai stata concretizzata a causa dell'inadattabilità dello standard probatorio ex art. 8 ARSIWA (direzione e controllo effettivo) rispetto allo spazio virtuale, nel presente elaborato verrà analizzata l'interessante posizione sviluppata dalla dottrina statunitense, particolarmente dedita alla tematica dei *cybercrimes* transnazionali, che considererebbe la condotta della Russia non corrispondente allo standard richiesto dalla *due diligence* nel diritto internazionale.

Il fenomeno della mafia russa e degli attacchi informatici che hanno fatto del territorio della Russia un luogo cardine in cui i crimini cibernetici originano, ha portato la dottrina ad analizzare meglio la posizione dello Stato nella scena del diritto internazionale.¹⁹⁶

In particolar modo, sulla scia dell'aumento dei *cybercrimes* ascritti alla mafia russa e della loro portata dannosa¹⁹⁷, viene osservata la posizione della Russia in merito alla

¹⁹⁶ Ortner, Daniel. "Cybercrime and Punishment: The Russian Mafia and Russian Responsibility to Exercise Due Diligence to Prevent Trans-Boundary Cybercrime." *Brigham Young University Law review*, vol. 2015, no. 1, 2015, p. 178.

¹⁹⁷ Si sottolinea il caso dell'enorme *data breach* nel 2013 nei confronti di 110 milioni di conti di proprietà di consumatori Statunitensi, causata da una violazione informatica di una grande catena di negozi U.S.A denominata Target, ascritta alla mafia russa.

responsabilità che questa possa avere nei confronti del fenomeno criminale cibernetico, attualmente inarrestato. _¹⁹⁸

In primo luogo, viene ribadito che per poter considerare la Russia responsabile per i crimini cibernetici di attori non statali, come la mafia russa, è inderogabilmente previsto dall'art. 8 ARSIWA, come già ampiamente esaminato, che si provi concretamente una direzione e un controllo effettivo dello Stato sugli attacchi, o che vi sia una complicità concreta e consapevole dello Stato._¹⁹⁹ Nella pratica, nel 2007 e poi nel 2008, l'Estonia accusò la Russia di essere coinvolta negli attacchi informatici sofferti dal paese in quanto vi fossero prove del fatto che i *cybercrimes* originassero dall'ausilio operativo di server appartenenti al governo russo. _²⁰⁰

Dal 2007 fin ad ora la Russia, che si è sempre dichiarata non colpevole, non sembrerebbe essere mai stata chiamata dalla CIG a rispondere ufficialmente delle accuse dell'Estonia in quanto lo standard probatorio richiesto dagli ARSIWA nel diritto internazionale e che la stessa Corte fissa per questa forma di responsabilità, parrebbe chiedere molto più che una fragile evidenza di complicità, in particolare modo in un ambiente anonimo e occulto come quello cibernetico. _²⁰¹

Se l'elemento potenziale della complicità, che si manifesta nella realizzazione congiunta del crimine o nell'accondiscendenza dello Stato affinché questo venga realizzato, e della direzione non possono costituire responsabilità internazionale dello Stato per

¹⁹⁸ Ortner, Daniel. "Cybercrime and Punishment: The Russian Mafia and Russian Responsibility to Exercise Due Diligence to Prevent Trans-Boundary Cybercrime." *Brigham Young University Law review*, vol. 2015, no. 1, 2015, p. 178.

¹⁹⁹ Ortner, Daniel. "Cybercrime and Punishment: The Russian Mafia and Russian Responsibility to Exercise Due Diligence to Prevent Trans-Boundary Cybercrime." *Brigham Young University Law review*, vol. 2015, no. 1, 2015, p. 179.

²⁰⁰ Ortner, Daniel. "Cybercrime and Punishment: The Russian Mafia and Russian Responsibility to Exercise Due Diligence to Prevent Trans-Boundary Cybercrime." *Brigham Young University Law review*, vol. 2015, no. 1, 2015, p. 179.

²⁰¹ Ortner, Daniel. "Cybercrime and Punishment: The Russian Mafia and Russian Responsibility to Exercise Due Diligence to Prevent Trans-Boundary Cybercrime." *Brigham Young University Law review*, vol. 2015, no. 1, 2015, p. 180.

impossibilità probatoria, viene qui ribadita l'ipotesi di configurare responsabilità internazionale fondata sulla violazione del principio di *due diligence* cibernetica, considerando che nel diritto internazionale consuetudinario lo Stato è chiamato ad assumersi, in via generale, la responsabilità delle condotte negligenti poste in essere in rispetto del principio della *due diligence*.²⁰²

Quanto appena affermato è stato concretizzato nella giurisprudenza internazionale a partire dal caso *U.S.A c. Canada* (1941)²⁰³, deciso dal tribunale arbitrale internazionale, considerato *leading case* nello sviluppo dell'applicazione della *due diligence*²⁰⁴, ulteriormente richiamato dalla giurisprudenza della CIG che ha ribadito nel caso *Pulp Mills* (Argentina c. Uruguay, CIG 2010) come gli obblighi di prevenzione internazionalmente previsti comportano: “*to act with due diligence in respect of all activities which take place under the jurisdiction and control of each party.*”²⁰⁵

In particolar modo, il caso USA c. Canada ha stabilito per primo come gli Stati, seppure non coinvolti nel crimine di privati, debbano adoperarsi al massimo per evitare che il proprio territorio possa divenire luogo attraverso cui perpetrare il crimine e causare danni a terzi, richiamando il principio di *due diligence* come dovere atto a prevenire che dal crimine transfrontaliero non derivino danni anch'essi transfrontalieri.²⁰⁶

²⁰² Ortner, Daniel. “Cybercrime and Punishment: The Russian Mafia and Russian Responsibility to Exercise Due Diligence to Prevent Trans-Boundary Cybercrime.” *Brigham Young University Law review*, vol. 2015, no. 1, 2015, p. 182.

²⁰³ International Arbitral Tribunal. *Trail Smelter Case. United States v. Canada*. International Arbitral tribunal, 1941.

²⁰⁴ Ortner, Daniel. “Cybercrime and Punishment: The Russian Mafia and Russian Responsibility to Exercise Due Diligence to Prevent Trans-Boundary Cybercrime.” *Brigham Young University Law review*, vol. 2015, no. 1, 2015, p. 198.

²⁰⁵ International Court of Justice. *Pulp Mills on the River Uruguay (Argentina v. Uruguay)*, Reports of Judgements, Advisory Opinions and Orders, 20 April 2010, para. 197, p. 69.

²⁰⁶ Ortner, Daniel. “Cybercrime and Punishment: The Russian Mafia and Russian Responsibility to Exercise Due Diligence to Prevent Trans-Boundary Cybercrime.” *Brigham Young University Law review*, vol. 2015, no. 1, 2015, p. 182.

Alla luce di tali presupposti giuridici posti a fondamento della *due diligence* e richiamati in giurisprudenza, è opportuno tornare all'analisi del caso oggetto della seguente trattazione. Come precedentemente accennato, la proliferazione del fenomeno mafioso e della sua evoluzione informatica in Russia ha portato la dottrina ad interrogarsi sullo standard di *due diligence* effettivamente attuato dallo Stato russo per reprimere e porre rimedio all'estensione delle attività illecite, e ancora, se questo effettivamente soddisfi il criterio di diligenza richiesta dal diritto internazionale.

In primo luogo, non essendo la Russia mai stata ufficialmente giudicata da nessun tribunale internazionale come responsabile di *cybercrimes* mafiosi per violazione o omissione della *due diligence* in materia, appare opportuno segnalare che, fermo restando il rispetto del dovere di *due diligence* da parte della Russia, l'analisi che si condurrà circa il criterio delle misure adottate vuole solo osservare se la diligenza applicata dallo Stato sia risultata effettivamente soddisfattiva dello standard richiesto dal diritto internazionale, e se possa dirsi coerente rispetto alle possibilità della Russia di adottare misure preventive rigide e della funzionalità di queste rispetto ai risultati raggiunti odiernamente.

Dopo gli attacchi nei confronti dell'Estonia e degli Stati Uniti (caso Target osservato prima) che rappresentano due degli agguati informatici più imponenti, la Russia si è dovuta interfacciare con il fenomeno degli attacchi informatici mirati a sottrarre denaro e dati personali da banche e internazionali. ²⁰⁷

Il governo della Russia parrebbe aver rispettato il dovere della *due diligence* divenendo più rigorosa nei controlli atti alla prevenzione della corruzione, applicando misure repressive del fenomeno del riciclaggio mafioso e infine incrementando gli sforzi per garantire che le attività redditizie della mafia non si espandessero. ²⁰⁸

Nonostante questo, la mafia non ha mai mostrato segni di debolezza, anzi si è evoluta nel mondo digitale divenendo più invasiva e meno governabile. Lo scenario proliferativo

²⁰⁷ McDougal, Trevor. "Establishing Russia's responsibility from Cyber-Crime Based on its hacker Culture." *Brigham Young University International Law and Management Review*, vol.11, no. 2, Summer 2015, p. 65.

²⁰⁸ Ortner, Daniel. "Cybercrime and Punishment: The Russian Mafia and Russian Responsibility to Exercise Due Diligence to Prevent Trans-Boundary Cybercrime." *Brigham Young University Law review*, vol. 2015, no. 1, 2015, pp. 202, 203.

della criminalità organizzata russa nel *cyberspace* potrebbe apparire estremamente complesso per gli Stati, ai quali il diritto internazionale chiede di applicare tutte le misure necessarie per prevenire e contrastare il fenomeno, con specifico riferimento a quelle misure che rientrino nelle capacità dello stato, come osservato dalla Corte nel caso *Pulp Mills* in cui ha sottolineato che le misure richieste agli Stati debbano essere: “appropriate”²⁰⁹ e dunque proporzionate alle facoltà dello Stato di intervenire.

Sebbene venga riconosciuto alla Russia di aver rispettato il dovere di *due diligence* con l’istituzione di gruppi informatici come il Russian Business Network²¹⁰, in passato impegnato nel perseguimento dei crimini informatici delle mafie legati alla pedopornografia e al furto di dati identificativi, tali misure di contrasto sono state considerate da gran parte della dottrina internazionale, come quella degli studiosi Ortner e McDougal, come insufficienti e spesso sproporzionate rispetto alle sofisticate facoltà informatiche e investigative di cui la Russia gode.²¹¹ Inoltre, la dottrina metterebbe in discussione il “*certain level of vigilance*”²¹² attuato dalla Russia in materia di vigilanza sulle infrastrutture informatiche del governo, in ragione del fatto che spesso si è osservato come, al fine di attuare il lancio di un attacco cibernetico, le organizzazioni mafiose russe siano state in grado di violare i server governativi avvalendosene, sollevando dei dubbi

²⁰⁹ International Court of Justice. *Pulp Mills on the River Uruguay (Argentina v. Uruguay)*, Reports of Judgements, Advisory Opinions and Orders 20 April 2010, para. 197, p. 69.

²¹⁰ RBN: il Russian Business Network è un gruppo informatico russo atto alla sorveglianza e alla repressione di crimini informatici attuati dalla mafia russa nel traffico virtuale.

²¹¹ Ortner, Daniel. “Cybercrime and Punishment: The Russian Mafia and Russian Responsibility to Exercise Due Diligence to Prevent Trans-Boundary Cybercrime.” *Brigham Young University Law review*, vol. 2015, no. 1, 2015, p. 203.

²¹² International Court of Justice. *Pulp Mills on the River Uruguay (Argentina v. Uruguay)*. Reports of Judgements, Advisory Opinions and Orders, 20 April 2010, para. 197, p.69.

circa il livello di vigilanza attuato dalla Russia sulle infrastrutture informatiche governative.²¹³

Pertanto, alla luce di tale osservazione, è possibile considerare che la diligenza attuata dalla Russia possa dirsi minima rispetto allo standard di *due diligence* richiesto e chiarito dalla giurisprudenza internazionale della Corte Internazionale di Giustizia e in particolare modo incoerente con le ampie capacità informatiche che la Russia detiene.

Difatti, in casi come *Bosnia c. Serbia* (2007)²¹⁴, *Argentina c. Uruguay* (2010)²¹⁵ e ancora *Regno Unito c. Albania* (1949)²¹⁶, la Corte ha definito il principio che impone l'adozione di misure di *due diligence* proporzionate e adeguate rispetto alle facoltà e alle capacità di cui lo Stato è in possesso, affermando come: “*A State is thus obliged to use all the means at its disposal in order to avoid activities which take place in its territory, or in any area of another State.*”²¹⁷

Al fine di pervenire ad una conclusione che possa dirsi completa si pone in evidenza come, nonostante il criterio attuato dalla Russia non abbia mai formato oggetto di attribuzione di responsabilità internazionale da parte della CIG, il Consiglio Federale russo (a partire dal 2013) si è adoperato per implementare il piano di sicurezza informatica statale al fine di innalzare lo standard di *due diligence* rispetto al fenomeno *cyber* mafioso, evidenziando quindi che le osservazioni critiche precedentemente esaminate sulle lacune

²¹³Ortner, Daniel. “Cybercrime and Punishment: The Russian Mafia and Russian Responsibility to Exercise Due Diligence to Prevent Trans-Boundary Cybercrime.” *Brigham Young University Law review*, vol. 2015, no. 1, 2015, p. 204.

²¹⁴ International Court of Justice. *Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro)*. I.C.J. 2007, p. 43.

²¹⁵ International Court of Justice. *Pulp Mills on the River Uruguay (Argentina v. Uruguay)*. Reports of Judgements, Advisory Opinions and Orders, 20 April 2010.

²¹⁶ Corte Internazionale di Giustizia. *Corfu Channel Case (Regno Unito v. Albania)*. Sentenza del 25 Marzo 1948, p.15.

²¹⁷ International Court of Justice. *Pulp Mills on the River Uruguay (Argentina v. Uruguay)*. Reports of Judgements, Advisory Opinions and Orders, 20 April 2010, para. 101, p. 46.

della Russia in materia di *cyber due diligence* possano effettivamente dirsi basate su un fondamento ragionevole. ²¹⁸

2.4 Conclusioni.

Il capitolo II, giunto a conclusione, ha voluto offrire un'analisi della tematica centrale su cui il presente elaborato si basa, inerente a come, nel diritto internazionale, lo Stato possa rispondere delle attività illecite dei privati, con particolare riferimento all'entità criminale delle mafie. Dopo un'ampia introduzione sulle origini e sull'evoluzione del concetto di responsabilità nel diritto internazionale, è stato introdotto ed esaminato il ruolo del Progetto ARSIWA che ha rappresentato l'opera di codificazione più rilevante dell'istituto della responsabilità internazionale. Rispetto all'oggetto del presente elaborato, incentrato sull'apparato criminale mafioso (tradizionale e moderno), è parsa coerente l'analisi dei criteri di attribuzione delle condotte illecite dei privati allo Stato, statuiti dall'articolo 8 ARSIWA. Se da una parte l'esame di tale norma ha messo in luce la possibilità di creare un collegamento tra lo Stato e le attività delle mafie in quanto è stato osservato come sia possibile includere nella categoria degli attori non statali ex art. 8 anche l'entità dei gruppi criminali mafiosi di cui l'elaborato tratta, dall'altra parte, tramite l'esame dei criteri di attribuzione dettati dalla norma, è stato possibile osservare come l'ascrizione delle condotte di tali gruppi allo Stato sia particolarmente complessa, poiché lo standard probatorio stabilito dall'art. 8 richiede la prova concreta di una direzione e di un controllo effettivo dello Stato sulle attività illecite dei gruppi, circostanza, oltre che complessa, attualmente mai riscontrata nella giurisprudenza internazionale. Alla luce della rigidità dello standard probatorio ex art. 8 ARSIWA è parso opportuno esaminare se il diritto internazionale potesse prevedere un ulteriore meccanismo giuridico in grado di attribuire, sulla base di un criterio più flessibile, la responsabilità internazionale allo Stato per le attività illecite commesse da privati come le organizzazioni criminali, non sulla base dell'ascrizione allo Stato del crimine in sé, bensì sull'attribuzione delle conseguenze che

²¹⁸ Ortner, Daniel. "Cybercrime and Punishment: The Russian Mafia and Russian Responsibility to Exercise Due Diligence to Prevent Trans-Boundary Cybercrime." *Brigham Young University Law review*, vol. 2015, no. 1, 2015, p. 213.

da questo sono derivate. Pertanto, l'elaborato ha voluto spostare l'attenzione sul principio internazionale della *due diligence*, il quale detiene un ruolo centrale in tema di responsabilità internazionale degli Stati e che conta di una concreta importanza pratica in giurisprudenza. Partendo ad analizzare l'intero contesto storico evolutivo del principio, la trattazione è poi giunta all'esame generale della fattispecie violativa ed omissiva del principio di *due diligence* da parte dello Stato, in particolare riferendo l'analisi alla violazione e all'omissione della diligenza che lo Stato è chiamato a porre in essere anche nel caso in cui siano i privati, come le organizzazioni criminali, a realizzare le attività illecite. Pertanto, l'elaborato ha voluto esaminare come, sebbene negli ARSIWA l'attribuzione delle condotte criminose dei gruppi privati allo Stato risulti complessa alla luce dell'onerosità del criterio probatorio ex art. 8 ARSIWA, ciò non esclude la configurazione della responsabilità internazionale dello Stato fondata sulla violazione o omissione del principio di *due diligence* circa le attività illecite di gruppi criminali privati. Vale a dire che allo Stato non viene attribuita responsabilità per la commissione del crimine, bensì per il fatto che abbia mancato di prevenirne l'avvenimento o non abbia limitato le conseguenze dannose derivanti da tale illecito.

Attualmente, l'ambito più problematico in tema attribuzione di responsabilità internazionale per gli illeciti attuati da privati, in particolare modo dalle organizzazioni criminali transnazionali, è il *cyberspace*. Alla luce del fatto che il dominio virtuale oggi rappresenta il luogo da cui le attività criminali originano, è parso opportuno analizzare se lo Stato possa essere chiamato a risponderne e sulla base di quale fondamento giuridico. Pertanto, dopo aver osservato come l'art. 8 possa dirsi particolarmente inoperabile nello spazio virtuale, per le caratteristiche occulte della rete, è stata analizzata la declinazione del principio della *due diligence* allo spazio cibernetico, al fine di esaminare in che modo questo potesse o meno risolvere il deficit di attribuzione della responsabilità allo Stato per le attività illecite delle mafie nel *cyberspace*.

Dall'analisi svolta è emerso come lo Stato sia chiamato ad attuare la diligenza dovuta anche nello spazio cibernetico, prevenendo e reprimendo le conseguenze dannose dei crimini informatici tramite l'attuazione di misure appropriate; pertanto, una violazione o omissione di tale obbligo di prevenzione porterebbe senz'altro all'attribuzione della responsabilità internazionale anche nel caso di *cybercrimes* a stampo mafioso. Al fine di concretizzare quanto analizzato nella teoria, l'elaborato ha preso in considerazione il

fenomeno dei *cyber* attacchi attuati dalla mafia russa con lo scopo di analizzare se lo Stato abbia effettivamente posto in essere la diligenza richiesta. Nonostante l'agire della Russia abbia evitato allo Stato di finire al centro di un'imputazione per responsabilità internazionale da violazione della *due diligence* in tema di *cybercrimes* attuati dalla mafia, la dottrina è apparsa molto severa nei confronti dello Stato, considerando il comportamento e le misure attuate dalla Russia come insoddisfacenti e sproporzionate rispetto al criterio di *due diligence* generalmente richiesto dal diritto internazionale consuetudinario.

Alla luce dell'analisi giuridica fin qui condotta, l'ultimo capitolo che segue vuole offrire un esame delle prospettive internazionali future che potrebbero portare gli Stati all'attuazione di misure preventive e repressive che possano dirsi attuali e funzionali rispetto all'entità mafiosa cibernetica che affligge gli Stati oggi. Difatti, costituirà oggetto di critica tanto il contenuto della Convenzione di Palermo, ritenuto potenzialmente obsoleto rispetto alle nuove forme di criminalità organizzata del *cyberspace*, quanto quello della Convenzione di Budapest, attualmente lo strumento convenzionale di riferimento in vigore, tuttavia non aggiornata sui nuovi modelli di *cybercrime* attuati dalle mafie.

In virtù delle critiche che si avanzeranno legate agli aspetti sopra citati, si analizzeranno le novità più recenti in tema di criminalità organizzata informatica, in particolar modo verrà esposta una la nuova frontiera di contrasto al crimine informatico offerta dal nuovo Trattato Globale sul *cybercrime*, adottato dalle Nazioni Unite che attualmente è in attesa di entrare in vigore, e ancora, il potenziale vantaggio che l'Intelligenza Artificiale e gli strumenti a questa connessi, possa offrire agli Stati nelle operazioni di contrasto all'entità cibernetica mafiosa.

Capitolo 3

I nuovi strumenti di repressione e di contrasto alla criminalità organizzata transnazionale.

3.1 Critica all'obsoleta Convenzione di Palermo rispetto alle nuove forme di mafie nel mondo *cyber*.

In questo capitolo conclusivo, dopo aver analizzato i profili giuridici legati alla posizione dello Stato rispetto alle attività illecite delle organizzazioni criminali nel mondo, sarà opportuno spostare l'attenzione sull'esame degli attuali strumenti di prevenzione e contrasto nei confronti dell'entità criminale organizzata transnazionale, fino ad arrivare all'esame delle soluzioni future che possano porvi rimedio. L'analisi descritta originerà da una critica alla Convenzione di Palermo del 2000 e alla sua natura obsoleta rispetto alle nuove forme di crimine nell'era digitale. É indiscusso che la Convenzione di Palermo rappresenti tutt'oggi lo strumento principale per la cooperazione internazionale degli Stati nella lotta alla criminalità organizzata transnazionale, ma potrebbe essere altrettanto evidente che l'evoluzione delle organizzazioni criminali nel settore cibernetico pongono la necessità di aggiornare ed integrare gli articoli della Convenzione che non apparirebbero più attuali e funzionali rispetto ai nuovi settori in cui le mafie si prestano ad operare. Sebbene parte della dottrina internazionale consideri tutt'ora la Convenzione come dinamica, in grado di rispondere all'evoluzione costante del globo, tuttavia, alla luce della proliferazione delle nuove strutture mafiose cibernetiche quanto detto parrebbe non trovare più evidenze pratiche.²¹⁹

Pertanto, a più di vent'anni dalla sua entrata in vigore, la Convenzione potrebbe risultare datata in confronto alla moltitudine di nuovi traffici realizzati dalla criminalità organizzata, basati quasi del tutto su transazioni online e su frodi e truffe digitalizzate.

²¹⁹ Mattarella Andrea, Balsamo Antonio, Tartaglia Roberto. *La Convenzione di Palermo: il futuro della lotta alla criminalità organizzata transnazionale*. G. Giappichelli Editore, 2020, p. 7.

Se è vero che la Convenzione si prefigge l'obiettivo ultimo di sradicare il fenomeno mafioso tramite la cooperazione internazionale e l'adozione di misure statali repressive, potrebbe dirsi altrettanto fondata la necessità di aggiornare e potenziare tali misure per essere funzionali.

Si analizzerà, nel paragrafo che segue, quali sono effettivamente gli aspetti obsoleti della Convenzione, attraverso un'analisi comparativa delle sfide criminali del passato rispetto a quelle del presente, suggerendo come tali minacce dovrebbero essere affrontate in maniera progressiva ed innovativa a partire dall'individuazione delle organizzazioni criminali tradizionali ma anche moderne.

3.1.1 Le criticità della Convenzione di Palermo rispetto all'evoluzione criminale nell'era digitale.

Il 29 settembre del 2023 è stato festeggiato il ventesimo anniversario dall'entrata in vigore della Convenzione delle Nazioni Unite contro la criminalità organizzata transnazionale che continua a rappresentare la cornice normativa internazionale della tematica di lotta al fenomeno del crimine organizzato.

Per tutti questi anni, i 193 Stati aderenti alla Convenzione hanno cercato di adottare quanto imposto da questa per la realizzazione di una cooperazione internazionale che potesse essere distruttiva per l'entità mafiosa, eppure potrebbe essere messo in discussione se tutto ciò abbia effettivamente portato ai risultati che Falcone auspicava trent'anni fa, in quanto si è dinnanzi ad un attuale fenomeno mafioso potenziato ed evoluto al punto tale da riuscire a sostenere attività criminali imponenti e invisibili perché virtuali. Tuttavia, rimane indiscusso il fatto che, nonostante le lacune che verranno osservate, la Convenzione di Palermo è riuscita nella configurazione di una giurisprudenza comune tra gli Stati in grado di riflettere la medesima unicità e specificità di cui le mafie sono composte, al fine ultimo di reprimerle. ²²⁰

²²⁰ Mattarella Andrea, Balsamo Antonio, Tartaglia Roberto. *La Convenzione di Palermo: il futuro della lotta alla criminalità organizzata transnazionale*. G. Giappichelli Editore, 2020, p. 15.

Attualmente la visione della Convenzione potrebbe apparire illusoria, a partire da alcune lacune che potrebbero essere causa di complicazione per la lotta alle organizzazioni criminali transnazionali.

Alla luce degli aspetti critici della Convenzione che saranno successivamente oggetto di trattazione, si osserverà come, nonostante i molteplici passi in avanti registrati nell'ambito della cooperazione giudiziaria internazionale, sono ancora molte le criticità da cui l'azione di repressione alla criminalità organizzata transnazionale è contrassegnata.²²¹

Una prima possibile mancanza della Convenzione potrebbe essere legata all'aspetto della cooperazione internazionale nel contrasto alla criminalità organizzata: seppure la Convenzione sia unica, gli approcci che gli Stati fanno di questa sono differenti tra loro, sia nella definizione delle minacce, sia in quella dei rischi.²²²

Rispetto a tale problematica si potrebbe aggiungere un'applicazione inefficace degli articoli regolati dalla Convenzione, in quanto le implementazioni che gli Stati aderenti fanno della Convenzione non sono state seguite da tutti gli Stati con leggi sufficientemente rigorose e definite.²²³

²²¹ Roberti Franco, Musacchio Vincenzo. “La lotta alle nuove mafie va combattuta a livello transnazionale”, *diritto penale e uomo*, 2021, consultabile sul sito https://dirittopenaleuomo.org/contributi_dpu/la-lotta-alle-nuove-mafie-va-combattuta-a-livello-transnazionale/

²²² Roberti Franco, Musacchio Vincenzo. “La lotta alle nuove mafie va combattuta a livello transnazionale.” *Diritto penale e uomo*, 2021, consultabile sul sito https://dirittopenaleuomo.org/contributi_dpu/la-lotta-alle-nuove-mafie-va-combattuta-a-livello-transnazionale/

²²³ Quanto detto si potrebbe fondare sul fatto che sono molteplici gli Stati che fanno parte della Convenzione, alcuni dotati di una legislazione più rigida e restrittiva in settori specifici del crimine organizzato, altri meno. Per tale motivo la Convenzione risulterebbe rispettata maggiormente da quegli Stati in cui vigono leggi severe e poco permissive, lo stesso non si potrebbe dire per quegli Stati in cui la legislazione è meno ristretta.

Tale frammentazione di approcci diversi da parte degli Stati rispetto alla Convenzione, potrebbe rendere estremamente limitata la possibilità di realizzare effettivamente un contrasto univoco efficace.²²⁴

Una seconda possibile mancanza potrebbe individuarsi nel meccanismo di supervisione sull'effettiva attuazione delle misure richieste dalla Convenzione da parte degli Stati aderenti.²²⁵

La Convenzione ha da sempre sottolineato l'importanza di prevedere dei meccanismi internazionali di controllo delle azioni che gli Stati pongono in essere per realizzare gli impegni ai quali la Convenzione li obbliga, un meccanismo di supervisione atto a garantire l'efficacia delle azioni Statali.²²⁶

Nonostante questo, all'interno della Convenzione, le Nazioni Unite non hanno mai previsto dei meccanismi vincolanti in grado di supervisionare che le misure imposte da questa venissero concretamente rispettate.

Allo stesso modo non viene previsto un sistema di monitoraggio dei programmi o delle azioni adottate dagli Stati (sulla base di ciò che la Convenzione chiede) per reprimere la criminalità organizzata transnazionale.

Quanto detto potrebbe costituire la causa principale del fatto che, nonostante l'impegno degli Stati e delle Nazioni Unite, a distanza di più di venti anni dalla nascita della

²²⁴ Roberti Franco, Musacchio Vincenzo. "La lotta alle nuove mafie va combattuta a livello transnazionale". *Diritto penale e uomo*, 2021, consultabile sul sito https://dirittopenaleuomo.org/contributi_dpu/la-lotta-alle-nuove-mafie-va-combattuta-a-livello-transnazionale/

²²⁵ Roberti Franco, Musacchio Vincenzo. "La lotta alle nuove mafie va combattuta a livello transnazionale". *Diritto penale e uomo*, 2021, consultabile sul sito https://dirittopenaleuomo.org/contributi_dpu/la-lotta-alle-nuove-mafie-va-combattuta-a-livello-transnazionale/

²²⁶ Roberti Franco, Musacchio Vincenzo. "La lotta alle nuove mafie va combattuta a livello transnazionale". *Diritto penale e uomo*, 2021, consultabile sul sito https://dirittopenaleuomo.org/contributi_dpu/la-lotta-alle-nuove-mafie-va-combattuta-a-livello-transnazionale/

Convenzione le più dannose attività realizzate dalle organizzazioni criminali sono ancora in auge e anzi si sono evolute.

Il terzo e probabilmente più lacunoso aspetto riguarderebbe la mancata regolamentazione del *cyber crime* mafioso, e in generale, dell'implementazione digitale attuata dalle organizzazioni criminali per realizzare le attività illecite.

Dopo più di venti anni dall'entrata in vigore della Convenzione non vi sono state delle revisioni atte ad immettere tra gli articoli di questa dei riferimenti al crimine informatico. Tutto ciò potrebbe rappresentare fonte di critica alla Convenzione in quanto, alla luce dell'evoluzione digitale che il crimine organizzato ha subito nell'arco degli ultimi tempi ²²⁷, la mancanza di un intervento al riguardo potrebbe rappresentare la causa della lacunosità delle azioni di contrasto adottate dagli Stati.

In conclusione, alla luce del fatto che le organizzazioni criminali transnazionali ad oggi si muovono maggiormente sulle reti web e attuano crimini grazie all'utilizzo di strumenti digitali, (come l'intelligenza artificiale) si potrebbe avanzare una critica all'arretratezza della Convenzione di Palermo, in quanto, per come la Convenzione è rimasta, potrebbe dirsi logico che gli Stati non riescano effettivamente ad adottare misure repressive che seguano effettivamente le attuali rotte invisibili dei traffici della mafia e quindi parrebbe conseguenziale che il fenomeno criminale accresca anziché diminuire.

3.1.2 La necessità per la Convenzione di essere aggiornata sulla criminalità informatica e sui nuovi crimini organizzati del web: il *phishing* e la tratta illecite nel *dark web*.

Nel paragrafo precedente si è trattato degli aspetti che potrebbero essere considerati lacunosi all'interno della Convenzione di Palermo, soffermandosi in particolare sul terzo

²²⁷ Per evoluzione digitale si intende il processo di trasformazione informatica che il mondo si trova a vivere e con il quale la criminalità organizzata transnazionale oggi opera. Tale fenomeno è dato dal fatto che nel mondo internet le mafie hanno saputo adattare i crimini rendendoli sempre più efficienti e sofisticati, trasformando il crimine tradizionale in cybercrimini che oggi rappresentano una delle minacce principali per il sistema socio-economico. (Gabrielli, Ivano. "Come le mafie si muovono nel mondo della rete." Scintille, Trimestrale della fondazione scintille di futuro, 2023, p. 28.)

aspetto indicato come il più critico: l'assenza all'interno della Convenzione di una regolamentazione aggiornata che riguardi il settore dei traffici illeciti virtuali, fonte di guadagno primaria per le più grandi organizzazioni criminali transnazionali.

Per quanto la Convenzione abbia rappresentato il passo più importante mai fatto nella storia globale della lotta alla criminalità organizzata transnazionale, bisognerebbe riconoscere la necessità di aggiornarla se si vuole effettivamente abbattere il fenomeno criminale, come Falcone auspicava.

La prima opera di aggiornamento potrebbe riguardare la visione che la Convenzione offre della criminalità organizzata transnazionale. La definizione di gruppo criminale organizzato transfrontaliero è quella puramente tradizionale, ossia riferita a quei gruppi di soggetti fondati su di una organizzazione strutturata e stabile che si prefiggono l'obiettivo comune di arricchirsi illecitamente a livello internazionale, sfruttando le attività più minatorie per la sicurezza della comunità internazionale, tra cui il traffico di stupefacenti, la tratta di persone e di migranti, nonché il riciclaggio e il traffico di beni culturali.²²⁸

Ad oggi la criminalità organizzata transnazionale continua ad esistere come un gruppo di soggetti organizzato e strutturato che delinque attraverso la realizzazione di tali attività, ma queste ultime hanno assunto una forma nettamente nuova rispetto al passato, il che rende necessario aggiornare o meglio implementare la concezione di criminalità organizzata transnazionale che la Convenzione enuncia agli Stati, rendendoli consapevoli delle nuove tipologie di organizzazioni criminali che oggi si trovano ad affrontare.

Quanto detto è estremamente rilevante per l'efficienza repressiva che gli Stati dovrebbero attuare, una strategia che si fonda sulla consapevolezza che la macchina del crimine organizzato si è evoluta divenendo non più assimilabile a come l'aveva combattuta e poi lasciata Falcone, ma opera con degli strumenti e in dei settori di pertinenza completamente nuovi rispetto al passato.²²⁹

²²⁸ United Nations Office of Drugs and Crime. *Digesto di casi di criminalità organizzata. Raccolta commentata di casi e lezioni apprese*. Vienna, Nazioni Unite, 2012, p. 9.

²²⁹ Mele, Pierluigi. "Radiologia delle nuove mafie: invisibili, tecnologiche e transnazionali" *Rai news*, 2025, consultabile sul sito

Le nuove forme di organizzazioni criminali transnazionali si sono evolute digitalmente soprattutto nel campo dell'informazione e della comunicazione, ma anche nel settore del commercio globale in cui l'evoluzione criminale ha progressivamente reso i traffici all'avanguardia attraverso l'utilizzo di piattaforme digitali. ²³⁰

Tra i crimini maggiormente realizzati dalle mafie odierne ve ne sarebbero due che la Convenzione dovrebbe prevedere oggi per poter riuscire a potenziarsi come strumento principale di lotta alla criminalità organizzata transnazionale: il *phishing* e le tratta illecite sul *dark web*.

Partendo dal *phishing*, questo rappresenta il crimine informatico più in voga tra le organizzazioni criminali, si tratta dell'organizzare truffe attraverso Internet, in grado di aggirare gli utenti e indurli ad offrire i loro dati sensibili come password, informazioni personali e dati bancari.²³¹

É un attacco estremamente dannoso che i gruppi criminali attuano assumendo l'identità di banche, enti pubblici o anche semplici persone.²³²

Il *phishing* attuato dalla mafia transnazionale avrebbe dovuto entrare a far parte della regolamentazione della Convenzione, in quanto strumento principe di contrasto al fenomeno; tuttavia, non essendo previsto dal trattato, oggi il crimine informatico del *phishing* ha avuto l'opportunità di evolversi.²³³

<https://www.rainews.it/articoli/2025/03/le-nuove-mafie-invisibili-tecnologiche-e-transnazionali-fcc547fb-65bb-4231-a5d1-1b6a1703c62a.html>

²³⁰ Mele, Pierluigi. "Radiologia delle nuove mafie: invisibili, tecnologiche e transnazionali" *Rai news*, 2025, consultabile sul sito <https://www.rainews.it/articoli/2025/03/le-nuove-mafie-invisibili-tecnologiche-e-transnazionali-fcc547fb-65bb-4231-a5d1-1b6a1703c62a.html>

²³¹ Tecnodigitale. "Cos'è il phishing: 10 segnali di allarme." *Informatec digital*, 2024, consultabile su <https://informatecdigital.com/it/cos%27%C3%A8-il-phishing/>

²³² Tecnodigitale. "Cos'è il phishing: 10 segnali di allarme." *Informatec digital*, 2024, consultabile su <https://informatecdigital.com/it/cos%27%C3%A8-il-phishing/>

²³³ Tecnodigitale. "Cos'è il phishing: 10 segnali di allarme." *Informatec digital*, 2024, consultabile su <https://informatecdigital.com/it/cos%27%C3%A8-il-phishing/>

È difatti emerso il c.d. “*spear phishing*”²³⁴, un modello di crimine informatico organizzato attraverso il quale le grandi organizzazioni criminali conducono attacchi estremamente più mirati e personalizzati; difatti, le e-mail che vengono generate attraverso tale crimine, vengono studiate al punto tale da essere personalizzate e accattivanti, in grado di riuscire ad ottenere la fiducia di qualsiasi utente.²³⁵

Oltre al *phishing* e allo *spear phishing*, la criminalità organizzata transnazionale realizza i traffici più potenti e oscuri nell’angolo nero della rete, ossia il *dark web*. Le sezioni oscure di internet come il *dark* e il *deep web* sono state già oggetto di trattazione nel primo capitolo, ma verranno qui ritrattate nell’ambito degli aspetti lacunosi della Convenzione delle Nazioni Unite.

Il *dark web* rappresenta il luogo sicuro di tutte le tratte illecite (esseri umani, migranti, armi, droga, organi ecc..) e dei guadagni delle organizzazioni criminali in tutto il mondo. Controllare l’identità degli utenti che sfruttano il *dark web* è un’operazione complessa data la natura anonima degli accessi in queste aree virtuali; tuttavia, apparirebbe incoerente con gli obiettivi della Convenzione non proporre un aggiornamento normativo su tale tematica, che possa menzionare l’esistenza del *Dark web* e ammonire gli Stati al riguardo.

L’obsolescenza della Convenzione delle Nazioni Unite potrebbe quindi discendere dalla concezione di criminalità organizzata transnazionale ormai passata in quanto riferita solo a quella forma di mafia visibile, tangibile nelle sue operazioni ed individuabile attraverso piani di azione tradizionali.

Ad oggi la maggior parte delle organizzazioni criminali (soprattutto quelle più note come ‘ndrangheta) non corrispondono più a quelle regolamentate dalla Convenzione, oggi le mafie sono invisibili, difficilmente riconoscibili ed estremamente istruite, soprattutto in campo informatico.

²³⁴ Tecnodigitale. “Cos’è il phishing: 10 segnali di allarme.” *Informattec digital*, 2024, consultabile su <https://informatecdigital.com/it/cos%27%C3%A8-il-phishing/>

²³⁵ Tecnodigitale. “Cos’è il phishing: 10 segnali di allarme.” *Informattec digital*, 2024, consultabile su <https://informatecdigital.com/it/cos%27%C3%A8-il-phishing/>

3.1.3 La mancanza di prospettive future nella Convenzione di Palermo.

Avendo trattato criticamente gli aspetti della Convenzione di Palermo considerati obsoleti, è opportuno analizzare un'ultima carenza da cui la Convenzione oggi potrebbe dirsi caratterizzata: l'assenza di prospettive future. Contrariamente a quella che era la visione futuristica di Falcone, la Convenzione, oltre a non trattare l'entità della criminalità organizzata informatica, non parrebbe essere caratterizzata da prospettive future sul contrasto alla mafia transnazionale, se per futuro si intende la sua evoluzione digitale. Alla luce di quanto osservato, è opportuno rimarcare come l'estrema rilevanza di Falcone in tema di lotta alla criminalità organizzata transnazionale rimarrà indiscussa nel tempo, tuttavia, lasciare che la Convenzione di Palermo rimanga eccessivamente ancorata alla concezione mafiosa degli anni 2000, potrebbe portare a risultati controproducenti. La visione di Falcone è figlia di un'epoca ben specifica, una realtà in cui la criminalità organizzata, sebbene complessa, non presentava delle caratteristiche così insidiose e occulte come oggi. Attualmente, la Convenzione di Palermo viene definita dalla maggior parte degli studi come *“uno strumento progettato guardando al futuro”*²³⁶

Ora, è opportuno affrontare due tematiche specifiche che potrebbero smentire tale concezione futuristica della Convenzione e che potrebbero avvalorare l'ipotesi dell'effettiva necessità di revisionarla attraverso un aggiornamento in grado da renderla concretamente futuristica.

La prima tematica che potrebbe mutare l'idea per cui la Convenzione è ancora l'unico strumento in grado di essere attuale in qualsiasi epoca nella lotta alla criminalità organizzata è legata agli strumenti da questa proposti per contrastare il fenomeno criminale.

La Convenzione è nata applicando gli strumenti che Falcone proponeva come necessari per il contrasto alla criminalità organizzata transnazionale che erano due: la cooperazione internazionale degli Stati e le operazioni investigative e di polizia congiunte tra gli Stati.

²³⁶ Centro studi Livatino. “La Convenzione di Palermo a vent'anni dalla sua entrata in vigore.” 2023, consultabile sul sito <https://www.centrostudilivatino.it/la-convenzione-di-palermo-a-ventanni-dalla-sua-entrata-in-vigore/>

Ora, non si intende discutere l'effettività e la funzionalità di tali strategie che sono state insindacabilmente il fulcro del sistema di lotta alla criminalità organizzata e che hanno portato a scovare numerosi gruppi criminali nella storia del contrasto alla mafia; ciò che si intende porre in evidenza è l'assenza di potenziamento e di aggiornamento di tali misure rispetto alle minacce odierne, presentate da una forma di crimine organizzato diverso rispetto al passato.

Il 16 ottobre del 2020 è stata adottata la c.d. "Risoluzione Falcone", un tentativo di aggiornamento della Convenzione presentata dall'Italia come la concretizzazione delle linee guida lasciate da Falcone venti anni prima.²³⁷

Tra le sue iniziative più incisive vengono sottolineate alcune nuove disposizioni inerenti alla raccolta delle prove elettroniche e all'utilizzo di tecniche investigative speciali che sfociano nella sorveglianza elettronica.²³⁸

Le Nazioni Unite, quindi, avrebbero incentrato l'opera di revisione della Convenzione verso l'armonizzazione della cooperazione giudiziaria internazionale, modernizzando le tecniche investigative speciali della Convenzione ed immettendo in queste ogni metodo avanzato di raccolta delle prove digitali.

Alla luce di quanto affermato, sorgerebbe una domanda rilevante: come si potrebbe definire la Convenzione di Palermo uno strumento vivente e attuale se nell'unica (e tardiva) opera di revisione che gli Stati hanno attuato, non vengono menzionate le nuove tecnologie criminali e non si formulano strategie informatiche future per i rischi che stanno invadendo il globo?

Potrebbe essere plausibile quindi, che alla luce di tutti gli aspetti potenzialmente datati, analizzati all'interno della Convenzione, la risposta non potrà che risultare negativa.

²³⁷ Centro studi Livatino. "La Convenzione di Palermo a vent'anni dalla sua entrata in vigore." 2023, consultabile sul sito <https://www.centrostudilivatino.it/la-convenzione-di-palermo-a-ventanni-dalla-sua-entrata-in-vigore/>

²³⁸ Centro studi Livatino. "La Convenzione di Palermo a vent'anni dalla sua entrata in vigore." 2023, consultabile sul sito <https://www.centrostudilivatino.it/la-convenzione-di-palermo-a-ventanni-dalla-sua-entrata-in-vigore/>

3.1.4 I possibili scenari futuri.

La seconda tematica che potrebbe far dubitare dell'idea per cui la Convenzione di Palermo sia ancora l'unico strumento in grado di risultare sempre attuale nella lotta alla criminalità organizzata transnazionale, risiede nel fatto che le Nazioni Unite stanno avvertendo la necessità di produrre nuovi strumenti convenzionali, che saranno oggetto di analisi nel corso del capitolo.

Alla luce di ciò, la critica mossa fino ad ora alla Convenzione potrebbe essere avvalorata: le zone d'ombra della Convenzione di Palermo e l'obsolescenza delle sue visioni devono essere colmate se gli Stati vogliono effettivamente contrastare la criminalità organizzata transnazionale.

In particolar modo, 40 paesi delle Nazioni Unite hanno firmato l'adozione del nuovo trattato globale sulla criminalità informatica, un apporto estremamente importante per la concretizzazione di un quadro giuridico internazionale effettivamente contrastante l'attuale criminalità organizzata transnazionale, quella informatica.²³⁹

In conclusione, se la Convenzione di Palermo fosse stata funzionalmente strutturata su visioni e aggiornamenti futuristici, sarebbe stato probabile che le nuove opere convenzionali non avrebbero avuto ragione di esistere.

Le Nazioni Unite invece, stanno avvertendo la necessità di incrementare il quadro giuridico internazionale di lotta alla criminalità organizzata transnazionale, sulla scorta dell'evoluzione digitale delle mafie e dei risultati che gli Stati probabilmente non sono riusciti ad ottenere nell'era odierna con le misure tradizionali lasciate dalla Convenzione di Palermo.

Dopo un'ampia panoramica di potenziale critica agli aspetti obsoleti della Convenzione di Palermo, sarà opportuno analizzare nel paragrafo successivo come, a partire dalla già nota Convenzione di Budapest, si stiano prospettando nuovi scenari proiettati a contrastare la criminalità organizzata transnazionale sul piano internazionale.

²³⁹ OnuItalia. "ONU adotta il primo trattato contro il cybercrime." *Onu Italia*, 2024, consultabile sul sito <https://onuitalia.com/2024/08/10/onu-adotta-il-primo-trattato-contro-il-cybercrimine/>

3.2 La Convenzione di Budapest tra aspetti positivi e criticità.

Trascorso poco tempo dalla Convenzione di Palermo incominciarono a farsi spazio i primi mutamenti legati alla natura delinquenziale della criminalità organizzata transnazionale, accrescendo la consapevolezza che un'evoluzione criminale in tal senso avrebbe portato alla necessità di instaurare una cooperazione internazionale anche nell'ambito dell'evoluzione informatica dei gruppi criminali.²⁴⁰

Mossi dalla consapevolezza di dover aggiornare le primissime leggi che erano state create da alcuni Stati per regolare il *cyber crime* (per esempio la legge italiana n. 547 risaliva al 1993²⁴¹), il Consiglio d'Europa propose l'adozione di una nuova Convenzione: la Convenzione di Budapest, entrata in vigore nel luglio del 2004.²⁴²

La Convenzione di Budapest, seppur ideata dal Consiglio d'Europa, costituisce un trattato su scala internazionale, in quanto la sua ratifica è stata aperta a tutti gli Stati del mondo, difatti alla Convenzione di Budapest hanno preso parte il Giappone, il Brasile, l'Australia e altri.²⁴³

²⁴⁰ Buccini, Alfonso. "Convenzione di Budapest sulla criminalità informatica a 20 anni dall'approvazione." *Csibologna*, 2021, consultabile sul sito <https://www.csigbologna.it/referenze/legislazione/convenzione-di-budapest-sulla-criminalita-informatica-a-20-anni-dallapprovazione/>

²⁴¹ Italia. Legge 23 dicembre 1993, n. 547. *Modificazioni ed integrazioni alle norme del Codice penale e del codice di procedura penale in tema di criminalità informatica*. G.U. n.305, 1993.

²⁴² Buccini, Alfonso. "Convenzione di Budapest sulla criminalità informatica a 20 anni dall'approvazione". *Csibologna*, 2021, consultabile sul sito <https://www.csigbologna.it/referenze/legislazione/convenzione-di-budapest-sulla-criminalita-informatica-a-20-anni-dallapprovazione/>

²⁴³ Buccini, Alfonso. "Convenzione di Budapest sulla criminalità informatica a 20 anni dall'approvazione". *Csibologna*, 2021, consultabile sul sito <https://www.csigbologna.it/referenze/legislazione/convenzione-di-budapest-sulla-criminalita-informatica-a-20-anni-dallapprovazione/>

Grazie alla Convenzione di Budapest la comunità internazionale ha potuto interfacciarsi per la prima volta con una regolamentazione integrata che potesse ammonire gli Stati dell'esistenza di crimini perpetrati da gruppi organizzati sul piano informatico, il che rappresentò l'inizio dell'evoluzione normativa internazionale al riguardo.

Difatti, saranno analizzati gli aspetti salienti della Convenzione e gli apporti di cui la comunità internazionale ha goduto, ponendo soprattutto un focus sui suoi caratteri innovativi che hanno saputo individuare (anche se in modo limitato) la minaccia dell'evoluzione informatica del crimine organizzato transnazionale.

Seguirà poi l'analisi dell'ultimo passo di innovazione attuato dall'ONU: il Trattato Globale contro la criminalità informatica, adottato all'unanimità nel 2024 dall'Assemblea Generale delle Nazioni Unite, attualmente in attesa di entrare in vigore.

Da tale constatazione sarà possibile intuire la consapevolezza, sempre più acuta, che le Nazioni Unite hanno della minaccia del *cyber crime* mafioso, un nemico sempre più sofisticato e invisibile che mina la sicurezza degli Stati del mondo, compromettendo la loro struttura governativa, economica e politica, e soprattutto che necessita di essere contrastato attraverso una cooperazione globale avanzata.

3.2.1 La convenzione di Budapest e i primi apporti offerti al contrasto dell'entità criminale informatica.

Come osservato sopra, la fase preliminare della regolamentazione internazionale sul *cybercrime* ha avuto origine con la Convenzione di Budapest, il primo accordo internazionale avente ad oggetto i crimini informatici, ossia quelli commessi attraverso l'utilizzo di internet e di altre sezioni oscure del dominio virtuale, come il *dark net*.²⁴⁴

²⁴⁴ Mattarella, Andrea. "La futura Convenzione Onu sul *cybercrime* ed il contrasto alle nuove forme di criminalità organizzata, rivista italiana antiriciclaggio." *Rivista italiana Antiriciclaggio*, 2022, pagina 72 consultabile sul sito https://www.antiriciclaggiocompliance.it/app/uploads/2022/03/3.3_Mattarella.pdf

Lo scopo principale della Convenzione era quello di reprimere in modo coordinato il crimine informatico attraverso una politica integrata fra tutti gli Stati membri. ²⁴⁵

Oltre a voler raggiungere un'armonizzazione dei sistemi normativi penali degli Stati, in materia di crimini informatici, l'obiettivo più innovativo della Convenzione all'epoca fu quello di prevedere che solo attraverso dei strumenti concreti di indagine informatica, il *cybercrime* potesse essere contrastato a livello operativo. ²⁴⁶

Sono stati i primi sviluppi criminali informatici a destare il sospetto che il *cybercrime* avrebbe stravolto l'accessibilità e la ricerca delle informazioni, configurando una minaccia non indifferente per i sistemi legali degli Stati, in quanto la tecnologia che ci si preparava ad affrontare non presentava confini geografici e non si sarebbe arrestata facilmente. ²⁴⁷

Di fronte alle ampie sfide della nuova era digitale che si prestava ad arrivare, gli Stati riconobbero che l'unico strumento repressivo e risolutivo del problema si incentrasse nella cooperazione ma soprattutto nella capacità del diritto internazionale di individuare una soluzione, nel totale rispetto dei diritti fondamentali dell'uomo. ²⁴⁸

²⁴⁵ Mattarella, Andrea. "La futura Convenzione Onu sul *cybercrime* ed il contrasto alle nuove forme di criminalità organizzata, rivista italiana antiriciclaggio." *Rivista Italiana Antiriciclaggio*, 2022, pagina 72 consultabile sul sito https://www.antiriciclaggiocompliance.it/app/uploads/2022/03/3.3_Mattarella.pdf

²⁴⁶ Mattarella, Andrea. "La futura Convenzione Onu sul *cybercrime* ed il contrasto alle nuove forme di criminalità organizzata." *Rivista Italiana Antiriciclaggio*, 2022, pagina 72 consultabile sul sito https://www.antiriciclaggiocompliance.it/app/uploads/2022/03/3.3_Mattarella.pdf

²⁴⁷ Mattarella, Andrea. "La futura Convenzione Onu sul *cybercrime* ed il contrasto alle nuove forme di criminalità organizzata". *Rivista Italiana Antiriciclaggio*, 2022, pagina 72 consultabile sul sito https://www.antiriciclaggiocompliance.it/app/uploads/2022/03/3.3_Mattarella.pdf

²⁴⁸ Mattarella, Andrea. "La futura Convenzione Onu sul *cybercrime* ed il contrasto alle nuove forme di criminalità organizzata". *Rivista Italiana Antiriciclaggio*, 2022, pagina 72 consultabile sul sito https://www.antiriciclaggiocompliance.it/app/uploads/2022/03/3.3_Mattarella.pdf

La Convenzione, divisa in sezioni, prima elenca una serie di nuovi crimini informatici che gli Stati debbono riconoscere come tali nel proprio ordinamento e che debbono sanzionare adeguatamente, (reati previsti dall'articolo 2 all'articolo 13 sezione I) poi fissa uno standard minimo di pena per tutti questi reati che, in base al proprio diritto interno, poteva essere aumentato o diminuito dagli Stati. ²⁴⁹

I reati principali che vengono riportati dalla Convenzione attengono a quelli che, da decenni a questa parte, compongono le attività più imponenti della criminalità organizzata informatica: si parla infatti di frodi virtuali e anche di tutte la serie di attività illecite inerenti al reato di riciclaggio potenziato con le nuove tecnologie. ²⁵⁰

Per alcuni paesi come l'Italia, la Convenzione di Budapest (che l'Italia ha adottato con la l. 18 marzo 2008 n. 48 ²⁵¹) ha rappresentato lo slancio necessario per costituire le basi dell'implementazione della lotta al crimine informatico. In conclusione, come si è visto, sono molti gli aspetti positivi della Convenzione che hanno rappresentato l'inizio della consapevolezza internazionale che vi sarebbero state sfide nuove che gli Stati avrebbero dovuto inevitabilmente affrontare, in cui la scelta di mantenere salda la cooperazione tra

²⁴⁹ Mattarella, Andrea. "La futura Convenzione Onu sul *cybercrime* ed il contrasto alle nuove forme di criminalità organizzata" *Rivista Italiana Antiriciclaggio*, 2022, pagina 73, 74, consultabile sul sito https://www.antiriciclaggiocompliance.it/app/uploads/2022/03/3.3_Mattarella.pdf

²⁵⁰ Mattarella, Andrea. "La futura Convenzione Onu sul *cybercrime* ed il contrasto alle nuove forme di criminalità organizzata". *Rivista Italiana Antiriciclaggio*, 2022, pagina 73, 74, consultabile sul sito https://www.antiriciclaggiocompliance.it/app/uploads/2022/03/3.3_Mattarella.pdf

²⁵¹ Italia. Legge 18 marzo 2008, n. 48. *Ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica, fatta a Budapest il 23 novembre del 2001, e norme di adeguamento all'ordinamento interno*. Gazzetta Ufficiale della Repubblica italiana, n.80, 4 aprile 2008.

loro sarebbe comunque rimasta la misura basilare per contrastare le nuove minacce criminali legate al mondo digitale. ²⁵²

3.2.2 Le criticità della Convenzione di Budapest alla luce dell'evoluzione digitale del crimine organizzato informatico.

La previsione e la regolamentazione internazionale sul crimine informatico organizzato oggi potrebbe essere considerata come scontata ma in realtà, all'epoca della Convenzione di Budapest, ha rappresentato il passo più rilevante e innovativo per una comunità internazionale che scovava una minaccia totalmente nuova. ²⁵³

Tutti gli aspetti legati alla cooperazione internazionale, agli strumenti tecnologici di indagine e alle categorie di crimini informatici previsti dalla Convenzione, configurano gli apporti che questa ha offerto agli Stati, ma come per la Convenzione di Palermo, nel tempo anche la Convenzione di Budapest ha maturato delle criticità. ²⁵⁴

I motivi delle possibili vulnerabilità che la Convenzione presenterebbe deriverebbero dall'epoca in cui questa entrò in vigore; agli albori degli anni 2000 il fenomeno del *cyber crime*, costituiva una tecnologia che le organizzazioni criminali transnazionali ancora non conoscevano, ma che si sarebbe evoluta.

²⁵² Buccini, Alfonso. "Convenzione di Budapest sulla criminalità informatica a 20 anni dall'approvazione." *Csibologna*, 2021, consultabile sul sito <https://www.csibologna.it/referenze/legislazione/convenzione-di-budapest-sulla-criminalita-informatica-a-20-anni-dallapprovazione/>

²⁵³ Mattarella, Andrea. "La futura Convenzione Onu sul *cybercrime* ed il contrasto alle nuove forme di criminalità organizzata." *Rivista Italiana Antiriciclaggio*, 2022, pagina 74 consultabile sul sito https://www.antiriciclaggiocompliance.it/app/uploads/2022/03/3.3_Mattarella.pdf

²⁵⁴ Mattarella, Andrea. "La futura Convenzione Onu sul *cybercrime* ed il contrasto alle nuove forme di criminalità organizzata." *Rivista Italiana Antiriciclaggio*, 2022, pagina 75 consultabile sul sito https://www.antiriciclaggiocompliance.it/app/uploads/2022/03/3.3_Mattarella.pdf

Difatti, la nascita della criminalità organizzata informatica che passava dalle attività illecite tradizionali (perché strettamente legate alla logica del controllo fisico del territorio) a quelle potenziate tramite l'utilizzo di internet, ha accresciuto le difficoltà di perseguire i crimini informatici in quanto gli strumenti digitali di contrasto previsti dalla Convenzione di Budapest hanno perso rilevanza rispetto alle tecniche criminali digitali, divenute estremamente sofisticate.

I classici reati informatici che elenca la Convenzione, come la pirateria informatica, per esempio, non corrispondono più alle minacce a cui gli Stati sono soggetti attualmente per mano delle organizzazioni criminali informatiche.

Pertanto, la necessità di aggiornare la Convenzione di Budapest deriverebbe dall'esistenza delle nuove tecnologie che oggi dominano le attività illecite delle organizzazioni criminali, come per esempio l'Intelligenza artificiale, cui la Convenzione non fa riferimento.

La necessità di un tale aggiornamento convenzionale potrebbe derivare inoltre dalla realizzazione di attività di intrusione e di spionaggio informatico odierne, poste in essere dalle mafie digitali per abbattere i sistemi di sicurezza Statali.

Tutte queste minacce informatiche potrebbero dirsi troppo evolute per essere contrastate dalla regolamentazione datata della Convenzione di Budapest, sulla base dell'elenco di reati informatici che questa prevede e che non contemplerebbero le nuove attività criminali informatiche.

Si analizzino nello specifico quali potrebbero essere gli aspetti della Convenzione che potrebbero configurare delle criticità.

In primo luogo, il quadro normativo offerto dalla Convenzione riguarderebbe solo determinate fattispecie criminose principalmente basate su *cybercrime* datati che non parrebbero corrispondere più alle forme di crimine informatico odierno in quanto hanno subito l'implementazione dell'intelligenza artificiale.²⁵⁵

Tutto ciò deriva dal fatto che le organizzazioni criminali hanno compreso con il tempo che strumenti come l'Intelligenza artificiale riescono a dare loro l'opportunità di studiare

²⁵⁵ Pellerito, Vittoria. "Cybercrime: verso una nuova Convenzione delle Nazioni Unite" *Ogie web*, 2022, consultabile sul sito <https://www.ogieweb.eu/cybercrime-verso-una-nuova-convenzione-delle-nazioni-unite/>

una quantità rilevante di dati e hanno integrato i processi di ottimizzazione dell'IA nelle loro operazioni illecite.²⁵⁶

Ulteriore aspetto potenzialmente critico della Convenzione di Budapest riguarderebbe l'assenza di una disciplina normativa specifica sulle prove elettroniche che permetterebbe di costituire una collaborazione statale effettivamente funzionale, in quanto, con una disciplina mirata, gli Stati sarebbero in grado di scambiarsi facilmente informazioni da utilizzare nel corso di procedimenti penali, garantendo inoltre che tali informazioni possano giovare di una sorveglianza disciplinata in grado di contrastare possibili attacchi informatici da parte delle organizzazioni criminali.²⁵⁷

Tuttavia, in presenza di questa mancanza, legata ad un'assente regolamentazione convenzionale al riguardo, potrebbe confermarsi come impossibile la memorizzazione e la conservazione di tali prove transnazionali (poiché presenti nel *cyber spazio*) su scala globale.²⁵⁸

Ciò che proverebbe che tali criticità convenzionali potrebbero avere motivo di essere sostenute, sarebbero le nuove soluzioni che l'ONU sta adottando in questo periodo storico circa il contrasto al *cybercrime*, sulla scorta degli aspetti datati della Convenzione di Budapest rispetto all'era digitale attuale.

Si analizzerà nel paragrafo che segue come le Nazioni Unite sono da tempo impegnate nell'elaborazione di un nuovo trattato globale sul contrasto al *cybercrime* e alla criminalità organizzata informatica, intento ad offrire finalmente una strategia repressiva globale quanto più innovativa e funzionale possibile.

²⁵⁶ Ciccarone, Giovanna. "L'Intelligenza Artificiale e la Cybermafia: il futuro del crimine organizzato." *Criminal meet*, 2024, consultabile sul sito <https://criminalmeet.it/intelligenza-artificiale-e-la-cybermafia-il-futuro-del-crimine-organizzato/>

²⁵⁷ Pellerito, Vittoria. "Cybercrime: verso una nuova Convenzione delle Nazioni Unite." *Criminal meet*, 2022, consultabile sul sito <https://www.ogieweb.eu/cybercrime-verso-una-nuova-convenzione-delle-nazioni-unite/>

²⁵⁸ Pellerito, Vittoria. "Cybercrime: verso una nuova Convenzione delle Nazioni Unite" *Ogie web*, 2022, consultabile sul sito <https://www.ogieweb.eu/cybercrime-verso-una-nuova-convenzione-delle-nazioni-unite/>

Inoltre, verrà altresì analizzato il nuovo metodo repressivo delle mafie cibernetiche adottato da molti Stati, interamente basato sull'utilizzo positivo dell'intelligenza artificiale.

3.3 La nuova frontiera offerta dalle Nazioni Unite per il futuro del contrasto del cyber crime: le possibili soluzioni tra il trattato globale dell'ONU e l'uso dell'IA.

In questa parte conclusiva del presente elaborato l'analisi condotta verterà ad esaminare le possibili soluzioni che la comunità internazionale sta elaborando per contrastare funzionalmente la minaccia della criminalità organizzata informatica e i pericoli cui l'utilizzo cattivo dell'intelligenza artificiale potrebbe apportare alla comunità internazionale, alla luce dell'attuale era digitale.

Dai nuovi scenari di contrasto che le Nazioni Unite esaminano, si confermerebbe la necessità della comunità internazionale, di potenziare la lotta alla criminalità organizzata informatica, anche detta *cybermafia*²⁵⁹, in quanto dalle ultime evoluzioni del crimine informatico, si avvertirebbe che la repressione di tale fenomeno richiederebbe un profondo mutamento di quelle che saranno le operazioni e le strategie di contrasto e sicurezza da utilizzare.²⁶⁰

Il dominio informatico in cui le organizzazioni criminali adesso operano è un luogo virtuale in cui le tradizionali operazioni di intercettazione e polizia non troverebbero il giusto riscontro a causa dell'utilizzo che le mafie fanno di strumenti di crittografia in grado di garantire un totale anonimato.

²⁵⁹ Termine utilizzato da Ciccarone Giovanna. "L'intelligenza artificiale e la Cybermafia: il futuro del crimine organizzato". *Criminal meet*, 2024, consultabile sul sito <https://criminalmeet.it/lintelligenza-artificiale-e-la-cybermafia-il-futuro-del-crimine-organizzato/>

²⁶⁰ Ciccarone, Giovanna. "L'intelligenza artificiale e la Cybermafia: il futuro del crimine organizzato" *Criminal meet*, 2024, consultabile sul sito <https://criminalmeet.it/lintelligenza-artificiale-e-la-cybermafia-il-futuro-del-crimine-organizzato/>

La critica che si è avanzata nei paragrafi precedenti circa la regolamentazione internazionale offerta dalla Convenzione di Palermo e da quella di Budapest, potenzialmente datate e non attuali rispetto alle nuove forme di mafie e di crimini perpetrati nell'era digitale, potrebbe trovare una soluzione grazie all'impegno delle Nazioni Unite degli ultimi tempi.

Il crimine organizzato informatico parrebbe attualmente in crescita e la mancanza di una regolamentazione internazionale specifica e attuale circa tale fenomeno, ha spinto le Nazioni Unite alla redazione di una Convenzione globale interamente dedicata alle nuove strategie a cui gli Stati adempiranno per contrastare la criminalità informatica attuale e rafforzare la cooperazione internazionale nella repressione di alcuni reati estremamente evoluti a causa dell'utilizzo dell'intelligenza artificiale.

Sarà opportuno osservare come la futura adozione del nuovo trattato globale potrebbe essere accompagnata da un'ulteriore possibile soluzione: la possibilità per gli Stati di avvalersi dell'utilizzo buono di sistemi di intelligenza artificiale per potenziare le strategie di contrasto al crimine informatico posto in essere dalle nuove mafie cibernetiche.

3.3.1 Come il trattato globale sulla criminalità informatica potrebbe sostituire la Convenzione di Budapest.

Il Trattato globale sulla criminalità informatica, il cui nome completo è: “*Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes*”²⁶¹, rappresenterà un passo storico per la lotta alla

²⁶¹ Cosentino Roberto. “Cosa dice il nuovo Trattato ONU contro la criminalità informatica e perché è controverso: possibili rischi per i diritti umani.”, 2024, consultabile sul sito https://www.corriere.it/tecnologia/24_agosto_14/cosa-dice-il-nuovo-trattato-onu-contro-la-criminalita-informatica-e-perche-e-controverso-a-rischio-i-diritti-umani-cd604f31-918a-4632-919d-27a67c8b0x1k.shtml

criminalità informatica e per la creazione di un quadro giuridico internazionale specificatamente incentrato nel contrasto all'attuale *cybercrime* organizzato...²⁶²

Il trattato, non ancora entrato in vigore, è stato adottato dalle Nazioni Unite all'unanimità lo scorso 8 agosto 2024, dopo essere stato proposto dalla Russia diversi anni prima.

Dopo cinque anni di lavoro da parte del Comitato intergovernativo di esperti, istituito mediante la Risoluzione 74/247 del 27/12/2019²⁶³ dall'Assemblea Generale delle Nazioni Unite, si è giunti alla finalizzazione del testo della Convenzione che, come affermato dal direttore esecutivo dell'UNDC²⁶⁴ *Ghada Waly*: *“è un passo fondamentale in quanto primo trattato multilaterale anticrimine in oltre 20 anni e prima Convenzione ONU contro la criminalità informatica in un momento in cui le minacce nel cyberspazio stanno crescendo rapidamente”*...²⁶⁵

Gli obiettivi fondamentali del nuovo trattato globale aspirano a rafforzare la cooperazione internazionale degli Stati parte per raggiungere un contrasto effettivo verso i nuovi reati

²⁶² Filacchioni, Marcello. “Passo storico: l'ONU adotta all'unanimità il Trattato globale sulla criminalità informatica, 2024, consultabile sul sito <https://www.redhotcyber.com/post/passo-storico-lonu-adotta-allunanimita-il-trattato-globale-sulla-criminalita-informatica/>

²⁶³ La Risoluzione 74/247 del 27/12/2019 è intitolata “Contrasto all'utilizzo delle tecnologie ICT per scopi criminali e costituisce la risoluzione mediante la quale il comitato intergovernativo di esperti è stato istituito dall'Assemblea generale delle Nazioni Unite.

²⁶⁴ UNDC: Ufficio delle Nazioni Unite per il controllo della droga e la prevenzione del crimine.

²⁶⁵ Cosentino, Roberto. “Cosa dice il nuovo Trattato ONU contro la criminalità informatica e perché è controverso: “possibili rischi per i diritti umani.” *Corriere*, 2024, consultabile sul sito https://www.corriere.it/tecnologia/24_agosto_14/cosa-dice-il-nuovo-trattato-onu-contro-la-criminalita-informatica-e-perche-e-controverso-a-rischio-i-diritti-umani-cd604f31-918a-4632-919d-27a67c8b0xlk.shtml

informatici, soprattutto quelli che concernono il settore dell'informazione e della comunicazione. ²⁶⁶

La preoccupazione delle Nazioni Unite e la necessità di arrivare all'adozione di un innovativo strumento convenzionale globale deriverebbero dalla crescita vertiginosa dei *cybercrimes* posti in essere dalla criminalità organizzata transnazionale attraverso l'utilizzo dei sistemi di intelligenza artificiale in grado di potenziarne sia la velocità che l'impatto. ²⁶⁷

Gli scopi della nuova Convenzione sono elencati all'articolo 1 e vertono nella adozione di misure innovative, rispetto a quelle promosse in passato dalla Convenzione di Budapest, atte ad assicurare i paesi più deboli da possibili attacchi informatici, garantendo una cooperazione internazionale in grado di reprimere tempestivamente le minacce informatiche. ²⁶⁸

Il Trattato, contrariamente al passato, si focalizzerà sul *modus operandi* delle nuove criminalità organizzate informatiche, atto alla realizzazione dei più grandi traffici illeciti attraverso la delocalizzazione e la diffusione delle fonti di attacco che affondano le loro radici nei paesi minormente sviluppati. ²⁶⁹

²⁶⁶ Cartisano, Marco. "Trattato globale ONU sulla criminalità informatica: perché è importante." *Cybersecurity 360*, 2024, consultabile sul sito <https://www.cybersecurity360.it/cybersecurity-nazionale/trattato-globale-onu-sulla-criminalita-informatica-perche-e-importante/>

²⁶⁷ Cartisano, Marco. "Trattato globale ONU sulla criminalità informatica: perché è importante." *Cybersecurity 360*, 2024, consultabile sul sito <https://www.cybersecurity360.it/cybersecurity-nazionale/trattato-globale-onu-sulla-criminalita-informatica-perche-e-importante/>

²⁶⁸ Cartisano, Marco. "Trattato globale ONU sulla criminalità informatica: perché è importante." *Cybersecurity 360*, 2024, consultabile sul sito <https://www.cybersecurity360.it/cybersecurity-nazionale/trattato-globale-onu-sulla-criminalita-informatica-perche-e-importante/>

²⁶⁹ Cartisano, Marco. "Trattato globale ONU sulla criminalità informatica: perché è importante." *Cybersecurity 360*, 2024, consultabile sul sito

Rispetto alla Convenzione di Budapest, il Trattato prevedrà nell'elenco dei reati informatici più sofisticati di cui gli Stati sono stati vittime negli ultimi tempi e che potrebbe in futuro essere motivo per la Convenzione di Budapest di essere oscurata dalla presenza del nuovo trattato e dalla portata delle sue novità; tra i più particolari saranno previsti quelli relativi all'utilizzo di materiale pornografico e quelli che tentano di adescare i minori per scopi illeciti. Seppure il nuovo trattato globale rappresenti un passo evolutivo di spicco nella lotta alla criminalità informatica sullo scenario internazionale, vi potrebbero essere degli aspetti controversi e delicati su cui le Nazioni Unite dovranno lavorare, riguardanti il rispetto dei diritti fondamentali dell'uomo. ²⁷⁰

La Convenzione non dimentica di ricordare tutte le garanzie di cui i diritti umani dovranno sempre continuare a godere anche, e soprattutto, di come: “*States parties shall ensure that the implementation of their obligations under this convention is consistent with their obligations under international human rights law.*”. ²⁷¹

Tuttavia, il bilanciamento tra il rispetto dei diritti umani e gli ampi poteri di sorveglianza informatica di cui saranno dotati gli Stati, potrebbe portare in futuro a possibili abusi

<https://www.cybersecurity360.it/cybersecurity-nazionale/trattato-globale-onu-sulla-criminalita-informatica-perche-e-importante/>

²⁷⁰ Cosentino, Roberto. “Cosa dice il nuovo trattato ONU contro la criminalità informatica e perché è controverso: Possibili rischi per i diritti umani”. *Corriere*, 2024, consultabile sul sito https://www.corriere.it/tecnologia/24_agosto_14/cosa-dice-il-nuovo-trattato-onu-contro-la-criminalita-informatica-e-perche-e-controverso-a-rischio-i-diritti-umani-cd604f31-918a-4632-919d-27a67c8b0xlk.shtml?refresh_ce

²⁷¹ United Nations General Assembly. *United Nations Convention against Cybercrime; Strengthening International Cooperation for Combating Certain Crimes Committed by Means of Information and Communications Technology Systems and for the Sharing of Evidence in Electronic Form of Serious Crimes*. UNDC, United Nations, A/RES/79/243, 31 December 2024, Chapter I, art. 6 (1), p. 7.

governativi nei confronti dei dati sensibili dei cittadini e della loro *privacy* digitale, in particolar modo in quei paesi in cui non vige un discreto rigore legislativo a riguardo.²⁷² Secondo *Katitza Rodriguez*, direttrice politica per la *privacy* globale dell'*Electronic Frontier Foundation*²⁷³: “La Convenzione Onu è un assegno in bianco per gli abusi di sorveglianza”²⁷⁴; un commento che potrebbe evidenziare la possibilità che il trattato venga utilizzato per reprimere la libertà d’espressione.

Tuttavia, queste visioni, attualmente prive di evidenze, potranno essere concretamente analizzate solo con l’entrata in vigore della Convenzione, attraverso cui poter operare le opportune e definitive considerazioni. Attualmente le prospettive offerte dalla Convenzione parrebbero fungere da strumento ideale e funzionale per arrivare a debellare tale insistente e complessa minaccia per la comunità internazionale.

Sarà opportuno analizzare come l’ONU, interfacciandosi con tale minaccia informatica, si immerga nella ricerca di tutte le possibili soluzioni (non solo quelle convenzionali dunque) da poter adottare per contrastarla in modo evoluto rispetto al passato.

In definitiva, sarà esaminato come le Nazioni Unite sembrerebbero prendere in considerazione il potenziale utilizzo benefico che gli Stati potrebbero attuare dell’Intelligenza artificiale, per potenziare le misure di contrasto adottate, dando a tale strumento un ruolo positivo nella lotta alla criminalità informatica.

²⁷² Cosentino, Roberto. “Cosa dice il nuovo trattato ONU contro la criminalità informatica e perché è controverso: Possibili rischi per i diritti umani”. *Corriere*, 2024, consultabile sul sito https://www.corriere.it/tecnologia/24_agosto_14/cosa-dice-il-nuovo-trattato-onu-contro-la-criminalita-informatica-e-perche-e-controverso-a-rischio-i-diritti-umani-cd604f31-918a-4632-919d-27a67c8b0x1k.shtml?refresh_ce

²⁷³ EFF: è una ONG atta a reprimere e contrastare attivamente eventuali minacce e danni arrecati ai diritti umani nel mondo virtuale.

²⁷⁴ Cosentino, Roberto. “Cosa dice il nuovo trattato ONU contro la criminalità informatica e perché è controverso: “Possibili rischi per i diritti umani”. *Corriere*, 2024, consultabile sul sito https://www.corriere.it/tecnologia/24_agosto_14/cosa-dice-il-nuovo-trattato-onu-contro-la-criminalita-informatica-e-perche-e-controverso-a-rischio-i-diritti-umani-cd604f31-918a-4632-919d-27a67c8b0x1k.shtml?refresh_ce

3.3.2 L'IA come possibile alleato nella lotta al *cybercrime* e alla criminalità informatica organizzata.

Il Trattato globale contro la criminalità informatica, come già analizzato, imporrà agli Stati parte nuove misure potenziate, da adottare per assicurare la comunità internazionale dalle minacce della criminalità informatica. Tuttavia, nell'odierna era digitale, le soluzioni e le strategie repressive di tale fenomeno potrebbero non esaurirsi con i rimedi convenzionali che offrirà il futuro Trattato globale.

Le stesse Nazioni Unite considerano necessaria, oltre all'adozione di soluzioni già formulate nel futuro Trattato, l'attuazione di un'ulteriore forma di contrasto alla criminalità organizzata, quella realizzata tramite l'utilizzo positivo dell'intelligenza artificiale.

Nell'articolo "*UNDP: 5 Modi per Affrontare le Crisi Mondiali Attraverso l'IA*"²⁷⁵, pubblicato sul sito dell'ONU, di *Devanand Ramiah* (direttore di preparazione, risposta e difesa del *United Nations development programme*) si affronta proprio la tematica dell'adozione di sistemi di IA e si osserva come le Nazioni Unite si mostrino assolutamente propense all'utilizzo dell'Intelligenza artificiale come possibile strategia di contrasto, non solo alla criminalità informatica ma a tutte le gravi criticità che impattano il globo.

I vantaggi che l'intelligenza artificiale apporterebbe agli attuali strumenti convenzionali di repressione della criminalità informatica organizzata potrebbero potenziare definitivamente gli Stati nelle misure repressive da loro adottate e portare a risultati completi. Implementare l'utilizzo dell'IA nelle misure repressive della criminalità informatica agevolerebbe gli Stati che potrebbero utilizzare tale tecnologia per preventivare gli attacchi *hacker* delle organizzazioni criminali informatiche grazie ai sistemi di IA in grado di elaborare una quantità enorme di dati, oppure potrebbero

²⁷⁵ Devanand, Ramiah. "UNPD: 5 Modi per Affrontare le Crisi Mondiali Attraverso l'IA". Nazioni Unite, *UNRIC*, 2025, consultabile sul sito <https://unric.org/it/undp-5-modi-per-affrontare-le-crisi-mondiali-attraverso-lia/#>

costituire delle risposte ai suddetti attacchi, automatizzandoli e ponendoli sotto il controllo e la direzione di sistemi di IA.²⁷⁶

La criminalità organizzata odierna detiene più della metà degli affari illeciti nelle attività di tratta virtuale nel *dark web*. Soprattutto in settori come questo, gli Stati potrebbero attuare misure potenziate dall'utilizzo dell'Intelligenza artificiale che siano in grado di porre in essere delle difese agli attacchi informatici contro il furto di dati dalle banche virtuali dei governi per immetterli nel *dark web*, piattaforma virtuale in cui informazioni simili sono estremamente ambite.²⁷⁷

Sviluppare strumenti sofisticati, basati su di un utilizzo sano e funzionale dell'IA preparerebbe non solo gli Stati a rispondere in modo consapevole ed evoluto alle minacce informatiche della criminalità organizzata transnazionale, bensì permetterebbe anche alle imprese e ai cittadini di godere di una sicurezza interna concreta rispetto al passato.²⁷⁸

3.4 Conclusioni

La minaccia informatica delle organizzazioni criminali odierne è rappresentata dalle attività illecite virtuali che vengono perpetrate dai gruppi criminali nel mondo virtuale, e con il potenziamento offerto dall'utilizzo dell'IA tali crimini subiscono attualmente una crescita vertiginosa.

L'emersione del nuovo volto della mafia, quella automatizzata, non sfugge al continuo monitoraggio degli Stati e delle Nazioni Unite che dopo un lungo periodo di inazione,

²⁷⁶ Akkodis. "L'Intelligenza Artificiale che sta rivoluzionando la cyber security." *Akkodis*, 2024, consultabile sul sito <https://www.akkodis.com/it/informazioni-utili/articoli/intelligenza-artificiale-cyber-security>

²⁷⁷ Akkodis. "L'Intelligenza Artificiale che sta rivoluzionando la cyber security". *Akkodis*, 2024, consultabile sul sito <https://www.akkodis.com/it/informazioni-utili/articoli/intelligenza-artificiale-cyber-security>

²⁷⁸ Ciccarone, Giovanna. "L'intelligenza artificiale e la Cybermafia: il futuro del crimine organizzato." *Criminal meet*, 2024, consultabile sul sito <https://criminalmeet.it/lintelligenza-artificiale-e-la-cybermafia-il-futuro-del-crimine-organizzato/>

hanno attualmente aperto la strada a nuovi scenari futuri di contrasto alla criminalità informatica.

La nuova strategia d'azione culmina nel nuovo trattato globale contro la criminalità informatica dell'Onu, in attesa di entrare in vigore, che dopo molto tempo sembra voler porre un definitivo rimedio alle mancanze strategiche che gli Stati hanno sofferto nella lotta alla mafia cibernetica dovuti da strumenti convenzionali oramai datati e non più attuali rispetto alle nuove forme di crimini digitali.

L'Onu prospetta nuovi piani d'azione, sempre basati sulla cooperazione internazionale che a differenza del passato, è rafforzata a livello globale e, da ciò che preannuncia il trattato, opererà contro i reati informatici più evoluti, elencati nella nuova Convenzione dell'Onu.

Il nuovo trattato offrirà agli stati parte l'opportunità di essere consapevoli degli strumenti utilizzati dalle mafie cibernetiche, prima fra tutti l'intelligenza artificiale che viene utilizzata dalla criminalità organizzata in modo da potenziare il crimine informatico e rendere estremamente difficoltosa l'attuale opera repressiva degli Stati.

Le Nazioni Unite, consapevoli dell'impatto allarmante che l'IA ha e che continuerà ad avere sulla sicurezza globale, intendono rendere consapevoli gli Stati che i crimini e le mafie sono diverse dal passato e che oggi la produzione illecita dei più grandi traffici di persone, armi e stupefacenti è totalmente invisibile ai loro occhi, in quanto virtuale e nascosta nei settori oscuri dello spazio cibernetico.

Le Nazioni Unite, coscienti di ciò, da una parte incrementano le misure degli Stati contro l'utilizzo illecito dell'IA, dall'altra si concedono anche un possibile futuro utilizzo della stessa come controffensiva alle minacce virtuali.

Difatti, un'altra possibile soluzione rispetto al Trattato globale che le Nazioni Unite parrebbero prendere in considerazione è quella di utilizzare l'intelligenza artificiale come risposta agli attacchi informatici.

L'Intelligenza artificiale potrebbe rappresentare un alleato estremamente funzionale per contrastare l'entità criminale informatica, tanto a livello internazionale quanto a livello globale, in quanto tale strumento offrirebbe delle capacità in grado di automatizzare le risposte degli Stati agli attacchi, ma soprattutto ridurrebbe le possibilità di ricevere un attacco inconsapevole, incrementando la facoltà degli Stati di scovarli per tempo.

In conclusione, le nuove prospettive internazionali dimostrerebbero che gli Stati rispetto al passato, hanno riconosciuto da una parte il forte cambiamento strutturale che la criminalità organizzata ha subito nel tempo, dall'altra come l'impegno effettivo inerente al contrasto delle mafie, sia tradizionali che cibernetiche, debba partire da strumenti convenzionali che siano sempre aggiornati, integrati con i sistemi tecnologici che abitano la società odierna e soprattutto attuali rispetto alle nuove minacce che minano i valori su cui la comunità internazionale si fonda, primo fra tutti la sicurezza globale.

CONCLUSIONI.

Nel contesto attuale la comunità internazionale continua a doversi interfacciare con una delle minacce più longeve che affligge gli Stati, la criminalità organizzata transnazionale. Le trasformazioni sociali e tecnologiche a cui il fenomeno della criminalità organizzata si è adattato nel tempo sono particolarmente tangibili nell'era digitale.

Le organizzazioni criminali odierne, così come quelle del passato, non hanno subito arresti o periodi di stasi, anzi sono riuscite a godere della digitalizzazione, ampliando il loro raggio d'azione criminale e permettendo loro di passare da attività illecite tradizionali a quelle all'avanguardia, sofisticate a tal punto da non necessitare più un controllo fisico ed effettivo del territorio, ma piuttosto un controllo dei traffici virtuali.

Nel corso dell'elaborato, dopo aver analizzato la struttura operativa dei gruppi criminali, sia tradizionali che moderni, è stato posto in evidenza il ruolo cardine dei soggetti internazionali principalmente coinvolti nel contrasto alla criminalità organizzata transnazionale: gli Stati.

Alla luce di ciò, l'elaborato ha voluto porre al centro della trattazione l'importanza di esaminare quale posizione giuridica ricoprono gli Stati rispetto alle attività illecite dei gruppi criminali mafiosi, al fine di capire se il diritto internazionale permetta o meno di configurare concretamente la responsabilità statale in materia di crimini organizzati. Rispetto all'obiettivo dell'elaborato quindi, si è resa necessaria l'analisi dell'istituto della responsabilità internazionale degli Stati, a partire dall'esame dell'evoluzione del concetto di responsabilità nel diritto internazionale. Nel processo di formalizzazione delle norme in tema di responsabilità internazionale, ha assunto una rilevanza focale la preminente opera di codificazione dell'istituto, ovvero il Progetto di articoli sulla responsabilità degli Stati per fatti internazionalmente illeciti, redatto dalla Commissione di Diritto Internazionale e adottato dall'Assemblea Generale delle Nazioni Unite nel 2001. L'analisi del Progetto è risultata determinante per osservare le fondamenta giuridiche atte alla configurazione della responsabilità internazionale dello Stato, costituite sia dall'elemento oggettivo che da quello soggettivo. Coerentemente con l'oggetto del presente elaborato inerente all'entità criminale mafiosa, la fattispecie normativa rilevante ai fini della trattazione è stata quella dell'articolo 8 ARSIWA circa la responsabilità internazionale dello Stato per atti illeciti posti in essere da privati. Sebbene la fattispecie ex art. 8

ARSIWA permetterebbe di comprendere l'entità criminale mafiosa all'interno della categoria di attori non statali per cui lo stato può dirsi responsabile, è stato osservato come la possibilità di attribuire responsabilità internazionale allo Stato per i crimini mafiosi tradizionali e cibernetici rimarrebbe solo una teoria, priva di evidenze pratiche nella giurisprudenza internazionale. Quanto detto trova spiegazione nella rigidità dei criteri di attribuzione imposti dall'art. 8 ARSIWA, quali la direzione e il controllo effettivo che costituirebbero uno standard probatorio eccessivamente oneroso per riuscire ad essere provato, soprattutto in tema di crimini informatici attuati dalle mafie nello spazio virtuale, essendo questo un luogo troppo occulto per permettere la raccolta di evidenze probatorie come una direzione effettiva dello Stato sulle attività criminali. Dopo aver osservato il limite operativo dell'art. 8 ARSIWA rispetto a tale circostanza, è parso opportuno esaminare l'ipotesi di attribuzione di responsabilità allo Stato sulla base della violazione del principio internazionale della *due diligence*. Al fine di giungere all'osservazione della forma di responsabilità internazionale fondata sull'omissione del principio della *due diligence*, ha costituito oggetto di analisi l'evoluzione storico concettuale della diligenza dovuta nel diritto internazionale che affonda le sue radici nel modello comportamentale del *bonus pater familias*, previsto già all'epoca del diritto romano. La trattazione ha posto in evidenza gli elementi focali del principio della *due diligence*, sottolineando il ruolo preminente che tale concetto assume nel diritto internazionale, in grado di orientare gli Stati verso l'attuazione di uno standard di condotta ragionevole in presenza di obblighi primari di prevenzione, al fine di evitare le conseguenze dannose di determinate attività illecite. Esaurita l'analisi strutturale del principio della *due diligence* e degli elementi che lo compongono, è parso opportuno soffermarsi sulla fattispecie inerente alla violazione del principio, in particolar modo sulla mancata attuazione della condotta diligente dovuta da parte dello Stato. Alla luce di ciò, sebbene la configurazione della responsabilità internazionale per violazione dell'art. 8 ARSIWA risulti difficilmente concretizzabile in tema di crimine organizzato data l'onerosità del criterio di attribuzione previsto, il diritto internazionale permetterebbe comunque la previsione di una diversa forma di responsabilità fondata sull'omissione della *due diligence*; quanto detto è supportato dalla giurisprudenza della Corte Internazionale di Giustizia che, come osservato nei casi esposti al capitolo due, ha adoperato il concetto della *due diligence* nella valutazione del comportamento dello Stato al momento della commissione dell'illecito, al fine di capire

se lo Stato, nonostante non abbia commesso il fatto, si sia adoperato per prevenirlo o per minimizzare i danni. Coerentemente con l'oggetto del presente elaborato legato non solo al fenomeno generale del crimine organizzato ma in particolare alla sua evoluzione cibernetica, è stata osservata la possibilità di ricondurre responsabilità internazionale allo Stato per omessa *due diligence* relativa alla commissione del crimine organizzato nello spazio virtuale da parte delle mafie cibernetiche odierne. Pertanto, dopo l'esame relativo all'adattabilità del principio della *due diligence* al dominio virtuale, sostenuta in dottrina dal Tallin Manual, si è osservato lo standard comportamentale che gli Stati sono chiamati a rispettare anche nello spazio virtuale al fine di prevenire e vigilare sulla commissione dei *cybercrimes* dei gruppi criminali. È parso palese che se da una parte lo standard probatorio dell'art. 8 ARSIWA continui a dirsi eccessivamente oneroso, soprattutto per essere provato nello spazio virtuale, ipotizzare responsabilità internazionale ex art. 8 per omissione della *due diligence* cibernetica impone dei criteri probatori più flessibili, poiché per poter essere configurata è necessaria solo la prova delle misure preventive applicate o meno dallo Stato al momento della commissione del *cybercrime*. Nonostante questa maggiore flessibilità probatoria e l'incremento del *cybercrime* mafioso, nonché le evidenze analizzate nel caso legato al comportamento attuato dalla Russia dopo gli attacchi *cyber* della mafia, nella giurisprudenza internazionale non si individua ancora un caso in cui la Corte abbia imputato in via definitiva responsabilità internazionale dello Stato per omessa *due diligence* relativa alla commissione dei *cyber* attacchi della mafia; quanto detto potrebbe dirsi legato alle caratteristiche occulte dello spazio virtuale che permetterebbe con difficoltà di rilevare esattamente se le misure applicate dagli Stati possano dirsi con certezza insufficienti rispetto allo standard di *due diligence* atto alla prevenzione e al controllo sui *cybercrimes*.

Per finire, nella parte conclusiva dell'elaborato è stato osservato come, sebbene gli Stati non possano dirsi responsabili per le attività tradizionali e moderne delle mafie, potrebbe essere tuttavia possibile l'avanzamento di una critica rivolta all'obsolescenza degli strumenti convenzionali attualmente previsti dal diritto internazionale in materia di contrasto all'entità criminale organizzata transnazionale, come la Convenzione di Palermo (2000) e la Convenzione di Budapest (2001). In particolare, l'elaborato ha voluto evidenziare le carenze e le lacune che ad oggi potrebbero aver giocato un ruolo rilevante nella repressione al fenomeno delle mafie, soprattutto nell'era digitale in cui tale

problematica risulta priva di una regolamentazione repressiva attuale, come analizzato nel corso della trattazione sulla Convenzione di Budapest.

Per tanto, l'elaborato ha voluto offrire una visione prospettica di risoluzioni future che potrebbero trovare concretizzazione prossimamente, sia attraverso l'entrata in vigore del nuovo Trattato Globale contro la criminalità informatica, sia tramite l'utilizzo di strumenti di IA in grado di fungere da alleato nella lotta al crimine cibernetico attuato dalle organizzazioni criminali transnazionali del mondo.

BIBLIOGRAFIA.

Akingbade, Adedayo. “Due Diligence in International Law: Cause for Optimism?”. *Irish Yearbook of International Law*, vol. 15, 2020, p 48.

Anzilotti, Dionisio. *Teoria generale della responsabilità dello Stato nel diritto internazionale (General theory of state responsibility in international law)*. Firenze, Lumachi editore, 1902.

Assemblea Generale delle Nazioni Unite. *Convenzione delle Nazioni Unite contro la criminalità organizzata transnazionale*. Nazioni Unite, Palermo, 2000, art.31, n. 1, p. 20.

Bonnitcha Jonathan, McCorquodale Robert. “The Concept of ‘Due Diligence’ in the UN Guiding Principles on Business and Human Rights.” *European Journal of International Law*, Volume 28, Issue 3, August 2017, p. 902, 903, 904.

Buchan Russell, Nicholas Tsagourias. “Special Issue: Non- State Actors and Responsibility in Cyberspace: State Responsibility, Individual Criminal Responsibility and Issues of Evidence.” *Journal of Conflict and Security Law, Oxford University Press*, vol. 21, no. 3, 2016, pp. 377, 378, 379. Hein Online.

Centonze, Alessandro. *Criminalità organizzata e reati transnazionali*. Osservatorio permanente Criminalità organizzata, vol. 10 di Osservatorio permanente sulla criminalità organizzata, Giuffrè Editore, 2008, pp. 4, 120, 123.

Chimni, B. S. “The Articles on State responsibility and the Guiding Principles of Shared Responsibility: A TWAIL Perspective.” *The European Journal of International Law*, Vol. 31, no. 4, Oxford University Press, 2020, p. 1213.

Coco Antonio, de Souza Dias Talita. “Cyber Due Diligence”. a Patchwork of Protective Obligations in International Law, *European Journal of International Law*, Oxford University Press, volume 32, issue 3, 2021, p. 780.

Colonna Vilasi, Antonella. *Mafie. Origini e sviluppo del fenomeno mafioso*. Dissensi, 2012, pp. 7, 43.

Conforti, Iovane. *Diritto Internazionale*. Editoriale Scientifica, Napoli, VI Edizione, 1997, p.4.

Conforti, Iovane. *Diritto Internazionale*. Edizione Scientifica, Napoli, XII Edizione, 2021, pp 3, 14, 418, 419, 420, 421, 422, 424, 425, 428, 429, 430, 431, 442, 465, 466.

Consiglio d'Europa. *Libro bianco sulla criminalità organizzata transnazionale*. Strasburgo, tipografia del Consiglio d'Europa, 2014, pp. 13, 16, 17, 38.

Corte Internazionale di Giustizia. *Attività militari e paramilitari in e contro il Nicaragua (Nicaragua c. Stati Uniti D'America)*. I.C.J. Reports, 1986, p. 14, para. 115.

Corte Internazionale di Giustizia. *Corfù Channel Case (Regno Unito c. Albania)*. Sentenza del 25 Marzo 1948, p. 4, 15.

Costante, Massimo. *Deep web e dark web: Cos'è e come funziona la rete nascosta del deep web e il fenomeno criminale dei black market nel Dark web*. Independently published, 2021, pp. 3, 10.

Crawford James, Pellet Alain, Olleson Simon, Parlett Kate. *The law of international responsibility*. Oxford, Oxford University Press, 2010, pp.7, 8, 9, 10, 11, 12, 199, 200.

D'Aspremont, Jean. "The Articles on the Responsibility of International Organizations: Magnifying the Fissures in the Law of International Responsibility." *International Organizations Law Review*, vol. 9, no. 1, 2012, p. 15.

Esposito Carlos, Parlett Kate. *The Cambridge Companion to the International Court of justice*. Cambridge Companions to Law, Cambridge University Press, 2023, p. 417.

Floridi Luciano, Cabitza Federico. *Intelligenza artificiale. L'uso delle nuove macchine*. Firenze, Milano, Giunti Editore S.p.a. / Bompiani, 2021, p. 29.

Gabrielli, Ivano. "Come le mafie si muovono nel mondo della rete." *Scintille, Trimestrale della fondazione scintille di futuro*, 2023, p. 28.

Gratteri Nicola, Nicaso Antonio. *Il grifone. Come la tecnologia sta cambiando il volto della 'ndrangheta*. Milano, Mondadori, 2023, pp. 2, 4, 5.

International Centre for Settlement of Investment Disputes. *Biwater Gauff (Tanzania) Ltd. V. United Republic of Tanzania*. ICSID Case no. ARB/05/22, Award, 2008.

International Court of Justice. *Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro)*. I.C.J. 2007, p. 43.

International Court of Justice. *Armed Activities on The Territory of the Congo (Democratic Republic of the Congo v. Uganda)*. International Courts of Justice, Judgement of 19 December 2005, I.C.J. Reports, 2005.

International Court of Justice. *Barcelona Traction, Light and Power Company. Limited Second Phase, Judgment*, I.C.J., Reports, 1970, para 36, p. 3.

International Court of Justice. *Pulp Mills on the River Uruguay (Argentina v. Uruguay)*. Reports of Judgements, Advisory Opinions and Orders, 20 April 2010, p.14, para. 197, p.69, para. 101, p. 46.

International Law Commission. *Draft Articles on Responsibility of States for Internationally Wrongful Acts, with Commentaries*. United Nations, 2001, p. 31.

International Law Commission. *Responsibility of States for Internationally Wrongful Acts*. United Nations, 2001, chapter II, art. 4, p. 2.

Italia. Legge 18 Marzo 2008, n. 48. *Ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica, fatta a Budapest il 23 novembre del 2001, e norme di adeguamento all'ordinamento interno*. Gazzetta Ufficiale della Repubblica italiana, n.80, 4 aprile 2008.

Italia. Legge 23 dicembre 1993, n. 547. *Modificazioni ed integrazioni alle norme del Codice penale e del codice di procedura penale in tema di criminalità informatica*. Gazzetta Ufficiale della Repubblica italiana, n.305, 1993.

Kavaliauskas, Aurimas. “Can the Concept of Due Diligence Contribute to Solving the Problem of Attribution with Respect to Cyber-Attacks Conducted by Non-State Actors which Are Used as Proxies by States?”. *Teises Apzvalga Law Review*, 26, 2022, pp. 8, 9,16, 17, 23, 24. Hein Online.

Kinnear, Meg. “ARSIWA, ISDS, and the Process of Developing an Investor–State Jurisprudence.” *ICSID Reports* 20, 2022, p. 3.

Kulesza, Joanna. *Due Diligence in International Law*. Leiden, Boston, Vol. 26, *Queen Mary Studies In International Law*, BRILL NIJHOFF, 2016, p. 1, 2.

Macak, Kubo. “Decoding Article 8 of the International Law Commission’s Articles on State Responsibility: Attribution of Cyber Operations by Non-State Actors.” *Journal of Conflict and Security Law*, Oxford University Press, 2016, pp. 426, 427, 428.

Mackenzie-Gray Scott, Richard. “Due Diligence as a secondary rule of General International Law.” *Leiden Journal of International Law* 34.2, 2021, pp. 343, 346, 362.

Marino, Giuseppe Carlo. *Globalmafia. Manifesto per un’internazionale antimafia*. RCS Libri S.p.a., Milano, Bompiani, Studio G. Due S.r.l, 2011, p. 102.

Mattarella Andrea, Balsamo Antonio, Tartaglia Roberto. *La Convenzione di Palermo: il futuro della lotta alla criminalità organizzata transnazionale*. G. Giappichelli Editore, 2020, p. 7, 15.

Mattarella, Andrea. “La futura Convenzione Onu sul *cybercrime* ed il contrasto alle nuove forme di criminalità organizzata”. *Rivista italiana antiriciclaggio*, 2022, p.72. consultabile sul sito https://www.antiriciclaggiocompliance.it/app/uploads/2022/03/3.3_Mattarella.pdf

McDonald, Neil. *The Role Of Due Diligence in International Law*. Cambridge University Press, *British Institute of International and Comparative Law*, 2019, pp. 1044, 1045, 1046, 1049.

McDougal, Trevor. “Establishing Russia’s responsibility from Cyber-Crime Based on its hacker Culture.” *Brigham Young University International Law and Management Review*, vol.11, no. 2, Summer 2015, p. 65.

Musci, Aldo. *Tutte le mafie del mondo. Una mappa della criminalità organizzata nell’epoca della globalizzazione*. Stampa alternativa/nuovi equilibri, Viterbo, 2011, pp. 8, 12, 20, 21, 22, 35, 36, 84, 85, 213, 214, 215, 233, 234.

Nazioni Unite. *Convenzione delle Nazioni Unite contro la Criminalità organizzata transnazionale*. Nazioni Unite, New York, 2000, art. 2, lett. a art. 3, para. 2, pp. 5, 6.

Nolte, Georg. “From Dionisio Anzilotti to Roberto Ago: The Classical International Law of State Responsibility and the Traditional Primacy of a Bilateral Conception of Interstate Relations.” *European Journal of International Law*, Volume 13, 2002, pp. 1083, 1084.

Ortner, Daniel. “Cybercrime and Punishment: The Russian Mafia and Russian Responsibility to Exercise Due Diligence to Prevent Trans-Boundary Cybercrime.” *Brigham Young University Law review*, vol. 2015, no. 1, 2015, pp. 178, 179, 180, 182, 198, 202, 203, 204, 213.

Permanent Court of Arbitration. *Yukos Universal Limited (Isle of Man) v. Russia Federation*. UNCITRAL, PCA, Case no. 2005-04/AA227, Final Award, 18 July 2014.

Pisillo Mazzeschi, Riccardo. “The Due Diligence Rule and The Nature of the International Responsibility of States.” *German Yearbook of International Law*, 1992, pp. 42, 44, 45, 46, 47.

Ponti, Christian. “Il diritto internazionale e la criminalità organizzata”. *Rivista Di Studi E Ricerche Sulla Criminalità organizzata*. Università degli Studi di Milano, vo. 1, 2015, pp. 23, 24, 25.

Pustorino, Pietro. *La responsabilità degli Stati*. Annali VII, 2014, pp. 908, 909, 910, 911.

Sabino, Marta. “Il Regime di responsabilità degli Stati nella prassi degli organi di controllo delle convenzioni a carattere regionale sui diritti umani. Tra frammentazione e sviluppo progressivo del diritto internazionale.” Tesi di dottorato, Università degli Studi di Roma “La Sapienza”, 2025, pp. 69, 70.

Schmid Evelyne, Erceis Ayse Ozge. “The Attribution of Omissions: Due Diligence in Cyberspace and State Responsibility.” *Swiss Review of International and European Law*, vol 33, no. 4, 2023, pp. 580, 582, 583. HeinOnline.

Schmitt, Michael N. *Tallin Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge University Press, 2017, Rule 6, pp. 30, 31, 32.

Supreme Court of U.K. *R (Smith) v. Secretary of State for Defence*. U.K., 2010

United Nations General Assembly, International Law Commission. *International Responsibility*. Second Report. Document A/CN.4/106, 15 Feb. 1957. Yearbook of the International Law Commission 1957, vol. II, p. 121.

United Nations General Assembly. *Resolution 74/247. Countering the use of information and communications technologies for criminal purposes*. United Nations, New York, 27 Dec., 2019.

United Nations General Assembly. *Responsibility of States for Internationally wrongful acts*. A/res/56/83, United Nations, 28 January 2002.

United Nations General Assembly. *United Nations Convention against Cybercrime; Strengthening International Cooperation for Combating Certain Crimes Committed by Means of Information and Communications Technology Systems and for the Sharing of Evidence in Electronic Form of Serious Crimes*. UNDC, United Nations, A/RES/79/243, 31 December 2024, Chapter I, art. 6 (1), p. 7.

United Nations Office of Drugs and Crime. *Digesto di casi di criminalità organizzata. Raccolta commentata di casi e lezioni apprese*. Vienna, Nazioni Unite, 2012, p. 9.

United Nations, International Law Commission. *Draft Articles on Responsibility of States for Internationally Wrongful Acts, With Commentaries*. United Nations, 2008, p.47, 48, 49, 81, 88, 89, 90, 91.

United Nations, International Law Commission. *Project of articles on International Responsibility of States for Internationally Wrongful Acts. With commentaries*. In Yearbook of International Law Commission, 2001, vol. II, part one, chapter I, II, art. 2, lett. b., p. 2, art.5,7,8, p.3, art. 30, p.8.

United Nations. *State Responsibility*. Yearbook of the International Law Commission, Volume 2, 1976, p. 75. HeinOnline.

SITOGRAFIA

Admin-PSF. “Intelligenza Artificiale e Criminalità Organizzata” *Progetto San Francesco*, 2023, consultabile sul sito <https://progettosanfrancesco.it/2023/05/11/39969/>

Akkodis. “L’Intelligenza Artificiale che sta rivoluzionando la cyber security”. *Akkodis*, 2024, consultabile sul sito <https://www.akkodis.com/it/informazioni-utili/articoli/intelligenza-artificiale-cyber-security>

Arena, Joska. “L’evoluzione della mafia nel cyberspazio: dal pizzo al dark web, dallo spaccio all’intelligenza artificiale”. *Il Sicilia*, 2024, consultabile sul sito <https://ilsicilia.it/evoluzione-della-mafia-nel-cyberspazio-dal-pizzo-al-dark-web-dallo-spaccio-allintelligenza-artificiale/>

Buccini, Alfonso. “Convenzione di Budapest sulla criminalità informatica a vent’anni dalla approvazione” *Csibologna*, 2021, consultabile sul sito <https://www.csibologna.it/referenze/legislazione/convenzione-di-budapest-sulla-criminalita-informatica-a-20-anni-dallapprovazione/>

Cartisano, Marco. “Trattato globale ONU sulla criminalità informatica: perché è importante.” *Cybersecurity 360*, 2024, consultabile sul sito <https://www.cybersecurity360.it/cybersecurity-nazionale/trattato-globale-onu-sulla-criminalita-informatica-perche-e-importante/>

Centro studi Livatino. “La Convenzione di Palermo a vent’anni dalla sua entrata in vigore.” 2023, consultabile sul sito <https://www.centrostudilivatino.it/la-convenzione-di-palermo-a-ventanni-dalla-sua-entrata-in-vigore/>

Cervi, Claudia. “Criptovalute: cosa sono e come funzionano?”. *Money.it*, 2022, consultabile su https://www.money.it/Criptovalute-cosa-sono-come-funzionano#google_vignette

Ciccarone, Giovanna. “L’Intelligenza Artificiale e la Cybermafia: il futuro del crimine organizzato”, *Criminal meet*, 2024, consultabile sul sito <https://criminalmeet.it/lintelligenza-artificiale-e-la-cybermafia-il-futuro-del-crimine-organizzato/>

Cosentino, Roberto. “Cosa dice il nuovo Trattato ONU contro la criminalità informatica e perché è controverso: “possibili rischi per i diritti umani.” *Corriere.it*, 2024, consultabile sul sito https://www.corriere.it/tecnologia/24_agosto_14/cosa-dice-il-nuovo-trattato-

[onu-contro-la-criminalita-informatica-e-perche-e-controverso-a-rischio-i-diritti-umani-cd604f31-918a-4632-919d-27a67c8b0xlk.shtml](https://www.onucontro-la-criminalita-informatica-e-perche-e-controverso-a-rischio-i-diritti-umani-cd604f31-918a-4632-919d-27a67c8b0xlk.shtml)

Crapanzano, Laura. “I rischi oscuri del dark web.” *Unione polizia locale italiana*, 2021, articolo consultabile su www.unionepolizialeitaliana.it/2021-15/

Devanand, Ramiah. “UNPD: 5 Modi per Affrontare le Crisi Mondiali Attraverso l’IA.” *Nazioni Unite*, 2025, consultabile sul sito <https://unric.org/it/undp-5-modi-per-affrontare-le-crisi-mondiali-attraverso-lia/#>

Filacchioni, Marcello. “Passo storico: l’ONU adotta all’unanimità il Trattato globale sulla criminalità informatica”. 2024, consultabile sul sito <https://www.redhotcyber.com/post/pass-storico-lonu-adotta-allunanimita-il-trattato-globale-sulla-criminalita-informatica/>

Forte, Monica. “Profondo nero web: la necessità di informare (e formare) giovani e adulti.” *Stampo antimafioso*, 2020, consultabile sul sito <https://www.stampoantimafioso.it/profondo-nero-web-la-necessita-di-informare-e-formare-giovani-e-adulti/>

GuruHiTech. “L’intelligenza artificiale sta aiutando il Cartello Messicano.” *Guru HiTech*, 2024, consultabile sul sito <https://guruhitech.com/lintelligenza-artificiale-sta-aiutando-il-cartello-messicano/>

Hattemer, Christiane. “Che cos’è esattamente il mercato nero del Dark Web Silk Road?” *Avira.com*, 2024, consultabile sul sito <https://www.avira.com/it/blog/mercato-nero-del-dark-web-silk-road?srsId=AfmBOoopZ2t7zCZGHcc1GIE354eF1saaEKubXCLPTLq4j5sbRZky0fn4>

Iezzi, Pierguido. “La mafia cavalca l’onda dell’innovazione digitale.” *Panorama*, 2023, consultabile sul sito <https://www.panorama.it/tecnologia/cyber-security/mafia-innovazione-digitale-computer-affari>

Mele, Pierluigi. “I nuovi strumenti nelle mani delle mafie del terzo millennio-Intervista a Vincenzo Musacchio.” *Rai News*, 2024, consultabile sul sito <https://www.rainews.it/articoli/2024/04/bitcoin-dark-web-nanotecnologie-droni-e-intelligenza-artificiale-nuovi-strumenti-nelle-mani-delle-mafie-del-terzo-millennio---intervista-a-vincenzo-musacchio-82e70793-a08d-47dd-961d-fe0e83c0a41f.html>

Mele, Pierluigi. “Lotta alla cyber-mafia. La nuova frontiera della criminalità organizzata.” *Rainews*, 2023, consultabile su <https://www.rainews.it/articoli/2023/04/lotta-alla-cyber->

[mafia-la-nuova-frontiera-della-criminalita-organizzata-4b56f11c-4f83-4a55-8433-d4fc7c19ecd9.html](https://www.mafia-la-nuova-frontiera-della-criminalita-organizzata-4b56f11c-4f83-4a55-8433-d4fc7c19ecd9.html)

Mele, Pierluigi. “Radiologia delle nuove mafie: invisibili, tecnologiche e transnazionali”. *Rai news*, 2025, consultabile sul sito <https://www.rainews.it/articoli/2025/03/le-nuove-mafie-invisibili-tecnologiche-e-transnazionali-fcc547fb-65bb-4231-a5d1-1b6a1703c62a.html>

Messina, Piero. “Cybercrime, il rischio cresce. Ecco delle piccole regole per difendersi dagli hacker.” *Innovation Island*, 2024, consultabile su <https://innovationisland.it/cybercrime-italia-regole-difendersi-attacchi-hacker/>

Morelli, E. “Europol: cos’è e come funziona.” *Forze italiane*, 2019, consultabile sul sito <https://www.forzeitaliane.it/europol-cos-e-e-come-funziona>

Musacchio, Vincenzo. “Criminalità organizzata transnazionale, globalizzazione e ruolo della cooperazione internazionale”. *Articolo 21*, 2018, consultabile su <https://www.articolo21.org/2018/04/criminalita-organizzata-transnazionale-globalizzazione-e-ruolo-della-cooperazione-internazionale/>

Oddo, Giuseppe. “La mafia: da soggetto infiltrato a soggetto integrato nell’economia legale”. *Stati Generali della lotta alla criminalità organizzata: Mafie e globalizzazione, Relazione finale*, a cura di Ernesto Savona, Tavolo Telematico n.1, *Transcrime*, 2023. www.transcrime.it/wp-content/uploads/2023/02/Mafie-e-Globalizzazione_Final-report.pdf

OnuItalia. “ONU adotta il primo trattato contro il cybercrime.” *ONU Italia*, 2024, consultabile sul sito <https://onuitalia.com/2024/08/10/onu-adotta-il-primo-trattato-contro-il-cybercrimine/>

Pavone, Gianmichele. “Criminalità transfrontaliera e meccanismi di contrasto dell’ordinamento internazionale”. *Altalex*, 2008, consultabile sul sito <https://www.altalex.com/documents/news/2014/03/08/criminalita-transfrontaliera-e-meccanismi-internazionali-di-contrasto>

Pellerito, Vittoria. “Cybercrime: verso una nuova Convenzione delle Nazioni Unite”. *Ogie web*, 2022, consultabile sul sito <https://www.ogieweb.eu/cybercrime-verso-una-nuova-convenzione-delle-nazioni-unite/>

Perego, Giorgio. “Dark web: come si entra e che succede se accedo.” 2023, consultabile sul sito https://www.insic.it/privacy-e-sicurezza/information-security/dark-web-come-si-entra-e-che-succede-se-accedo/#Cosa_succede_nel_Dark_Web

Polimeni, Francesca. “Criptovalute e cyberriciclaggio: l’arma segreta della criminalità organizzata.” *Giuridicamente*, 2022, consultabile sul sito <https://www.giuridicamente.com/l/criptovalute-e-cyber-riciclaggio-larma-segreta-della-criminalita-organizzata/>

Rijtano, Rosita. “Cybercrime, l’allarme dell’Interpol: “Con l’intelligenza artificiale sarà a portata di tutti”. *La via libera*, 2024, consultabile sul sito <https://lavialibera.it/it-schede-1781-cybercrime-interpol-intelligenza-artificiale>

Roberti Franco, Musacchio Vincenzo. “La lotta alle nuove mafie va combattuta a livello transnazionale.” *Diritto penale uomo*, 2021, consultabile sul sito https://dirittopenaleuomo.org/contributi_dpu/la-lotta-alle-nuove-mafie-va-combattuta-a-livello-transnazionale/

Savona, Ugo Ernesto, Lasco Federico, Di Nicola Andrea. “Processi di globalizzazione e criminalità organizzata transnazionale”. *Università degli Studi di Trento*, 1998. Consultabile su: eprints.biblio.unitn.it/197/1/Globalizzazione_e_criminalit%C3%A0.pdf

Sbaraglia, Giorgio. “Tor: cos’è e come usare il browser e la darknet in sicurezza per navigare nel Dark Web”. *Cybersecurity*, 2022, consultabile sul sito www.cybersecurity360.it/soluzioni-aziendali/tor-cose-e-come-usarlo-in-sicurezza-per-navigare-nel-dark-web/

Silvis, Piernicola. “Mafie e criptovalute: contro l’evoluzione tecnologica, le armi investigative sono spuntate”. *Il fatto quotidiano*, 2022, consultabile sul sito <https://www.ilfattoquotidiano.it/2022/07/23/mafie-e-criptovalute-contro-levoluzione-tecnologica-le-armi-investigative-sono-spuntate-3/6617135/>

Tecnodigitale. “Cos’è il phishing: 10 segnali di allarme.” *Informattec digital*, 2024, consultabile su <https://informatecdigital.com/it/cos%27%C3%A8-il-phishing/>

Venezia, Lorenzo. “Il SOCTA 2017 dell’Europol: un’analisi sulla criminalità”. *Diritto Consenso*, 2018, consultabile sul sito <https://www.dirittoconsenso.it/2018/03/26/socata-2017-europol-analisi-sulla-criminalita/>